# Introduction to quadratic forms

Bill Casselman
University of British Columbia
cass@math.ubc.ca

This essay is intended to be a brief and largely self-contained introduction to the theory of quadratic forms over arbitrary fields.

I begin with a basic discussion of bilinear forms and quadratic forms. The distinction between the two is particularly important, since I do not generally assume the characteristic to be odd (by which I mean either zero or finite and odd). I include here versions of theorems about quadratic forms that are independent of the particular coefficient field, except for distinctions based on characteristic. Eventually, I shall be interested only in quadratic forms over finite and local fields, which is why I can get by with such a brief discussion of the general theory here. I'll discuss these topics elsewhere, but thought that some general background would be useful.

The theory in odd characteristic is well known, but the theory in characteristic 2 is still considered somewhat arcane. [Dickson:1901] classified quadratic forms over finite fields, but the original source of most of the general theory in characteristic 2 seems to be [Arf:1941]. There have been many developments since, covered well in the recent book [Elman et al.:2008] (although I have to say, their reference to Cahit Arf seems rather slighting). I have followed it closely for fields of even characteristic. [Lorenz-Roquette:2009] is a very readable account of Arf's work (including remarks on a rather subtle error in Arf's treatment). For the Arf invariant, I have also used [Dye:1978] and [Dieudonné:1955].

**Contents**

1. Bilinear and quadratic forms
2. Non-degenerate quadratic forms
3. Binary forms
4. Quaternion algebras
5. Symplectic groups
6. The orthogonal group
7. *Appendix.* Arithmetic of Galois extensions
8. References

Throughout, $F$ will be an arbitrary field, except for occasional distinctions of characteristic, and $V$ a vector space over $F$, usually of dimension $d$.

## 1. Bilinear and quadratic forms

A **bilinear form** on $V$ is a function $\nabla$ on $V \times V$ separately linear in each factor. It is **symmetric** if $\nabla(x, y) = \nabla(y, x)$. Given a coordinate system, a symmetric bilinear form has an expression

$$\nabla(x, y) = \sum\nolimits_{i,j} a_{i,j} x_i y_j$$

with $a_{i,j} = a_{j,i}$. If $M_\nabla$ is the matrix $(a_{i,j})$ then

$$\nabla(x, y) = {}^t x \cdot M_\nabla \cdot y\,.$$

If the relevant basis is $(e_i)$ then the matrix entry $a_{i,j} = B(e_i, e_j)$.

A bilinear form $\nabla$ on a vector space $V$ determines a map I'll also write as $\nabla$ from $V$ to its dual $\widehat{V}$:

$$v \longmapsto \nabla_v\colon\ u \longmapsto \nabla(v, u)\,.$$

With respect to dual bases the matrix $M_\nabla$ is the matrix of that linear transformation. The bilinear form is said to be **non-degenerate** if this transformation—or, equivalently, its matrix—is invertible.

Any map from $f\colon V \to \widehat{V}$ determines a transpose map $\widehat{f}\colon \widehat{\widehat{V}} \to \widehat{V}$. Upon identifying $V$ with $\widehat{\widehat{V}}$, the form $\nabla$ is symmetric if and only if the map is equal to its own transpose.

Suppose we choose a new basis. Let $X$ be the matrix whose columns are the coordinates of the new basis in terms of the old. The matrix of the bilinear form becomes

$$ {}^tX \cdot M \cdot X \,.$$

Since $\det(AB) = \det(A)\,\det(B)$, the determinant of $M$ changes by a factor in $(F^\times)^2$. Its image in $F^\times/(F^\times)^2$ is therefore an invariant of the bilinear form, usually called its **discriminant**. It is a weak invariant—for example, the forms

$$\sum\nolimits_1^4 x_i y_i,\ -\sum\nolimits_1^4 x_i y_i, \sum\nolimits_1^2 x_i y_i - \sum\nolimits_3^4 x_i y_i$$

of dimension $4$ all have the same discriminant $1$.

A **quadratic form** on $V$ is a function $Q$ on $V$ satisfying the two conditions (a) $Q(cx) = c^2 Q(x)$ for $c$ in $F$ and (b) the function $\nabla_Q(x,y) = Q(x+y) - Q(x) - Q(y)$ is bilinear. If a coordinate system is chosen, it is defined by an expression

$$Q(x) = \sum\nolimits_{i\le j} a_{i,j} x_i x_j \,.$$

A quadratic form is not necessarily associated to a matrix. There is, however, a close relationship between bilinear forms and quadratic forms, one that can lead to some confusion. First of all, every bilinear form $\nabla$ gives rise to a quadratic form

$$Q_\nabla(x) = \nabla(x,x)\,.$$

If the matrix of $\nabla$ is $(a_{i,j})$ the formula for $Q_\nabla$ is

$$Q_\nabla(x) = \sum_i a_{i,i} x_i^2 + \sum_{i<j} 2a_{i,j} x_i x_j \,.$$

As you can see, the quadratic forms that arise in this way are special—the coefficients of the cross terms are always even (and vanish in characteristic 2).

On the other hand, every quadratic form $Q$ determines the bilinear form $\nabla_Q$. If $Q(x) = \sum_{i\le j} a_{i,j} x_i x_j$ its formula is

$$\begin{aligned}
\nabla_Q(x,y) &= \sum_{i\le j} a_{i,j}\big((x_i+y_i)(x_j+y_j) - x_i x_j - y_i y_j\big) \\
&= \sum_{i\le j} a_{i,j}(x_i y_j + x_j y_i) \\
&= \sum_i 2a_{i,i} x_i y_i + \sum_{i<j} a_{i,j} x_i y_j + \sum_{i>j} a_{j,i} x_i y_j \,.
\end{aligned}$$

Again, only certain bilinear forms arise in this way from quadratic forms.

If we start with a bilinear form $\nabla$, construct $Q = Q_\nabla$, then go on to construct $\nabla_Q$, we get $2\nabla$. In a diagram, the composite map

$$\text{symmetric bilinear forms} \overset{\nabla\mapsto Q_\nabla}{\longrightarrow} \text{quadratic forms} \overset{Q\mapsto\nabla_Q}{\longrightarrow} \text{symmetric bilinear forms}$$

amounts to multiplication by 2. Hence if 2 is invertible, the form $Q$ is always defined in terms of a bilinear form, namely $(1/2)\nabla_Q(x,y)$, since

$$\nabla_Q(x,x) = Q(2x) - 2Q(x) = 2Q(x), \quad Q(x) = (1/2)\nabla_Q(x,x)\,.$$

All these distinctions are unimportant if the characteristic of $F$ is odd, but if it is 2 they are crucial.

**Example.** In characteristic two the bilinear forms associated to the quadratic forms

$$x^2 + xy + ay^2, \quad xy$$

are the same, but these two forms are equivalent if and only if $a$ lies in the image of the Artin-Schreier map $x \mapsto x^2 + x$.

