ALGEBRAIC GROUPS: PART I

EYAL Z. GOREN, MCGILL UNIVERSITY

Contents

References:

- Springer, T. A.: **Linear algebraic groups.** Reprint of the 1998 second edition. Modern Birkhuser Classics. Birkhuser Boston, Inc., Boston, MA, 2009.
- Borel, Armand: **Linear algebraic groups.** Second edition. Graduate Texts in Mathematics, 126. Springer-Verlag, New York, 1991.
- Humphreys, James E.: **Linear algebraic groups.** Graduate Texts in Mathematics, No. 21. Springer-Verlag, New York-Heidelberg, 1975.
- Goodman, Roe; Wallach, Nolan R.: **Symmetry, representations, and invariants.** Graduate Texts in Mathematics, 255. Springer, Dordrecht, 2009.
- Shimura, G.: **Arithmetic and analytic theories of quadratic forms and Clifford groups.** Mathematical Surveys and Monographs, 109. American Mathematical Society, Providence, RI, 2004.
- Jacobson, Nathan: *Basic algebra. I & II.* Second edition. W. H. Freeman and Company, New York, 1989.

Date: Winter 2011.

1. Introduction

This course is about **linear algebraic groups**. These are varieties V over a field k, equipped with a group structure such that the group operations are morphisms, and, in addition, V is affine. It turns out that then V is a closed subgroup of $\mathrm{GL}_n(k)$, for some n, and for that reason they are called linear.

On the other side of the spectrum are the projective algebraic groups. Such a group, if it's connected, is automatically commutative and therefore one call the connected projective algebraic groups **abelian varieties**. Their theory is very different from the theory of linear algebraic groups. Linear algebraic groups have plenty of linear representations, and their Lie algebra has rich structure. On the other hand, abelian varieties have only trivial linear representations and their Lie algebras are commutative and so of little interest. On other hand, the arithmetic of abelian varieties is very deep; abelian varieties produce some of the most interesting Galois representations, while linear algebraic group have less rich structure when it comes to Galois representations (which is not to say there aren't very deep issues going on there as well).

The two aspects of algebraic groups are connected, but hardly mix in practice, and the development of their theories is completely different. The theories connect, for example, in a special class of algebraic groups - the semi-abelian varieties - but, from the point of view of a general theory, this is a very particular case, and so, by and large, one studies the two classes of algebraic groups separately.

Notation. We shall use the letters k or F to denote fields and $\overline{k}$, k^{sep}, $\overline{F}$, F^{sep} to denote their algebraic and separable closures. Γ_k and Γ_F will denote then the Galois groups of k^{sep}/k and F^{sep}/F, respectively.

2. First Definitions

Let k be a field. A **linear**, or **affine**, **algebraic group** G over k, is an affine variety[1] G over k, equipped with a k-rational point $e \in G$ and k-morphisms

$$\mu : G \times G \to G, \qquad i : G \to G,$$

such that $G(\overline{k})$ becomes a group with identity e, multiplication $xy = \mu(x, y)$ and inverse $x^{-1} = i(x)$.

Write $k[G]$ for the ring of regular functions on G then μ and i corresponds to a homomorphisms of k-algebras

$$\Delta : k[G] \to k[G] \otimes_k k[G], \quad \iota : k[G] \to k[G],$$

(called **comultiplication** and **coninverse**, respectively) and e is defined by a k-homomorphism (the counit)

$$\epsilon : k[G] \to k.$$

One expresses the group axioms as properties of the morphisms Δ, ι, ϵ (for example, associativity is $(\Delta \otimes 1) \circ \Delta = (1 \otimes \Delta) \circ \Delta$, and so on.) In return, given an affine variety G and given morphisms Δ, ι, ϵ with these properties, one gets an algebraic group structure on G.

A **closed subgroup** H of G defined over k is a closed subset H of G defined over k, thus an affine variety, which is also closed under the group law. It then follows that Δ, ι and ϵ induce k-algebra homomorphisms $k[H] \to k[H] \otimes_k k[H], \quad \iota : k[H] \to k[H]$ and $\epsilon : k[H] \to k$. A homomorphism of algebraic groups over k is defined in the obvious manner.

Let G, G_1 be linear algebraic groups over k. We say that G_1 is a **form** of G if G and G_1 are isomorphic over $\overline{k}$.

[1]An affine variety over k is defined to be a closed subset of the affine space $\mathbb{A}^n_{\overline{k}}$, defined by an ideal of $\overline{k}[x_1, \ldots, x_n]$ that has a generating set of polynomials in $k[x_1, \ldots, x_n]$.

3. The main examples

We would want to carry with us throughout the course the examples of the classical groups. Besides illustrating the theory, they are also the most useful and frequently occurring algebraic groups.

