RATIONAL ORBIT DECOMPOSITIONS OF PREHOMOGENEOUS VECTOR SPACES

AKIHIKO YUKIE

ABSTRACT. In this course we consider rational orbit decompositions of some prehomogeneous vector spaces, especially those which are related to field extensions.

CONTENTS

Date: June 15, 2000.
1991 *Mathematics Subject Classification.* Primary ; Secondary .
Key words and phrases. field extensions, prehomogeneous vector spaces, Galois cohomology.

1. Introduction

In this course we consider rational orbit decompositions of prehomogeneous vector spaces. Roughly speaking, a prehomogeneous vector space is a vector space on which a nice group acts with an open orbit. We shall define the notion of prehomogeneous vector spaces more precisely later. We try to explain what we are trying to do by a few examples in this introduction.

Let k be a field of characteristic not equal to two. We consider isomorphism classes of extensions of k of degrees up to two. Such fields are of the form $k(\sqrt{\alpha})$ where $\alpha \in k^\times$. Two such fields $k(\sqrt{\alpha})$, $k(\sqrt{\beta})$ are isomorphic if and only if there exists $t \in k^\times$ such that $\alpha = t^2\beta$. Consider the action of $k^\times$ on the 1-dimensional vector space k defined by $t \cdot \alpha = t^2\alpha$. So for each "generic point" $\alpha \neq 0$, we can consider a field $k(\sqrt{\alpha})$ and its isomorphism class is determined by the orbit of α under the action of the group $k^\times$. Note that if k is an algebraically closed field, for any $\alpha, \beta \in k^\times$, there exists $t \in k^\times$ such that $t^2 = \alpha\beta^{-1}$. So it is more interesting to consider this orbit space *rationally* over the ground field k. This is why we consider orbit decompositions of prehomogeneous vector spaces rationally over the ground field.

We consider another example. Recall that $\mathrm{GL}(n)$ is the group of invertible $n \times n$ matrices. If we consider $\mathrm{GL}(n)$ over a commutative ring R with 1, we use the notation $\mathrm{GL}(n)_R$. Let k be a field again and consider the action of $k^\times \times \mathrm{GL}(2)_k$ on the vector space V of binary cubic forms. Elements of V are expressed as

$$x = x(v) = x_0v_1^3 + x_1v_1^2v_2 + x_2v_1v_2^2 + x_3v_2^3, \tag{1.1}$$

where v_1, v_2 are variables and $x_i \in k$ for all i. We denote $x = (x_0, x_1, x_2, x_3)$ also. The action of $(t, g) \in k^\times \times \mathrm{GL}(2)_k$ on x is defined by $x(v) \to tx(vg)$ regarding $v = (v_1, v_2)$ as a row vector

For any x, we can associate the field extension $k(x)$ of k generated by the roots of x. Let $\alpha_1, \alpha_2, \alpha_3$ be the roots of $x(v)$, i.e.,

$$x(v) = x_0(v_1 - \alpha_1v_2)(v_1 - \alpha_2v_2)(v_1 - \alpha_3v_2).$$

Then $k(x)$ is generated by $\alpha_1, \alpha_2, \alpha_3$ and is a splitting field of a (possibly reducible) cubic equation. We only consider x with distinct roots. We denote the set of x with distinct roots by V_k^{ss}. Points in this set are "generic" in some sense. It turns out that in this case also, the orbit space $(k^\times \times \mathrm{GL}(2)_k)\backslash V_k^{\mathrm{ss}}$ corresponds bijectively with isomorphism classes of splitting fields of cubic equations.

For simplicity we only consider the case when the splitting field becomes a Galois extension of k with the Galois group $\mathfrak{S}_3$ ($\mathfrak{S}_n$ is the group of permutations of $\{1, \cdots, n\}$). It is obvious that any such field is of the form $k(x)$. Suppose $x = (x_0, x_1, x_2, x_3)$, $y = (y_0, y_1, y_2, y_3) \in V_k^{\mathrm{ss}}$ and $k(x) = k(y)$. Applying an element of the group to x, we may assume that $x_0 = 1$. Let $\alpha_1, \alpha_2, \alpha_3$ (resp. $\beta_1, \beta_2, \beta_3$) be roots of $x(v)$ (resp. $y(v)$). Since $\alpha_1, \alpha_2, \alpha_3$ are conjugate, we may assume that $k(\alpha_1) = k(\beta_1)$. Put $\alpha = \alpha_1, \beta = \beta_1$. Since $[k(\alpha) : k] = 3$, there exist $a_0, a_1, a_2 \in k$ such that $\beta = a_0\alpha^2 + a_1\alpha + a_2$.

We try to find $A, B, C, D \in k$ such that $\beta = (C\alpha + D)^{-1}(A\alpha + B)$. Suppose $a_0 \neq 0$. Let $C, D \in k$. Then

$$\begin{aligned}(C\alpha + D)\beta &= Ca_0\alpha^3 + (Ca_1 + Ba_0)\alpha^2 + (Ca_2 + Da_1)\alpha + Da_2 \\ &= (Ca_1 + Da_0 - Ca_0x_1)\alpha^2 + A\alpha + B,\end{aligned}$$

where $A = Ca_2 + Da_1 - Ca_0x_2,\ B = Da_2 - Ca_0x_3$. Since $a_0 \neq 0$, we may choose C, D so that $Ca_1 + Da_0 - Ca_0x_1 = 0$. If $a_0 = 0$, we may put $C = 0,\ D = 1,\ A = a_1,\ B = a_2$.

We put $g = \left(\begin{smallmatrix} A & C \\ B & D \end{smallmatrix}\right)$. If $\det g = 0$, $\beta \in k$, which is a contradiction. So $\det g \neq 0$. Consider $z(v) = x(vg^{-1})$. Let $w = \begin{pmatrix} w_1 & w_2 \end{pmatrix} = vg^{-1}$. If $\gamma_1, \gamma_2, \gamma_3$ are roots of $z(v)$, the corresponding w_1/w_2's are $\alpha_1, \alpha_2, \alpha_3$. Since

$$v = w \begin{pmatrix} A & C \\ B & D \end{pmatrix} = \begin{pmatrix} Aw_1 + Bw_2 & Cw_1 + Dw_2 \end{pmatrix},$$

roots of $z(v)$ are $\beta_1, \beta_2, \beta_3$.

Since $y(v), z(v)$ have the same roots, there exists $t \in k^\times$ such that $y(v) = tz(v) = tx(vg^{-1})$. This proves that y is in the orbit of x.

In this manner, we parametrized quadratic fields and cubic fields. But why do we want to do this? One reason is that this kind of problems of parametrizing mathematical objects are called moduli problems and are considered fundamental problems in any field of mathematics. Besides that there is a more concrete reason why we consider such parametrizations.

For each of the above cases, we can define the "zeta function" which counts the objects in question. We will not discuss the zeta function in this course. However, we point out that one can prove the following statements by considering the zeta functions for the above cases.

For simplicity, we consider the case $k = \mathbb{Q}$. For a number field k, we denote its discriminant by Δ_k.

Theorem 1.2.

$$\lim_{X \to \infty} \frac{1}{X} \sum_{\substack{[k:\mathbb{Q}]=2 \\ |\Delta_k| \leq X}} 1 = \frac{1}{\zeta(2)}.$$

Theorem 1.3. (Davenport–Heilbronn)

$$\lim_{X \to \infty} \frac{1}{X} \sum_{\substack{[k:\mathbb{Q}]=3 \\ |\Delta_k| \leq X}} 1 = \frac{1}{\zeta(3)}.$$

This kind of theorems are called *density theorems* in analytic number theory. To prove the above theorems, parametrizations of quadratic and cubic extensions are very crucial. There are other reasons, but proving this kind of density theorems is one of the main reasons why we consider rational orbit decompositions of prehomogeneous vector spaces.

2. Review of algebra

In this section we review some notions in algebra which will be needed in this course.

We first review the notion of infinite Galois extensions.

Definition 2.1. A field extension K/F is called a *Galois extension* if K is a union of finite Galois extensions of F contained in K.

For example, for any field F the union F^{sep} of separable extensions of F contained in the algebraic closure $\bar{F}$ is called the separable closure of F and is a Galois extension of F.

If K/F is a Galois extension, the Galois group $\mathrm{Gal}(K/F)$ is defined as in the case of finite Galois extensions; it is the set of automorphisms of K fixing elements of F. We denote the action of the Galois group element g on $x \in K$ by x^g. We introduce the following topology on the Galois group $\mathrm{Gal}(K/F)$. Let $G = \mathrm{Gal}(K/F)$.

If $F \subset L \subset K$ is an intermediate field, we put $G_L = \mathrm{Gal}(K/L)$. We may regard $G_L = \{g \in G \mid x^g = x \text{ for } x \in L\}$. We define that a subset of G is open if it is a union of subsets of the form gG_L (called a translate of G_L) where $g \in G$ and $[L : F] < \infty$. It is easy to verify that this is indeed a topology. This topology is called the *profinite topology.* This topology is compatible with the group action and so G becomes a topological group. If $H \subset G$ is a closed subgroup, we put $K^H = \{x \in K \mid x^h = x \text{ for } h \in H\}$. If L is a finite Galois extension of F contained in K, $[G : G_L] = [L : F]$ and $G/G_L \cong \mathrm{Gal}(L/F)$. In particular, G/G_L is a finite group. We regard G/G_L as a discrete group, i.e., a topological group with the discrete topology.

