Journal of Lie Theory
Volume **27** (2017) 155–176

Generalizations of the Cartan and Iwasawa Decompositions for $\mathrm{SL}_2(k)$

Amanda K. Sutherland

Communicated by G. Ólafsson

Abstract. The Cartan and Iwasawa decompositions of real reductive Lie groups play a fundamental role in the representation theory of the groups and their corresponding symmetric spaces. These decompositions are defined by an involution with a compact fixed-point group, called a Cartan involution. For an arbitrary involution, one can consider similar decompositions. We offer a generalization of the Cartan and Iwasawa decompositions for algebraic groups defined over an arbitrary field k and a general involution.
Mathematics Subject Classification 2010: 20G15.
Key Words and Phrases: Linear algebraic groups, Cartan decomposition, Iwasawa decomposition, generalized symmetric spaces.

1. Introduction

The Cartan decomposition of a real reductive Lie group G factors the group into HQ where H is maximal compact and Q is the symmetric space with respect to the Cartan involution. The Cartan decomposition generalizes the polar decomposition or singular value decomposition of matrices. The Iwasawa decomposition of a real reductive Lie group factors the group into its analytical subgroups HP where H is maximal compact and P is a minimal parabolic $\mathbb{R}$-subgroup. This decomposition results from combining the Cartan decomposition of a semisimple Lie algebra and the root space decomposition of its complexification.

The Cartan and Iwasawa decompositions of real reductive Lie groups play an important role in representation theory and in the structure of their corresponding real reductive symmetric spaces. The reader is referred to Helgason [7] for a more complete description of these decompositions. In [9], a generalization of the notion of a Cartan involution is given and the Cartan and Iwasawa decompositions are generalized to groups with such an involution.

In this paper, we let $G = \mathrm{SL}_2(\bar{k})$ be an algebraic group defined over a field k of characteristic not 2 and develop a decomposition which resembles a combination of the Cartan and Iwasawa decompositions. We extend the notion of the Cartan and Iwasawa decompositions to G defined over other fields. Specifically,

ISSN 0949–5932 / $2.50

we consider the real, rational, and $\mathfrak{p}$-adic numbers, as well as the finite fields. We also generalize the factors of the decompositions by defining them with respect to any involution of the group.

In section 2, we review results and notation needed to prove our main results. In section 3, we show $\mathrm{SL}_2(k)$ can be factored to $H_k^\theta \widetilde{Q^\theta} U_k$ where H^θ is the fixed-point group of some involution θ, $\widetilde{Q^\theta} = \{g \in G \mid \theta(g) = g^{-1}\}$ is the extended symmetric space of the involution θ, and U a unipotent subgroup of G. In section 4, we discuss the structure of the symmetric and extended symmetric spaces. In sections 5-7, we refine our decomposition of $\mathrm{SL}_2(k)$ and analyze the factors in more detail for specific fields and involutions.

2. Preliminaries

We borrow most notation from Springer and Borel [11, 4, 3, 2]. Let k be a field of characteristic not equal to 2 and $\bar{k}$ the algebraic closure of k. We will use $G = \mathrm{SL}_2(\bar{k})$ and $G_k = \mathrm{SL}_2(k)$, the k-rational points of G. In general, for a group A defined over k, A_k will denote the k-rational points of A. For $B \in \mathrm{GL}_2(k)$, let $\mathrm{Inn}(B)$ denote the automorphism of G defined by $\mathrm{Inn}(B)(X) = BXB^{-1}$ for all $X \in G$. Let $\mathrm{Aut}(G, G_k)$ denote the group of automorphisms of G which keep G_k invariant. We say $\phi, \theta \in \mathrm{Aut}(G, G_k)$ are isomorphic (over k) if there exists a third automorphism $\chi \in \mathrm{Aut}(G, G_k)$ such that $\chi\phi\chi^{-1} = \theta$. This is denoted $\phi \simeq \theta$ when the field k is clear from context. Combining results from [2] and [10], we have the following lemma.

Lemma 2.1. *All automorphisms $\phi \in \mathrm{Aut}(G, G_k)$ are isomorphic over k to $\mathrm{Inn}(A)$ for some $A \in \mathrm{GL}_2(k)$.*

For a field k, let k^* denote the product group of non-zero elements from k and $(k^*)^2$ the normal subgroup of squares in k^* defined by $(k^*)^2 = \{a^2 \mid a \in k^*\}$. The quotient group $k^*/(k^*)^2$ is the set of square classes in k. From [10, 8] we borrow the following results about automorphisms of order 2, called involutions, of G_k.

Theorem 2.2. *All involutions $\theta \in \mathrm{Aut}(G, G_k)$ are isomorphic over k to $Inn(B)$, where $B = \left(\begin{smallmatrix} 0 & 1 \\ b & 0 \end{smallmatrix}\right)$ for some $b \in k^*$.*

Theorem 2.3. *Let $M = \left(\begin{smallmatrix} 0 & 1 \\ m & 0 \end{smallmatrix}\right)$ and $N = \left(\begin{smallmatrix} 0 & 1 \\ n & 0 \end{smallmatrix}\right)$ be the matrices corresponding to $\mathrm{Inn}(M), \mathrm{Inn}(N) \in \mathrm{Aut}(G, G_k)$, respectively. Then $\mathrm{Inn}(M) \simeq \mathrm{Inn}(N)$ if and only if m and n are in the same square class of k.*

Corollary 2.4. *The number of isomorphy classes of involutions of G which keep G_k invariant is $|k^*/(k^*)^2|$.*

Let m be a representative of the square class of $\overline{m}$ in $k^*/(k^*)^2$. We will use θ_m to denote the involution $\mathrm{Inn}(M)$ of G with $M = \left(\begin{smallmatrix} 0 & 1 \\ m & 0 \end{smallmatrix}\right)$. For all involutions $\theta \in \mathrm{Aut}(G, G_k)$, we can assume $\theta \simeq \theta_m$ where $m \in k^*$ is the representative of the

square class $\overline{m}$. For the class of squares, we use $m = 1$. Let $\mathcal{G}$ be a group and ϕ an automorphism of $\mathcal{G}$. Denote H^ϕ as the fixed-point group of ϕ in $\mathcal{G}$.

Example 2.5. For G with the involution θ_m, the fixed point group is H^{θ_m}, where

$$H_k^{\theta_m} = \left\{ \begin{pmatrix} a & b \\ mb & a \end{pmatrix} \;\middle|\; a, b \in k,\ a^2 - mb^2 = 1 \right\}.$$

Definition 2.6. For a group $\mathcal{G}$ with the involution θ, the *symmetric space* is defined as $Q^\theta = \{g\theta(g)^{-1} \mid g \in \mathcal{G}_k\}$, and the *extended symmetric space* is defined as $\widetilde{Q^\theta} = \{g \in \mathcal{G}_k \mid \theta(g) = g^{-1}\}$.

Remark 2.7. For a group $\mathcal{G}$ with the involution θ, the symmetric space is isomorphic to $\mathcal{G}/H^\theta$.

Example 2.8. For G with the involution θ_m, the extended symmetric space is $\widetilde{Q^{\theta_m}}$, where

$$\widetilde{Q^{\theta_m}} = \left\{ \begin{pmatrix} x & y \\ -my & z \end{pmatrix} \;\middle|\; x, y, z \in k,\ xz + my^2 = 1 \right\}.$$

Definition 2.9. An element $g \in \mathcal{G}$ is *θ-split* if $\theta(g) = g^{-1}$. A subset is *θ-split* if all of its elements are θ-split, i.e. $\widetilde{Q^\theta}$ is θ-split by definition. An element is *k-split* if it can be diagonalized over the field k. A torus is *k-split* if all of its elements are k-split. A torus is *(θ, k)-split* if it is both θ-split and k-split.

Lemma 2.10. *For a group $\mathcal{G}$ with an involution θ, the symmetric space is contained within the extended symmetric space. i.e. $Q^\theta \subset \widetilde{Q^\theta}$.*

Proof. Let $g\theta(g)^{-1} \in Q^\theta$ for some $g \in \mathcal{G}$, then

$$\theta(g\theta(g)^{-1}) = \theta(g)\theta^2(g)^{-1} = \theta(g)g^{-1} = (g\theta(g)^{-1})^{-1}.$$

Hence, $g\theta(g)^{-1} \in \widetilde{Q^\theta}$. ∎

Lemma 2.11. *The symmetric space of a connected group is connected. Furthermore, $(\widetilde{Q^\theta})^\circ = Q^\theta$, where $(\widetilde{Q^\theta})^\circ$ denotes the connected component of the extended symmetric space containing the identity.*

Proof. Consider a connected group $\mathcal{G}$ defined over k, a field with a topology. Then Q^θ is connected because it is the image of the continuous mapping defined by $g \mapsto g\theta(g)^{-1}$ for $g \in \mathcal{G}$. Since $(\mathrm{Id})\theta(\mathrm{Id})^{-1} = \mathrm{Id}$, the identity matrix is always contained in the symmetric space. Therefore, the symmetric space is the connected component of the extended symmetric space containing the identity, $Q^\theta = (\widetilde{Q^\theta})^\circ$. ∎

Definition 2.12. A subgroup A is *k-isotropic* if it contains a k-split torus.