3.1. **Additive groups.** The group $\mathbb{G}_a$ - the **additive group** - is simply k with addition,

$$\mu(x, y) = x + y;$$

more precisely, it is $\mathbb{A}^1$ - the affine line over k. The coordinate ring is $k[x]$ and the homomorphism Δ is given by

$$x \mapsto x \otimes 1 + 1 \otimes y \in k[x] \otimes k[y].$$

(Under the isomorphism $k[x] \otimes_k k[y] \cong k[x, y]$, we have $x \otimes 1 + 1 \otimes y \mapsto x + y$.) The group $\mathbb{G}_a^n$ is the affine n space $\mathbb{A}^n$ over k, and often we shall identify $\mathbb{G}_a^{n^2}$ with M_{n^2} - the $n \times n$ matrices.

3.2. **Tori.** The group $\overline{k}^\times$ of the non-zero elements of $\overline{k}$ under multiplication is a linear algebraic group defined over k. It is isomorphic to the affine variety V defined by $\{(x, y) \in \mathbb{A}^2 : xy = 1\}$:

$$\overline{k}^\times \to V, \qquad t \mapsto (t, 1/t).$$

The group law is given by

$$(x_1, y_1)(x_2, y_2) \mapsto (x_1x_2, y_1y_2),$$

and μ is the homomorphism determined by

$$x \mapsto x \otimes x, \qquad y \mapsto y \otimes y.$$

(These are viewed as elements of $R \otimes_k R$, where $R = k[x, y]/(xy - 1)$.) Note that it is well-defined: $1 = xy \mapsto (x \otimes x)(y \otimes y) = xy \otimes xy = 1 \otimes 1 = 1$.

We denote this algebraic group by $\mathbb{G}_m$, and call it the **multiplicative group**; we also denote it by GL_1. If we need to emphasize the field of definition, we shall write $\mathbb{G}_{m,k}$ and $\mathrm{GL}_{1/k}$. A **torus** over k is an algebraic group T over k, which is a form of $\mathbb{G}_{m,k}^n$, for some n.

Let K be a number field. We consider K^* as an algebraic group over $\mathbb{Q}$ as follows: choose a basis $\alpha_1, \ldots, \alpha_n$ for K as a vector space over $\mathbb{Q}$. Then every element in K can be written as $x_1\alpha_1 + \cdots + x_n\alpha_n$. The multiplication then has the form

$$(\sum x_i\alpha_i)(\sum y_i\alpha_i) = (\sum f_i\alpha_i),$$

where the f_i are bihomogenous polynomials, with rational coefficients, in the set of variables $\{x_i\}$ and $\{y_i\}$. The condition that $\sum x_i\alpha_i$ has an inverse can be phrased in the form $g(x_1,\dots,x_n)\neq 0$ for some rational polynomial g (exercise!) and so we get an algebraic group over $\mathbb{Q}$, which is the open subset of $\mathbb{A}^n$ defined as $g(x_1,\dots,x_n)\neq 0$ (this set can be realized as the affine set in $\mathbb{A}^{n+1}$ defined by $\{(x_1,\dots,x_n,y) : g(x_1,\dots,x_n)y-1=0\}$). The map Δ is nothing else then $x_i\mapsto f_i$. We denote this algebraic group $\mathrm{Res}_{K/\mathbb{Q}}\mathbb{G}_m$; its $\mathbb{Q}$-points are $\mathrm{Res}_{K/\mathbb{Q}}\mathbb{G}_m(\mathbb{Q})=K^*$.

Here is a simple example. Let $K=\mathbb{Q}(\sqrt{5})$, with the basis $\alpha_1=1,\alpha_2=\sqrt{5}$. Then,

$$(x_1+x_2\sqrt{5})(y_1+y_2\sqrt{5})=x_1y_1+5x_2y_2+(x_1y_2+x_2y_1)\sqrt{5}.$$

We can write the inverse of $x_1+x_2\sqrt{5}$ as $\frac{x_1-x_2\sqrt{5}}{x_1^2-5x_2^2}$. The polynomial $g(x_1,x_2)$ is thus $x_1^2-5x_2^2$ and we get the algebraic group

$$G=\{(x_1,x_2) : x_1^2-5x_2^2\neq 0\},$$

with comultiplication

$$x_1\mapsto x_1\otimes y_1+5x_2\otimes y_2,\quad x_2\mapsto x_1\otimes y_2+x_2\otimes y_1,$$

coinverse

$$x_1\mapsto \frac{x_1}{x_1^2-5x_2^2},\quad x_2\mapsto \frac{-x_2}{x_1^2-5x_2^2},$$

and counit

$$x_1\mapsto 1,\quad x_2\mapsto 0.$$

This is a torus, which is a form of $\mathbb{G}_{m,\mathbb{Q}}^2$. Indeed, already over the field $\mathbb{Q}(\sqrt{5})$, the map

$$(x_1,x_2)\mapsto(x_1+x_2\sqrt{5},x_1-x_2\sqrt{5}),$$

is an isomorphism to $\mathbb{G}_m^2$.