The following theorem extends the Galois theory to infinite Galois extensions. Suppose K/F is a Galois extension.

Theorem 2.2. (1) *There is a bijective correspondence between intermediate fields $F \subset L \subset K$ and closed subgroups $H \subset G$ by the correspondence $L \to G_L$, $H \to K^H$.*

(2) *An intermediate field L is a Galois extension of F if and only if G_L is a closed normal subgroup of G. If so,* $\mathrm{Gal}(L/F) \cong G/G_L$ *as topological groups.*

(3) *The group G is the profinite completion of itself, i.e.,*

$$G = \varprojlim_{[L:F]<\infty} G/G_L$$

as topological groups.

(4) *The group G is totally disconnected and is compact.*

Next we review some notions in commutative algebra. In this course, we usually consider rings which are commutative and contain a field, say k. Such rings are called k-algebras. When we consider homomorphisms of k-algebras, we assume that the homomorphisms fix elements of k. If the field in question is obvious from the context, we may simply say algebras, algebra homomorphisms instead.

Let A be a k-algebra. An ideal $\mathfrak{p} \subset A$ is a primes ideal if $A/\mathfrak{p}$ is an integral domain. Let $I \subset A$ be an ideal. Then the radical of I is the following ideal

$$\sqrt{I} = \{a \in A \mid a^n \in I \text{ for some } n > 0\}.$$

It is known (see [16, p. 5]) that $\sqrt{I}$ is the intersection of all prime ideals containing I. The radical $\sqrt{(0)}$ of the zero ideal is called the radical of A. If $\sqrt{(0)} = (0)$, A is said to be *reduced*. Obviously, $A_{\mathrm{red}} = A/\sqrt{(0)}$ is reduced.

A finite sequence of $n+1$ prime ideals

$$\mathfrak{p}_0 \supsetneqq \mathfrak{p}_1 \supsetneqq \cdots \supsetneqq \mathfrak{p}_n \tag{2.3}$$

is called a prime chain of length n. Let $\mathfrak{p}$ be a prime ideal. The supremum of the lengths of prime chains with $\mathfrak{p}_0 = \mathfrak{p}$ is called the *height* of $\mathfrak{p}$ and is denoted by $\mathrm{ht}(\mathfrak{p})$. The *dimension* of A is defined to be the supremum of heights of prime ideals of A. It is also called the Krull dimension of A.

If A is a finitely generated integral domain over k, then it is known (see [16, p. 84]) that for any prime ideal $\mathfrak{p}$,

$$\dim(A/\mathfrak{p}) + \mathrm{ht}(\mathfrak{p}) = \dim(A).$$

Any ring which satisfies this property is said to be catenarian. So if A is a finitely generated integral domain over k, any maximal chain of prime ideals has the length n. Also if $a_1, \cdots, a_n \in A$ and $I = (a_1, \cdots, a_n)$, then

$$\dim(A/I) \geq \dim(A) - n.$$

Let A be a k-algebra, and M, N be A-modules. Let F be the set of all formal finite sums of the form

$$\sum_{i=1}^{\ell} a_i(m_i, n_i), \tag{2.4}$$

where $a_i \in A$, $m_i \in M$, and $n_i \in N$ for all i. We define an A-module structure on F in the obvious manner. Let

$$M \otimes_A N = F/\langle (am, n) - (m, an) \mid a \in A,\ m \in M,\ n \in N \rangle. \tag{2.5}$$

This module is called the *tensor product* of M, N and becomes an A-module again. When there is no confusion, we use the notation $M \otimes N$ also. We denote the class of (m, n) by $m \otimes n$. There are natural A-homomorphisms

$$i_1 : M \ni m \to m \otimes 1 \in M \otimes N,\ i_2 : N \ni n \to 1 \otimes n \in M \otimes N.$$

The tensor product is characterized by the following universal property.

Theorem 2.6. *Let V be an A-module, and $\phi : M \times N \to V$ be a map such that it is A-linear with respect to each factor and $\phi(am, n) = \phi(m, an)$ for all $a \in A$, $m \in M, n \in N$. Then there is a unique A-homomorphism $\psi : M \otimes N \to V$ such that $\psi(m \otimes n) = \phi(m, n)$.*

If $f : A \to B$ is an algebra homomorphism, B can be regarded as an A-module. For an A-module M, we may sometimes write $f_*(M)$, $M \otimes_f B$ instead of $M \otimes_A N$. This is because there may be many homomorphisms from A to B. If $h : M \to N$ is a homomorphism of A-module, the induced homomorphism $M \otimes_A B \to N \otimes_A B$ is denoted by $f_*(h)$ or $h \otimes \mathrm{id}_B$.

Consider a sequence of A-homomorphism between A-modules as follows.

$$\cdots \longrightarrow M_1 \xrightarrow{d_1} M_2 \xrightarrow{d_2} M_3 \xrightarrow{d_3} \cdots \tag{2.7}$$

We say that the sequence (2.7) is a *complex* if $d_{i+1} \circ d_i = 0$ for all i. If (2.7) is a complex, $\mathrm{Im}(d_i) \subset \mathrm{Ker}(d_{i+1})$. If $\mathrm{Ker}(d_{i+1}) = \mathrm{Im}(d_i)$ for all i, (2.7) is called an *exact sequence*. An exact sequence of the form

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0 \tag{2.8}$$

is called a short exact sequence.

It is known that given a short exact sequence (2.8) and an A-module N, the sequence

$$0 \longrightarrow M_1 \otimes N \longrightarrow M_2 \otimes N \longrightarrow M_3 \otimes N \longrightarrow 0 \tag{2.9}$$

is exact except for the injectivity of the first homomorphism (in other words *right exact*).

Definition 2.10. (1) An A-module N is *flat* if for any short exact sequence (2.8), the sequence (2.9) is exact.
(2) An A-module N is faithfully flat if it is flat and without assuming the exactness of the sequence (2.8), the exactness of (2.9) implies the exactness of (2.8).

The set A^n of column vectors of dimension n with entries in A has the obvious A-module structure. Modules of the form A^n are called free modules. Free modules are flat.

It is easy to verify that in the definition of flat or faithfully flat modules, one only has to consider finitely generated modules M_1, M_2, M_3. So if A is a field, any non-zero module is faithfully flat.

Now we discuss local rings.

Definition 2.11. A k-algebra A is called a *local ring* if it has a unique maximal ideal. If A, B are local rings, $\mathfrak{m}, \mathfrak{n}$ are their maximal ideals, and $f : A \to B$ is a homomorphism, then we say that f is a *local homomorphism* if $f(\mathfrak{m}) \subset \mathfrak{n}$.

A typical way a local ring arises is by localization at a prime ideal as we describe it as follows.

Let $S \subset A$ be a multiplicative subset (i.e., closed under multiplication). Consider pairs of the form (a, s) where $a \in A$ and $s \in S$. Two such pairs (a_1, s_1), (a_2, s_2) are defined to be equivalent if there exists $s_3 \in S$ such that $s_3(a_1 s_2 - a_2 s_1) = 0$. We denote the set of equivalence classes by $S^{-1}A$. We define a k-algebra structure on $S^{-1}A$ in the obvious manner. The k-algebra $S^{-1}A$ is called the *localization* of A by S. It is easy to see that $S^{-1}A = 0$ if and only if S contains 0.

If $f \in A$ and $S = \{f^n \mid n \in \mathbb{N}\}$, then we use the notation A_f instead of $S^{-1}A$. If $\mathfrak{p} \subset A$ is a prime ideal, $S = A \backslash \mathfrak{p}$ is a multiplicative subset. We use the notation $A_\mathfrak{p}$ instead of $S^{-1}A$. The localization $A_\mathfrak{p}$ is a local ring. For example, if A is the polynomial ring $k[x_1, \cdots, x_n]$ and $\mathfrak{p} = (x_1, \cdots, x_n)$, then $A_\mathfrak{p}$ consists of rational functions of the form $f(x)/g(x)$ where $g(0) \neq 0$. So we are considering functions defined around 0.

Finally we discuss the Hilbert Nullstellensatz, which is probably the most important subject in the theory of commutative algebra. There are a few versions, but the following form is the most convenient for our purposes. Suppose $k = \bar{k}$.

Theorem 2.12. *Let $A = k[x_1, \cdots, x_n]$, and $I \subset A$ an ideal. Then $\sqrt{I}$ is the intersection of all maximal ideals of A containing I. Moreover, all maximal ideals are in the form $(x_1 - a_1, \cdots, x_n - a_n)$ where $a_1, \cdots, a_n \in k$.*

The following corollary follows easily from the above theorem.

Corollary 2.13. *Let* $A = k[x_1, \cdots, x_n]$, *and* $\mathfrak{p} = (f_1(x), \cdots, f_m(x))$ *be a prime ideal. Let* $X = \{a \in k^n \mid \forall_i \; f_i(a) = 0\}$. *If* $f \in A$ *and* $f(a) = 0$ *for all* $a \in X$, *then* $f \in \mathfrak{p}$.