---

The bilinear form associated to a quadratic form is what is called in calculus its gradient, since

$$Q(x+y) = Q(x) + \nabla_Q(x,y) + Q(y)\,.$$

Thus if $F = \mathbb{R}$

$$\lim_{t\to 0}\left[\frac{Q(x+ty)-Q(x)}{t}\right] = \nabla_Q(x,y)\,.$$

Bilinear forms and quadratic forms may be defined with elements of any ring, most notably $\mathbb{Z}$, as coefficients. But in the literature there is some confusion about exactly what qualifies as an integral quadratic form. During much if not all of the nineteenth century, starting with Gauss and running through Minkowski, integral quadratic forms were taken to be only the ones defined in terms of a bilinear form, hence with a factor of 2 in all coefficients of cross terms $x_ix_j$. This is often the case even in modern times, for example in the book [Cassells:1978]. There is some convenience in being able to associate to a quadratic form a matrix, but even so it is not clear to me why this tradition has persisted in number theory. For example, excluding the integral quadratic form $x^2 + xy + y^2$, which is the norm form on the ring of algebraic integers in $\mathbb{Q}(\sqrt{-3})$, seems rather eccentric. Nowadays there are many applications in which it is important to work with symmetric bilinear forms, for example in considering the intersection of cycles in the middle dimension on a manifold. Integral bilinear forms share much of the life of integral quadratic forms, but have a career of their own.

In any case, this essay will be about quadratic forms—I shall not in general assume the cross-term coefficients to be even, although doing so will play a role elsewhere in the process of interpreting Minkowski in modern terms.

In odd characteristic the bilinear form $\nabla_Q/2$ makes sense, and the discriminant of the quadratic form is defined to be the discriminant of this form. In characteristic 2 there is no useful definition of the discriminant of a quadratic form.

### 2. Non-degenerate quadratic forms

The **radical** of a bilinear form $\nabla$ is the subspace

$$\mathfrak{rad}_\nabla = \left\{ v \in V \,\middle|\, \nabla(v,V) = 0 \right\},$$

which is also the kernel of the map from $V$ to $\widehat{V}$. The radical of the quadratic form $Q$ is

$$\mathfrak{rad}_Q = \left\{ v \in \mathfrak{rad}_{\nabla_Q} \,\middle|\, Q(v) = 0 \right\}.$$

Thus $\mathfrak{rad}_Q \subseteq \mathfrak{rad}_{\nabla_Q}$. The following is immediate:

**2.1. Proposition.** *If the characteristic of $F$ is odd, then these two radicals are the same.*

This is certainly not true in characteristic two. For example, if $Q = x^2$ on $F$ itself then the radical of $\nabla_Q$ is all of $F$ but $\mathfrak{rad}_Q = 0$.

**Example.** Say

$$Q(x) = \sum\nolimits_1^d c_i x_i^2 \quad (c_i \neq 0)$$

in dimension $d$. In odd characteristic both radicals are trivial. In even characteristic, $\mathfrak{rad}_\nabla$ is all of $V$, but $\mathfrak{rad}_Q$ depends on the exact values of the $c_i$. If all $c_i$ are squares—for example if $F$ is perfect—then $\mathfrak{rad}_Q$ has codimension one, since the form is then equivalent to

$$\sum x_i^2 = \Big(\sum x_i\Big)^2 .$$

This example is typical in one sense. The following is immediate:

**2.2. Lemma.** *In characteristic* 2 *the space* $V$ *is equal to* $\mathfrak{rad}\nabla_Q$ *if and only if*

$$Q(x) = \Big(\sum x_i\Big)^2$$

*for some choice of coordinates.*

It may happen that $\mathfrak{rad}_{\nabla_Q} = V$ but $\mathfrak{rad}_Q = 0$, even if the dimension of $V$ is greater than one. For example, if $a \neq 0$ is not a square, then the radical of $x^2 + ay^2$ is 0. But this is not a stable situation in the sense that after base field extension $\mathfrak{rad}_Q$ becomes a line. There is in fact some point to singling out those forms which are stable in that sense. This should motivate somewhat the following definitions.

Suppose $(V, Q)$ to be a quadratic space, with $\nabla = \nabla_Q$. Following [Elman et al.:2008] loosely, I say it is **strictly non-degenerate** if $\mathfrak{rad}_\nabla = 0$, **weakly non-degenerate** if $\mathfrak{rad}_Q = 0$, and and simply **non-degenerate** if $\mathfrak{rad}_Q = 0$ and $\mathfrak{rad}_\nabla$ has dimension one.

The quadratic form $Q$ determines a quadratic form $\overline{Q}$ on $V/\mathfrak{rad}_Q$. Ther quotient is weakly non-degenerate. If $U$ is any complement to $\mathfrak{rad}_Q$ the $Q|U$ is isomorphic to this quotient form, and $V$ is the orthogonal sum of $U$ and $\mathfrak{rad}_Q$, on which $Q$ vanishes.

If $u$, $v$ lie in $V$ and $x$, $y$ in $\mathfrak{rad}_\nabla$ then $\nabla(u + x, v + y) = \nabla(u, v)$. Therefore one can define a quotient bilinear form $\overline{\nabla}$ on $V/\mathfrak{rad}_\nabla$. It will be non-degenerate. But what happens with respect to $Q$ is not so simple. There is in particular no canonical quadratic form on this quotient, as we'll see in a moment. That is to say, the isomorphism class of the restriction of $Q$ to a complement of $\mathfrak{rad}_\nabla$ is not uniquely determined. In fact, there is a large literature devoted to the notion of equivalence suggested by this problem. When looking at finite and local fields, this problem will turn out not to be significant.

**Example.** Assume characteristic 2. Suppose $a \neq 0$, and consider the quadratic forms

$$xy + z^2, \quad x^2 + xy + ay^2 + z^2 .$$

*These two forms are always equivalent.* This is easily seen, since we can rewrite the second form as

$$(x + z)^2 + y(x + ay) .$$

However, as long as the Artin-Schreier map $\mathfrak{P}\colon\ x \longmapsto x^2 + x$ is not surjective—for example, if $F$ is finite—we can find $a$ for which the two forms

$$xy, \quad x^2 + xy + ax^2$$

are not equivalent.

---

In any case, what the remark about quotients means is that every quadratic space can be represented as the direct orthogonal sum of two pieces, one of which is completely trivial, and the other both weakly non-degenerate and uniquely determined up to isomorphism. For this reason, it is not a serious restriction to consider only weakly non-degenerate quadratic spaces. But I shall be interested only in spaces that are are in fact non-degenerate, and from now on I'll generally assume this to be the case.

In some situations this is not such a strong assumption.

