On Involutions of the First Kind

Ina Kersten

Abstract. We give a new definition of orthogonal and symplectic involutions of the first kind and relate these notions to classical groups. The discriminant of an involution recently was described by Knus, Parimala, and Sridharan [3] via Galois descent. Here we give a short proof that this discriminant is well defined and that the discriminant of a symplectic involution is trivial.

1991 Mathematics Subject Classification. 16R50

Introduction. An *involution* on a ring A is a map $I : A \to A, a \mapsto a^I$, satisfying

$$(a+b)^I = a^I + b^I, \quad (ab)^I = b^I a^I, \quad a^{I^2} = a$$

for all $a, b \in A$. If A is an algebra over a field k and I is a k-linear involution, then I is called an *involution of the first kind*. The theory of involutions on simple algebras goes back to A.A.Albert [1, Chap.X]. He showed that a central simple algebra A admits an involution of the first kind if and only if A has exponent one or two [1, Chap.X, Th.19]. This happens, for example if A is a full matrix ring over k or A is a tensor product of quaternion algebras. Involutions on simple algebras are closely related to hermitian forms over skew fields [4, Chap.8], and they are essential for studying classical groups [5, Table II].

In this note we give a new definition of orthogonal and symplectic involutions of the first kind and relate these notions to classical groups. The discriminant of an involution recently was described by Knus, Parimala, and Sridharan [3] via Galois descent. In 3.1 below we give a short proof that this discriminant is well defined and that the discriminant of a symplectic involution is trivial.

Notations. Let A be a central simple algebra of even degree $n = 2m$ over a field k, admitting an involution $I : A \to A,\ a \mapsto a^I$, of the first kind. For $\delta \in \{\pm 1\}$ we define

$$A_I^\delta := \{a + \delta a^I \mid a \in A\} \quad \text{and} \quad S(A)_I^\delta := \{a \in A \mid a^I = \delta a\}.$$

Let A^* denote the group of units in A. If $A = \mathrm{M}_n(k)$ is a matrix ring, then transposition on A is denoted by t. Write $A_K := A \otimes_k K$ for any field $K \supseteq k$.

1. Orthogonal and Symplectic Involutions

Investigations on involutions are based on the simple fact that the composition of two involutions is an automorphism and hence an inner automorphism by the Skolem-Noether theorem.

1.1 Lemma (Albert). *For every involution J of the first kind on A, there is an element $u = u_J \in A^*$, which is unique up to a central factor, such that $a^J = ua^Iu^{-1}$ for all $a \in A$, Moreover, there is an $\varepsilon \in \{\pm 1\}$ such that $u^J = u^I = \varepsilon u$. We have $uA_I^\delta = A_J^{\delta\varepsilon}$ and $uS(A)_I^\delta = S(A)_J^{\delta\varepsilon}$.*

Proof. By the Skolem-Noether theorem [4, Chap.8, Cor.4.3] there is an element $u \in A^*$ (which is unique up to a central factor) such that $a^{IJ} = uau^{-1}$ for all $a \in A$. This implies $u^{IJ} = u$, hence $u^J = u^I$. Also we have $a^J = a^{I^2J} = ua^Iu^{-1} = uu^{-J}a^Ju^Ju^{-1}$ for all $a \in A$. Hence $\varepsilon := u^Ju^{-1}$ is central and therefore $u = u^{J^2} = \varepsilon^2 u$ which yields $\varepsilon \in \{\pm 1\}$. The last statements now follow from $u(a + \delta a^I) = ua + \delta\varepsilon(ua)^J$ and $u^{-1}(a + \varepsilon\delta a^J) = u^{-1}a + \delta(u^{-1}a)^I$, and $(us)^J = \varepsilon\delta us$ for $s \in S(A)_I^\delta$. □

Recall that a matrix $x \in \mathrm{M}_n(k)$ is said to be *alternating* if $x^t = -x$ and the diagonal elements of x are 0.