Exercise 2.14. Suppose N is a flat A-module. Then show that if (2.7) is exact, the sequence

$$\longrightarrow M_1 \otimes N \xrightarrow{d_1 \otimes \mathrm{id}_N} M_2 \otimes N \xrightarrow{d_2 \otimes \mathrm{id}_N} M_3 \otimes N \xrightarrow{d_3 \otimes \mathrm{id}_N} \cdots$$

is exact.

3. Review of schemes

We review the notion of schemes varieties in this section. Let k be a field, and A a k-algebra. As a set, we define

$$\operatorname{Spec} A = \{\mathfrak{p} \subset A \mid \mathfrak{p} \text{ is a prime ideal}\}. \tag{3.1}$$

We may regard $\operatorname{Spec} A_f$ as a subset of $\operatorname{Spec} A$ of prime ideals $\mathfrak{p}$ such that $f \notin \mathfrak{p}$. We define that a subset of $\operatorname{Spec} A$ is open if it is a union of subsets of the form $\operatorname{Spec} A_f$. This is indeed a topology on $\operatorname{Spec} A$ and is called the *Zariski topology.* It is easy to verify that $\operatorname{Spec} A$ is quasi-compact with respect to this topology, i.e., any open covering of $\operatorname{Spec} A$ has a finite subcovering. If A is noetherian, any open covering of an open set has a finite subcovering. Recall that a topological space is compact if it is quasi-compact and separable. Note that $\operatorname{Spec} A$ is not separable.

If $\mathfrak{p} \in \operatorname{Spec} A$ and $\{\mathfrak{p}\} \subset \operatorname{Spec} A$ is a closed subset, $\mathfrak{p}$ is called a *closed point.* If $F \subset \operatorname{Spec} A$ is a closed subset, there exists a subset $S \subset A$ such that

$$F = \operatorname{Spec} A \setminus (\cup_{f\in S} \operatorname{Spec} A_f).$$

If $\mathfrak{p} \in \operatorname{Spec} A$, $\mathfrak{p} \in F$ if and only if $f \in \mathfrak{p}$ for all $f \in S$. Let $I \subset A$ be the ideal generated by S. Then $\mathfrak{p} \in F$ if and only if $I \subset \mathfrak{p}$. If $\mathfrak{p}$ is a closed point, let $I \subset A$ be the ideal corresponding to $\{\mathfrak{p}\}$. If $\mathfrak{q} \in \operatorname{Spec} A$ and $\mathfrak{p} \subset \mathfrak{q}$, then $I \subset \mathfrak{q}$. This implies that $\mathfrak{q} \in \{\mathfrak{p}\}$ and so $\mathfrak{q} = \mathfrak{p}$. Therefore, $\mathfrak{p}$ is a maximal ideal. It is easy to verify the converse also. This shows that a point $\mathfrak{p} \in \operatorname{Spec} A$ is a closed point if and only if it is a maximal ideal.

Definition 3.2. If $X = \operatorname{Spec} A$ and $I \subset A$ is an ideal, we denote the set of prime ideals $\mathfrak{p}$ such that $I \subset \mathfrak{p}$ by $V(I)$. We call $V(I)$ the *zero set* of I.

By the above argument, $V(I)$ is a closed subset.

It is not convenient to consider $\operatorname{Spec} A$ only as a topological space. One reason is that two algebras A, B may not be isomorphic but $\operatorname{Spec} A, \operatorname{Spec} B$ may be homeomorphic. Roughly speaking, the set $\operatorname{Spec} A$ and the topology may not carry enough algebraic information. So around each point, we consider algebraic functions defined around the point, thus arriving at the notion of *sheaves.* For simplicity, we only consider sheaves of algebras. It is defined as a contravariant functor $\mathscr{A}$ from the set of open subsets $U \subset X$ to the category of algebras $\mathscr{A}(U)$.

The collection of all algebras is not a set because it is too big and so such a collection is called a category. A correspondence involving categories is called a functor instead of a function. Any element of $\mathscr{A}(U)$ is called a section over U. If $U = X$, it is called a global section. The word "contravariant" means that whenever there is an inclusion $U \subset U'$, there is a map called the *restriction* $\mathscr{A}(U') \ni s \to s|_U \in \mathscr{A}(U)$. If $U \subset U' \subset U''$ and $s \in \mathscr{A}(U'')$, then $(s|_{U'})|_U$ must be $s|_U$.

Definition 3.3. A sheaf of algebras on a topological space X is a contravariant functor $\mathscr{A}$ from the set of open subsets $U \subset X$ to the category of algebras $\mathscr{A}(U)$ satisfying the following compatibility condition:

(*) Suppose $U_i \subset X$ is an open set for all i and $U = \cup_i U_i$. If $s_i \in \mathscr{A}(U_i)$ is given for all i and $s_i|_{U_i\cap U_j} = s_j|_{U_i\cap U_j}$, then there exists a unique $s \in \mathscr{A}(U)$ such that $s|_{U_i} = s_i$ for all i.

This definition is not bad at all. For example, if $X = \mathbb{C}$, for any open set $U \subset \mathbb{C}$, we may consider the set $\mathscr{A}(U)$ of holomorphic functions on U. The set $\mathscr{A}(U)$ has a natural algebra structure over $\mathbb{C}$. If there is an inclusion $U \subset U'$, one can restrict the functions. If holomorphic functions are given locally and if they coincide on intersections, they of course define a holomorphic function on the union of open sets. So the above compatibility condition simply means that the sheaf is something like considering functions locally.

If $\mathscr{A}$ is a sheaf of algebras on a topological space and $x \in X$, the *stalk* of $\mathscr{A}$ at x is defined to be

$$\mathscr{A}_x = \varinjlim_{x \in U} \mathscr{A}(U).$$

If $U \subset X$ is an open set, $U \supset V \to \mathscr{A}(V)$ for open sets V is a sheaf on U. This sheaf is called the *restriction* of $\mathscr{A}$ to U and will be denoted by $\mathscr{A}|U$.

If $\mathscr{A}$ is a sheaf of algebras, one can define the notion of sheaves of $\mathscr{A}$-modules in a similar manner.

It is known that on $X = \operatorname{Spec} A$, there exists a sheaf of algebras $\mathcal{O}_X$ such that if $U = \operatorname{Spec} A_f$, $\mathcal{O}_X(U) = A_f$. Moreover, the stalk of $\mathcal{O}_X$ at $x = \mathfrak{p}$ is the local ring $A_\mathfrak{p}$. This $\mathcal{O}_X$ is called the *structure ring* of X. We denote the stalk at x by $\mathcal{O}_{X,x}$. The pair $(X, \mathcal{O}_X)$ is called an *affine scheme*. If M is an A-module, there exists a sheaf $\widetilde{M}$ of $\mathcal{O}_X$-modules such that if $U = \operatorname{Spec} A_f$, $\widetilde{M}(U) = M_f$.

We do not worry too much about this structure ring $\mathcal{O}_X$, but keep in mind that an affine scheme is not just a topological space. If $\mathfrak{p} \in X = \operatorname{Spec} A$, the quotient field of $A/\mathfrak{p}$ is denoted by $k(\mathfrak{p})$ and is called the quotient field of $\mathfrak{p}$. If $k(\mathfrak{p}) = k$, $\mathfrak{p}$ is called a k-rational point.

We consider examples of affine schemes. For simplicity, we assume that k is an algebraically closed field.

Example 3.4. Let $A = k[x_1, \cdots, x_n]$. Then any maximal ideal is in the form $\mathfrak{m} = (x_1 - a_1, \cdots, x_n - a_n)$ where $a_1, \cdots, a_n \in k$. We identify $\mathfrak{m} \in \operatorname{Spec} A$ with the point $(a_1, \cdots, a_n) \in k^n$. In this manner, maximal ideals can be regarded as ordinary points on k^n in this case. We denote $\operatorname{Aff}^n = \operatorname{Spec} k[x_1, \cdots, x_n]$ and call it the n-dimensional affine space.

Example 3.5. Let $A = \operatorname{Spec} k[x_1, \cdots, x_n]/I$ where $I = (f_1(x), \cdots, f_m(x))$ is an ideal. We consider maximal ideals of A again. If $\mathfrak{m} \subset A$ is a maximal ideal, it is in the form $\mathfrak{m}'/I$ where $I \subset \mathfrak{m}' \subset k[x_1, \cdots, x_n]$ is a maximal ideal. As above $\mathfrak{m}'$ is in the form $\mathfrak{m}' = (x_1 - a_1, \cdots, x_n - a_n)$. Then $\mathfrak{m}'$ contains I if and only if $f_1(a) = \cdots = f_m(a) = 0$. So maximal ideals in A can be regarded as ordinary points a on k^n satisfying the polynomial equations $f_1(a) = \cdots = f_m(a) = 0$.

Suppose $\phi : A \to B$ is an algebra homomorphism. Let $X = \operatorname{Spec} X$, $Y = \operatorname{Spec} B$. Then if $\mathfrak{p} \subset B$ is a prime ideal, $\phi^{-1}(\mathfrak{p})$ is a prime ideal of A. This defines a map $\phi^* : Y \to \operatorname{Spec} X$. If $f \in A$, $(\phi^*)^{-1}(\operatorname{Spec} A_f) = \operatorname{Spec} B_{\phi(f)}$. So ϕ^* is continuous. Moreover, if $U = \operatorname{Spec} A_f$, there is a natural homomorphism $\mathcal{O}_X(U) = A_f \to B_{\phi(f)} = \mathcal{O}_Y((\phi^*)^{-1}(U))$. This implies that for any open sets $U \subset X$, $V \subset (\phi^*)^{-1}(U)$, there is a homomorphism $\mathcal{O}_X(U) \to \mathcal{O}_Y(V)$. Therefore, if $\phi^*(y) = x$, then we have a homomorphism

$$\mathcal{O}_{X,x} \to \mathcal{O}_{Y,y}. \tag{3.6}$$

This is a local homomorphism between local rings. Intuitively, this means that if we pull back a function which is zero at x, we get a function which is zero at y.