Otherwise, A is *k-anisotropic*. An involution θ of a group is a *generalized Cartan involution* if the fixed-point group of θ is k-anisotropic.

If $k = \mathbb{R}$, this is the regular Cartan involution. $\mathbb{R}$-anisotropic is equivalent to compact. By abuse of terminology, we will refer to a generalized Cartan involution as a Cartan involution.

Example 2.13. Consider G defined over $k = \mathbb{R}$. The square classes of $\mathbb{R}$ are represented by $\{1, -1\}$. Up to isomorphy over $\mathbb{R}$, there are two involutions of G which keep $G_{\mathbb{R}}$ invariant, namely θ_1 and θ_{-1}.

The fixed-point group of θ_{-1} is the special orthogonal group $\mathrm{SO}(2)$ which is compact and hence θ_{-1} is a Cartan involution. The symmetric space of θ_{-1} is the set of positive definite symmetric matrices, while the extended symmetric space is the set of symmetric matrices.

For the involution θ_1, the fixed-point group is the subgroup $\mathrm{SO}(1,1)$.

The following results from [7] give us the Cartan and Iwasawa decompositions, respectively.

Theorem 2.14 (Cartan Decomposition)**.** *Let $\mathcal{G}$ be a real semisimple Lie group and θ a Cartan involution of $\mathcal{G}$. Define Q and H to be the symmetric space and fixed-point group with respect to θ, respectively, and A a maximal (θ, k)-split torus in $\mathcal{G}$. Then θ induces the following equivalent Cartan decompositions:*

$$\mathcal{G} = HQ = H^\circ Q = HAH = H^\circ A^\circ$$

where H° denotes the connected component of H containing the identity.

Theorem 2.15 (Iwasawa Decomposition)**.** *Let $\mathcal{G}$ be a real semisimple Lie group and θ a Cartan involution of $\mathcal{G}$. Let H be the fixed-point group and P a minimal parabolic $\mathbb{R}$-subgroup. Then θ induces the Iwasawa decomposition:*

$$\mathcal{G} = HP.$$

Remark 2.16. For an $\mathbb{R}$-split group, as is the case with G, we can write $G_{\mathbb{R}} = H_{\mathbb{R}} A_{\mathbb{R}} U_{\mathbb{R}}$, where A is the maximal $(\theta, \mathbb{R})$-split torus and U a maximal unipotent subgroup defined over $\mathbb{R}$. In fact, $P_{\mathbb{R}} = Z_{G_{\mathbb{R}}}(A) U_{\mathbb{R}} = A_{\mathbb{R}} U_{\mathbb{R}}$ since A is a maximal torus.

From [9], we have a condition which equates the Iwasawa and Cartan decompositions.

Theorem 2.17. *Let $\mathcal{G}$ be a real Lie group defined over a field k and θ a generalized Cartan decomposition of $\mathcal{G}$ such that the fixed-point group H_k is k-anisotropic, the symmetric space Q consists of semisimple elements, $(Z_G(A)(H))_k = A_k H_k$, where A is a θ-stable maximal (θ, k)-split torus of a minimal parabolic subgroup P. If $(k^*)^2 = (k^*)^4$, then the following decompositions are equivalent:*

$$\mathcal{G}_k = H_k^\circ A_k H_k^\circ = H_k A_k H_k = H_k^\circ Q = H_k Q = H_k^\circ A_k U_k = H_k A_k U_k$$

where $H, A, Q,$ and U are as defined in Theorem 2.14 and Remark 2.16.

The criteria for a generalized Cartan involution in [9], listed in Theorem 2.17, is much stronger than in this paper. These additional requirements guaranteed the existence of generalized Cartan and Iwasawa decompositions in their paper.

3. Generalizing the Decompositions to Algebraic Groups

As previously discussed, the Cartan and Iwasawa decompositions are defined for real semisimple Lie groups when paired with a Cartan involution. In general, for any field k with a general involution θ, the set $H_k^\theta Q^\theta$ is contained in, but not equal to, G_k.

Example 3.1. Let G be defined over $k = \mathbb{R}$ and $\theta = \theta_1$ the involution of G. Consider

$$g = \begin{pmatrix} 1 & 2(\sqrt{5}-3)^{-1} \\ \frac{1}{2}(\sqrt{5}-3) & 2 \end{pmatrix} \in G_{\mathbb{R}}.$$

We will show $g \notin H_{\mathbb{R}}^\theta \widetilde{Q^\theta}$ and thus $g \notin H_{\mathbb{R}}^\theta Q^\theta \subset H_{\mathbb{R}}^\theta \widetilde{Q^\theta}$. Assume to the contrary that $g \in H_{\mathbb{R}}^\theta \widetilde{Q^\theta}$, then there exists $h^{-1} = \left(\begin{smallmatrix} a & -b \\ -b & a \end{smallmatrix}\right) \in H_{\mathbb{R}}^\theta$ such that $h^{-1}g \in \widetilde{Q^\theta}$. Then the matrix equation

$$\theta(h^{-1}g) = \begin{pmatrix} 2a - \frac{2b}{\sqrt{5}-3} & a\left(\frac{\sqrt{5}-3}{2}\right) - b \\ \frac{2a}{\sqrt{5}-3} - 2b & 2a - \frac{2b}{\sqrt{5}-3} \end{pmatrix} = \begin{pmatrix} 2a - \frac{2b}{\sqrt{5}-3} & 2b - \frac{2a}{\sqrt{5}-3} \\ b - a\left(\frac{\sqrt{5}-3}{2}\right) & 2a - \frac{2b}{\sqrt{5}-3} \end{pmatrix} \tag{1}$$

has a solution such that $h \in H_{\mathbb{R}}^\theta$. However, the only solution to (1) is $a = -b$. Therefore, $h \notin H_{\mathbb{R}}^\theta$ and the traditional Cartan decomposition does not hold.

To account for the missing elements, we introduce the unipotent subgroup U of G consisting of upper triangular matrices with ones on the diagonal, where

$$U_k = \left\{ \begin{pmatrix} 1 & u_1 \\ 0 & 1 \end{pmatrix} \middle| u_1 \in k \right\}. \tag{2}$$

With the addition of the new subgroup, we have the following result.

Theorem 3.2. *For G with the involution θ, $G_k = H_k^\theta \widetilde{Q^\theta} U_k$, where $H^\theta, \widetilde{Q^\theta}$, and U are the fixed-point group, extended symmetric space, and unipotent subgroup of G, respectively.*

This decomposition serves as a generalization of both the Cartan and Iwasawa decompositions. It contains the fixed-point group and symmetric space similar to the Cartan decomposition. Additionally, because the maximal (θ, k)-split torus A is contained in $\widetilde{Q^\theta}$ and we have a unipotent subgroup, it generalizes the Iwasawa decomposition. To prove Theorem 3.2, we use the Bruhat Decomposition as in [3].

Theorem 3.3. *For an algebraic group $\mathcal{G}$, let P be a minimal parabolic k-subgroup of $\mathcal{G}$, A a maximal k-split torus in P, and $W(A)$ the Weyl group of A. Then $\mathcal{G}_k$ decomposes as the disjoint union of the double cosets of P_k parameterized by $W(A)$,*

$$\mathcal{G}_k = \bigcup_{\omega \in W(A)}^{\cdot} P_k \omega P_k.$$

Remark 3.4 (Bruhat Decomposition of G)**.** For a k-split group, $P = B$ is a Borel subgroup and $A = T$ is a maximal torus. For G_k, the Bruhat decomposition is

$$G_k = \bigcup_{\omega \in W(T)}^{\cdot} B_k \omega B_k.$$

Let the maximal torus T be the subgroup of diagonal matrices in G, the Borel subgroup $B \supset T$ be the upper triangular matrices in G. Then T_k and B_k are their respective k-rational points where,

$$B_k = \left\{ \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \middle| x, y, z \in k, xz = 1 \right\} \quad \text{and} \quad T_k = \left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \middle| a \in k^* \right\}. \tag{3}$$

Let Id be the 2×2 identity matrix, then we can define the Weyl group $W(T)$ and Bruhat decomposition of G_k as

$$W(T) = \left\{ \mathrm{Id}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\} \quad \text{and} \quad G_k = B_k \bigcup^{\cdot} B_k \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} B_k. \tag{4}$$

For the Borel subgroup B, we can write $B = TU$, where T is the k-split maximal torus and U is the unipotent radical.