Proposition 3.2.1. *We have* $\mathrm{End}(\mathbb{G}_m^n)=M_n(\mathbb{Z})$.

Proof. Because $\mathrm{Hom}(X\times Y,Z)=\mathrm{Hom}(X,Z)\times\mathrm{Hom}(Y,Z)$ and $\mathrm{Hom}(X,Y\times Z)=\mathrm{Hom}(X,Y)\times\mathrm{Hom}(X,Z)$, it is enough to prove the proposition for $n=1$. Given an integer n, the function

$$x\mapsto x^n,$$

is a homomorphism of $\mathbb{G}_m$ and we get $\mathbb{Z} \hookrightarrow \mathrm{End}(\mathbb{G}_m)$. Let now $f : \mathbb{G}_m \to \mathbb{G}_m$ be a homomorphism of algebraic groups. This means that the following diagram commutes:

$$\begin{array}{ccc} \mathbb{G}_m \times \mathbb{G}_m & \xrightarrow{\mu} & \mathbb{G}_m \\ {\scriptstyle f\times f}\downarrow & & \downarrow{\scriptstyle f} \\ \mathbb{G}_m \times \mathbb{G}_m & \xrightarrow{\mu} & \mathbb{G}_m \end{array}$$

Then, we must have

$$\Delta \circ f^* = (f^* \otimes f^*) \circ \Delta.$$

Abuse notation and write $f(x)$ for the polynomial $f^*(x)$, where $f^* : k[x, x^{-1}] \to k[x, x^{-1}]$ is the k-algebra homomorphism corresponding to f. It follows then from this relation that

$$f(x \otimes y) = f(x) \otimes f(y),$$

in $k[x, x^{-1}] \otimes_k k[y, y^{-1}]$. Write $f(x) = \sum_{n=-N}^{N} a_n x^n$. We then get that

$$\sum_{n=-N}^{N} a_n x^n \otimes y^n = (\sum_{n=-N}^{N} a_n x^n) \otimes (\sum_{n=-N}^{N} a_n y^n) = \sum a_n a_m x^n \otimes y^m.$$

Let n_0 be such that $a_{n_0} \neq 0$. Then, it follows that, for $n \neq n_0$, $a_n = 0$ (since $a_n a_{n_0} x^n \otimes y^{n_0}$ must be zero). Further, since $a_{n_0} x^{n_0} \otimes y^{n_0} = a_{n_0}^2 x^{n_0} \otimes y^{n_0}$, we must have $a_{n_0} = 1$. If follows that f is the homomorphism $x \mapsto x^{n_0}$. □

For a general linear group G, elements $f \in k[G]$ such that $\Delta(f) = f \otimes f$ are called "group-like" elements. They correspond to homomorphisms $G \to \mathbb{G}_m$.

3.3. **The general linear group** GL_n**.** For a field k, the group GL_n over k is the affine variety in $\mathbb{A}^{n^2}$ - thought of $n \times n$ matrices (x_{ij})- which is the complement of the closed subvariety $\det(x_{ij}) = 0$. It is an affine variety, as it is isomorphic to the affine variety in $\mathbb{A}^{n^2+1}$ with coordinates x_{ij} and y, defined by the equation $\det(x_{ij}) \cdot y - 1 = 0$. The group law is, of course, matrix multiplication. It is called the **general linear group**. The map

$$\mathrm{GL}_n \to \mathbb{G}_m, \qquad (x_{ij}) \mapsto \det(x_{ij}),$$

is a group homomorphism.

Here are some closed subgroups of GL_n.

(1) The torus $T = \{\mathrm{diag}(x_1, \ldots, x_n) : x_1 x_2 \cdots x_n \neq 0\}$.
(2) The so-called **Borel subgroup** of upper-triangular matrices

$$B = \{(x_{ij}) \in \mathrm{GL}_n : x_{ij} = 0, i > j\}.$$

(3) The group of unipotent matrices

$$U = \{(x_{ij}) \in B : x_{ii} = 1, \forall i\}.$$

Note that

$$B = TU = UT \cong T \times U.$$

Let V be an n-dimensional vector space over k. A **flag** F of type $(d_1, \dots d_t)$, where $0 \leq d_1 < d_2 < \cdots < d_t \leq n$ are integers is a series of subspaces $\{V_i\}$ of V such that $\dim(V_i) = d_i$ and $V_1 \subset V_2 \subset \cdots \subset V_d$. A **maximal flag** is a flag of type $(0, 1, 2, \dots, n)$. The collection of flags of type (d) is an algebraic variety of dimension $d(n-d)$, called the **Grassmann variety** $\mathscr{G}(n, d)$. The collection of flags of type $(d_1, \dots d_t)$ is a closed subvariety $\mathscr{F}_{(d_1,\dots,d_t)}$ of $\mathscr{G}(n, d_1) \times \mathscr{G}(n, d_2) \times \cdots \times \mathscr{G}(n, d_t)$.