The map $\phi^* : Y \to X$ together with homomorphisms $\mathcal{O}_X(U) \to \mathcal{O}_Y((\phi^*)^{-1}(U))$ is called a *morphism* of affine schemes. In general, a morphism from Y to X is a continuous function $Y \to X$ together with functorial homomorphisms $\mathcal{O}_X(U) \to \mathcal{O}_Y((\phi^*)^{-1}(U))$ such that if $\phi^*(y) = x$, then the induced homomorphism (3.6) is local.

A topological space X with a sheaf of algebras $\mathscr{A}$ is a scheme if it has an open covering $X = \cup U_i$ such that U_i with the restriction of $\mathscr{A}$ to U_i is an affine scheme for all i. Morphisms between schemes are defined locally also.

In the case of affine schemes, it turns out that morphisms always arise from algebra homomorphisms $A \to B$. Roughly speaking, this is because A, B are the set of global sections on X, Y respectively, and by pulling back global sections, one get global sections, thus getting a homomorphism $A \to B$. It is in principle a straight forward argument to show that the morphism is induced by this homomorphism. In general the following proposition holds (see Ch. II, §§1–2 [20]).

Theorem 3.7. *Let $X = \operatorname{Spec} A$ be an affine k-scheme, and Y any k-scheme. Then morphisms $Y \to X$ are in bijective correspondence with k-homomorphisms $A \to \mathcal{O}_Y(Y)$.*

Example 3.8. Let $A = k[x_1, \cdots, x_n]$, $B = k[y_1, \cdots, y_m]$. If $\phi : A \to B$ is an algebra homomorphism, ϕ is determined by $f_1(y) = \phi(x_1), \cdots, f_n(y) = \phi(x_n)$. if $\mathfrak{m} = (y_1 - a_1, \cdots, y_m - a_m)$, $\phi^{-1}(\mathfrak{m}) = (x_1 - f_1(a), \cdots, x_n - f_n(a))$. Therefore, if we only consider maximal ideals, ϕ^* is the map

$$a \to (f_1(a), \cdots, f_n(a)).$$

Conversely, if there is a morphism $\Phi : \operatorname{Spec} B \to \operatorname{Spec} A$, by considering pull backs of global sections, we get a homomorphism $\phi : A \to B$, and it turns out that $\Phi = \phi^*$.

Example 3.9. Let A be a k-algebra, and $B = k[\epsilon]/(\epsilon^2)$. Put $X = \operatorname{Spec} A$, $Y = \operatorname{Spec} B$. The algebra B is called the ring of dual numbers. The only prime ideal of B is $\mathfrak{m} = (\epsilon)/(\epsilon^2)$. Suppose $\phi : A \to B$ is an algebra homomorphism. Then $\phi^*(Y)$ consists of a single point $\mathfrak{p} = \phi^{-1}(\mathfrak{m})$, which is a maximal ideal. Note that $A/\mathfrak{p} \cong k$. Since $\epsilon^2 = 0$ in B, $\mathfrak{p}^2 \subset \operatorname{Ker}(\phi)$. So to give ϕ is the same as to give a homomorphism $A/\mathfrak{p}^2 \to B$. If $t \in \mathfrak{p}$, we write $\phi(t) = \ell(t)\epsilon$. Then $t \to \ell(t)$ is k-linear. Conversely any k-linear map $t \to \ell(t)$ defines a homomorphism $\phi : A/\mathfrak{p}^2 \to B$. Therefore, morphisms from Y to X are in one-to-one correspondence with pairs $(\mathfrak{p}, \ell)$ where $\mathfrak{p} \in X$ such that $A/\mathfrak{p} \cong k$ and $\ell \in (\mathfrak{p}/\mathfrak{p}^2)^*$ (the dual vector space). If $x = \mathfrak{p}$, the vector space $T(X)_x = (\mathfrak{p}/\mathfrak{p}^2)^*$ is called the *tangent space* of X at x. The above consideration shows that the tangent space at $\mathfrak{p}$ is in one-to-one correspondence with the set of morphisms $\psi : \operatorname{Spec} B \to \operatorname{Spec} A$ such that $\psi((\epsilon)/(\epsilon^2)) = \mathfrak{p}$.

Let $x = \mathfrak{p} \in \operatorname{Spec} A$ be a point such that $k(x) = k$. We give an alternative definition of $T(X)_x$. Let $\pi_x : A \to k(x) = k$ be the natural map. A map $D : A \to k(x)$ is called a k-derivation if $D(t) = 0$ for all $t \in k$ and

$$D(fg) = D(f)\pi_x(g) + \pi_x(f)D(g).$$

If D is as above, $D(\mathfrak{p}^2) = 0$ since $\pi_x(\mathfrak{p}) = 0$. So D can be regarded as a map from $A/\mathfrak{p}^2$ to k. Since $D(t) = 0$ for all $t \in k$, D is determined by its restriction to $\mathfrak{p}/\mathfrak{p}^2$. It is easy to verify that this defines a bijective correspondence between k-derivations as above and the dual space of $\mathfrak{p}/\mathfrak{p}^2$. Therefore, we may regard $T(X)_x$ as the space of derivations.

Suppose $A = k[x_1, \cdots, x_n]/I$ where $I = (f_1(x), \cdots, f_N(x))$ and $I \subset \mathfrak{m} = (x_1 - a_1, \cdots, x_n - a_n)$. The tangent space at $\mathfrak{m}$ is the set of homomorphisms $\phi : A \to k[\epsilon]/(\epsilon^2)$ such that

$$\phi(x_i) = a_i + b_i \epsilon$$

for some $b_i \in k$ for $i = 1, \cdots, n$. Given $b_1, \cdots, b_n$, the above map is well defined if and only if $f_i(a_i + b_i \epsilon) = 0$. This condition can easily be written explicitly because $\epsilon^2 = 0$.

In general, let A be a noetherian local ring with maximal ideal $\mathfrak{m}$ and residue field $k = A/\mathfrak{m}$. Then $\mathfrak{m}/\mathfrak{m}^2$ is a vector space over k. Its dual space $(\mathfrak{m}/\mathfrak{m}^2)^*$ is called the tangent space. It is known that

$$\dim A \leq \dim_k (\mathfrak{m}/\mathfrak{m}^2)^*.$$

Definition 3.10. If the equation $\dim A = \dim_k (\mathfrak{m}/\mathfrak{m}^2)^*$ holds, A is called a *regular local ring.*

If X is a scheme and $x \in X$, we denote the tangent space of $\mathcal{O}_{X,x}$ by $T(X)_x$. This definition coincides with the above definition.

If $\mathcal{O}_{X,x}$ is a regular local ring, x is called a *non-singular point.* If x is not non-singular, it is called a *singular point.* If $X \to Y$ is a morphism of schemes and $f(x) = y$, it induces a linear map between the tangent spaces $T(X)_x \to T(Y)_y$. We denote this map by df.

Suppose $A \to B, C, D$ are algebra homomorphisms, and put

$$X = \operatorname{Spec} A, Y = \operatorname{Spec} B, Z = \operatorname{Spec} C, W = \operatorname{Spec} D.$$

Then there are morphisms $Y, Z, W \to X$. Suppose $B, C \to D$ are A-homomorphisms, which means that the diagrams

$$\begin{array}{ccc} A & \longrightarrow & B \\ \downarrow & & \downarrow \\ D & = & D \end{array} \qquad \begin{array}{ccc} A & \longrightarrow & C \\ \downarrow & & \downarrow \\ D & = & D \end{array}$$

are commutative. Then by the universal property of the tensor product, there is a unique homomorphism $B \otimes_A C \to D$ such that $B \to B \otimes_A C \to D$, $C \to B \otimes_A C \to D$ are the given maps. This in turn gives us a morphism $W \to \operatorname{Spec} B \otimes_A C$ such that $W \to \operatorname{Spec} B \otimes_A C \to Y$, $W \to \operatorname{Spec} B \otimes_A C \to Z$ are the given morphisms. Because of this universality, we denote $Y \times_X Z = \operatorname{Spec} B \otimes_A C$ and call it the fiber product of Y, Z over X, or the base change of the X-scheme Y with respect to the extension of the base $Z \to X$ (this can be said to Z also). We may use the notation $Y \times_A Z$ or $Y \times_A C$ also. This notion of product can be generalized to arbitrary schemes Y, Z over X.

If R is any k-algebra, the set of morphisms $\psi : \operatorname{Spec} R \to X \times_k R$ such that $\operatorname{Spec} R \to X \times_k R \to \operatorname{Spec} R$ is the identity map is denoted by X_R. Any morphism in

X_R is called an R-rational point of X. If $\mathfrak{p} \in X$, the natural map $A \to A/\mathfrak{p} \to k(\mathfrak{p})$ determines a $k(\mathfrak{p})$-rational point of X. For $f \in A$ and $x = \mathfrak{p}$, we denote the image of f in $k(\mathfrak{p})$ by $f(x)$ and call it the value of f at x.