**2.3. Proposition.** *Assume $F$ to be a perfect field of characteristic 2. A quadratic space is non-degenerate if and only if it is weakly non-degenerate.*

I recall that a perfect field of characteristic 2 is one for which $x \mapsto x^2$ is an automorphism. In particular, all finite fields $\mathbb{F}_{2^n}$ are perfect.

*Proof.* Only the implication one way need be argued. Suppose $(V, Q)$ to be a weakly non-degenerate quadratic space over $F$. If $u$, $v$ are linearly independent in $\mathfrak{rad}_\nabla$, then

$$Q(au + bv) = a^2 Q(u) + b^2 Q(v)\,.$$

By assumption $Q(u)$, $Q(v) \neq 0$ and $F$ is perfect, so we may solve $Q(au + bv) = 0$ by setting $b = 1$, $a = \sqrt{Q(v)/Q(u)}$. Since $au + bv$ is in $\mathfrak{rad}_\nabla$, this contradicts the definition of weak non-degeneracy. ∎

If $U$ is a subspace of $V$ then there exists a canonical map $\nabla \,|\, U$ from $V$ to $\widehat{U}$, taking $v$ to the restriction $\nabla_v \,|\, U$. Its kernel is $U^\perp$, the subspace orthogonal to $U$. So the sequence

$$0 \longrightarrow U^\perp \longrightarrow V \xrightarrow{\nabla|U} \widehat{U}$$

is certainly exact. The right hand map is not always surjective, but it is under a mild hypothesis:

**2.4. Proposition.** *If $U$ is a vector subspace of the quadratic space $(V, Q)$ such that $U \cap \mathfrak{rad}_{\nabla_Q} = 0$, then*

$$0 \longrightarrow U^\perp \longrightarrow V \xrightarrow{\nabla|U} \widehat{U} \longrightarrow 0$$

*is exact.*

*Proof.* We have in general the exact sequence

$$0 \longrightarrow U \cap \mathfrak{rad}_\nabla \longrightarrow U \xrightarrow{\nabla} \widehat{V}$$

whose transpose diagram, since $\nabla_Q$ is symmetric, is

$$V \xrightarrow{\nabla|U} \widehat{U} \longrightarrow \widehat{(U \cap \mathfrak{rad}_\nabla)} \longrightarrow 0\,.$$

The claim follows, since $U \cap \mathfrak{rad}_\nabla = 0$. ∎

**2.5. Proposition.** *If $(V, Q)$ is a quadratic space over $F$ and $U$ a subspace of $V$ such that the restriction of $Q$ to $U$ is strictly non-degenerate, then $V = U \oplus U^\perp$.*

In these circumstances, I call $U$ a strictly non-degenerate subspace of $(V, Q)$.

*Proof.* We want to define a projection $P$ from $V$ onto $U$ such that $v - P(v)$ lies in $U^\perp$. Let $(e_i)$ be basis of $U$, let $M_\nabla = \nabla(e_i, e_j)$ be the matrix of $\nabla|U$. By assumption it is non-singular. Given $v$, we are looking for $u = \sum c_i e_i$ such that

$$\nabla\Big(v - \sum c_i e_i, e_j\Big) = 0, \quad \sum c_i \nabla(e_i, e_j) = \nabla(v, e_j)$$

for all $j$. But this is a system of equations for the unknowns $c_i$ with invertible coefficient matrix. ∎

A vector $v$ is called **anisotropic** if $Q(v) \neq 0$ and **isotropic** if $v \neq 0$ but $Q(v) = 0$. A subspace of $V$ is called isotropic if it contains an isotropic vector, and **totally isotropic** if $Q$ vanishes identically on it. Then $\nabla_Q$ also does.

One non-degenerate quadratic space that exists for all fields is the hyperbolic plane $(F^2, H)$ for which $H(x, y) = xy$. In $H$ the isotropic vectors are those on the $x$- and $y$-axes.

**2.6. Proposition.** *Suppose $(V, Q)$ to be a non-degenerate quadratic space, $U$ to be a totally isotropic subspace of dimension $d$ with basis $(u_i)$. There exists a totally isotropic complement $W$ of the same dimension with basis $(w_i)$ such that*

$$\nabla(u_i, w_j) = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{otherwise.} \end{cases}$$

*Proof.* I shall construct the $w_k$ by induction such that

$$\begin{aligned} \nabla(w_k, u_k) &= 1 \\ \nabla(w_k, u_i) &= 0 \quad (i < k) \\ \nabla(w_k, w_i) &= 0 \quad (i < k)\,. \end{aligned}$$

For $k = 1$, we can apply  to the space $U$, and for $k > 1$ to the space spanned by $U$ and the $w_i$ for $i < k$. The hypothesis of  is satisfied since $\mathfrak{rad}_\nabla$ does not contain any isotropic vectors. ∎

**2.7. Corollary.** *Every non-degenerate quadratic space containing a totally isotropic subspace of dimension $n$ is isomorphic to $nH$ plus an orthogonal complement.*

**2.8. Corollary.** *Any non-degenerate quadratic space $(V, Q)$ may be expressed as the orthogonal sum of copies of $H$ and an anisotropic subspace.*

Every non-degenerate quadratic space decomposes into a direct sum of smaller spaces, but exactly how this happens depends on the field's characteristic.

**2.9. Proposition.** *In characteristic $\neq 2$, every non-degenerate quadratic space is an orthogonal sum of non-degenerate lines.*

That is to say, in some coordinate system

$$Q(x) = \sum c_i x_i^2\,.$$

*Proof.* By induction. ∎

**2.10. Proposition.** *Suppose the characteristic to be 2, and $V$ non-degenerate. If $V$ has even dimension, it is an orthogonal sum of strictly non-degenerate two-dimensional quadratic spaces. If the dimension of is odd, it is the orthogonal sum of a line and a subspace $U$ which is strictly non-degenerate.*

*Proof.* Also by induction. It suffices to suppose the dimension of $V$ to be even. It is then non-degenerate. Suppose $Q(u) \neq 0$. Since $Q$ is non-degenerate, there exists $v$ such that $\nabla_Q(u, v) = 1$. But then the space spanned by $u$ and $v$ is non-degenerate, and it possesses a non-degenerate orthogonal complement, to which we can apply induction. ∎

**LOW DIMENSIONS.** In the next few sections I'll explain the classification of strictly non-degenerate forms in small dimensions. Here is a rough outline:

(a) In dimension one, two forms $cx^2$ are isomorphic if and only if $c \neq 0$ is a square in $F^\times$.
(b) In dimension two, there is exactly one form, the hyperbolic plane, that possesses isotropic vectors. Any other is $cN_{K/F}$ with $K/F$ a quadratic extension field.
(c) In three dimensions (odd characteristic) the forms with an isotropic vector are of the form $H \oplus cx^2$, and the rest of the form $N_{K/F} \oplus cx^2$. It's not clear to me that much more can be said without having precise information about $F$.
(d) In four dimensions, there are forms $H \oplus H$, $H \oplus cN_{K/F}$, $cN_{B/F}$ for $B$ a quaternion division algebra.

