系 统 科 学 与 数 学
J. Sys. Sci. & Math. Scis.
6 (4) (1986), 286—290

ISOMORPHISMS OF ROTATION GROUPS OF BINARY QUADRATIC SPACES

EDWARD A. CONNORS
(Department of Mathematics and Statistics, University of Massachusetts)

INTRODUCTION

Results of Dieudonné and Hahn establish the rotation groups as invariants of their underlying spaces, namely isomorphic rotation groups represent semi-linearly isometric spaces. Refer to §3 of[1] for a complete statement in the infinite case. For the purposes of this introduction suffice it to say that subject to a mild dimension assumption an isomorphism of rotation groups (or even of proper subgroups containing the commutator subgroups) forces the following space conditions: equality of dimension, isomorphy of the coefficient fields, and semi-linear isometry (with respect to the field isomorphism cited above). Moreover, the form of the group isomorphism is usually directly induced by the semi-linear isometry (there are some interesting exceptions, for example, in the eight dimensional Cayley case).

The situation for rotation groups of binary quadratic spaces is quite different however. Clearly, if one of the groups is a rotation group of a binary space then any isomorphic group is also abelian and, hence, the group of a binary quadratic space (see 43: 12b of [2]). However, equality of dimensions is the only one of the three conditions necessary on the underlying spaces. In §2 we produce a series of examples: isomorphic rotation groups defined over non isomorphic fields (in fact fields of different characteristic) and isomorphic rotation groups defined over the same field, but representing anisotropic and isotropic quadratic spaces. In particular, the geometry of the underlying space is not determined by its rotation group. We then take a natural turn to consider the implications of an isomorphism between the rotation groups of isotropic (hyperbolic) and anisotropic planes defined over the same field. We provide some examples of such fields among global fields and we develop necessary and sufficient conditons for existence of isomorphisms in the global field setting. We conclude our investigation by developing a set of conditions necessary for a field to support an anisotropic plane whose rotation group is isomorphic to the rotation group of the hyperbolic plane over the same field. Our main result (which appears as Theorem 3.4) provides that such a field F (called norm 1 fields) satisfy the following conditions:

(1) F is infinite of characteristic 0 or 3;

(2) $F(\sqrt{-1})$ is a proper extension of F which is not algebraically closed;

This paper was completed in preparation for the author's visit to the Institute of Systems Science, Beijing, P.R.C., June 1985. The author wishes to express his appreciation and gratitude to his hosts at the Institute of Systems Science and Academia Sinica for their superb hospitality and gracious generosity.
Received September 23, 1985.

(3) F is not real closed;

(4) F admits at least 4 distinct square classes.

§0. Preliminaries: Notation and Terminology

We employ the notation and terminology of [2] specialized as follows: H denotes a hyperbolic plane and $O^+(H)$ denotes its rotation group, A denotes an anisotropic plane and $O^+(A)$ denotes its rotation group, P denotes an arbitrarp plane, not assumed a priori to be either anisotropic or hyperbolic, and $O^+(P)$ denotes its rotation group. If we wish to highlight the coefficient field F we use $O^+(H, F)$, $O^+(A, F)$, and $O^+(P, F)$. All our fields have characteristic 0 or $p \neq 2$ and all quadratic spaces are regular (non degenerate) and binary (two dimensional).

we use $\boldsymbol{Q}$ for the field of rational numbers, $\boldsymbol{F}_q$ for the finite field with q elements, and $F(t)$ for the field of rational functions in the transcendental t.

As is well known, $O^+(P, F)$ is isomorphic to a subgroup of the multiplicative group of a field ([3], p. 51) in fact $O^+(H, F)$ is isomorphic to F^*, the multiplicative group of F, and $O^+(A, F)$ is isomorphic to the norm 1 group of the quadratic extension $E = F(\sqrt{-dA})$ where dA is the discriminant of the anisotropic plane A. In the latter case we simplify and extend the notation as follows: we use d for dA and δ for $\sqrt{-d}$, we use σ for the non trivial F automorphism of $E = F(\delta)$-conjugation, N for the norm map from E to F and $E^{N=1}$ for the norm 1 group of E. A typical element x of E has a unique expression as $x = a + b\delta$ with a and b in F and $N(x) = x \cdot \sigma(x)$ ($x \cdot x^\sigma$ in exponential notation). Of course x is an element of norm 1 if and only if $x^\sigma = x^{-1}$; in particular the only elements of F that are of norm 1 are ± 1.

§ 1. Examples

1.1. The multiplicative groups of $\boldsymbol{Q}$ and $\boldsymbol{F}_3(t)$ are isomorphic——each is a direct product of a cyclic group of order 2 and a weak direct product of countable number of infinite cyclic groups. Thus $O^+(H, \boldsymbol{Q})$ is isomorphic to $O^+(H, \boldsymbol{F}_3(t))$ but the underlying fields have differing characteristic and, hence, are not isomorphic. The geometry is isotropic in both examples, however.