If A is a finitely generated k-algebra and $X = \operatorname{Spec} A$, then X_k may be regarded as the set of elements in $X_{k^{\mathrm{sep}}}$ which are invariant under the action of the Galois group $\operatorname{Gal}(k^{\mathrm{sep}}/k)$.

If X_1, X_2 are closed subsets of an affine scheme such that $X_1 \not\subset X_2$, $X_2 \not\subset X_1$, and $X = X_1 \cup X_2$, then X is said to be *reducible*. If X is not reducible, it is said to be *irreducible*. By Zorn's lemma, every irreducible subspace is contained in a maximal one. It is easy to see that a maximal irreducible subspace of X is closed. Since a point is irreducible, X is a union of maximal irreducible subspaces. Maximal irreducible subspaces are called *irreducible components*.

If A is a k-algebra, then irreducible components of $\operatorname{Spec} A$ are in bijective correspondence with minimal prime ideals of A. If A is a noetherian, it is known (see COROLLARY [16, p. 56]) that $\sqrt{(0)}$ is an intersection of a finite number of prime ideals. Therefore, the number of minimal ideals is finite. This implies that $\operatorname{Spec} A$ has a finite number of irreducible components. If a scheme X is covered by a finite union of affine schemes, X is a finite union of irreducible components $X_1, \cdots, X_n$. We call $X = \cup_i X_i$ the irreducible decomposition of X.

If $X = \operatorname{Spec} A$ and A is reduced, X is said to be *reduced*. If a scheme is a union of reduced affine schemes, it is said to be reduced.

If a scheme is irreducible and reduced, it is said to be *integral*. If A is a k-algebra, $\operatorname{Spec} A$ is integral if and only if A is an integral domain.

Definition 3.11. Suppose X is a scheme.

(1) An open subscheme of X is a scheme U whose topological space is an open set of X and the structure ring is the restriction of $\mathcal{O}_x$ to U. If $Y \to X$ is an open subscheme, this morphism is called an *open immersion*.
(2) A closed subscheme of X is a scheme Y and a morphism $Y \to X$ such that the map between underlying topological spaces is an injective map to a closed subset of X and that if $x \in X$ maps to $y \in Y$, then the induced map between stalks $\mathcal{O}_{X,x} \to \mathcal{O}_{Y,y}$ is surjective. If $Y \to X$ is a closed subscheme, this morphism is called a *closed immersion*.

Note that if Y is a closed subscheme of X, there is a sheaf of ideals $\mathfrak{I}$ of $\mathcal{O}_X$ such that the structure ring of Y is the restriction of $\mathcal{O}_X/\mathfrak{I}$ to Y.

If $X = \operatorname{Spec} A$ and $F \subset X$ is a closed subset, there exists an ideal I such that $F = V(I)$ and A/I is reduced. Then $\operatorname{Spec} A/I$ is a closed subscheme of X whose underlying topological space is F. Unless otherwise stated, we consider the structure of the reduced closed subscheme for any closed subset of X. This may be generalized to closed subsets of arbitrary schemes. If X is a scheme, we denote the reduced scheme whose underlying topological space is X by X_{red}.

Definition 3.12. (1) If the diagonal morphism $X \to X \times_k X$ is a closed immersion, X is said to be *separated*.
(2) If X is a finite union of affine schemes of the form $\operatorname{Spec} A$ where A is a finitely generated algebra over k, then X is said to be of *finite type* over k.

The notion of separated schemes is an analogue of separable topological space. In Zariski topology, two open sets usually intersect and so it is not separable in the usual sense. However, if a scheme is separated, the following property holds and this is the reason why we consider this notion.

Proposition 3.13. *Suppose that X is a reduced scheme over k and Y is a separated scheme over k. Then if f, g are two morphisms from X to Y which coincide on a dense open subset of X, then $f = g$.*

We leave the proof of this proposition to the reader (Exercise 3.31).

If $X \times_k \bar{k}$ is irreducible (resp. integral), X is said to be *absolutely irreducible* (resp. *absolutely integral*). If X, Y are absolutely integral, $X \times_k Y$ is absolutely integral also and any $\bar{k}$-rational point of $X \times_k Y$ is in the form (x, y) where x, y are $\bar{k}$-rational points of X, Y respectively.

Definition 3.14. A variety over k is an absolutely integral separated k-scheme of finite type.

The following proposition is proved in 13.3 Corollary [2, p. 28].

Proposition 3.15. *If X is a variety over k, the set $X_{k^{\mathrm{sep}}}$ is Zariski dense in X.*

We now discuss projective varieties. Let $x_0, \cdots, x_n$ be variables.

Definition 3.16. We define the projective space $\mathbb{P}^n$ of dimension n to be the union of affine spaces

$$U_i = \operatorname{Spec} k\left[\frac{x_0}{x_i}, \cdots, \frac{x_n}{x_i}\right]$$

for $i = 0, \cdots, n$ such that

$$U_i \cap U_j = \operatorname{Spec} k\left[\frac{x_0}{x_i}, \cdots, \frac{x_n}{x_i}, \frac{x_i}{x_j}\right].$$

If $k = \bar{k}$, closed points in $\mathbb{P}^n$ are in bijective correspondence with equivalence classes of non-zero vectors $(x_0, \cdots, x_n) \in k^{n+1}$ where two vectors are identified if they are scalar multiples of each other.

If X is a closed subscheme of $\mathbb{P}^n$ and is a variety over k, it is called a projective variety. It is known that any affine scheme and any closed subscheme of $\mathbb{P}^n$ are separated (see Proposition 4.1, Theorem 4.9 [6, pp. 96,103]).

A very important property of projective varieties is that they are complete, which we shall now define.

Definition 3.17. A morphism $X \to Y$ is *closed* if the image of any closed subset is closed. A separated scheme of finite type over k is *complete* if for any scheme Y over k, the morphism $X \times_k Y \to Y$ is closed.

The following theorem is well known (see Theorem 4.9 [6, 103]).

Theorem 3.18. *Closed subschemes of $\mathbb{P}^n$ are complete.*

Remark 3.19. It is known that if X is a complete variety over $\mathbb{C}$, then $X_{\mathbb{C}}$ with the classical topology is compact.

Definition 3.20. A morphism $f : X \to Y$ is said to be finite if for any affine open subset $U = \operatorname{Spec} A \subset Y$, $f^{-1}(U) = \operatorname{Spec} B$ is affine and B is a finite A-module.

It is known that if $X = \operatorname{Spec} B$, $Y = \operatorname{Spec} A$ and B is an A algebra which is finite as an A-module, then $X \to Y$ is finite. If $X \to Y$ is a finite morphism, it is a closed map by Theorem 5 [16, p. 33]. If $X \to Y$ is finite, then for any Z, $X \times_k Z \to Y \times_k Z$ is finite. Therefore, we have the following proposition.

Proposition 3.21. *If $X \to Y$ is finite and Y is complete, then X is complete.*

Suppose $k = \bar{k}$, X is a variety, and $x \in X$. If $\mathcal{O}_{X,x}$ is a regular local ring, x is called a non-singular point. Otherwise, it is called a singular point. The following theorem is known (see Theorem 5.3 [6, p. 33]).

Theorem 3.22. *If X is a variety, then the set of singular points of X is a proper closed subset of X.*

We now discuss the dimension of schemes.

Definition 3.23. If X is a topological space, the (combinatorial) *dimension* of X is the supremum of the length n of chains

$$F_0 \subsetneqq F_1 \subsetneqq \cdots \subsetneqq F_n$$

of irreducible closed subspaces.

Let A be a k-algebra, and $X = \operatorname{Spec} A$. We discussed the notion of the dimension of a k-algebra A in section 2. Since irreducible closed subspaces of $\operatorname{Spec} A$ are in bijective correspondence with prime ideals,

$$\dim X = \dim A.$$

In particular, if A is a finitely generated algebra over k, $\dim X < \infty$. (It is known that there is a noetherian k-algebra A such that $\dim A = \infty$).

If $X = \operatorname{Spec} A, Y = \operatorname{Spec} B$ and A, B are finitely generated integral domains over k, we say that a morphism $f : X \to Y$ is dominant if the image of f is dense in Y. This condition is equivalent to the condition that the induced homomorphism $B \to A$ is injective. A subset of a topological space is called a *locally closed* subset if it is an intersection of an open subset and a closed subset. A finite union of locally closed subsets is called a *constructible set.* The following two theorems are well known.

Theorem 3.24. (See Theorem 6 [16, p. 42].) *The image $f(X)$ is a constructible set.*

Theorem 3.25. (See Theorem 52 [16, p. 156] and Proposition 7.5 [6, p. 256].) *If $f : X \to Y$ is dominant, there exists $f \neq 0$ such that B_f is flat as an A_f-module. If so, there exists a dense open subset $U \subset Y$ such that if $y \in U$, then*

$$\dim X = \dim Y + \dim f^{-1}(y).$$

Definition 3.26. Let $f : X \to Y$ be a morphism of schemes of finite type and $f(x) = y$. Let $\mathfrak{m}_x, \mathfrak{m}_y$ be the maximal ideals of $\mathcal{O}_{X,x}, \mathcal{O}_{Y,y}$.