Lemma 3.5. *Let θ be an involution of G and T the k-split maximal torus of diagonal matrices. Then T is invariant under θ and is maximal (θ, k)-split.*

Proof. Let $\theta = \theta_m$ be an involution of G and $t = \left(\begin{smallmatrix} a & 0 \\ 0 & a^{-1} \end{smallmatrix} \right) \in T$. Then T is θ-split, because

$$\theta(t) = \begin{pmatrix} 0 & 1 \\ m & 0 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \begin{pmatrix} 0 & m^{-1} \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix} = t^{-1} \in T.$$

Thus, T is invariant under θ. ∎

A subgroup which is invariant under an automorphism ϕ is said to be ϕ-stable.

Lemma 3.6. *Let G be defined over k and θ an involution of G. If $H_k^\theta = \{\pm \mathrm{Id}\}$, then $k \simeq \mathbb{F}_3$. For G defined over $k = \mathbb{F}_3$, $H_k^{\theta_m} = \{\pm \mathrm{Id}\}$ only for $m \in (k^*)^2$.*

Proof. From [9], the fixed-point group of an involution is always reductive. Thus, the fixed-point group is a torus. Because $H \simeq \overline{k^*}$, if $|H| = 2$, it must be that $k \simeq \mathbb{F}_3$.

For $k = \mathbb{F}_3$, the set of squares is $(\mathbb{F}_3^*)^2 = \{1\}$. For $h = \left(\begin{smallmatrix} a & b \\ mb & a \end{smallmatrix} \right) \in H_{\mathbb{F}_3}^{\theta_m}$, it must be that $a^2 - mb^2 = 1$. If $m \in (\mathbb{F}_3^*)^2$, the only solution to the determinant equation

is $a = \pm 1$ and $b = 0$. Hence $h = \pm \mathrm{Id}$. If $m \notin (\mathbb{F}_3^*)^2$, i.e. $m = 2$, solutions to the determinant equation include $a = 0$ and $b = \pm 1$. Therefore, h is not necessarily $\pm \mathrm{Id}$. ∎

Proof of Theorem 3.2. Let θ be an involution of G. Because $H_k^\theta, \widetilde{Q^\theta}$, and U_k are contained in G_k, $H_k^\theta \widetilde{Q^\theta} U_k \subset G_k$ is clear. We will show the reverse containment, $G_k \subset H_k^\theta \widetilde{Q^\theta} U_k$ by replacing G_k with its Bruhat decomposition as in (4), giving us the equivalent statement

$$B_k \bigcup\!\!\cdot\, B_k \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} B_k \subset H_k^\theta \widetilde{Q^\theta} U_k. \tag{5}$$

First, consider $g \in B_k$. By Remark 3.4, $gu^{-1} = t$ for some $u^{-1} \in U_k$ and $t \in T_k$. By Lemma 3.5, $gu^{-1} = t$ is θ-split, hence $gu^{-1} \in \widetilde{Q^\theta}$. Therefore $g \in \widetilde{Q^\theta} U_k \subset H_k^\theta \widetilde{Q^\theta} U_k$.

Second, consider $g \in B_k \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) B_k$. For some $a, b \in k^*$ and $\alpha, \beta \in k$, we rewrite g as

$$g = \begin{pmatrix} a & \alpha \\ 0 & a^{-1} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} b & \beta \\ 0 & b^{-1} \end{pmatrix}. \tag{6}$$

If $\alpha \neq 0$, let

$$u = \begin{pmatrix} 1 & \frac{ma^2 - b^2 - m\alpha\beta ab}{m\alpha ab^2} \\ 0 & 1 \end{pmatrix},$$

then $gu \in \widetilde{Q^\theta}$ because

$$\theta(gu) = \begin{pmatrix} -\frac{a^2 m - b^2}{a^2 bm\alpha} & -\frac{b}{ma} \\ \frac{b}{a} & -\alpha b \end{pmatrix} = (gu)^{-1}. \tag{7}$$

Therefore, $g \in \widetilde{Q^\theta} U_k \subset H_k^\theta \widetilde{Q^\theta} U_k$. If $\alpha = 0$, let

$$h = \begin{pmatrix} a_1 & b_1 \\ mb_1 & a_1 \end{pmatrix} \in H_k^\theta \smallsetminus \{\pm \mathrm{Id}\} \quad \text{and} \quad u = \begin{pmatrix} 1 & \frac{ma^2 a_1 - mbb_1\beta - a_1 b^2}{mb^2 b_1} \\ 0 & 1 \end{pmatrix} \in U_k. \tag{8}$$

Then $hgu \in \widetilde{Q^\theta}$ because

$$\theta(hgu) = \begin{pmatrix} \frac{mb^2 b_1 - ma^2 + b^2}{mabb_1} & -\frac{a_1 b}{ma} \\ \frac{a_1 b}{a} & -\frac{b_1 b}{a} \end{pmatrix} = (hgu)^{-1}. \tag{9}$$

Therefore $g \in H_k^\theta \widetilde{Q^\theta} U_k$.

For $k = \mathbb{F}_3$ and $m \in (\mathbb{F}_3^*)^2$, we have $H_{\mathbb{F}_3}^\theta = \{\pm \mathrm{Id}\}$. If $\alpha = 0$ we must use an h different than that in (8). Assume $\theta = \theta_1$, then G defined over $k = \mathbb{F}_3$ has 24 elements, many of which already belong to $H_{\mathbb{F}_3}^\theta$, $\widetilde{Q^\theta}$, or $\pm U_{\mathbb{F}_3}$. The only elements of $G_{\mathbb{F}_3}$ of concern are

$$\begin{pmatrix} a & 0 \\ b & a \end{pmatrix}, \begin{pmatrix} a & a \\ a & b \end{pmatrix}, \text{ or } \begin{pmatrix} a & b \\ b & b \end{pmatrix}, \tag{10}$$

where $a, b \neq 0$. Choosing $u \in U_{\mathbb{F}_3}$ from Table 1 will yield $gu \in \widetilde{Q^\theta}$ and hence $g \in H_{\mathbb{F}_3}^\theta \widetilde{Q^\theta} U_{\mathbb{F}_3}$. ∎

$g \in G_{\mathbb{F}_3}$	$u \in U_{\mathbb{F}_3}$
$\begin{pmatrix} a & 0 \\ b & a \end{pmatrix}$	$\begin{pmatrix} 1 & -\frac{b}{a} \\ 0 & 1 \end{pmatrix}$
$\begin{pmatrix} a & a \\ a & b \end{pmatrix}$	$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$
$\begin{pmatrix} a & b \\ b & b \end{pmatrix}$	$\begin{pmatrix} 1 & \frac{b}{a} \\ 0 & 1 \end{pmatrix}$

Table 1: $u \in U_{\mathbb{F}_3}$ such that $gu \in \widetilde{Q^\theta}$

For a general field k and involution θ, $G_k \neq H_k^\theta Q^\theta U_k$ and thus expanding to the extended symmetric space is necessary. Further on, we give cases in which the symmetric space will suffice.

Remark 3.7. Let G be defined over a field k and θ an involution of G. The $(H_k^\theta \times U_k)$-orbits on G_k are defined by $(h,u) \bullet g := hgu$ for $h \in H_k^\theta, u \in U_k$, and $g \in G_k$. By Theorem 3.2, we can choose orbit representatives in $\widetilde{Q^\theta}$. Similarly, the twisted U_k-orbits on $\widetilde{Q^\theta}$ are defined by the twisted action $u * q := u^{-1}q\theta(u)$ for $u \in U_k$ and $q \in Q^\theta$. By Remark 2.7, $Q^\theta \simeq G_k/H_k^\theta$, thus the U_k-orbits on Q^θ are in bijective correspondence with the $(H_k^\theta \times U_k)$-orbits on G_k if and only if $H_k^\theta Q^\theta U_k = H_k^\theta \widetilde{Q^\theta} U_k$.

The following example exhibits the necessity of the extended symmetric space using a specific case where the symmetric space does not suffice.

Example 3.8. Let G be defined over $k = \mathbb{Q}$ and $\theta = \theta_{-1}$ the involution of G. For convenience, we will use $Q^\theta = \{g^{-1}\theta(g) | g \in G_{\mathbb{Q}}\}$. Let the $(H_{\mathbb{Q}}^\theta \times U_{\mathbb{Q}})$-orbits on $G_{\mathbb{Q}}$ and twisted $U_{\mathbb{Q}}$-orbits on Q^θ be defined as in Remark 3.7. Consider the map from $U_{\mathbb{Q}} * Q^\theta$ to $(H_{\mathbb{Q}}^\theta \times U_{\mathbb{Q}}) \bullet G_{\mathbb{Q}}$ defined by

$$U_{\mathbb{Q}} * q \mapsto (H_{\mathbb{Q}}^\theta \times U_{\mathbb{Q}}) \bullet g$$

where $q = g^{-1}\theta(g)$. For $q \in Q^\theta$, assume there exists $g_1, g_2 \in G_{\mathbb{Q}}$ such that $q = g_1^{-1}\theta(g_1) = g_2^{-1}\theta(g_2)$. Then $g_1 = hg_2$ for some $h \in H_{\mathbb{Q}}^\theta$ because

$$g_1^{-1}\theta(g_1) = g_2^{-1}\theta(g_2) \Rightarrow \theta(g_1 g_2^{-1}) = g_1 g_2^{-1} \Rightarrow g_1 g_2^{-1} \in H_{\mathbb{Q}}^\theta. \tag{11}$$

The map is well-defined because it is independent of coset representative and surjective by definition of Q^θ.