We say that an **algebraic group** G **acts on a variety** V if we are given a morphism

$$G \times V \to V, \qquad (g, v) \mapsto gv,$$

such that

$$g_1(g_2 v) = (g_1 g_2)v, \qquad ev = v,$$

for all $v \in V, g_1, g_2 \in G$. Let $v \in V$ and $\mathrm{Stab}(v) = \{g \in G : gv = v\}$ be its **stabilizer**. It is a closed subgroup of G.

Let $V = k^n$. The group GL_n acts transitively on $\mathscr{F}_{(d_1,\dots,d_t)}$. Pick a flag F of type $\mathscr{F}_{(d_1,\dots,d_t)}$. Then $\mathrm{Stab}(F)$ is a closed subgroup of GL_n, called a **parabolic subgroup** of type $\mathscr{F}_{(d_1,\dots,d_t)}$. Choosing a basis $\{e_1, \dots, e_n\}$ for V such that the first d_1 vectors span V_1, the first d_2 span V_2 and so on, the parabolic subgroup consists of matrices of the form

$$\begin{pmatrix} A_1 & * & * & \dots & * \\ & A_2 & * & \dots & * \\ & & A_3 & \dots & * \\ & & & \ddots & \\ & & & & A_{t+1} \end{pmatrix},$$

where A_1 is a square matrix of size d_1, A_2 is a square matrix of size $d_2 - d_1$, A_3 is a square matrix of size $d_3 - d_2$ and so on, and A_{t+1} is of size $n - d_t$.

For the maximal flag $F = \{\mathrm{Span}(e_1), \mathrm{Span}(e_1, e_2), \dots, \mathrm{Span}(e_1, e_2, \dots, e_n)\}$ we get back the Borel subgroup B.

Exercise 1. Calculate the dimension of a parabolic subgroup and, using that, calculate the dimension of the variety $\mathscr{F}_{(d_1,\dots,d_t)}$.

3.3.1. *The unitary groups $U_{p,q}$.* Consider the hermitian form on $\mathbb{C}^n$ given by

$$\langle (x_1,\dots,x_n),(y_1,\dots,y_n)\rangle = \sum_{i=1}^{p} x_i\bar{y}_i - (\sum_{i=p+1}^{n} x_i\bar{y}_i),$$

where $1 \le p \le n$ (and $q = n-p$). Let $U(p,q)$ be the matrices of $M_n(\mathbb{C})$ that preserve this form. Seperating real and imaginary parts, we get a collection of algebraic equations with rational coefficients that define $U(p,q)$. Indeed, writing a matrix as $\begin{pmatrix} A & B \\ C & D \end{pmatrix}$ with A of size $p\times p$, B of size $p\times q$, etc., and then $A = A_1 + iA_2$, etc., we find the relations

$$\begin{pmatrix} {}^tA_1 + i{}^tA_2 & {}^tC_1 + i{}^tC_2 \\ {}^tB_1 + i{}^tB_2 & {}^tD_1 + i{}^tD_2 \end{pmatrix} \begin{pmatrix} I_p & 0 \\ 0 & -I_q \end{pmatrix} \begin{pmatrix} A_1 - iA_2 & B_1 - iB_2 \\ C_1 - iC_2 & D_1 - iD_2 \end{pmatrix} = \begin{pmatrix} I_p & 0 \\ 0 & -I_q \end{pmatrix}.$$

Multiplying through and separating real and imaginary parts, we find a collection of quadratic equations with integer coefficients. Thus, the group $U(p,q)$ is defined over $\mathbb{Q}$ and its real points, $U(p,q)(\mathbb{R})$ (denoted often just by $U(p,q)$) are the matrices of $M_n(\mathbb{C})$ that preserve the form $\sum_{i=1}^{p} x_i\bar{y}_i - (\sum_{i=p+1}^{n} x_i\bar{y}_i)$.

Exercise 1. *Prove that over the complex numbers the group $U(p,q)$ is isomorphic to the unitary group $U(n)$.*

The group $U(n)$, in turn, is isomorphic over the complex numbers to the group GL_n. Indeed, the elements of $U(n)(\mathbb{C})$ are pairs of complex matrices (A,B) such that ${}^tAA + {}^tBB = I_n$ and ${}^tAB$ is symmetric (this implies $({}^tA + i{}^tB)(A - iB) = I_n$).The group law is given by $(A,B)(C,D) = (AC - BD, AD + BC)$. Define a map

$$U(n)(\mathbb{C}) \to \mathrm{GL}_n(\mathbb{C}), \qquad (A,B) \mapsto A + iB.$$

This is a well-defined group homomorphism. It is injective, because, letting $M = A + iB$, we have $A - iB = {}^tM^{-1}$ and so

$$A = \frac{1}{2}(M + {}^tM^{-1}), \qquad B = \frac{1}{2i}(M - {}^tM^{-1}).$$

This map is also surjective: given any $M \in \mathrm{GL}_n(\mathbb{C})$ define A, B by these formulas. One then checks that ${}^tAA + {}^tBB = I_n$ and ${}^tAB$ is symmetric. Thus, the unitary groups $U(p,q)$

are forms of GL_n over $\mathbb{Q}$. The calculation above shows that in fact $U(p,q)$ is isomorphic to GL_n over $\mathbb{Q}(i)$.