(1) The morphism f is *flat at x* if $\mathcal{O}_{X,x}$ is a flat $\mathcal{O}_{Y,y}$ module.
(2) The morphism f is *unramified* at x if $\mathfrak{m}_{Y,y}\mathcal{O}_{X,x} = \mathfrak{m}_x$, and $k(x)/k(y)$ is a finite separable extension.
(3) The morphism f is *etale* at x if f is flat and unramified at x.

Let $f : X \to Y$ be a morphism of k-schemes of finite type, and $\Omega^1_{X/Y}$ the sheaf of relative differentials (for the notion of differentials, see II.8 [6] and Chapter 10 [16]).

Definition 3.27. The morphism f is *smooth* of relative dimension n if f is flat and for each point $y \in Y$, the absolute fiber $X \times_Y \overline{k(y)}$ ($\overline{k(y)}$ is the algebraic closure) is regular of equidimension n (the dimensions of all irreducible components are n).

An alternative definition (see Definition (1.1) [1, p. 128]) is that locally f is etale over an affine n-space over Y. It is easy to see that smoothness is preserved by base change. It satisfies the property of "faithfully flat descent" (see Corollary (5.11) [1, p. 154]). Therefore, if $f : X \to Y$ is a morphism between k-schemes of finite type, f is smooth if and only if the induced map $X \times_k \bar{k} \to Y \times_k \bar{k}$ is smooth. In particular, if X is a k-scheme, then X is smooth over k if and only if it is regular after changing the base to $\overline{k}$. With these in mind, the equivalence of the two definitions is proved in Theorem (1.8) [1, p. 130]. These definitions are equivalent to the one given in [6] also (see Theorem (10.2) [6, p. 269]).

Suppose that k is algebraically closed, and both X, Y are smooth over k. The following proposition is an important criterion of smoothness (see Corollary (5.5) [1, p. 149]).

Proposition 3.28. *A morphism $f : X \to Y$ is smooth if and only if for all $x \in X$, the induced map between the tangent spaces $T(X)_x \to T(Y)_{f(x)}$ is surjective*

Also if $f : X \to Y$ is smooth and X is smooth over k, then Y is smooth over k. One can see this in the following manner.

Let $f(x) = y$ and $h : X \to \mathrm{Aff}^n \times_k Y$ (Aff^n is the affine n-space) be an etale morphism in a neighborhood of x such that the composition with the projection to Y is f. Let $h(x) = (z, y)$, and $\mathrm{pr}_1, \mathrm{pr}_2$ be the projections from $\mathrm{Aff}^n \times_k Y$ to Aff^n, Y. Then by Proposition (4.9) [1, p. 117],

$$\Omega^1_{X/k} \cong h^*\Omega^1_{(\mathrm{Aff}^n \times_k Y)/k} \cong h^*(\mathrm{pr}_1^*\Omega^1_{\mathrm{Aff}^n/k} \oplus \mathrm{pr}_2^*\Omega^1_{Y/k})$$

in a neighborhood of x. Since f is surjective, it is easy to see that $\dim \Omega^1_{Y/k} \otimes k(y) = \dim Y$ for all $y \in Y$. Therefore, by the definition of smoothness in [6, p. 268], Y is smooth over k.

Exercise 3.29. Let $X = \operatorname{Spec} k[x, y, z, w]/(xw - yz)$. Describe the tangent space at $\mathfrak{m} = (x - 1, y - 1, z - 1, w - 1) \in X$.

Exercise 3.30. Find an example of an affine scheme X over a field k, which is non-singular everywhere and $X \times_k \bar{k}$ is singular.

Exercise 3.31. Prove Proposition 3.13.

4. Algebraic groups

We shall define and discuss examples of algebraic groups in this section. Basic references for the theory of algebraic groups are Borel [2], Springer [25], and Humphreys [9].

Definition 4.1. (1) A *group scheme* G over k is a a scheme of finite type over k with a section $e : \operatorname{Spec} k \to G$ called the identity, a morphism $\beta : G \to G$ called the inverse, and a morphism $\mu : G \times_k G \to G$ called the product which satisfies the usual group laws.

(2) If a group scheme G is a smooth variety over k, it is called an *algebraic group* over k.

In Definition 4.1(1) above, for example, $x \cdot x^{-1} = 1$ in usual groups correspond to the relation

$$\mu \circ (\mathrm{id}_G \times \beta) \circ \Delta = e \circ \pi$$

where $\Delta : G \to G \times_k G$ is the diagonal morphism and $\pi : G \to \operatorname{Spec} k$ is the canonical morphism.

If there is no confusion, we use the set theoretic notation such as $e \in G,\ g^{-1},\ g \cdot h$. We sometimes write 1 instead of e also. We sometimes say groups "defined over k" instead of groups over k.

Let $G = \operatorname{Spec} A$ be an algebraic group over k. If $A \to B$ is a k-algebra homomorphism, we define

$$\operatorname{Der}_k(A, B) = \left\{ D : A \to B \,\middle|\, \begin{matrix} D(f+g) = D(f) + D(g),\ D(t) = 0, \\ D(fg) = D(f)g + fD(g)\ \forall f, g \in A,\ t \in k \end{matrix} \right\}, \tag{4.2}$$

and call it the set of k-derivations from A to B.

Recall that if $x = \mathfrak{p} \in G$ and $f \in A$, $f(x) \in k(x)$ is the image of f in $k(x)$ by the natural map $A \to A/\mathfrak{p} \to k(\mathfrak{p}) = k(x)$. Let $\lambda_x : A \to A \otimes_k k(x)$ be the map defined by $(\lambda_x f)(y) = f(x^{-1}y)$. More precisely, it is the image of f by the map $A \to A \otimes A \to k(x) \otimes A \cong A \otimes k(x)$ where $A \to A \otimes A$ is the homomorphism which corresponds to $(x, y) \to x^{-1}y$. We define

$$L(G)_k = \{D \in \operatorname{Der}_k(A, A) \mid \lambda_x \circ D = D \circ \lambda_x \text{ for all } x \in G\} \tag{4.3}$$

In other words, $L(G)_k$ is the set of left invariant derivations of G.

If $D \in L(G)_k$, its composition with the evaluation at e ($A \ni f \to Df \to (Df)(e) \in k$) is a k-derivation from A to $k = k(e)$. This defines a map $L(G)_k \to T(G)_e$. The following proposition is well known.

Proposition 4.4. *If G is an algebraic group over k, the map $L(G)_k \to T(G)_e$ is bijective.*

We shall not prove this proposition. However, we point out that if $X \in T(G)_e$ the corresponding element $\theta(X) \in L(G)_k$ can be constructed as follows.

Let $\Delta : A \to A \otimes A$ be the homomorphism which corresponds to the multiplication $(x, y) \to xy$, $f \in A$, and $\Delta(f) = \sum_i f_i \otimes g_i$. Then define

$$\theta(X)(f) = \sum_i f_i(Xg_i).$$

It is shown in 3.4 Theorem [2] or in 4.4.5 Proposition [25] that θ is indeed the inverse of the natural map $L(G)_k \to T(G)_e$.

From now on, we identify $L(G)_k$ with $T(G)_e$. It is easy to see that if $D_1, D_2 \in L(G)_k$,

$$[D_1, D_2] = D_1 \circ D_2 - D_2 \circ D_1$$

is again an element of $L(G)_k$. The operation $[\ ,\ ]$ is obviously k-linear and $[D, D] = 0$ for all D. It is easy to verify that

$$[D_1, [D_2, D_3]] + [D_2, [D_3, D_1]] + [D_3, [D_1, D_2]] = 0 \tag{4.5}$$

for all D_1, D_2, D_3.

Any vector space L over k with a bilinear form $[\ ,\ ]$ such that $[D, D] = 0$ for all $D \in L$, satisfying the relation (4.5) is called a *Lie algebra* over k. The Lie algebra $L(G)_k = T(G)_e$ is called the Lie algebra of G. Notions such as homomorphisms, isomorphisms between Lie algebras, Lie subalgebras, are defined in the obvious manner. If $\mathfrak{g}$ is a Lie algebra and $\mathfrak{h} \subset \mathfrak{g}$ is a subspace, it is called an *ideal* if $[X, Y] \in \mathfrak{h}$ for all $X \in \mathfrak{g}$ and $Y \in \mathfrak{h}$.

In general, if R is a k-algebra, not necessarily commutative or even associative, one can define $\mathrm{Der}_k(R, R)$ and $[\ ,\ ]$ as before and call it the set of k-derivations. Then the operation $[\ ,\ ]$ satisfies the property (4.5) also. Therefore, $\mathrm{Der}_k(R, R)$ is a Lie algebra. The relation (4.5) implies that if $D \in L(G)_k$, the map $\mathrm{ad}(D) : L(G)_k \to L(G)_k$ defined by $\mathrm{ad}(D)(D_1) = [D, D_1]$ is a derivation with respect to the operation $[\ ,\ ]$. This $\mathrm{ad}(D)$ is called the *adjoint representation.*

If G_1, G_2 are group schemes over k, a homomorphism from G_1 to G_2 is a morphism $G_1 \to G_2$ such that if R is any k-algebra, $G_{1\,R} \to G_{2\,R}$ is set-theoretically a homomorphism of groups. Moreover, if $G_2 = \operatorname{Spec} A$ and $G_1 = \operatorname{Spec} A/I$ where $I \subset A$ is an ideal, we say G_1 is a subgroup scheme of G_2. If G_1, G_2 are algebraic groups and G_1 is a subgroup scheme of G_2, we say G_1 is a subgroup of G_2. If G_1, G_2 are subgroups and $G_1 \to G_2$ is a homomorphism, it induces a map

$$L(G_1)_k \cong T(G_1)_e \to T(G_2)_e \cong L(G_2)_k.$$

It turns out that this map is compatible with the bracket $[\ ,\ ]$ and so is a homomorphism of Lie algebras. If G_1 is a subgroup, the map $L(G_1)_k \to L(G_2)_k$ is injective and so $L(G_1)_k$ is a Lie subalgebra of $L(G_2)_k$.