In the next section I'll explain the classification of non-degenerate quadratic spaces of dimension two. This will enable us to define for non-degenerate forms in characteristic 2 an analogue of the discriminant called its **Arf invariant**.

### 3. Binary forms

One possible non-degenerate quadratic form of dimension two is the hyperbolic plane $H$, and any non-degenerate plane with an isotropic vector is isomorphic to it. To classify all binary forms, we have only to classify the anisotropic ones.

There is a simple way to get one. Let $K$ be a separable quadratic extension of $F$, and let $N_{K/F}(x) = x\overline{x}$ be the norm map from $K$ to $F$. It is a quadratic form on $K$ considered as a vector space of dimension two over $F$. Related forms are the $aN_{K/F}$, with $a$ in $F^\times$, and $aN_{K/F}$ and $bN_{K/F}$ are equivalent if and only if $a/b$ lies in the image of $N_{K/F}K^\times$ in $F^\times$.

**3.1. Proposition.** *Every non-degenerate quadratic space of dimension 2 is isomorphic either to $H$ or to some $aN_{K/F}$.*

*Proof.* Any quadratic form in dimension two has a formula $Q(x,y) = Ax^2 + Bxy + Cy^2$. If both $A$ and $C$ are 0, this is the hyperbolic plane. Otherwise, swapping $x$ and $y$ if necessary we may assume $A \neq 0$, and now the form factors as $A(x - \alpha y)(x - \beta y)$ over an algebraic closure of $F$. If $\alpha$ and $\beta$ are in $F$, we may change variables to get this of the form $Ax(x-\gamma)$. If $\gamma = 0$, the form will be degenerate. Otherwise, we can change variables again to make it $Axy$, so once more we have the hyperbolic plane.

We may now assume $\alpha \neq \beta$ to be conjugates in a quadratic extension $K/F$, and this is $AN_{K/F}$.

This adds content to .

We can now discuss the Arf invariant. Assume $F$ to be of characteristic 2. Any separable quadratic field $K/F$ will be generated by the root of an irreducible Artin-Schreier polynomial $x^2 + x + \gamma$. Even if this polynomial is reducible, we are looking at a separable algebra $F[x]/(x^2+x+\gamma)$. In all cases, the algebra will be completely characterized by $\gamma$ modulo the image of the Artin-Schreier map

$$\mathfrak{P}\colon\ F \longrightarrow F, \quad x \longmapsto x^2 + x\,,$$

which is linear. Its kernel is the copy of $\mathbb{F}_2$ in $F$.

In other words, separable quadratic extensions are parametrized by $F/\mathfrak{P}(F)$, just as in odd characteristics field extensions are parametrized by $F^\times/(F^\times)^2$. This includes the case $\gamma = 0$, in which case we recover the quadratic algebra $F \times F$. The norm form $N_{K/F}$ is $x^2 + xy + \gamma y^2$, which is equivalent to $xy$ if $\gamma = 0$.

Any nondegenerate binary form in characteristic 2 will be equivalent to some $ax^2 + xy + by^2$, which is also $a(x^2 + x(y/a) + (ab)(y/a)^2)$, equivalent to $aN_{K/F}$ if $K$ is the quadratic extension parametrized by $ab$. The constant $ab$ modulo $\mathfrak{F}$ is therefore an invariant of the form, called its Arf invariant, which distinguishes the quadratic field associated to the form. As I say, it is an analogue of the discriminant.

If $Q$ is the orthogonal sum $\oplus\, Q_i$ of nondegenerate quadratic forms, the Arf invariant determined by that decomposition is the sum of the separate Arf invariants.

**3.2. Proposition.** *Any two binary decompositions of a nondegenerate form in an even number of variables in characteristic two determine the same Arf invariant.*

So the Arf invariant is really an invariant of the form.

*Proof.* The following argument is due to [Dye:1968]. He first formulates the recipe for the Arf sum in this way. Choose a symplectic basis $(e_i)$ for $\nabla_Q$, then set the invariant to be

$$\sum Q(e_i)Q(e_{i+n})\,.$$

The point is to show it does not depend on the choice of basis $e_i$. But any two bases are transformed one to the other by a product of transvections, so it suffices to show that changing the basis by a single transvection doesn't affect Arf's sum. The computation is straightforward.

Examined closely, this recalls that the determinant $\det(AB)$ is the product $\det(A)\ \det(B)$, which can be done by representing $A$ or $B$ as a product of shears and a diagonal matrix.

[Dieudonné:1955] gives another proof, characterizing the invariant in terms of the Clifford algebra.

**3.3. Corollary.** *Over a perfect field of characteristic two, every nondegenerate quadratic space is isomorphic to $nH$ or to some $(n-1)H \oplus N_{K/F}$ for a unique separable extension $K/F$.*

*Proof.* Since $F$ is perfect, any anisotropic form $ax^2 + xy + by^2$ can be written

$$\alpha^2 x^2 + (\alpha x)(y/\alpha) + (\alpha^2 b)(y/\alpha)^2$$

and is equivalent to

$$x^2 + xy + \alpha^2 b y^2$$

which is some $N_{K/F}$. Thus the sum of any two nondegenerate forms is isotropic. ∎

**3.4. Corollary.** *If $Q$ is a non-degenerate quadratic form of dimension $n$ then $Q \oplus -Q$ is isomorphic to $nH$.*

*Proof.* In odd characteristic, this is an immediate consequence of , since $x^2 - y^2$ is equivalent to $H$. In even characteristic, this follows from the case of $Q = N = N_{K/F}$, becuse of .

This case can be dealt with explicitly. Suppose $K$ is generated by a root of the Artin-Schreier polynomial $x^2 + x + \gamma$. The sum $N \oplus N$ is then

$$x_1^2 + x_1 y_1 + \gamma y_1^2 + x_2^2 + x_2 y_2 + \gamma y_2^2 \,.$$

Let the $(e_i, f_i)$ be corresponding bases. Then a basis giving rise to $H \oplus H$ is

$$\begin{aligned} &e_1 + e_2 \\ &f_1 + \gamma(e_1 + e_2) \\ &f_1 + f_2 \\ &e_2 + (f_1 + f_2)\,. \end{aligned}$$

∎

## 4. Quaternion algebras

A quaternion algebra is an algebra $B$ whose center is $F$ such that $K \otimes B$ is isomorphic to $M_2(K)$ for some algebraic extension $K$.