We may also reverse the map,

$$(H_{\mathbb{Q}}^\theta \times U_{\mathbb{Q}}) \bullet g \mapsto g^{-1}\theta(g). \tag{12}$$

By Theorem 3.2, let $g = hqu$, $q \in \widetilde{Q^\theta}$. Then $(H_{\mathbb{Q}}^\theta \times U_{\mathbb{Q}}) \bullet g$ maps to $U_{\mathbb{Q}} * q_0$ for some $q_0 = q^{-2} \in Q^\theta$,

$$(g)^{-1}\theta(g) = (hqu)^{-1}\theta(hqu) = u^{-1}q^{-1}h^{-1}\theta(h)\theta(q)\theta(u) = u^{-1}q^{-1}\theta(q)u = u * q_0.$$

Over $k = \mathbb{Q}$, this map is not surjective because not all elements of Q^θ can be written as q^{-2} for some $q \in \widetilde{Q^\theta}$.

From [9, Proposition 6.6], the U_k-orbits on Q^θ can always be represented by an element from the normalizer in G of a θ-stable maximal k-split torus A, $N_G(A)$. In this case, $N_G(A) \cap Q^\theta$ is the set of diagonal elements in $G_\mathbb{Q}$.

Furthermore, an element $X \in N_G(A) \cap Q^\theta$ can not be mapped to another element $Y \in N_G(A) \cap Q^\theta$ under the action of $(H^\theta_\mathbb{Q} \times U_\mathbb{Q})$, unless $Y = -X$. Consider the following elements,

$$X = \begin{pmatrix} x_1 & 0 \\ 0 & x_1^{-1} \end{pmatrix}, Y = \begin{pmatrix} y_1 & 0 \\ 0 & y_1^{-1} \end{pmatrix} \in N_G(A) \cap Q^\theta.$$

Additionally, we will let

$$h = \begin{pmatrix} a & b \\ b & -a \end{pmatrix} \in H^\theta_\mathbb{Q} \text{ and } u = \begin{pmatrix} 1 & u_1 \\ 0 & 1 \end{pmatrix} \in U_\mathbb{Q}.$$

For the action of $(H^\theta_\mathbb{Q} \times U_\mathbb{Q})$ on X to map to Y, it must be that

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} x_1 & 0 \\ 0 & x_1^{-1} \end{pmatrix} \begin{pmatrix} 1 & u_1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} ax_1 & ax_1u_1 + bx_1^{-1} \\ -bx_1 & -bx_1u_1 + ax_1^{-1} \end{pmatrix} = \begin{pmatrix} y_1 & 0 \\ 0 & y_1^{-1} \end{pmatrix} \tag{13}$$

where $a^2 + b^2 = 1$. Solving (13) implies $h = \pm \mathrm{Id}$ and $u = \mathrm{Id}$, hence $Y = -X$.

For

$$q^{-1} = \begin{pmatrix} x & y \\ y & z \end{pmatrix} \in \widetilde{Q^\theta}$$

the only $U_\mathbb{Q}$-orbits on Q^θ which correspond to the $(H^\theta_\mathbb{Q} \times U_\mathbb{Q})$-orbits on $G_\mathbb{Q}$ are the ones whose representative in $N_G(A)$ is of the form

$$q_0 = \begin{pmatrix} x^2 + y^2 & 0 \\ 0 & y^2 + z^2 \end{pmatrix}.$$

For

$$g = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_1^{-1} \end{pmatrix} \in G_\mathbb{Q}$$

such that $\lambda_1 > 0$ and λ_1 is not the sum of two squares, $(H^\theta_\mathbb{Q} \times U_\mathbb{Q}) \bullet g$ can not be obtained as a $U_\mathbb{Q}$-orbit on Q^θ. Hence $G \neq H^\theta_\mathbb{Q} Q^\theta U_\mathbb{Q}$.

4. Symmetric and Extended Symmetric Spaces

To understand the structure of the symmetric and extended symmetric spaces of G for any field and involution, we will analyze the relationship between the spaces.

Recall from Lemma 2.10 that $Q^\theta \subset \widetilde{Q^\theta}$ for all groups. Example 2.13 demonstrates that the symmetric space and extended symmetric space are not equivalent in general. We will determine for which cases we get equality.

Theorem 4.1. *Let G be defined over $k = \bar{k}$ and $\theta = \theta_1$ the involution of G. Then the extended symmetric space is equivalent to the symmetric space.*

Proof. Let

$$q = \begin{pmatrix} a & b \\ -b & c \end{pmatrix} \in \widetilde{Q^\theta}.$$

For q to be in the symmetric space, we need $g \in G$ such that $q = g\theta(g)^{-1} \in Q^\theta$. Depending on the value of c, choose $g \in G$ according to Table 2. Choosing the appropriate g will yield $q = g\theta(g)^{-1} \in Q^\theta$. The reverse containment follows from Lemma 4.1. ∎

c	b	$g \in G$
$c \neq 0$	-	$\begin{pmatrix} \frac{1}{\sqrt{c}} & \frac{b}{\sqrt{c}} \\ 0 & \sqrt{c} \end{pmatrix}$
$c = 0$	b=1	$\begin{pmatrix} 0 & \sqrt{-a} \\ \frac{\sqrt{-a}}{a} & -\frac{\sqrt{-a}}{a} \end{pmatrix}$
$c = 0$	$b = -1$	$\begin{pmatrix} 1 & -1 \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}$

Table 2: $g \in G$ such that $q = g\theta(g)^{-1} \in Q^\theta$ for $k = \bar{k}$

Theorem 4.2. *Let G be defined over $k = \mathbb{R}$ and $\theta = \theta_1$ the involution of G. Then the extended symmetric space is equivalent to the symmetric space.*

Proof. Let

$$q = \begin{pmatrix} a & b \\ -b & c \end{pmatrix} \in \widetilde{Q^\theta}.$$

As in the proof of Theorem 4.1, we need $g \in G_{\mathbb{R}}$ such that $q = g\theta(g)^{-1} \in Q^\theta$. Depending on the value of a, choose $g \in G_{\mathbb{R}}$ according to Table 3. Choosing the appropriate g will yield $g\theta(g)^{-1} = q \in Q^\theta$. The reverse containment follows from Lemma 2.10. ∎

a	b	$g \in G_{\mathbb{R}}$
$a > 0$	-	$\begin{pmatrix} \sqrt{a} & 0 \\ -\frac{b}{\sqrt{a}} & \frac{1}{\sqrt{a}} \end{pmatrix}$
$a < 0$	-	$\begin{pmatrix} 0 & \sqrt{-a} \\ \frac{\sqrt{-a}}{a} & -\frac{b\sqrt{-a}}{a} \end{pmatrix}$
$a = 0$	$b = 1$	$\begin{pmatrix} 1 & 1 \\ \frac{c-1}{2} & \frac{c+1}{2} \end{pmatrix}$
$a = 0$	$b = -1$	$\begin{pmatrix} 1 & -1 \\ \frac{1-c}{2} & \frac{c+1}{2} \end{pmatrix}$

Table 3: $g \in G_{\mathbb{R}}$ such that $q = g\theta(g)^{-1} \in Q^\theta$ for $k = \mathbb{R}$

In [5], the structure of the symmetric space of G defined over $k = \mathbb{F}_q$ is analyzed, including the following result.

Theorem 4.3. *Let G be defined over $k = \mathbb{F}_q$ with characteristic of k not 2, and θ an involution of G, then the symmetric space is equivalent to the extended symmetric space.*

We now consider G defined over $k = \mathbb{Q}_p$ with the involution $\theta = \theta_1$. For

$$q = \begin{pmatrix} a & b \\ -b & c \end{pmatrix} \in \widetilde{Q^\theta},$$

we must show there exists

$$g = \begin{pmatrix} x & y \\ z & w \end{pmatrix} \in G_{\mathbb{Q}_p}$$

such that

$$q = \begin{pmatrix} a & b \\ -b & c \end{pmatrix} = \begin{pmatrix} x^2 - y^2 & wy - xz \\ -(wy - xz) & w^2 - z^2 \end{pmatrix} = g\theta(g)^{-1}. \tag{14}$$

To find such $g \in G_{\mathbb{Q}_p}$, we solve for $x, y, z, w \in \mathbb{Q}_p$ such that the following equations from (14) and $\det(g) = 1$ hold:

$$1 = xw - yz \tag{15}$$

$$a = x^2 - y^2 \tag{16}$$

$$c = w^2 - z^2 \tag{17}$$

$$b = yw - xz \tag{18}$$

Using Hilbert's symbol, we obtain solutions to (16) and (17) in $\mathbb{Q}_p$.