Example 4.6. Let

$$\begin{aligned} \mathrm{GL}(n) &= \{g = (g_{ij}) \mid \det g \neq 0\} \\ &= \operatorname{Spec} k[t, g_{ij} \mid i, j]/(t \det(g_{ij}) - 1), \\ \mathrm{SL}(n) &= \{g = (g_{ij}) \mid \det(g_{ij}) = 1\}. \end{aligned} \tag{4.7}$$

Note that if we don't worry about t, the condition $t \det(g_{ij}) - 1 = 0$ is equivalent to the condition $\det(g_{ij}) \neq 0$. So if R is a k-algebra, the set $\mathrm{GL}(n)_R$ of R-valued points of $\mathrm{GL}(n)$ is the set of maps $\operatorname{Spec} R \to \operatorname{Spec} R[t, g_{ij} \mid i, j]/(t \det(g_{ij}) - 1)$, i.e. the set of $n \times n$ matrices whose determinants are invertible (rather than non-zero).

Consider the Lie algebra. Let $\mathrm{M}(m, n)$ be the set of $m \times n$ matrices. We regard $\mathrm{M}(m, n)$ as a variety over k. So if R is a k-algebra, $\mathrm{M}(m, n)_R$ is the set of $m \times n$ matrices with entries in R.

Consider the ring of dual numbers $k[\epsilon]/(\epsilon^2)$. If $A \in \mathrm{M}(n,n)_k$, $(I_n+\epsilon A)(I_n-\epsilon A) = I_n$. So $I_n+\epsilon A$ is always invertible and so the Lie algebra of $\mathrm{GL}(n)$ is $\mathrm{M}(n,n)$ as a set. It turns out that if $X,Y \in \mathrm{M}(n,n)_k$, $[X,Y] = XY-YX$. We denote the Lie algebras of $\mathrm{GL}(n)$, $\mathrm{SL}(n)$ by $\mathfrak{gl}(n)$, $\mathfrak{sl}(n)$.

Example 4.8. We define $\mathbb{G}_{\mathrm{a}} = \operatorname{Spec} k[t]$ and $\mathbb{G}_{\mathrm{m}} = \operatorname{Spec} k[t,t^{-1}]$ where the multiplication is defined by $t \to t\otimes 1 + 1\otimes t \in k[t]\otimes k[t]$, $t\otimes t \in k[t,t^{-1}]\otimes k[t,t^{-1}]$ respectively. These are abelian groups.

The groups $\mathbb{G}_{\mathrm{m}}$ and $\mathrm{GL}(1)$ are isomorphic, and the Lie algebra is abelian, i.e., if X,Y are any two elements of the Lie algebra, then $[X,Y]=0$. The group $\mathbb{G}_{\mathrm{a}}$ may be identified with the subgroup

$$\left\{ \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} \middle| u \in \mathrm{Aff}^1 \right\},$$

of $\mathrm{GL}(2)$ and the Lie algebra is identified with

$$\left\{ \begin{pmatrix} 0 & u \\ 0 & 0 \end{pmatrix} \middle| u \in \mathrm{Aff}^1 \right\}.$$

So the Lie algebras of both $\mathbb{G}_{\mathrm{a}}, \mathbb{G}_{\mathrm{m}}$ are the abelian 1-dimensional Lie algebra.

We consider a couple of examples of subgroups of $\mathrm{GL}(n)$ and consider their Lie algebras. Since we know the operation $[\ ,\ ]$ of $\mathrm{GL}(n)$, it is enough to determine the Lie algebra as a set for each case.

Example 4.9. Suppose $\operatorname{ch} k \neq 2$. Let Q be an $n\times n$ symmetric matrix such that $\det Q \neq 0$. We define

$$\begin{aligned} \mathrm{O}(Q) &= \{g=(g_{ij}) \mid gQ{}^tg = Q\}, \\ \mathrm{GO}(Q) &= \{g=(g_{ij}) \mid gQ{}^tg = c(g)Q \text{ for some } c(g)\neq 0\}. \end{aligned} \tag{4.10}$$

Let $gQ{}^tg = (p_{ij}(g))$ and $Q=(q_{ij})$. Then as a scheme, $\mathrm{GO}(Q)$ is defined as

$$\operatorname{Spec} k[t, g_{ij} \mid i,j]/(tp_{ij}(g) - q_{ij} | i,j). \tag{4.11}$$

If

$$Q = \begin{cases} \begin{pmatrix} 0 & 0 & I_m \\ 0 & -1/2 & 0 \\ I_m & 0 & 0 \end{pmatrix} & n = 2m+1, \\ \\ \begin{pmatrix} 0 & I_m \\ I_m & 0 \end{pmatrix} & n = 2m, \end{cases}$$

we use the notation $\mathrm{O}(n), \mathrm{GO}(n)$ instead of $\mathrm{O}(Q), \mathrm{GO}(Q)$. These are the "split forms" and some people denote them by $\mathrm{O}(m,m+1), \mathrm{O}(m,m)$, etc.

Consider the Lie algebra. If $A \in \mathrm{M}(n,n)$,

$$(I_n+\epsilon A)Q{}^t(I_n+\epsilon A) = Q + \epsilon(AQ + Q{}^tA).$$

So $I_n+\epsilon A$ is in the Lie algebra if and only if $AQ+Q{}^tA = 0$. We denote the Lie algebras of $\mathrm{O}(Q), \mathrm{GO}(Q), \mathrm{O}(n), \mathrm{GO}(n)$ by $\mathfrak{o}(Q), \mathfrak{go}(Q), \mathfrak{o}(n), \mathfrak{go}(n)$.

Example 4.12. Let J be a $2n \times 2n$ skew-symmetric matrix (${}^tJ = -J$) such that $\det J \neq 0$. We define

$$
\begin{aligned}
\mathrm{Sp}(J) &= \{g = (g_{ij}) \mid gJ^tg = J\}, \\
\mathrm{GSp}(J) &= \{g = (g_{ij}) \mid gJ^tg = c(g)J \text{ for some } c(g) \neq 0\}.
\end{aligned} \tag{4.13}
$$

If $J = \begin{pmatrix} & I_n \\ -I_n & \end{pmatrix}$, we use the notation $\mathrm{Sp}(2n), \mathrm{GSp}(2n)$ instead of $\mathrm{Sp}(J), \mathrm{GSp}(J)$.

Similarly as in Example 4.9, $I_n + \epsilon A$ is in the Lie algebra if and only if $AJ + J^tA = 0$. We denote the Lie algebras of $\mathrm{Sp}(2n), \mathrm{GSp}(2n)$ by $\mathfrak{sp}(2n), \mathfrak{gsp}(2n)$.

If G is an algebraic group over k, the connected component containing e is called the identity component and is denoted by G°. It is known (see [2, p. 47]) that $G^\circ \times_k \bar{k}$ is connected and so is absolutely irreducible (since it is smooth).

If $\mathrm{ch}\, k = 0$, there is a well known correspondence between subgroups and Lie subalgebras as follows,

Proposition 4.14. *Suppose* $\mathrm{ch}\, k = 0$ *and G is a connected algebraic group over k. If $H_1, H_2 \subset G$ are closed connected subgroups of G with the same Lie algebra, then $H_1 = H_2$.*

The above proposition is discussed in Chapter V [9].

Definition 4.15. Suppose X is a variety and G an algebraic group both defined over k. Then G acts from the left (resp. right) on X if there is a morphism $G \times_k X \to X$ which satisfies the usual axioms of left actions (resp. right actions).

Example 4.16. Let $G = \mathrm{GL}(n)$ and $X = \mathrm{Aff}^n$, We identify X with the space of column vectors. Then G acts on X from the left. In general, if G is an algebraic group and $G \to \mathrm{GL}(n)$ is a homomorphism, G acts on Aff^n. It is called a *representation* of G. If G is an algebraic group, any $g \in G_k$ induces an isomorphism $\mathrm{Int}(g) : G \ni h \to ghg^{-1}$. Since $\mathrm{Int}(g)(e) = e$, it induces a map $\mathrm{Ad}(g) : L(G)_k \to L(G)_k$. It turns out that $\mathrm{Ad}(g)$ is compatible with $[\ ,\ ]$ and so is a Lie algebra isomorphism. So $\mathrm{Ad}(g)$ defines a representation of G called the adjoint representation. Its differential $d\,\mathrm{Ad}$ is denoted by ad. and this is a Lie algebra representation from $\mathfrak{g}$ to $\mathfrak{gl}(\mathfrak{g})$. This is called the adjoint representation of $\mathfrak{g}$. It is proved in 3.14 [2, p. 70] that $\mathrm{ad}(X)(Y) = [X, Y]$ where $[X, Y]$ is the Lie bracket.