Of course $M_2(F)$ is one of these. Are there others? There is one simple way to obtain them, if they exist. Suppose $E/F$ to be a separable quadratic extension. Choose $\alpha$ in $F^\times$, and let $B$ be the algebra over $E$ with basis $1, \sigma$ and relations

$$x\sigma = \sigma\overline{x}, \quad \sigma^2 = \alpha\,.$$

The field $E$ acts on the right on this, so the identification with $E^2$ is the map

$$(x, y) \longmapsto x + \sigma y\,.$$

Acting by multiplication on the left, $B$ commutes with $E$. This gives us an embedding of $B$ into $M_2(E)$. Explicitly, $x + \sigma y$ takes

$$\begin{aligned} 1 &\longmapsto x + \sigma y \\ \sigma &\longmapsto x + \sigma y \sigma \\ &= x\sigma + \sigma^2 \overline{y} \\ &= \sigma\overline{x} + \alpha\overline{y}\,. \end{aligned}$$

In other words, it corresponds to the matrix

$$\mu(x + \sigma y) = \begin{bmatrix} x & \alpha\overline{y} \\ y & \overline{x} \end{bmatrix}\,.$$

The determinant of $\mu(x+\sigma y)$ is

$$x\overline{x} - \alpha y\overline{y}\,.$$

This lies in $F$, and defines the norm map $N_{H/F}$ from $H$ to $F$. Considering $E$ as a vector space over $E$, this gives us a non-degenerate quadratic form of dimension $4$.

The norm map can be expressed as

$$N(x+\sigma y) = (x+\sigma y)(\overline{x} - \overline{y}\sigma) = (x+\sigma y)(\overline{x+\sigma y})\,.$$

I define the conjugate of $x+\sigma y$ to be $\overline{x}+\overline{y}\sigma$. It is an involutory anti-automorphism.

If $\alpha$ lies in $NE^\times$, then $B$ is isomorphic to $M_2(F)$. If it does not, then $N(z) \neq 0$ unless $z=0$, and $z$ has as inverse $\overline{z}/N(z)$. In this case, $B$ is a division algebra.

Over a local field $F$, distinct quadratic extensions $E/F$ give rise to the same quaternion algebra, which is in fact the unique division algebra of dimension $4$ over $F$. This will be proved elsewhere by the classification of quadratic forms over local fields, using Fresnel integrals. We shall also describe in that case the image of the norm in $F^\times$.

In odd characteristic, the quadratic forms derived from quaternion algebras are precisely those of dimension $4$ with trivial discriminant. In characteristic $2$, they are those with trivial Arf invariant.

### 5. Symplectic groups

In odd characteristic, the linear group preserving a non-degenerate bilinear form is the same as that preserving the associated quadratic form, but in even characteristic it is the same as a symplectic group.

Let $V$ be a vector space of dimension $2n$ over the arbitrary field $F$, Assume given a non-degenerate alternating form. In a suitable coordinate system, it becomes

$$\langle x, y\rangle = \sum\nolimits_1^n (x_i y_{i+n} - x_{i+n} y_i) = {}^t x \cdot \Omega \cdot y$$

with matrix

$$\Omega = \begin{bmatrix} 0 & I \\ -I & 0 \end{bmatrix}\,.$$

The symplectic group $\mathrm{Sp}_\Omega$ is that of all linear transformations of $V$ preserving this form.

If $u$ is any vector in $V$, the linear transformation

$$\tau_u\colon\ v \longmapsto v + \langle u, v\rangle u$$

is a symplectic transformation, called a **symplectic transvection**.

**5.1. Theorem.** *The symplectic group is generated by symplectic transvections.*

*Proof.* I follow loosely the proof of Theorem 3.25 in §III.5 of [Artin:1957].

The basic tools will be these two analogues of results proved earlier for quadratic forms. Proofs are essentially the same.

**5.2. Lemma.** *If $U$ is a vector subspace on which $\Omega$ is non-degenerate, then $V = U \oplus U^\perp$.*

**5.3. Lemma.** *If $U$ is a totally isotropic subspace, there exists a subspace $W$ of dimension equal to that of $U$ and in the complement of $U$ such that $\Omega\,|\,U \oplus W$ is non-degenerate .*

Now for the proof of the Theorem. Let $G$ be the subgroup of $\mathrm{Sp}_\Omega$ generated by symplectic transvections.

**Step 1.** *The group $G$ acts transitively on non-zero vectors in $V$.*

If $\langle u, v\rangle \neq 0$ then $u$, $v$ span a hyperbolic plane $H$. The following is an easy calculation, and concludes the proof in this case.

**5.4. Lemma.** *If $u, v \neq 0$ in $V$, and $\langle u, v\rangle \neq 0$, let $c = 1/\langle v, u\rangle$, $w = c(u - v)$. Then $\tau_w$ takes $v$ to $u$, and acts trivially on $H^\perp$.*

Otherwise, we have $\langle u, v\rangle = 0$. Let $U$ be the span of $u, v$, a totally isotropic subspace of $V$. We can find a complement $W$ such that the restriction of $\Omega$ to $U \oplus W$ is a non-degenerate four-dimensional symplectic space $V_0$. The claim then reduces to one about totally isotropic planes and $\mathrm{Sp}_4$. We can find a $w$ in $V_0$ with $\langle u, w\rangle \neq 0$, $\langle v, w\rangle \neq 0$. Apply  twice to find a pair of transvections taking $u$ to $w$ and then to $v$.

**Step 2.** A **hyperbolic pair** in $V$ is a pair $u$, $v$ such that $\langle u, v\rangle = 1$. *The group $G$ acts transitively on hyperbolic pairs.*

In dimension two, the set of hyperbolic pairs is a principal homogeneous space for $\mathrm{Sp}_2 = \mathrm{SL}_2$. Furthermore,

$$\begin{bmatrix} 1 & x \\ \circ & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & \circ \\ x & 1 \end{bmatrix}$$

are symplectic transvections that generate $\mathrm{SL}_2$.

In general, suppose $u_i$, $v_i$ ($i = 1, 2$) to be two hyperbolic pairs. We can find a product of transvections that take $u_1$ to $u_2$, so we are reduced to the case $u_1 = u_2 =$ (say) $u$. We want to find a product of transvections taking $u$ to itself and $v_1$ to $v_2$, given only that $\langle u, v_1\rangle = \langle u, v_2\rangle = 1$. This means at least that $\langle u, v_2 - v_1\rangle = 0$.

If $\langle v_1, v_2\rangle \neq 0$ then we can apply a transvection with direction $v_2 - v_1$ that takes $v_1$ to $v_2$ and fixes $u$, so we are done.

So suppose $\langle v_2, v_2\rangle = 0$. It suffices, by , to find a vector $w$ such that

$$\begin{aligned} \langle v_1, w\rangle &\neq 0 \\ \langle v_2, w\rangle &\neq 0 \\ \langle w - v_1, u\rangle &= 0 \\ \langle w - v_2, u\rangle &= 0\,. \end{aligned}$$

For this, take $w = v_1 + u$.