Definition 4.4. The polynomial $ax^2 + bx^2 - z^2$ is *isotropic over* $\mathbb{Q}_p$ if there exists non-trivial (x, y, z) in $\mathbb{Q}_p^3$ such that $ax^2 + bx^2 - z^2 = 0$. For $a, b \in \mathbb{Q}_p$, the *Hilbert symbol* is defined as

$$(a, b)_p = \begin{cases} 1 & ax^2 + by^2 - z^2 \text{ is isotropic} \\ -1 & \text{otherwise} \end{cases}$$

In [6], several useful properties of the Hilbert symbol are given.

Proposition 4.5 (Properties of the Hilbert Symbol)**.**
For all $a, b \in \mathbb{Q}_p$, we have

1. $(a, b)_p = (b, a)_p$
2. $(a, b)_p = 1$ *then* $a \in (\mathbb{Q}_p^*)^2$
3. $(a, -a)_p = 1$

We can rewrite (16) equivalently as,

$$0 = x^2 - y^2 - a \text{ or } 0 = \left(\frac{1}{a}\right)x^2 + \left(-\frac{1}{a}\right)y^2 - 1. \tag{19}$$

This new equation corresponds to the Hilbert Symbol $\left(\frac{1}{a}, -\frac{1}{a}\right)_p$. Note that we have scaled the equation in Definition 4.4 so that $z^2 = 1$. By Proposition 4.5, Property 3, $(\frac{1}{a}, -\frac{1}{a})_p = 1$. Therefore (19) has a non-trivial solution $(x, y, 1)$ in $\mathbb{Q}_p^3$, and by extension, (16) has a solution (x, y) in $\mathbb{Q}_p^2$. Similar calculations show (18) has a solution.

For a simultaneous solution to (15)-(18), let

$$x = \frac{-b + \alpha w}{\beta}, y = \alpha, z = \beta,$$

where

$$\alpha = \frac{wb \pm \sqrt{w^2 - c}}{c}, \beta = \pm\sqrt{w^2 - c}.$$

We can verify that $\sqrt{w^2 - c}$ is defined in $\mathbb{Q}_p$ for all $c \in \mathbb{Q}_p$, using the Hilbert symbol. The equation

$$\beta^2 = w^2 - c \tag{20}$$

can be shown to have a solution in $\mathbb{Q}_p$ with the same method as in (19).

Depending on the value of c, choose $g \in G_{\mathbb{Q}_p}$ according to Table 4. Choosing the appropriate g will yield $g\theta(g)^{-1} = q \in Q^\theta$. Because the reverse containment is clear by Lemma 2.10, we have the following result.

c	b	$g \in G_{\mathbb{Q}_p}$
$c \neq 0$	-	$\begin{pmatrix} \frac{-bc+w^2b+w\sqrt{w^2-c}}{c\sqrt{w^2-c}} & \frac{wb+\sqrt{w^2-c}}{c} \\ \sqrt{w^2-c} & w \end{pmatrix}$
$c = 0$	b=1	$\begin{pmatrix} -\frac{1}{2} & -\frac{1}{2} \\ 1 & -1 \end{pmatrix}$
$c = 0$	$b = -1$	$\begin{pmatrix} -1 & 1 \\ -\frac{1}{2} & -\frac{1}{2} \end{pmatrix}$

Table 4: $g \in G_{\mathbb{Q}_p}$ such that $q = g\theta(g)^{-1} \in Q^\theta$ for $k = \mathbb{Q}_p$

Theorem 4.6. *Let G be defined over $k = \mathbb{Q}_p$ with $p \neq 2$ and $\theta = \theta_1$ the involution of G, then the extended symmetric space is equivalent to the symmetric space.*

By Corollary 2.4, there are four classes of involutions of $\mathrm{Aut}(G, G_{\mathbb{Q}_p})$ because $\left|\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2\right| = 4$. These classes are represented by $\{\theta_1, \theta_p, \theta_{N_p}, \theta_{pN_p}\}$, where N_p is a non-square in $\mathbb{Q}_p$ not in the same square class as p. For $\theta = \theta_m$ with $m \neq 1$, we can show by example that the extended symmetric space and symmetric space are not equivalent.

For each involution, we consider the cases when $p \equiv 1 \mod 4$ and $p \equiv 3 \mod 4$ separately. The key difference is that, as in the finite fields, -1 is a square when $p \equiv 1 \mod 4$ and is -1 not a square when $p \equiv 3 \mod 4$. When $p \equiv 1 \mod 4$, we use the square class representatives $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2 = \{1, p, N_p, pN_p\}$. When $p \equiv 3 \mod 4$, we use the square class representatives $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2 = \{1, p, -1, -p\}$.

Example 4.7. Let $p = 3$ and consider the involution $\theta = \theta_3$. The extended symmetric space is defined as

$$\widetilde{Q^\theta} = \left\{ \begin{pmatrix} a & b \\ -3b & c \end{pmatrix} \middle| a, b, c \in \mathbb{Q}_p \text{ and } ac + 3b^2 = 1 \right\}.$$

Let

$$q = \begin{pmatrix} \frac{1}{3} & 0 \\ 0 & 3 \end{pmatrix} \in \widetilde{Q^\theta}.$$

Then $q = g\theta(g)^{-1}$ implies g is equal to

$$g_1 = \begin{pmatrix} \frac{\sqrt{3}}{3} & 0 \\ 0 & \sqrt{3} \end{pmatrix} \quad \text{or} \quad g_2 = \begin{pmatrix} \frac{1}{3}d & \pm\frac{1}{9}\alpha \\ \pm\alpha & d \end{pmatrix},$$

where $\alpha = \sqrt{3d^2 - 9}$.

Because $3 \notin (\mathbb{Q}_3^*)^2$, $g_1 \notin G_{\mathbb{Q}_p}$. For g_2, $\alpha = \sqrt{3d^2 - 9} = \sqrt{3}\sqrt{d^2 - 3} \in \mathbb{Q}_p$ if and only if $d^2 - 3$ is in the same square class as 3, which implies $d = \sqrt{3(1 + x^2)}$ for some $x \in \mathbb{Q}_p$. Note that $3(1 + x^2) \notin (\mathbb{Q}_p^*)^2$, thus $d \notin \mathbb{Q}_p$.

There is no $g \in G_{\mathbb{Q}_p}$ such that $q = g\theta(g)^{-1} \in Q^\theta$ and therefore, the symmetric space and extended symmetric space are not equivalent for the involution $\theta = \theta_p$ when $p \equiv 3 \mod 4$.

Using similar calculations, one can show there exists $q \in \widetilde{Q^\theta}$ such that $q \notin Q^\theta$ in the following cases: $\theta = \theta_p$ with $p \equiv 1 \mod 4, \theta = \theta_{N_p}$ with $p \equiv 1 \mod 4$ and $p \equiv 3 \mod 4$, and $\theta = \theta_{pN_p}$ with $p \equiv 1 \mod 4$ and $p \equiv 3 \mod 4$. These examples serve to show for G defined over $k = \mathbb{Q}_p$ with the involution θ, $\widetilde{Q^\theta} = Q^\theta$ only when $\theta = \theta_1$.

Using the following theorem from [6], we can prove a similar result for $k = \mathbb{Q}$.

Theorem 4.8 (Strong Hasse Principle)**.** *Let f be a regular quadratic form over $\mathbb{Q}$. Then f is isotropic over $\mathbb{Q}$ if and only if f is isotropic over $\mathbb{Q}_p$ for all p, including $p = \infty$.*

Theorem 4.9. *Let G be defined over $k = \mathbb{Q}$ and $\theta = \theta_1$ the involution of G, then the extended symmetric space is equivalent to the symmetric space.*

Proof. The equations (15)-(18) have a simultaneous solution over $k = \mathbb{Q}_p$ ($p \neq 2$) by Theorem 4.6 and over $k = \mathbb{R} = \mathbb{Q}_\infty$ by Theorem 4.2. Applying the Strong Hasse Principle, equations (15)-(18) must also have a simultaneous solution over $k = \mathbb{Q}$. ∎

Corollary 4.10. *For G defined over k and $\theta = \theta_1$ the involution of G, we have $Q^\theta = \widetilde{Q^\theta}$ for $k = \bar{k}, \mathbb{R}, \mathbb{F}_p, \mathbb{Q}_p$ and $\mathbb{Q}$.*

Corollary 4.11. *For G defined over a field listed in Corollary 4.10 with the involution $\theta = \theta_1$ or G defined over $k = \mathbb{F}_q$ with any involution θ, the decomposition in Theorem 3.2 can be simplified to $G_k = H_k^\theta Q^\theta U_k$.*

5. Refining the Decomposition

For some cases, we can refine the decomposition, $G_k = H_k^\theta \widetilde{Q^\theta} U_k$, by removing elements from each of the factors which are not necessary. To do so we will examine intersections of the factors, including $H_k^\theta \widetilde{Q^\theta} \bigcap U_k, H_k^\theta \bigcap \widetilde{Q^\theta}, U_k \bigcap H_k^\theta, U_k \bigcap \widetilde{Q^\theta}$, $H_k^\theta \bigcap \widetilde{Q^\theta} U_k$, and $H_k^\theta U_k \bigcap \widetilde{Q^\theta}$.