1.2 Proposition. *There is a unique $\varepsilon \in \{\pm 1\}$ such that $\dim A_I^{-\varepsilon} = (n/2)(n-1)$. If $A = \mathrm{M}_n(k)$ is a matrix ring, then $u := u_t$ is alternating if and only if $1 \in A_I^{-\varepsilon}$.*

Proof. By passing to a splitting field of A we may assume $A \cong M_n(k)$. Then, using 1.1 with $J = t$ and $\delta = -\varepsilon$, we have $uA_I^{-\varepsilon} = A_t^{-1}$, hence $\dim A_I^{-\varepsilon} = (n/2)(n-1)$. Also, $u \in A_t^{-1}$ if and only if $1 \in A_I^{-\varepsilon}$. □

The following definition was suggested by U. Rehmann.

1.3 Definition. The involution I is said to be *orthogonal* if $1 \notin A_I^{-\varepsilon}$ and *symplectic* if $1 \in A_I^{-\varepsilon}$. The number ε in 1.2 is called the *type* of the involution I.

If $\operatorname{char} k \neq 2$, then I is of type -1 if and only if I is symplectic; and I is of type $+1$ if only if I is orthogonal. If $\operatorname{char} k = 2$, then clearly $\pm\varepsilon = 1 = \pm\delta$, and we set $A_I := A_I^\delta$ and $S(A)_I := S(A)_I^\delta$. In both cases we have $A_I^\delta \subseteq S(A)_I^\delta$.

1.4 Remark.

a) *If* $\operatorname{char} k \neq 2$, *then* $A_I^\delta = S(A)_I^\delta$ *and* $A = A_I^1 \oplus A_I^{-1}$. *We also have* $\dim A_I^\delta = (n/2)(n + \delta\varepsilon)$.

b) *If* $\operatorname{char} k = 2$, *then* $\dim A_I = (n/2)(n-1)$ *and* $\dim S(A)_I = (n/2)(n+1)$.

c) *The sets A_I^δ and, for* $\operatorname{char} k = 2$, *also $S(A)_I \setminus A_I$ contain elements of A^*.*

Proof. For $\operatorname{char} k \neq 2$, we have $a = (a + \delta a^I)/2$ for every $a \in A$ such that $a^I = \delta a$, hence $A_I^\delta = S(A)_I^\delta$. Also we have $a = (a + a^I)/2 + (a - a^I)/2$ for every $a \in A$, which yields the direct sum decomposition. The dimension formulas follow from passing to a splitting field and applying 1.1 and 1.2. Statement iii) is easily verified for a matrix ring, in particular, if k is finite. For an infinite k it follows that the invertible elements of the affine space A define an open and dense subset in the Zariski topology, which intersects non-trivially the quasiprojective subvariety V defined by A_I^ε (resp. by $S(A)_I^\delta \setminus A_I^\varepsilon$), therefore this intersection is open and dense in V. Then A_I^ε (resp. $S(A)_I^\delta \setminus A_I^\varepsilon$) is a dense subset of V, hence our claim follows. □

2. Connection with Classical Groups

For $v \in S(A)_I^\delta \cap A^*$ we define the affine k-group G_v by $G_v(k) = \{x \in A^* \mid x^I v x = v\}$. If K is a splitting field of A, then A_K is a matrix ring, and we choose $u = u_t \in A_K^*$ as in 1.2. We then have $x^I = u^{-1}x^t u$ hence $v = u^{-1}x^t uvx$ and

$$G_v(K) = \{x \in A_K^* \mid x^t uvx = uv\}.$$

Thus G_v is orthogonal (resp. symplectic) if $uv \notin (A_K)_t^{-1}$ (resp. $uv \in (A_K)_t^{-1}$), and we obtain the following criteria in terms over k:

i) $\operatorname{char} k \neq 2$: The group G_v is orthogonal (resp. symplectic) if $v \in S(A)_I^\varepsilon$ (resp. $v \in S(A)_I^{-\varepsilon}$).

ii) $\operatorname{char} k = 2$: The group G_v is orthogonal (resp. symplectic) if $v \in S(A)_I \setminus A_I$ (resp. $v \in A_I$).