**Step 3.** We now apply induction and the previous step. ∎

### 6. The orthogonal group

Let $(V, Q)$ be a quadratic space. The **isometry group** or **orthogonal group** $O(Q)$ is the group of linear maps of $V$ to itself preserving $Q$.

At this point we know almost nothing about isometries. If $\sigma$ is an isometry and $\sigma u = v$ then $Q(u) = Q(v)$. But what about the converse? *Suppose $Q(u) = Q(v)$. Does there exist an isometry taking $u$ to $v$?* This is the question I shall investigate next.

There are three basic tools in constructing isometries, which I shall now examine.

• **Reflections.** I start with a simple result that we shall see used several times.

**6.1. Lemma.** *Suppose $u, v$ to be two vectors in $V$, with $Q(v) \neq 0$. Then $Q(u) = Q(u - tv)$ if and only if $t = 0$ or $t = -\nabla(u, v)/Q(v)$.*

*Proof.* Because

$$Q(u + tv) = Q(u) + t\nabla(u, v) + t^2 Q(v) = Q(u)$$

if and only if $t\nabla(u, v) = -t^2 Q(v)$. ∎

If $v$ is anisotropic, the linear map

$$r_v\colon x \longmapsto x - \frac{\nabla(x, v)}{Q(v)}\, v\,.$$

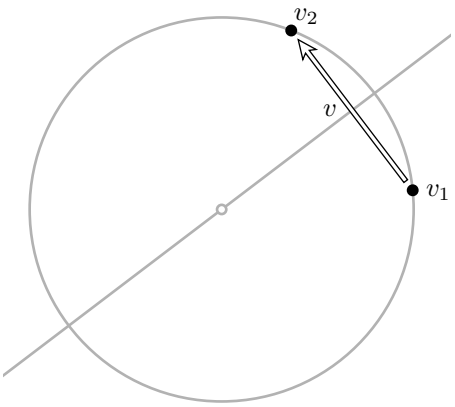
is therefore an isometry. It fixes a vector $x$ if and only if $\nabla(x,v)=0$. If $y=r_v x$ then

$$\nabla(y,v)=\nabla(x,v)-\frac{\nabla(x,v)}{Q(v)}\nabla(v,v)=-\nabla(x,v)$$
$$r_v^2 x=r_v y=y-\frac{\nabla(y,v)}{Q(v)}v=x\,,$$

so $r_v$ has order 2. It takes $v$ to $-v$, and in odd characteristic we cannot have $\nabla(v,v)=0$, so it is a reflection in the hyperplane $\nabla(x,v)=0$. In even characteristic $\nabla(v,v)=2Q(v)=0$ so $v$ always lies in the plane $\nabla(x,v)=0$, and $r_v$ is a shear parallel to that hyperplane. Nonetheless, I'll call it a reflection in all cases.

There is another way to state this Lemma: *If $\nabla(u,v)\neq 0$ the vector $r_v u$ is the unique vector $w$ other than $u$ on the line $t\mapsto u+tv$ with $Q(w)=Q(u)$.*

We'll find this useful for visualization. What does this have to do with the problem of finding an isometry that takes $v_1$ to $v_2$? Suppose for the moment that $R=\mathbb{R}$ and $Q(x,y)=x^2+y^2$ on the Euclidean plane. Given $v_1$ and $v_2$ of the same length, we can reflect $v_1$ in the line between them and get $v_2$.




This line is the line perpendicular to $v=v_2-v_1$, and the reflection subtracts from $x$ the projection of $x$ onto the line through $v$. In the standard notation of dot products, this projection is $(v_1\bullet v)/(v\bullet v)v$, and the formula for a reflection is therefore

$$x\longmapsto x-2\left(\frac{v\bullet x}{v\bullet v}\right)v$$

But the Euclidean norm is that determined by the dot-product, so we have here $B_Q(u,v)=2(u\bullet v)$, and this formula says that in our terminology $r_v v_1=v_2$. This is a general fact:

**6.2. Proposition.** *Suppose $v_1\neq v_2$ to be two vectors with $Q(v_1)=Q(v_2)$. If $v=v_2-v_1$ is anisotropic then $r_v v_1=v_2$.*

*Proof.* An immediate consequence of . ∎

The following is trivial, but it will be useful for me to be able to refer to:

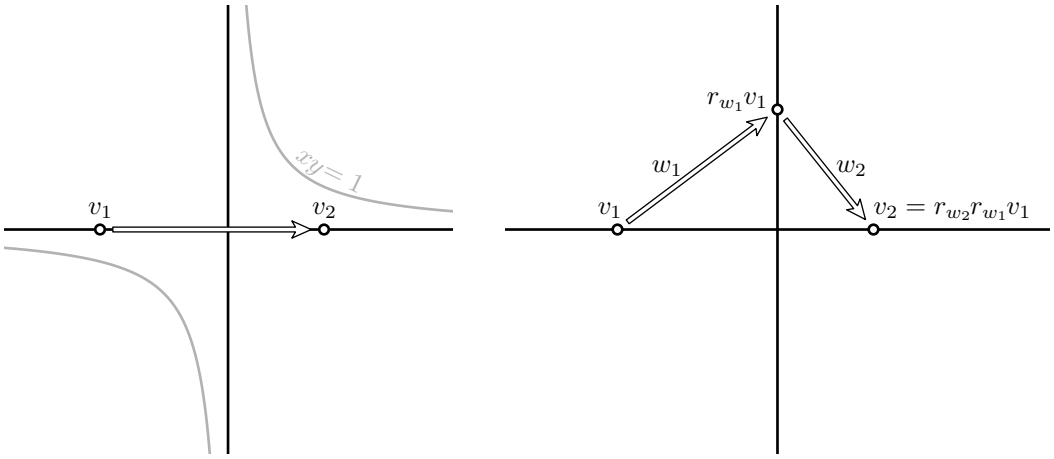
**6.3. Lemma.** *If $Q(v_1)=Q(v_2)$ and $v=v_2-v_1$ then $\nabla(v,v_2)=-\nabla(v,v_1)=Q(v)$.*

*Proof.* We have

$$\begin{aligned}\nabla(v,v_1)&=\nabla(v_2-v_1,v_1)\\&=\nabla(v_2,u_1)-\nabla(v_1,v_1)\\&=\nabla(v_2,u_1)-2Q(v_1)\\&=-Q(v_2)+\nabla(v_2,v_1)-Q(v_1)\\&=-Q(v)\,.\end{aligned}$$

∎

• **Composites of reflections.** But now suppose that $Q(v_1) = Q(v_2)$, $v = v_2 - v_1$, but $Q(v) = 0$. We cannot reflect $v_1$ into $v_2$ in one shot. The Euclidean model will not suggest anything, because $V$ possesses isotropic vectors. Instead, we take as our model the real hyperbolic plane with $Q(x, y) = xy$. As the first picture below should make clear, in this example if $Q(v_1) = Q(v_2)$ and $Q(v_2 - v_1) = 0$ then we must have $Q(v_1) = Q(v_2) = 0$. As the second picture should make clear, we can obtain $v_2$ by a composite of two reflections, with respect to anisotropic vectors $w_1$, $w_2$, with $w_1$ chosen more or less randomly, and $w_2$ then chosen so as to move $r_{w_1} v_1$ to $v_2$. Not quite randomly—one condition is that the reflection $r_{w_1}$ must actually move $v_1$ so as to get $w_2$ anisotropic. This is not quite sufficient.