For the following propositions, let $\theta = \theta_m$ be the involution of G, H^θ the fixed-point group, $\widetilde{Q^\theta}$ the extended symmetric space, and U the unipotent subgroup of G consisting of upper triangular matrices with 1's on the diagonal.

Proposition 5.1.

$$H_k^\theta \bigcap \widetilde{Q^\theta} = U_k \bigcap H_k^\theta = U_k \bigcap \widetilde{Q^\theta} = \{\pm \mathrm{Id}\}$$

Proof. This is clear by the definitions of $H_k^\theta, \widetilde{Q^\theta}$, and U_k. ∎

Proposition 5.2.

$$H_k^\theta \widetilde{Q^\theta} \bigcap U_k = \left\{ \begin{pmatrix} 1 & \frac{2b}{a} \\ 0 & 1 \end{pmatrix} \middle| \; a \in k^*, \; b \in k, \; a^2 - mb^2 = 1 \right\} \tag{21}$$

Proof. First, construct $X \in H_k^\theta \widetilde{Q^\theta}$ using

$$h = \begin{pmatrix} a & b \\ mb & a \end{pmatrix} \in H_k^\theta \quad \text{and} \quad q = \begin{pmatrix} x & y \\ -my & z \end{pmatrix} \in \widetilde{Q^\theta},$$

where $a^2 - mb^2 = 1$ and $xz + my^2 = 1$ as in Examples 2.5 and 2.8, so

$$X = hq = \begin{pmatrix} ax - mby & ay + bz \\ m(bx - ay) & mby + az \end{pmatrix} \in H_k^\theta \widetilde{Q^\theta}.$$

Since X is in the intersection, X may also be written as an element of U_k,

$$X = \begin{pmatrix} ax - mby & ay + bz \\ m(bx - ay) & mby + az \end{pmatrix} = \begin{pmatrix} 1 & u_1 \\ 0 & 1 \end{pmatrix}, \tag{22}$$

for some $u_1 \in k$. Solving the matrix equation (22), we obtain $u_1 = \frac{2b}{a}$. ∎

The cardinality of the set (21) is equivalent to the cardinality of H_k^θ minus the elements of H_k^θ with zeroes on the diagonal, which is equal to

$$|H_k^\theta \widetilde{Q^\theta} \bigcap U_k| = |H_k^\theta| - \left| \left\{ b \in k^* \mid b = \pm \frac{1}{\sqrt{-m}} \right\} \right|.$$

Proposition 5.3.

$$H_k^\theta \bigcap \widetilde{Q^\theta} U_k = \left\{ \begin{pmatrix} a & b \\ mb & a \end{pmatrix} \middle| \; a \in k^*, \; b \in k, \; a^2 - mb^2 = 1 \right\} \tag{23}$$

Proof. First, construct $X \in \widetilde{Q^\theta} U_k$ using

$$q = \begin{pmatrix} x & y \\ -my & z \end{pmatrix} \in \widetilde{Q^\theta} \quad \text{and} \quad u = \begin{pmatrix} 1 & u_1 \\ 0 & 1 \end{pmatrix}$$

where $xz + my^2 = 1$ and $u_1 \in k$ as in Example 2.8 and Equation (2), so

$$X = qu = \begin{pmatrix} x & u_1 x + y \\ -my & -myu_1 + z \end{pmatrix} \in \widetilde{Q^\theta} U_k.$$

Since X is in the intersection, X may also be written as an element of H_k^θ,

$$X = \begin{pmatrix} x & u_1 x + y \\ -my & -myu_1 + z \end{pmatrix} = \begin{pmatrix} a & b \\ mb & a \end{pmatrix}. \tag{24}$$

Solving the matrix equation (24) and including the fact that $a^2 - mb^2 = 1$, we obtain $x = a$, $y = -b$ and $u_1 = \frac{2b}{a}$. ∎

The cardinality of the set (23) is the cardinality of H_k^θ minus the elements in H_k^θ with zeroes on the diagonal. Furthermore, the cardinality of the intersection (23) is equivalent to the cardinality of the intersection in Proposition 5.2 (21),

$$|(H_k^\theta \bigcap \widetilde{Q^\theta} U_k)| = |H_k^\theta \widetilde{Q^\theta} \bigcap U_k| = \left|H_k^\theta\right| - \left|\left\{ b \in k^* \mid b = \pm \frac{1}{\sqrt{-m}} \right\}\right|.$$

This intersection is almost equivalent to H_k^θ,

$$H_k^\theta \smallsetminus (H_k^\theta \bigcap \widetilde{Q^\theta} U_k) = \left\{ \begin{pmatrix} 0 & b \\ mb & 0 \end{pmatrix} \,\middle|\, b \in k,\ -mb^2 = 1 \right\},$$

leading to the following result.

Lemma 5.4. *Let G be defined over k and $\theta = \theta_m$ the involution of G. Then $H_k^\theta \subset \widetilde{Q^\theta} U_k$ if and only if $-m \notin (k^*)^2$.*

Proof. This proof follows from a chain of equivalent statements.

$$\begin{aligned} H_k^\theta \subset \widetilde{Q^\theta} U_k & \qquad \Leftrightarrow \\ H_k^\theta \smallsetminus (H_k^\theta \bigcap \widetilde{Q^\theta} U_k) = \left\{ \left(\begin{smallmatrix} 0 & b \\ mb & 0 \end{smallmatrix}\right) \,\middle|\, b \in k,\ -mb^2 = 1 \right\} = \varnothing & \qquad \Leftrightarrow \\ b = \pm \frac{1}{\sqrt{-m}} \notin k & \end{aligned}$$

∎

Example 5.5. When $H_k^\theta \subset \widetilde{Q^\theta} U_k$, we do not necessarily have $G_k = \widetilde{Q^\theta} U_k$. Let G be defined over $k = \mathbb{R}$ and $\theta = \theta_1$ the involution of G. By Lemma 5.4, $H_\mathbb{R} \subset \widetilde{Q^\theta} U_\mathbb{R}$. Let

$$g = \begin{pmatrix} 0 & \frac{1}{2} \\ -2 & 0 \end{pmatrix} \in G_\mathbb{R},$$

then $gu \notin \widetilde{Q^\theta}$ since

$$\theta(gu) = \begin{pmatrix} -2u_1 & -2 \\ \frac{1}{2} & 0 \end{pmatrix} \neq \begin{pmatrix} -2u_1 & -\frac{1}{2} \\ 2 & 0 \end{pmatrix} = (gu)^{-1},$$

for any

$$u = \begin{pmatrix} 1 & u_1 \\ 0 & 1 \end{pmatrix} \in U_{\mathbb{R}}.$$

Therefore $G_{\mathbb{R}} \neq \widetilde{Q^\theta} U_{\mathbb{R}}$.

Proposition 5.6.

$$H_k^\theta U_k \bigcap \widetilde{Q^\theta} = \left\{ \begin{pmatrix} x & y \\ -my & z \end{pmatrix} \middle| \; x \in k^*,\; y, z \in k,\; xz + my^2 = 1 \right\} \tag{25}$$

Proof. First, construct $X \in H_k^\theta U_k$ using

$$\begin{pmatrix} a & b \\ mb & a \end{pmatrix} \in H_k^\theta \quad \text{and} \quad u = \begin{pmatrix} 1 & u_1 \\ 0 & 1 \end{pmatrix} \in U_k$$

where $a^2 - mb^2 = 1$ and $u_1 \in k$ as in Example 2.5 and Equation (2), so

$$X = hu = \begin{pmatrix} a & u_1 a + b \\ mb & mbu_1 + a \end{pmatrix} \in H_k^\theta U_k.$$

Since X is in the intersection, X may also be written as an element in $\widetilde{Q^\theta}$,

$$X = \begin{pmatrix} a & u_1 a + b \\ mb & mbu_1 + a \end{pmatrix} = \begin{pmatrix} x & y \\ -my & z \end{pmatrix}. \tag{26}$$

Solving the matrix equation (26) and including the fact that $xz + my^2 = 1$, we obtain $a = x$, $b = -y$, and $u_1 = \frac{2y}{x}$. ∎

Remark 5.7. Similar to the previous proposition, (25) is almost equivalent to the extended symmetric space,

$$\widetilde{Q^\theta} \smallsetminus (H_k^\theta U_k \bigcap \widetilde{Q^\theta}) = \left\{ \begin{pmatrix} 0 & y \\ -my & z \end{pmatrix} \middle| \; y \in k,\; my^2 = 1 \right\},$$

leading to the following result.