3.4. **The orthogonal group $\mathcal{O}_q$.** In this section we assume that $\mathrm{char}(k) \neq 2$.

3.4.1. *Quadratic forms.* Let V be a finite-dimensional vector space over k of dimension n. A **bilinear form** on V is a function

$$B : V \times V \to k,$$

such that $B(x,y)$ is a linear map in each variable separately. It is called **symmetric** if in addition $B(x,y) = B(y,x)$. We then let

$$q : V \to k \qquad q(x) = B(x,x),$$

be the associated **quadratic form**.[2] If

$$q : V \to k$$

is a function satisfying $q(\lambda x) = \lambda^2 q(x)$, such that the function

$$B : V \times V \to k, \qquad B(x,y) = \frac{1}{2}(q(x+y) - q(x) - q(y)),$$

is a symmetric bilinear form, then we call q a quadratic form. Note that $q(x) = B(x,x)$ then.

Given a bilinear form B we define the **orthogonal group** $\mathcal{O}_B = \mathcal{O}_q$:

$$\begin{aligned}\mathcal{O}_B &= \{A \in \mathrm{GL}(V) : B(Ax, Ay) = B(x,y), \forall x, y \in V\} \\ &= \{A \in \mathrm{GL}(V) : q(Ax) = q(x), \forall x \in V\}.\end{aligned}$$

If one introduces coordinates on V then we can can write

$$B(x,y) = {}^t[x]M[y],$$

where $[x]$ are the coordinates of x and M is a symmetric $n \times n$ matrix. Then,

$$\mathcal{O}_B = \{A \in \mathrm{GL}_n(k) : {}^tAMA = M\}.$$

We see that $\mathcal{O}_B$ is a closed subgroup of GL_n, defined by quadratic equations. We let $S\mathcal{O}_B$ be $\mathcal{O}_B \cap \mathrm{SL}(V)$ (and in coordinates: $\mathcal{O}_B \cap \mathrm{SL}_n(k)$). We note that B is **non-degenerate** (namely, if $B(x,y) = 0$ for a fixed x and all y, then $x = 0$) iff $\det(M) \neq 0$.

The **classical orthogonal group**, denoted simply $\mathrm{O}(n)$, is a special case of this construction, when the matrix M is I_n (and so the quadratic form is, in coordinates, $x_1^2 + x_2^2 +$

[2] In many texts the normalization is $q(x) = \frac{1}{2}B(x,x)$, and that can matter a lot sometimes.

$\cdots + x_n^2$. Note that if B is non-degenerate then $\mathcal{O}_B$ is a form of $\mathrm{O}(n)$, and $S\mathcal{O}_B$ is a form of $\mathrm{SO}(n)$).

Let V, W be vector spaces with bilinear forms B_V, B_W. An **isometry** $T : V \to W$ is an isomorphism of vector spaces such that $B_W(Tx, Ty) = B_V(x, y)$. For example, $\mathcal{O}_B$ is the group of isometries from V to itself.

Theorem 3.4.1 (Witt's extension theorem)**.** *Let V be a vector space equipped with a bilinear form B. Any isometry $T : U \to U'$, between subspaces U, U' of V, can be extended to an isometry of V. (For the proof see, e.g., Jacobson, Part I, p. 369.)*

3.4.2. *Clifford algebras.* Let V be a vector space over k (still $\mathrm{char}(k) \neq 2$) and q a quadratic form on k. There is a pair $(\mathrm{Cliff}(V, q), p)$ consisting of a k-algebra $\mathrm{Cliff}(V, q)$ and a k-linear map

$$p : V \to \mathrm{Cliff}(V, q),$$

with the following properties:

- $\mathrm{Cliff}(V, q)$ is generated as k-algebra by $p(V)$ and 1.
- $p(v)^2 = q(v) \cdot 1$.
- $(\mathrm{Cliff}(V, q), p)$ has the following universal property. Given any other k-algebra A with a k-linear map $p_1 : V \to A$ such that $p_1(v)^2 = q(v) \cdot 1_A$, there is a unique map

  $$f : \mathrm{Cliff}(V, q) \to A,$$

  of k-algebras such that $f \circ p = p_1$.