According to , we may choose $w_2 = v_2 - r_{w_1} v_1$. But then

$$\begin{aligned} w_2 &= v_2 - \left( v_1 - \frac{\nabla(w_1, v_1)}{Q(w_1)}\, w_1 \right) \\ &= v + \frac{\nabla(w_1, v_1)}{Q(w_1)}\, w_1 \\ Q(w_2) &= Q(v) + \frac{\nabla(w_1, v_1)\nabla(w_1, v_1)}{Q(w_1)} + \frac{\nabla(w_1, v_1)\nabla(w_1, v_2 - v_1)}{Q(w_1)} \\ &= \frac{\nabla(v_1, w_1)\nabla(v_2, w_1)}{Q(w_1)}\,. \end{aligned}$$

Hence we have proved the following:

**6.4. Lemma.** *Suppose $v_1$, $v_2$ to be two vectors with $Q(v_1) = Q(v_2)$. Let $v = v_2 - v_1$ and suppose that $Q(v) = 0$.*

*If $w_1$ is an anisotropic vector that is not perpendicular to either $v_1$ or $v_2$, then $w_2 = v_2 - r_{w_1} v_1$ lies in the span of $v$ and $w_1$, is also anisotropic, and $r_{w_2} r_{w_1} v_1 = v_2$.*

• **Shears.** Now to define a different type of orthogonal transformation, one that exists only for quadratic spaces with sufficiently many isotropic vectors.

The pair $u$, $v$ is called totally isotropic if $Q(u)$, $Q(v)$, and $\nabla(u, v)$ all vanish, or equivalently if the span $\langle\langle u, v \rangle\rangle$ of $u$ and $v$ is totally isotropic.

Define $\tau_{u,v}$ to be the linear transformation

$$\tau_{u,v} \colon x \longmapsto x + \nabla(x, v)u - \nabla(x, u)v\,.$$

If $u$ and $v$ span a line this is just the identity, and otherwise (a) it fixes vectors on the linear space $\{\nabla(x, u) = 0 \cap \nabla(x, v) = 0\}$, and (b) shifts vectors parallel to the plane spanned by $u$ and $v$. If $u$, $v$ are totally isotropic, it is a **shear** or **transvection**.

**6.5. Lemma.** *If $u$ and $v$ are an isotropic pair, $\tau_{u,v}$ is an isometry.*

*Proof.* Because

$$\begin{aligned} Q(\tau_{u,v}x) &= Q(x) \\ &\quad + \nabla(x,v)\nabla(x,u) - \nabla(x,u)\nabla(x,v) \\ &\quad\quad - \nabla(x,u)\nabla(x,v)\nabla(u,v) + \nabla(x,u)^2Q(v) + \nabla(x,v)^2Q(u) \\ &= Q(x)\,. \end{aligned}$$

The following is a version of the extension theorem due to Ernst Witt in odd characteristic.

**6.6. Theorem.** *Suppose $(V,Q)$ to be any quadratic space over $F$ with bilinear form $\nabla = \nabla_Q$. If $U_1, U_2$ are subspaces of $V$ such that $U_1 \cap \mathfrak{rad}_\nabla = U_2 \cap \mathfrak{rad}_\nabla = 0$, any isometry $\sigma\colon U_1 \to U_2$ may be extended to an isometry of $V$.*

In other words, $O(Q)$ acts transitively on certain embedded quadratic subspaces forming a Zariski-open subset of the relevant Grassmannian. Some restriction is necessary, as we know from the example of form $x^2 + xy + ay^2 + z^2$ in characteristic 2. In this space, as we have seen, the complement of the form $z^2$ has non-isomorphic complements.

*Proof.* This is 8.3 of [Elman et al.:2008]. In odd characteristic this is well known and relatively easy, but in even characteristic more difficult. For the most part I follow the proof found in [Elman et al.:2008], except that I have modified their proof to make it (in principle) constructive. The proof is rather intricate. We start with this:

◇ *We are given an isometry $\sigma\colon U_1 \to U_2$. These subspaces satisfy the condition $U_i \cap \mathfrak{rad}_\nabla = 0$ for $i = 1, 2$. We wish to extend $\sigma$ to an isometry of $V$.*

**Step 1.** The proof goes by induction on the common dimension of $U_1$ and $U_2$. The result is trivial when this dimension is 0. So now assume this dimension to be $n > 0$, and assume the result to be true in dimension $n-1$. Let $W_1$ be a subspace of $U_1$ of codimension 1, $W_2 = \sigma(W_1)$. By the induction hypothesis, we may find an isometry of $V$ extending $\sigma|W_1$. Replacing $U_1$ by $\sigma(U_1)$, we may now assume:

◇ *The intersection of $U_1$ and $U_2$ is a subspace $W$ of codimension 1 in each, and there exists an isometry $\sigma\colon U_1 \to U_2$ which is $I$ on $W$. We wish to find an extension of $\sigma$ to all of $V$.*

**Step 2.** Choose $u_1$ in $U_1 - W$, and set $u_2 = \sigma(u_1)$. Let $u = u_2 - u_1$. If $u = 0$, $u_1 = u_2$ and we are done.

◇ *We have vectors $u_i$ spanning $U_i/W$, with $u_2 = \sigma(u_1)$, $u = u_2 - u_1 \neq 0$.*

**Step 3.** For $w$ in $W$

$$\nabla(u_1, w) = \nabla(\sigma u_1, \sigma w) = \nabla(u_2, w)$$

and hence $u$ lies in $W^\perp$. If $u$ is anisotropic then the reflection $r_w$ takes $u_1$ to $u_2$ and fixes all vectors in $W$. We are again through. Otherwise, by , we may now assume:

◇ *We have $\nabla(u, W) = \nabla(u, u_1) = \nabla(u, u_2) = Q(u) = 0$.*

**Step 4.** At this point I call on the assumption that $U_i \cap \mathfrak{rad}_\nabla = 0$. Because of , we can find $v_i$ in $V$ such that $\nabla(v_i, W) = 0$ and $\nabla(v_i, u_i) \neq 0$. Thus:

◇ *Each subspace $H_i$ of $W^\perp$ where $\nabla_{u_i} = 0$ is a proper subspace of $W^\perp$.*

**Step 5.** Note that $u$ lies in the intersection of the $H_i$. According to , if we can find $x$ anisotropic in $W^\perp$ that lies neither in $H_1$ nor $H_2$, we can find a composite of reflections that takes $u_1$ to $u_2$ and fixes all $w$ in $W$. This may not be possible, but when it is not we shall be able to use a transvection instead.