1.2. $O^+(H, \boldsymbol{F}_q)$ is cyclic of order $q - 1$ and $O^+(A, \boldsymbol{F}_q)$ is cyclic of order $q + 1$. Thus $O^+(A, \boldsymbol{F}_5)$ and $O^+(H, \boldsymbol{F}_7)$ are isomorphic cyclic groups of order 6. More generally, for any pair of twin primes p and $q = p + 2$ $O^+(A, \boldsymbol{F}_p)$ and $O^+(H, \boldsymbol{F}_q)$ are isomorphic cyclic groups of order $p + 1$.

In this example the coefficient fields are non isomorphic and the geometry is isotropic in one and anisotropic in the other.

Examples 1.1 and 1.2 naturally lead to the question of the existence of fields F with $O^+(H, F)$ isomorphic to $O^+(A, F)$. Of course this can be regarded as a field theoretic question (no reference to geometry). Namely, the existence of fields F which admit quadratic extensions E whose norm 1 group, $E^{N=1}$, is isomorphic to F^*. It is this question which occupies our attention in the remainder of this paper.

1.3. **Definition.** F is called a norm 1 field if F admits a quadratic extension E with

$E^{N=1}$ isomorphic to F^*.

§2. Global Fields

In this paragraph k will be a global field and K will be a finite galois (normal, separable) extension of k with $G = \mathrm{Gal}(K/k)$ as galois group. We use N for the G-norm and $K^{N=1}$ as norm 1 group in K. See [2] for basic definitions and results on global fields. The setting that is pertinent to this paper has K as a quadratic extension of k (and $K = E$, $k = F$, in the notation used elsewhere in the paper). We use $O(k)$ for the ring of k integers (in the sense of Dedekind), $I(k)$ the group of $O(k)$ fractional ideals (i.e. finitely generated $O(k)$ modules), and $P(k)$ the group of fractional principal ideals. Then $I(k) = I$ is a free $\boldsymbol{Z}$-module with countable rank, $P(k) = P$ is a submodule of I and I/P is a finite group. Since submodules of free modules over principal ideal domains are free P is a free $\boldsymbol{Z}$-module, and it has countable rank since I/P is finite. Let $U(k) = U$ be the group of Dirichlet units of k and let $C(k) = C$ be the (finite cyclic) group consisting of the roots of unity in k.

2.1. **Example.** The structure of k^* is readily determined——it is a direct product of $C(k)$ and a free $\boldsymbol{Z}$-module of countable rank. This follows from the Dirichlet Unit Theorem and the split exact sequence

$$1 \longrightarrow U \longrightarrow k^* \longrightarrow P \longrightarrow 1.$$

2.2. **Proposition.** k^* is isomorphic to $K^{N=1}$ if and only if $C(k) = C\ (K)^{N=1}$.

Proof. $K^{N=1}$ is a direct sum of $C_K^{N=1}$ and a free $\boldsymbol{Z}$-module. The proposition follows if the free part has countably infinite rank. That this is the case follows because there are an infinite number of k primes $\mathfrak{p}$ that split completely in K, namely let $\mathfrak{p}$ be one such prime and let P be one of its factors in K. Then P^m is principal for some power m, so $P^m = (\beta_{\mathfrak{p}})$, $\beta \in K$. Then set $\alpha_{\mathfrak{p}} = \beta_{\mathfrak{p}}^{1-\sigma}$ for σ in G, $\sigma \neq 1$. Observe that these $\alpha_{\mathfrak{p}}$ generate a free $\boldsymbol{Z}$-module of infinite rank in $K^{N=1}$. Q. E. D.

2.3. **Example.** Let $k = \boldsymbol{Q}$. If $K = k(i)$ or $k(\omega)$ where ω is a primitive cube root of unity. Then $C_K^{N=1}$ is cyclic of order 4 if $K = k(i)$ and cyclic of order 6 if $K = k(\omega)$. Since $C_k = \{\pm 1\}$, C_k and $C_K^{N=1}$ are not equal, so k^* is not isomorphic to $K^{N=1}$ by 2.2. But if K is any other quadratic extension then $C_K^{N=1} = C_k$. In particular, $\boldsymbol{Q}$ is a norm 1 field and $O^+(H, \boldsymbol{Q}) \approx O^+(A, \boldsymbol{Q})$ for appropriate anistropic planes over $\boldsymbol{Q}$-namely, A is a quadratic extension (but not $\boldsymbol{Q}(i)$ or $\boldsymbol{Q}(\omega)$) and A is given the "norm" form.

2.4. **Example.** It is not difficult to verify that $\boldsymbol{F}_3(t)$ is a norm 1 field. In §4 we show that this example is the only one among the function fields $\boldsymbol{F}_q(t)$.

§3. Norm 1 Fields

In this paragraph we assume that F is a norm 1 field and we deduce a series of necessary conditions on F. Refer to §1 for the notation. We use τ for the isomorphism from F^* to $E^{N=1}$.

3.1 F is infinite and -1 is a non-square in F^*.

Proof. If F were $\boldsymbol{F}_q$ then F^* has $q-1$ elements and $E^{N=1}$ has $q+1$ elements, so F^* and $E^{N=1}$ can not be isomorphic if F is finite.