Lemma 5.8. *Let G be defined over k and $\theta = \theta_m$ the involution of G. Then $\widetilde{Q^\theta} \subset H_k^\theta U_k$ if and only if $m \notin (k^*)^2$.*

Proof. This proof follows from a chain of equivalent statements.

$$\begin{aligned} \widetilde{Q^\theta} \subset H_k^\theta U_k & \qquad \Leftrightarrow \\ \widetilde{Q^\theta} \smallsetminus (H_k^\theta U_k \bigcap \widetilde{Q^\theta}) = \left\{ \begin{pmatrix} 0 & y \\ -my & z \end{pmatrix} \middle| \; y \in k,\; my^2 = 1 \right\} = \varnothing & \qquad \Leftrightarrow \\ y = \pm \frac{1}{\sqrt{m}} \notin k & \end{aligned}$$

∎

The following result is a more precise generalization of the Iwasawa decomposition.

Theorem 5.9. *Let G be defined over k and $\theta = \theta_m$ the involution of G. If $m \notin (k^*)^2$, then $G_k = H_k^\theta U_k$.*

Proof. Let $g \in G_k$ and $\theta = \theta_m$ the involution of G with $m \notin (k^*)^2$. By Theorem 3.2 write $g = hqu$ for some $h \in H_k^\theta, q \in \widetilde{Q^\theta}$ and $u \in U_k$. By Lemma 5.8, write $q = h_1 u_1$ for some $h_1 \in H_k^\theta$ and $u_1 \in U_k$. Thus, $g = hh_1 u_1 u \in H_k^\theta U_k$. The reverse containment in clear. ∎

Theorem 5.10. *Let G be defined over k and $\theta = \theta_1$ the involution of G. Then $G_k = \bigcup_{\omega \in W(T)} H_k^\theta \omega U_k$, where $W(T)$ is the Weyl group of the maximal k-split torus.*

Proof. Let $W(T)$ be as in (4) and $g \in G_k$. If $g \in H_k^\theta U_k \bigcap \widetilde{Q^\theta}$, then $g \in H_k^\theta U_k$. If $g \notin H_k^\theta U_k \bigcap \widetilde{Q^\theta}$, write $g = hqu$ as in Theorem 3.2 with $q \in \widetilde{Q^\theta} \setminus (H_k^\theta U_k \bigcap \widetilde{Q^\theta})$. By Remark 5.7, let

$$q = \begin{pmatrix} 0 & 1 \\ -1 & z \end{pmatrix} \quad \text{and} \quad u_1 = \begin{pmatrix} 1 & -z \\ 0 & 1 \end{pmatrix},$$

then $g \in H_k^\theta \omega U_k$, $\omega \in W(T)$ since

$$g = hqu = h \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} u_1 u \in H_k^\theta \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} U_k.$$ ∎

6. Retaining Semisimplicity

In the traditional Cartan decomposition we get the added property that the symmetric space consists of semisimple elements. We will determine in which cases this property still holds. From [9] and [1], respectively, we have the following results.

Theorem 6.1. *Let k be a field with characteristic zero. If H^θ is k-anisotropic, then the symmetric space consists of semisimple elements.*

Theorem 6.2. *Let G be defined over k and $\theta = \theta_m$ the involution of G. The fixed-point group of θ_m is k-anisotropic if and only if $m \neq 1$.*

Combing the previous two theorems, we have the following corollary.

Corollary 6.3. *Let G be defined over a field k with characteristic zero and $\theta = \theta_m$ the involution of G. If $m \neq 1$ then the symmetric space consists of semisimple elements.*

Example 6.4. For G defined over a field k with the involution θ_m, the corresponding symmetric space consists of semisimple elements in the following cases:

i. $k = \mathbb{R}$ and $m = -1$

ii. $k = \mathbb{Q}_p$ and $m = p, N_p,$ or pN_p

To extend Theorem 6.1 and Corollary 6.3 to fields of characteristic not 2, we need to determine if the symmetric space contains only semisimple elements for the involution θ_m, $m \neq 1$, over fields with prime characteristic p. Once we have done so, we will be able to add the case when $k = \mathbb{F}_q$ and $m = N_p$ to the list in Example 6.4.

Theorem 6.5. *Let G be defined over a field k and $\theta = \theta_m$ the involution of G. If $m \notin (k^*)^2$ then the extended symmetric space consists of semisimple elements.*

Proof. Let

$$q = \begin{pmatrix} a & b \\ -mb & c \end{pmatrix} \in \widetilde{Q^\theta}.$$

To determine if q is semisimple we analyze its eigenvalues, given by

$$\left\{ \frac{1}{2} \left(a + c \pm \sqrt{c^2 - 2ac + a^2 - 4mb^2} \right) \right\}. \tag{27}$$

If q has two distinct eigenvalues, then q is semisimple. The cases of concern are when q has one eigenvalue with multiplicity 2. By (27) and $\det(q) = 1$,

$$(a - c)^2 = 4mb^2 \tag{28}$$

is a necessary and sufficient condition for q to have one eigenvalue. Since $m \notin (k^*)^2$, equation (28) has no solutions. ∎

By Corollary 2.4, there are two classes of involutions of $\mathrm{Aut}(G, G_{\mathbb{F}_q})$. These classes are represented by $\{\theta_1, \theta_{N_p}\}$ where N_p is the smallest non-square in the field.

Corollary 6.6. *Let G be defined over k and $\theta = \theta_m$ the involution of G. If $m \notin (k^*)^2$ then the symmetric space consists of semisimple elements.*

Proof. By Lemma 2.10 and Theorem 6.5, the elements of the symmetric space must be semisimple. ∎

While combining Theorems 6.1 and 6.2 proves this result for fields with characteristic zero, our result and proof hold for any field with characteristic not 2. However, these do not extend to cases with the involution $\theta = \theta_1$ as illustrated with the following results.

Lemma 6.7. *Let G be defined over k and $\theta = \theta_1$ the involution of G, then there exists elements in the symmetric space which are not semisimple.*

Proof. We will construct an element in the symmetric space with a unipotent factor. Let

$$g = \begin{pmatrix} x+2 & x+1 \\ -(x+1) & -x \end{pmatrix} \in G_k$$

for some $x \in k \setminus \{-1\}$. Then $q = g\theta(g)^{-1} \in Q^\theta$ has a Jordan decomposition with a unipotent factor and thus q is not semisimple,

$$g\theta(g)^{-1} = \begin{pmatrix} 3+2x & 2+2x \\ -(2+2x) & -(2x+1) \end{pmatrix} = S^{-1}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} S. \qquad \blacksquare$$

Corollary 6.8. *Let G be defined over k and $\theta = \theta_1$ the involution of G, then there exists elements in the extended symmetric space which are not semisimple.*

Proof. This follows from Lemmas 2.10 and 6.7. $\blacksquare$

Corollary 6.9. *Let G be defined over k and $\theta = \theta_m$ the involution of G, then the symmetric space and extended symmetric space consist of semisimple elements if and only if $m \notin (k^*)^2$.*

Proof. If $m \in (k^*)^2$ apply Lemma 6.7. If $m \notin (k^*)^2$ apply Theorem 6.5. $\blacksquare$

Lemma 6.10. *Let G be defined over k, θ an involution of G, and A a θ-split torus of G. The image of A_k under conjugation by H_k^θ is contained in the extended symmetric space.*

Proof. Let $a \in A_k$ and $h \in H_k^\theta$. Then

$$\theta(hah^{-1}) = \theta(h)\theta(a)\theta(h^{-1}) = ha^{-1}h^{-1} = (hah^{-1})^{-1}.$$

Hence, $hah^{-1} \in \widetilde{Q^\theta}$. $\blacksquare$

Theorem 6.11. *Let G be defined over k and $\theta = \theta_m$ the involution of G. If $m \notin (k^*)^2$ then the extended symmetric space decomposes as the disjoint union of the H_k^θ-orbits of the maximal (θ, k)-split tori $\{A_i \mid i \in I\}$,*

$$\widetilde{Q^\theta} = \bigcup_{i \in I}^{\cdot} H_k^\theta \cdot (A_i)_k.$$

Proof. Let $\theta = \theta_m$ with $m \notin (k^*)^2$. By Lemma 6.10, $H_k \cdot (A_i)_k \subset \widetilde{Q^\theta}$ for all $\{A_i | i \in I\}$. For $q \in \widetilde{Q^\theta}$, q is θ-split and semisimple by Corollary 6.9. Thus q must be contained in the H_k^θ-conjugacy class of some k-split torus $(A_i)_k$. $\blacksquare$

Corollary 6.12. *Let G be defined over k and $\theta = \theta_m$ the involution of G. If $m \notin (k^*)^2$ then G_k decomposes as*

$$G_k = \bigcup_{i \in I}^{\cdot} H_k^\theta (A_i)_k H_k^\theta U_k$$

where $\{A_i \mid i \in I\}$ are the H_k^θ-conjugacy classes of maximal (θ, k)-split tori.