Clearly these properties determine $(\mathrm{Cliff}(V, q), p)$ up to a unique isomorphism. One further proves the following properties:

- The map p is injective. (This is clear if every non-zero vector v is anisotropic: $q(v) \neq 0$, but the vector space may have isotropic vectors even when B is non-degenerate.) We shall therefore write v for $p(v)$ and think of V as a subset of $\mathrm{Cliff}(V, q)$, whenever convenient.
- If $e_1, \ldots, e_n$ are a basis for V over k then the 2^n elements $e_{i_1} e_{i_2} \cdots e_{i_t}$, where $1 \leq i_1 < i_2 < \cdots < i_t \leq n$, are a basis of $\mathrm{Cliff}(V, q)$ as a k-vector space (the empty product is understood as 1).
- One can construct $\mathrm{Cliff}(V, q)$ as $T(V)/\langle x^2 - q(x) : x \in V \rangle$, where $T(V) = \oplus_{n=0}^{\infty} V^{\otimes n}$ is the tensor algebra ($V^{\otimes 0} := k$). The natural map $V = V^{\otimes 1} \to T(V)$ induces the

map $p : V \to \mathrm{Cliff}(V,q)$. Note that since the ideal $\langle x^2 - q(x) : x \in V\rangle$ is graded, the Clifford algebra has a $\mathbb{Z}/2\mathbb{Z}$-grading.

Example 3.4.2. Since $2B(x,y) = q(x+y) - q(x) - q(y) = (x+y)^2 - x^2 - y^2 = xy + yx$, we have the relation in $\mathrm{Cliff}(V,q)$

$$\boxed{xy + yx = 2B(x,y), \qquad \forall x, y \in V}$$

In particular, if x, y are **orthogonal**, namely, if $B(x,y) = 0$ then $xy = -yx$.

Suppose that B is identically zero. Then $\mathrm{Cliff}(V,q)$ is the exterior algebra of V. This is easy to see given the statement about a basis of $\mathrm{Cliff}(V,q)$ and the relation $xy = -yx$ holding for all $x, y \in V$, or from the assertion that the Clifford algebra is equal to $T(V)/\langle x^2 : x \in V\rangle$.

Definition 3.4.3. The **canonical automorphism** of $\mathrm{Cliff}(V,q)$ is the automorphism induced by the map

$$p_1 : V \to \mathrm{Cliff}(V,q), \qquad p_1(v) = -p(v).$$

This induced automorphism, denoted

$$a \mapsto a',$$

is uniquely determined by the property

$$x' = -x, \qquad \forall x \in V$$

(where now we identify V with its image under p; alternately, it is the property $p(v)' = -p(v)$).

Note that $\mathrm{Cliff}(V,q)^{op}$, the opposite k-algebra, equal to $\mathrm{Cliff}(V,q)$ as a k-vector space, but with multiplication $a \times b = ba$, where on the right we have the multiplication in $\mathrm{Cliff}(V,q)$, is indeed a k-algbera. The map $p : V \to \mathrm{Cliff}(V,q)^{op}$ satisfies the properties of a Clifford algebra and so we get a map

$$\mathrm{Cliff}(V,q) \to \mathrm{Cliff}(V,q)^{op},$$

extending the identity map on V. Denote this map by $a \mapsto a^*$. It is a k-linear **involution** on $\mathrm{Cliff}(V,q)$; it is uniquely determined by the property $(ab)^* = b^*a^*$ (the involution property) and

$$x^* = x, \qquad \forall x \in V.$$

The **even Clifford algebra** $\mathrm{Cliff}(V,q)^+$ is defined by

$$\mathrm{Cliff}(V,q)^+ = \{a \in \mathrm{Cliff}(V,q) : a' = a\}.$$

It is indeed a k-algebra. We also define

$$\mathrm{Cliff}(V,q)^- = \{a \in \mathrm{Cliff}(V,q) : a' = -a\}.$$

Then $\mathrm{Cliff}(V,q)^-$ is a k-vector space, which is a $\mathrm{Cliff}(V,q)^+$-module and

$$\mathrm{Cliff}(V,q) = \mathrm{Cliff}(V,q)^+ \oplus \mathrm{Cliff}(V,q)^-.$$

Given the description of a basis for $\mathrm{Cliff}(V,q)$, it is easy to see that $\mathrm{Cliff}(V,q)^\pm$, are each 2^{n-1}-dimensional; a basis of $\mathrm{Cliff}(V,q)^+$ (resp. $\mathrm{Cliff}(V,q)^-$) is given by the elements $e_{i_1}e_{i_2}\cdots e_{i_n}$, for n even (resp., n odd).

3.4.3. *The Clifford and Spin groups.* From this point on assume that B is non-degenerate. That is, if $x \in V$ and $B(x,y) = 0$ for all y then $x = 0$. Note that this doesn't preclude the existence of $x \neq 0$ such that $q(x) = 0$.

Given a quadratic space (V,q), put

$$G(V,q) = \{a \in \mathrm{Cliff}(V,q)^\times : a^{-1}Va = V\}.$$

Further, let

$$G^+(V,q) = G(V,q) \cap \mathrm{Cliff}(V,q)^+.$$

We call $G(V,q)$ the **Clifford group** and $G^+(V,q)$ the **even Clifford group**.