Set $\tau(x) = \alpha + \beta\delta$ for a typical x in F^*. Then $\tau(x^{-1}) = \alpha - \beta\delta$ and $\tau(-x) = -\alpha - \beta\delta$ since $\tau(x)$ has norm 1 and $\tau(-1) = -1$. Assume $-1 = x^2$ or, equivalently, that $1 = -x^2 = (-x)(x)$. Then $1 = \tau(1) = \tau(-x) \cdot \tau(x)$ so $\tau(-x) = \tau(x)^{-1}$, and $\alpha = 0$. Thus $\tau(x) = \beta\delta$ and $-1 = \tau(-1) = \tau(x^2) = (\tau(x))^2 = \beta^2\delta^2 = -\beta^2 d$ or, equivalently, $1 = \beta^2 d$. Thus d is also a square if -1 is a square-but this forces $-d$ to also be a square and this is a contradiction. O. E. D.

By 3.1 a norm 1 field F admits the quadratic extension $F(\sqrt{-1})$ and F has at least 2 distinct square classes (e. g. the classes containing 1 and -1). Use $[\alpha]$ to denote the square class of α in F. Thus $[-1] \neq [1]$ and $[-d] \neq [1]$. If $[-d] = [-1]$ then $[d] = [1]$ i.e. d is a square. If this is so, then $E = F(\sqrt{-1})$. But this is absurd since $F(\sqrt{-1})$ has 4 distinct elements of norm 1, each a solution to the equation $x^4 = 1$ (i. e. $\{\pm 1, \pm\sqrt{-1}\}$) and F^* has only 2 such solutions. Conversely, if $[d] = [1]$ then $[-d] = [-1]$ and $E = F(\sqrt{-1})$. Of course $[\alpha] = [1]$ if and only if $x^2 - \alpha$ is reducible over $F[x]$. Thus we have shown the following

3.2. F has at least 4 square classes namely $[1]$, $[-1]$, $[d]$, and $[-d]$.

In fact we have essentially established the following

3.3. $F(\sqrt{-1})$ is not algebraically closed and F is not real closed.

Proof. $x^2 \pm d$ remain irreducible in $F(\sqrt{-1})[x]$ lest we have $F[\sqrt{-1}] = E$ and a contradiction as before. The second part follows from the first and [4 Theorem 1.8 or Theorem 2.5]. Q. E. D.

Now let us assume that F has characteristic $p > 2$. Hence F contains $\boldsymbol{F}_p$ as prime field and F^* contains $\boldsymbol{F}_p^*$-but $\boldsymbol{F}_p^*$ is characterized as the splitting field of $x^{p-1} - 1 = 0$. If $E^{N=1}$ is isomorphic to F^* then $E^{N=1}$ must also contain $\boldsymbol{F}_p^*$. Since $\boldsymbol{F}_p$ is in the fixed field of σ this forces $p = 3$. Combining these remarks with 3.1, 3.2, and 3.3 we have

3.4. **Theorem.** *If F is a norm 1 field with $E = F(\sqrt{-d})$ and $E^{N=1}$ isomorphic to F^* then*

(1) *F is infinite of characteristic 0 or 3;*

(2) *$F(\sqrt{-1})$ is a proper extension of F which is not algebraically closed;*

(3) *F is not real closed;*

(4) *F admits at least 4 distinct square classes, namely $[1]$,$[-1]$, $[d]$, and $[-d]$.*

References

[1] Hahn, A., On the isomorphisms of the projective orthogonal groups and their congruence subgroups, *J. Reine Angew. Math.*, 273(1975), 1—22.

[2] O'Meara, O.T., Introduction to Quadratic forms, Springer-Verlag, Berlin-Göttingen-Heidleberg, 1963.

[3] Dieudonné, J., La Géométrie des Groupes Classiques, Seconde Edition, Spring-Verlag, Berlin-Göttingen-Heidleberg, 1963.

[4] Lam, T. Y., The Algebraic Theory of Quadratic Forms, Benjamin, Reading, 1973.

二元二次空间旋转群的同构

爱德华·康纳斯
(麻省大学数学和统计系)

摘　　要

定义在Q和$F_3(t)$上的双曲平面的旋转群是同构的. 除此之外，还有许多对不同构的域F_1和F_2具有同构的群$O^+(H,F_1)$和$O^+(A,F_2)$的例子,这里H是F_1上的一个双曲平面,A是F_2上的一个非迷向平面，O^+表示相应的旋转群. 例如,对于每对孪生素数都存在这样一对域. 这些例子说明二维空间的旋转群与高维空间的旋转群之间的明确差异，并建议研究具同构的群$O^+(H,F)$和$O^+(A,F)$的域F. 在全局域中举出了这种域的例子,也提供了对于全局域的一个充要条件. 一般说来,如$O^+(H,F)$和$O^+(A,F)$同构,则F的特征为 0 或 3 的无限域,$F(\sqrt{-1})$是F的真二次扩域但不是代数闭的. 而且F至少有 4 个相异平方类.