◇ *At this point we look separately at two alternatives. Either (1) $u^\perp \cap W^\perp \subseteq H_1$ or (2) there exists $x$ in $u^\perp \cap W^\perp$ not in $H_1$.*

**Step 6.** Suppose (1) $H = u^\perp \cap W^\perp \subseteq H_1$. Then in fact $H = H_1 = H_2$. Choose an arbitrary $x$ in $W^\perp - H$ such that $\nabla(x, u) \neq 0$. We have

$$Q(x+u) = Q(x) + \nabla(x,u) + Q(u) = \nabla(x,u) + Q(u)\,,$$

so that either $x$ or $x + u$ is anisotropic, and we are again done.

**Step 7.** Suppose (2) $u^\perp$ intersects $W^\perp - H_1$.

Suppose (a) there exists an anisotropic vector in $u^\perp - H_1$. If $x$ lies in this, then necessarily $\nabla(x, u_2) \neq 0$ as well, and we are again done.

**Step 8.** Or (b) all $x$ in $u^\perp - H_1$ are isotropic. Pick one. We may scale it so that $\nabla(x, u_1) = \nabla(x, u_2) = 1$. Then $x$, $u$ form an isotropic pair. The transvection $\tau_{u,w}$ fixes $w$ in $W$ and takes

$$u_1 \longmapsto u_1 + \nabla(w, u_1)u + \nabla(u, u_1)w = u_1 + u = u_2 \,.$$

and we are done.

The proof of  is finally complete.

**6.7. Corollary.** *Suppose $(V, Q)$ a non-degenerate quadratic space, $u_1$ and $u_2$ in $V$ with $Q(u_1) = Q(u_2)$, neither in $\mathfrak{rad}_\nabla$. There exists an isometry of $V$ taking $u_1$ to $u_2$.*

Even proving this simple case is not much easier than proving the general result.

For example, if $Q$ is a non-degenerate quadratic form of dimension $n$ over an algebraically closed field of characteristic 2, then $Q \oplus x_{n+1}^2$ is non-degenerate. The space $\mathfrak{rad}_\nabla$ is spanned by $\varepsilon = (0, 0, \ldots, 1)$. The unit sphere is the union of two orbits under the orthogonal group, $\varepsilon$ and its complement.

*Proof.* This is just a special case of .

**6.8. Corollary.** *Any two decompositions of the non-degenerate $(V, Q)$ into a multiple of $H$ plus an anisotropic subspace are equivalent by an isometry of $V$.*

*Proof.* Suppose $V = n_1 H \oplus U_1 = n_2 H \oplus U_2$, with $U_1$, $U_2$ anisotropic. Suppose $n_1 \leq n_2$. By Witt's Theorem we may find an isometry of $V$ taking $n_1 H$ into $n_2 H$. But then $(n_2 - n_1)H \oplus U_2 \cong U_1$, so $n_2 = n_1$ and $U_1 \cong U_2$.

## 7. *Appendix.* Arithmetic of Galois extensions

For the moment, suppose $F$ to be any field, $L/F$ a Galois extension with Galois group $\mathcal{G}$. I recall the basic technical Lemma of Galois theory.

**7.1. Proposition.** *The automorphisms in $\mathcal{G}$ are linearly independent over $F$.*

This is well known, but I'll include a proof here.

*Proof.* It is to be proved that if $S$ is any finite subset of $\mathcal{G}$ and

$$\sum_S a_s x^s = 0$$

for all $x$ in $K$, then all $a_s = 0$. The proof will be by induction on the size of $S$. The claim is trivial for $|S| = 1$, so now we assume it is true for any subset smaller than $S$. Suppose $|S| = n$ and that

$$\sum_{i=1}^{n} a_{s_i} x^{s_i} = 0$$

for all $x$ in $L$. Then also

$$\sum_i a_{s_i} (xy)^{s_i} = \sum_S a_{s_i} x^{s_i} y^{s_i} = 0$$

for all $x$, $y$. Multiply the first equation by $y^{s_n}$ to get

$$\sum_i a_{s_i} x^{s_i} y^{s_n} = 0$$

and then subtract to get

$$\sum_{i=1}^{n-1} a_{s_i}(y^{s_n} - y^{s_i})x^{s_i} = 0\,.$$

We may apply the induction hypothesis to deduce that

$$a_{s_i}(y^{s_n} - y^{s_i}) = 0$$

for all $i$ and all $y$. But $s_n$ is different from all the $s_i$, so for each $i$ we may find $y$ with $y^{s_n} \neq y^{s_i}$.

If $K/F$ is any finite field extension, let $L/F$ be a Galois extension containing $K$. The trace map from $K$ to $F$ is

$$\mathrm{trace}_{K/F}\colon\ x \longmapsto \sum_{\mathrm{Gal}(L/K)\backslash\mathrm{Gal}(L/F)} x^g\,.$$

**7.2. Corollary.** *The trace map* $\mathrm{trace}_{K/F}$ *is surjective.*

*Proof.* Apply the Proposition to $L/K$, $L/F$.

## 8. References


**1.** Cahit Arf, 'Untersuchungen der quadratischen Formen in Körpen de Charakteristik 2', *Journal für die reine and angewandte Mathematik* **183** (1941), 148–167.

**2.** Emil Artin, **Geometric algebra**, Wiley, 1957.

**3.** J. W. S. Cassels, **Rational quadratic forms**, Academic Press, 1978. Reprinted by Dover in 2008.

**4.** Leonard Eugene Dickson, **Linear groups**, Teubner, 1901. This is now available at

`https://archive.org/details/lineargroupswith00dickuoft`

**5.** Jean Dieudonné, 'Pseudo-invariant and Dickson invariant', *Pacific Journal of Mathematics* **5** (1955), 907–910.

**6.** Roger H. Dye, 'On the Arf invariant', *Journal of Algebra* **53** (1978), 36–39.

**7.** Richard Elman, Nikita Karpenko, and Alexander Merkurjev, **The algebraic and geometric theory of quadratic forms**, A. M. S., 2008.

**8.** Falko Lorenz and Peter Roquette, 'On the Arf invariant in historical perspective', posted February 2010 at

`http://www.rzuser.uni-heidelberg.de/ ci3/arf.pdf`