Exercise 2. *Prove that $G(V,q)$ and $G(V,q)^+$ are algebraic groups over k.*

For $a \in G(V,q)$ define $\tau(a) \in \mathrm{GL}(V)$ by

$$x\tau(a) = a^{-1}xa, \qquad (x \in V).$$

Linear transformation will act here on the right so that we have $\tau(ab) = \tau(a)\tau(b)$ and we get a homomorphism

$$G(V,q) \to \mathrm{GL}(V).$$

In fact, the image of this homomorphism is in the orthogonal group $\mathcal{O}_q$:

$$\begin{aligned} q(x\tau(a)) &= (x\tau(a))^2 \\ &= (a^{-1}xa)^2 \\ &= a^{-1}q(x)a \\ &= q(x). \end{aligned}$$

Therefore, we have a homomorphism of algebraic groups:

$$G(V,q) \to \mathcal{O}_q.$$

Suppose that $x \in V$ is invertible in $\mathrm{Cliff}(V,q)$, then also $x^2 = q(x)$ is invertible and so $q(x) \neq 0$. Conversely, if $q(x) \neq 0$ then x is invertible in $\mathrm{Cliff}(V,q)$ and the inverse is $q(x)^{-1} \cdot x$. Thus, the elements of V that are invertible in $\mathrm{Cliff}(V,q)$ are precisely the anisotropic vectors - the vectors x with $q(x) \neq 0$. Such vectors v are contained in $G(V,q)$ as for any $u \in V$, $v^{-1}uv = v^{-1}(2B(u,v) - vu) = 2B(u,v) \cdot q(v)^{-1} \cdot v - u \in V$; Therefore, a product of an even number of such vectors is in $G(V,q)^+$. It is a theorem that $G(V,q)^+$ consists of all the products of an even number of elements of V that are invertible in $\mathrm{Cliff}(V,q)$, namely products of an even number of anisotropic vectors (see below).

Define a function

$$\nu : G(V,q)^+ \to k^*, \qquad \nu(a) = aa^*.$$

If $a = x_1 x_2 \dots x_{2r}$, $x_i \in V, q(x_i) \neq 0$, then

$$\nu(a) = q(x_1)q(x_2)\cdots q(x_{2r}).$$

Thus, ν is a group homomorphism. We define the **spin group** of (V,q) by

$$\mathrm{Spin}(V,q) = \{a \in G(V,q)^+ : \nu(a) = 1\}.$$

It is an algebraic group and we have a homomorphism

$$\tau : \mathrm{Spin}(V,q) \to \mathcal{O}_B.$$

One can show that the kernel of τ on $G(V,q)^+$ is precisely k^*. Since $k^* \cap \mathrm{Spin}(V,q) = \{\pm 1\}$, there is an injection,

$$\mathrm{Spin}(V,q)/\{\pm 1\} \hookrightarrow \mathcal{O}_q.$$

The truth is the following. The image of $\mathrm{Spin}(V,q)$ is $S\mathcal{O}_q$ and so one obtains an exact sequence:

$$1 \to \{\pm 1\} \to \mathrm{Spin}(V,q) \to S\mathcal{O}_q \to 1. \tag{3.4.1}$$

This is an exact sequence over $\bar{k}$, and so is also an exact sequence of algebraic groups. In order to understand why the sequence is exact we need to go deeper into the structure of the orthogonal group and the spin group.

3.4.4. *Reflections.* Let $x \in V$ with $q(x) \neq 0$. Let $x^\perp = \{v \in V : B(x,v) = 0\}$. We have the orthogonal decomposition

$$V = k \cdot x \oplus x^\perp.$$

There is a unique element of $\mathcal{O}_q$ taking x to $-x$ and acting as the identity on $x^\perp$; we call it a **reflection in** $x^\perp$. In fact, this linear transformation is $-\tau(x)$. Indeed, if $v \in x^\perp$

then $xv = -vx$ and so $-v\tau(x) = -x^{-1}vx = -x^{-1}(-x)v = v$ and, of course $-x^{-1}xx = -x$. We note that $\det(-\tau(x)) = -1$.

Every element of $\mathcal{O}_q$ is a product of reflections. This can be proved by an elementary argument using induction on the dimension of q.[3] Let us also admit that the intersection of the center of $\mathrm{Cliff}(V,q)$ with $\mathrm{Cliff}(V,q)^+$ is k.[4] If $\tau(x) = 1_V$ then x commutes with any element of V and so x is in the center of $\mathrm{Cliff}(V,q)$ and a fortiori in the center of $\mathrm{Cliff}(V,q)^+$; that is, $x \in k^\times$. Now, let $a \in G(V,q)^+$. Then we may write $\tau(a) = \tau(x_1)\cdots\tau(x_m)$ for some $x_1, \ldots, x_m$ in V. It follows that $a = (cx_1)\cdots x_m$ for some $c \in k^*$ and we see that every element of $G(V,q)^+$ is a product of elements of V. Because $a \in G(V,q)^+$, it follows directly from the definition of the canonical automorphism that m is even, $m = 2r$. Since $\det(-\tau(a)) = \prod \det(-\tau(y_i)) = -1^{2r} = 1$, we conclude that $\mathrm{Spin}(V,q)$ maps into $S\mathcal{O}_q$.