Proof. Let $g \in G$. By Theorem 3.2, $g = hqr$ for some $h \in H_k^\theta$, $q \in \widetilde{Q^\theta}$ and $u \in U_k$. By Theorem 6.11, $q = h_1 a h_1^{-1}$ for some $h_1 \in H_k^\theta$ and $a \in A_i$, where A_i is some H_k^θ-conjugacy class of maximal (θ, k)-split tori. Thus, $g = hh_1 a h_1^{-1} u \in H_k^\theta (A_i)_k H_k^\theta U_k$. The reverse containment is clear. ∎

7. Commutivity of the Factors

In the following lemmas, let θ be the involution of G and $H^\theta, \widetilde{Q^\theta}$, and U be the fixed-point group, the extended symmetric space, and the unipotent subgroup, respectively.

Lemma 7.1. *Let G be defined over k and θ an involution of G, then $H_k^\theta \widetilde{Q^\theta} = \widetilde{Q^\theta} H_k^\theta$.*

Proof. Let $g \in \widetilde{Q^\theta} H_k^\theta$. Then $g = qh$ for some $h \in H_k^\theta$ and $q \in \widetilde{Q^\theta}$. We can multiply g on the left by (hh^{-1}) to obtain $g = (hh^{-1})qh = h(h^{-1}qh) \in H_k^\theta \widetilde{Q^\theta}$ since $h^{-1}qh \in \widetilde{Q^\theta}$ by Lemma 6.10. Recall that the extended symmetric space is θ-split by definition. .

Similarly, let $g \in H_k^\theta \widetilde{Q^\theta}$, then $g = hq$ for some $h \in H_k^\theta$ and $q \in \widetilde{Q^\theta}$. We can multiply g on the right by $(h^{-1}h)$ to obtain $g = hq(h^{-1}h) = (hqh^{-1})h \in \widetilde{Q^\theta} H_k^\theta$ since $hqh^{-1} \in \widetilde{Q^\theta}$ by Lemma 6.10. ∎

Example 7.2. In general, $U_k H_k^\theta \neq H_k^\theta U_k$ and $U_k \widetilde{Q^\theta} \neq \widetilde{Q^\theta} U_k$. First, we will show that the fixed-point group and the unipotent subgroup do not commute when $k = \mathbb{R}$ and $\theta = \theta_1$. Consider

$$g = \begin{pmatrix} 2 & \sqrt{3} \\ \sqrt{3} & 2 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 2+\sqrt{3} \\ \sqrt{3} & 2+\sqrt{3} \end{pmatrix} \in H_{\mathbb{R}}^\theta U_{\mathbb{R}}.$$

If $H_{\mathbb{R}}^\theta U_{\mathbb{R}} = U_{\mathbb{R}} H_{\mathbb{R}}^\theta$, then there exists

$$h^{-1} = \begin{pmatrix} a & b \\ b & a \end{pmatrix} \in H_{\mathbb{R}}^\theta$$

such that

$$gh^{-1} = \begin{pmatrix} 2a + (2+\sqrt{3})b & 2b + (2+\sqrt{3})a \\ a\sqrt{3} + (2+\sqrt{3})b & b\sqrt{3} + (2+\sqrt{3})a \end{pmatrix} = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \in U_{\mathbb{R}} \tag{29}$$

for some $x \in \mathbb{R}$. Solving the (2,1)-entry in the matrix equation (29), we get $a = -b - \frac{2\sqrt{3}}{3} b$, which contradicts the determinant of h^{-1} being one. Hence, $H_{\mathbb{R}}^\theta U_{\mathbb{R}} \neq U_{\mathbb{R}} H_{\mathbb{R}}^\theta$ when $\theta = \theta_1$.

Second, we will show the extended symmetric space and the unipotent subgroup do not commute when $k = \mathbb{R}$ and $\theta = \theta_{-1}$. Recall from Example 2.13 that the extended symmetric space is the set of symmetric matrices in this case. Consider

$$g = \begin{pmatrix} -5 & 2 \\ 2 & -1 \end{pmatrix} \begin{pmatrix} 1 & \frac{1}{2} \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} -5 & -\frac{1}{2} \\ 2 & 0 \end{pmatrix} \in \widetilde{Q^\theta} U_{\mathbb{R}}.$$

If $\widetilde{Q^\theta}U_\mathbb{R} = U_\mathbb{R}\widetilde{Q^\theta}$, then there exists

$$u^{-1} = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \in U_\mathbb{R}$$

such that

$$u^{-1}g = \begin{pmatrix} -5+2x & -\frac{1}{2} \\ 2 & 0 \end{pmatrix} \in \widetilde{Q^\theta}$$

for some $x \in \mathbb{R}$. However, $u^{-1}g$ is not a symmetric matrix for any x value. Hence, $\widetilde{Q^\theta}U_\mathbb{R} \neq U_\mathbb{R}\widetilde{Q^\theta}$ when $\theta = \theta_{-1}$.

Lemma 7.3. *Let G be defined over k and θ the involution of G, then $G_k = U_k H_k^\theta \widetilde{Q^\theta}$. and $G_k = \widetilde{Q^\theta} U_k H_k^\theta$.*

The proof of Lemma 7.3 follows the same techniques as the proof of Theorem 3.2, using the Bruhat decomposition and a similar construction of $u_1, u_2 \in U_k$ and $h_1, h_2 \in H_k^\theta$ such that $h_1 u_1 g \in \widetilde{Q^\theta}$ and $g h_2 u_2 \in \widetilde{Q^\theta}$ for all $g \in G_k$.

Corollary 7.4. *Let G be defined over k and θ the involution of G. The following decompositions of G_k are equivalent:*

i. $G_k = H_k^\theta \widetilde{Q^\theta} U_k$ *iii.* $G_k = \widetilde{Q^\theta} H_k^\theta U_k$ *v.* $G_k = U_k H_k^\theta \widetilde{Q^\theta}$

ii. $G_k = H_k^\theta U_k \widetilde{Q^\theta}$ *iv.* $G_k = \widetilde{Q^\theta} U_k H_k^\theta$ *vi.* $G_k = U_k \widetilde{Q^\theta} H_k^\theta$

Proof. This corollary is a combination of Lemmas 7.1, 7.3, and Theorem 3.2. ∎

References

[1] Buen, S. L., and A. G. Helminck, *On the classification of orbits of symmetric subgroups acting on flag varieties of* $\mathrm{SL}(2,\mathrm{k})$, Comm. Algebra **37** (2009), 1334–1352.

[2] Borel, A., "Linear algebraic groups," second ed., Graduate Texts in Mathematics **126**, Springer-Verlag, 1991.

[3] Borel, A., and J. Tits, *Groupes réductifs*, Inst. Hautes Études Sci. Publ. Math. **27** (1965), 55–150.

[4] —, *Compléments à l'article: "Groupes réductifs."* Inst. Hautes Études Sci. Publ. Math. **41** (1972), 253–276.

[5] Buell, C., A. G. Helminck, V. Klima, J. Schaefer, C. Wright, and E. Ziliak, *On the structure of generalized symmetric spaces of* $\mathrm{SL}_2(\mathbb{F}_\mathrm{q})$ *and* $\mathrm{GL}_2(\mathbb{F}_\mathrm{q})$, to appear.

[6] Cassels, J. W. S., "Rational quadratic forms," London Mathematical Society Monographs **13**, Academic Press, Inc., 1978.

[7] Helgason, S., "Differential geometry, Lie groups, and symmetric spaces," Pure and Applied Mathematics **80**, Academic Press, Inc., 1978.

[8] Helminck, A. G., *On the classification of k-involutions*, Adv. Math. **153** (2000), 1–117.

[9] Helminck, A. G., and S. P. Wang, *On rationality properties of involutions of reductive groups*, Adv. Math. **99** (1993), 26–96.

[10] Helminck, A. G., and L. Wu, *Classification of involutions of* $\mathrm{SL}(2,\mathrm{k})$, Comm. Algebra **30** (2002), 193–203.

[11] Springer, T. A., "Linear algebraic groups," second ed., Birkhäuser Boston, Inc., 2009.

Amanda K. Sutherland
Department of Mathematical Sciences
Shenandoah University
1460 University Drive
Winchester, VA 22601, USA
asutherl@su.edu

Received March 19. 2015
and in final form June 13, 2016