Consequence. *The involution I is orthogonal (resp. symplectic) if and only if the group G_1 is orthogonal (resp. symplectic).*

We note that $G_v(k)$ is the unitary group of the δ-hermitian form $h_v : A \times A \to A$ defined by $h(a,b) := a^I vb$. We have $h(b,a)^I = (b^I va)^I = a^I v^I b = \delta a^I vb = \delta h(a,b)$, and $h(ga, gb) = (ga)^I v(gb) = a^I g^I vgb = a^I vb = h(a,b)$ for $g \in G_v(k)$. The associated bilinear form is $(a,b)_v := h(a+b, a+b) - h(a,a) - h(b,b) = a^I vb + b^I va$, hence obviously $(a,b)_v \in A_I^\delta$.

3. The Discriminant of an Involution

Let N denote the reduced norm of A (cf. [4, Chap.8, §5]).

3.1 Proposition (Tits [6, p.26]). *For $x, y \in A_I^{-\varepsilon}$ we have $\mathrm{N}x\mathrm{N}y \in k^2$. If I is symplectic and $x \in A_I^{-\varepsilon}$, then $\mathrm{N}x \in k^2$.*

Proof. We may assume that x, y are invertible. Let K be a field extension of k which splits A. Then $A_K \cong \mathrm{M}_n(K)$. Choose $u \in A_K^*$ as in 1.2. Then $u(A_K)_I^{-\varepsilon} = (A_K)_t^{-1}$, hence $\det ux$, $\det uy \in K^{*2}$ [7, p.32]. Therefore $\mathrm{N}x\mathrm{N}y = \det u^{-2} \det ux \det uy \in K^{*2} \cap k^*$.

Under the conditions of the second statement we have $u \in (A_K)_t^{-1}$, hence in this case $\det u \in K^{*2}$ by [l. c.], and we then have $\mathrm{N}x \in K^{*2} \cap k^*$.

Let K be a generic splitting field of A, then k is algebraically closed in K (cf. [2]) and therefore $K^{*2} \cap k^* = k^{*2}$. □

3.2 Definition [3]. Let $x \in A_I^{-\varepsilon} \cap A^*$. The square class of $\mathrm{N}x$ in k^*/k^{*2} is called the *discriminant* of the involution I.

It follows from 3.1 that this notion is well defined and that the discriminant of a symplectic involution is trivial.

3.3 Example. Let $\operatorname{char} k \neq 2$ and A be a quaternion algebra. Then conjugation provides an involution I on A by $a^I := \bar{a}$ for all $a \in A$. Then $A_I^1 = k$ is one-dimensional, hence the involution is of type -1, and its discriminant is 1.

REFERENCES

1. *A. A. Albert:* Structures of algebras, Amer. Math. Soc. Colloq. Publ. XXIV, New York, 1939, revised ed., 1961.
2. *S. A. Amitsur:* Generic splitting fields of central simple algebras. Ann. of Math. 62 (1955), 8-43.
3. *M.-A. Knus, R. Parimala, R. Sridharan:* On the discriminant of an involution, Bull. Soc. Math. Belgique, Sér. A, 43 (1991), 89-98.
4. *W. Scharlau:* Quadratic and Hermitian forms. Springer-Verlag 1985.
5. *J. Tits:* Classification of algebraic semisimple groups. Proc. Sympos. Pure Math. IX (1966), 33-62.
6. *J. Tits:* Formes quadratiques, groupes orthogonaux et algèbres de Clifford. Invent. Math. 5 (1968), 19-41.
7. *B. L. v. d. Waerden:* Algebra, 5. Auflage, 2. Teil, Heidelberger Taschenbücher 23, Springer-Verlag, 1967.