Let us assume that k is algebraically closed (it suffices that it contains all square roots of $q(V)$). Then, further, if $\nu(a) = 1$, we may assume that $a = y_1\cdots y_{2r}$, $y_i \in V$, and that $\nu(y_i) = 1$ for $i > 1$. It then follows that $\nu(y_1) = 1$ as well. It follows that *every element a of* $\mathrm{Spin}(V,q)$ *is a product of an even number of elements $y_i \in V$ with* $\nu(y_i) = q(y_i) = 1$.

On the other hand, since every element in $S\mathcal{O}_q$ is a product of an even number of reflections, each of the form $-\tau(x)$, where wlog $q(x) = 1$, it follows that it is the image of an element in $\mathrm{Spin}(V,q)$.

3.5. **The symplectic group.** Let V be an even dimensional vector space over a field k of characteristic different from 2. A symplectic form on V is an alternating perfect pairing

$$\langle\cdot,\cdot\rangle : V \times V \to k.$$

There's always a basis $\{x_1, \ldots, x_n, y_1, \ldots, y_n\}$ of V such that in this basis $\langle y_i, y_j\rangle = \langle x_i, x_j\rangle = 0$ and $\langle x_i, y_j\rangle = \delta_{ij}$. (Thus, any two such pairings are equivalent under a suitable change of basis.) In this basis the form is given by a $2n \times 2n$ matrix of the form

$$J := \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix}.$$

[3]For the proof, see Jacobson, Part I, p. 371, or Shimura. In fact, every element of the orthogonal group of q is a product of atmost n reflections. The proof is in Jacobson, Part I, p. 372; this statement is called the Cartan-Dieudonné theorem.

[4]Choose an orthonormal basis $\{e_1, \ldots, e_n\}$ for V and let $\delta = e_1e_2\cdots e_n$. Then:

(1) If $n > 0$ is even then the center of $\mathrm{Cliff}(V,q)$ is k and the center of $\mathrm{Cliff}(V,q)^+$ is $k + k\delta$.
(2) If n is odd then the center of $\mathrm{Cliff}(V,q)$ is $k + kz$ and the center of $\mathrm{Cliff}(V,q)^+$ is k.

(See Shimura, Theorem 2.8)

Some prefer to reorder the basis elements such that the pairing is given by

$$\begin{pmatrix} & & & & 0 & \cdots & 0 & 1 \\ & & & & 0 & \cdots & 1 & 0 \\ & & & & & \iddots & & \\ & & & & 1 & & & 0 \\ 0 & \cdots & 0 & -1 & & & & \\ 0 & \cdots & -1 & 0 & & & & \\ & \iddots & & & & & & \\ -1 & & & 0 & & & & \end{pmatrix}.$$

The **symplectic group** $\mathrm{Sp}(2n, k)$ are the linear transformations T of V preserving this pairing. In terms of matrices, these are the matrices M such that

$$^tMJM = J.$$

There is an injective homomorphism

$$\mathrm{GL}_n \to \mathrm{Sp}_{2n}, \qquad A \mapsto \begin{pmatrix} A & \\ & {}^tA^{-1} \end{pmatrix}.$$

The image is a closed subgroup of Sp_{2n}, consisting of all symplectic matrices $\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)$ ($n \times n$ matrices), such that $B = C = 0$. There is also an injective homomorphism

$$\mathbb{G}_a^{n(n+1)/2} \to \mathrm{Sp}_{2n}, \qquad B \mapsto \begin{pmatrix} I & B \\ & I \end{pmatrix},$$

where $\mathbb{G}_a^{n(n+1)/2}$ is interpreted as symmetric matrices of size n. The symplectic group is generated by the the image of $\mathbb{G}_a^{n(n+1)/2}$, the image of GL_n and the matrix $\left(\begin{smallmatrix} 0 & I \\ -I & 0 \end{smallmatrix}\right)$.

Let $u \in V$ be a non-zero vector and $c \in k$. Then the function

$$\tau_{u,c} v \mapsto v + c\langle v, u\rangle \cdot u$$

is a symplectic automorphism of V, called a **transvection**. One can prove (Jacobson, Part I, p. 392) that the symplectic group is generated by transvections. Note that if k is algebraically closed, or just closed under taking square roots, we can simply take $c = 1$ by the cost of replacing u by $\sqrt{c} \cdot u$. Note the formula

$$\eta \tau_{u,c} \eta^{-1} = \tau_{\eta u, c}, \qquad \eta \in \mathrm{Sp}_{2n}.$$

—— ◇ ——