If $x \in X_k$,

$$G_x = \{g \in G \mid gx = x\} \tag{4.17}$$

makes sense as a group scheme and is called the *stabilizer* of x.

Example 4.18. Suppose $\mathrm{ch}\, k \neq 3$. Let $G = \mathrm{GL}(3)$. We consider the vector space V of cubic forms (i.e., homogeneous polynomials of degree three) in three variables $v = \begin{pmatrix} v_1 & v_2 & v_3 \end{pmatrix}$. We define an action of G on V by $f(v) \to f(vg)$. Let $F(v) = v_1^3 + v_2^3 + v_3^3$. We shall determine the Lie algebra of the stabilizer of $F(v)$.

Let $A = (a_{ij}) \in \mathrm{M}(3,3)_k$. Then

$$
\begin{aligned}
&v(I_3 + \epsilon A) \\
&= v + \epsilon \begin{pmatrix} a_{11}v_1 + a_{21}v_2 + a_{31}v_3 & a_{12}v_1 + a_{22}v_2 + a_{32}v_3 & a_{13}v_1 + a_{23}v_2 + a_{33}v_3 \end{pmatrix}.
\end{aligned}
$$

So

$$\begin{aligned} F(v(I_3+\epsilon A)) &= (v_1+\epsilon(a_{11}v_1+a_{21}v_2+a_{31}v_3))^3 \\ &\quad + (v_2+\epsilon(a_{12}v_1+a_{22}v_2+a_{32}v_3))^3 \\ &\quad + (v_3+\epsilon(a_{13}v_1+a_{23}v_2+a_{33}v_3))^3 \\ &= F(v)+3\epsilon(v_1^2(a_{11}v_1+a_{21}v_2+a_{31}v_3) \\ &\quad + 3\epsilon(v_2^2(a_{12}v_1+a_{22}v_2+a_{32}v_3) \\ &\quad + 3\epsilon(v_3^2(a_{13}v_1+a_{23}v_2+a_{33}v_3)). \end{aligned}$$

It is easy to verify that $(I_3+\epsilon A)$ is in the stabilizer if and only if $A=0$. Since $\dim G_F \leq \dim_k T(G_F)_e$, the stabilizer of $F(v)$ is a finite group.

We now discuss the notion of solvability. We first quote the following convenient proposition (see 1.4 Corollary [2, p. 47]).

Proposition 4.19. *If $f: G_1 \to G_2$ is a homomorphism between algebraic groups over k, then its image $f(G_1)$ is a closed subset. If we consider the reduced structure on $f(G_1)$, it becomes a closed subgroup of G_2 defined over k.*

Let G be an abstract group. If $H, F \subset G$ are subgroups, we denote the commutator subgroup of H, F by (H, F) (we do not use the notation $[H, F]$ to avoid confusion with the Lie algebra bracket). The derived series $(\mathscr{D}^n G)(n \geq 0)$; and the descending central series $(\mathscr{C}^n G)(n \geq 0)$ are defined inductively by

$$\begin{aligned} &\mathscr{D}^0 G = G, \quad \mathscr{D}^{n+1} G = (\mathscr{D}^n G, \mathscr{D}^n G),\ (n \geq 0), \\ &\mathscr{C}^0 G = G, \quad \mathscr{C}^{n+1} G = (G, \mathscr{C}^n G),\ (n \geq 0). \end{aligned}$$

By 2.3 Proposition [2, p. 58], $\mathscr{D}^n G, \mathscr{C}^n G$ are closed subsets of G for all n, and with the reduced structures, they become closed subgroups of G all defined over k. More precisely, we first consider $\mathscr{D}^n G, \mathscr{C}^n G$ set theoretically over $\bar{k}$. What is proved in 2.3 Proposition [2, p. 58] is that there exist subgroups in G such that after extending the base from k to $\bar{k}$, they become the subgroups $\mathscr{D}^n G, \mathscr{C}^n G$ with the reduced structures. By abuse of notation, we denote these groups over k by $\mathscr{D}^n G, \mathscr{C}^n G$.

Definition 4.20. We say that G is *solvable* (resp. *nilpotent*) if $\mathscr{D}^n G = \{e\}$ (resp. $\mathscr{C}^n G$) for some n

If $\mathfrak{g}$ is a Lie algebra over k, we define the solvability and nilpotency of $\mathfrak{g}$ by using the Lie bracket $[\ ,\ ]$ instead of the commutator $(\ ,\ )$.

In general, the Lie algebra of (G, G) may not coincide with $[\mathfrak{g}, \mathfrak{g}]$ (see 3.15 [2, pp. 70,71]). However, the following proposition is known (see 3.18 Corollary [2, p. 72]).

Proposition 4.21. *If G is a solvable (resp. nilpotent, abelian) algebraic group, then its Lie algebra $\mathfrak{g}$ is solvable (resp. nilpotent, abelian).*

If $H \subset G$ is a closed subgroup, we denote the normalizer and the centralizer by $N_G(H)$ and $Z_G(H)$. We use the notation $Z(G)$ for $Z_G(G)$. If $\mathfrak{h} \subset g$ is a Lie subalgebra, we define

$$\begin{aligned} \mathfrak{n}_{\mathfrak{g}}(\mathfrak{h}) &= \{X \in \mathfrak{g} \mid [X, Y] \in \mathfrak{h} \text{ for all } Y \in \mathfrak{h}\}, \\ \mathfrak{z}_{\mathfrak{g}}(\mathfrak{h}) &= \{X \in \mathfrak{g} \mid [X, Y] = 0 \text{ for all } Y \in \mathfrak{h}\}. \end{aligned}$$

The subalgebras $\mathfrak{n}_{\mathfrak{g}}(\mathfrak{h}), \mathfrak{z}_{\mathfrak{g}}(\mathfrak{h})$ are called the normalizer and the centralizer of $\mathfrak{h}$ respectively.

Exercise 4.22. Let p be a prime number and $\phi_p : \mathbb{G}_m \to \mathbb{G}_m$ be the homomorphism defined by $\phi_p(t) = t^p$. When is $\mathrm{Ker}(\phi_p)$ smooth over k?

Exercise 4.23. Describe $\mathrm{GO}(3)$ as a scheme explicitly.

Exercise 4.24. Consider the natural action of $\mathrm{GL}(6)$ on $\wedge^3 \mathrm{Aff}^6$. Determine the Lie algebra of the stabilizer of

$$w(v) = v_1 \wedge v_2 \wedge v_3 + v_4 \wedge v_5 \wedge v_6.$$

5. Quotients by algebraic groups

In this section we discuss the notion of quotients by algebraic groups. Let $G = \operatorname{Spec} A$ be an algebraic group, $X = \operatorname{Spec} B$ a variety over k which is absolutely integral, and $\mu : G \times_k X \to X$ an action of G on X. Let

$$\lambda, h : B \to A \otimes_k B$$

be the homomorphisms which correspond to μ and the projection p from $G \times_k X$ to X (i.e., $h(b) = 1 \otimes b$).

Definition 5.1. The ring of invariants in B is the following subring

$$B^G = \{b \in B \mid \lambda(b) = h(b)\}.$$

Lemma 5.2. *If $k \subset K$ is a field extension,*

$$(B \otimes_k K)^{G \times_k K} = B^G \otimes_k K.$$

Proof. Since $k \to K$ is flat,

$$\begin{aligned}
(B \otimes_k K)^{G \times_k K} &= \{\bar{b} \in B \otimes_k K \mid (\lambda \otimes \mathrm{id}_K)(\bar{b}) = h(\otimes \mathrm{id}_K)(\bar{b})\} \\
&= \{\bar{b} \in B \otimes_k K \mid ((\lambda - h) \otimes \mathrm{id}_K)(\bar{b}) = 0\} \\
&= \{b \in B \mid (\lambda - h)(b) = 0\} \otimes K \\
&= \{b \in B \mid \lambda(b) = h(b)\} \otimes_k K \\
&= B^G \otimes_k K.
\end{aligned}$$

□

As before, if $G_k \subset G$ is Zariski dense (for example if $k = \bar{k}$), we may consider B^G set-theoretically.

Let Y be a k-scheme. A morphism $X \to Y$ is G-invariant if the diagram

$$\begin{array}{ccc}
G \times_k X & \xrightarrow{\mu} & X \\
{\scriptstyle p}\big\downarrow & & \big\downarrow \\
X & \longrightarrow & Y
\end{array}$$

is commutative.

Definition 5.3. A scheme Y of finite type over k and a morphism $\pi : X \to Y$ is called a *categorical quotient* if π is G-invariant and any G-invariant morphism $X \to Z$ factors through Y uniquely.

Note that the categorical quotient is obviously unique. It is not necessarily a "good" quotient. It is generally considered that the geometric quotient is the good quotient. This notion is stronger than the notion of the categorical quotient and is defined as follows (see Definition 0.6 [21, p. 4]).

Definition 5.4. A scheme Y of finite type over k and a morphism $\pi : X \to Y$ is called a *geometric quotient* if

(1) π is G-invariant,
(2) For any $y \in Y$, the geometric fiber $\pi^{-1}(y) \times_{k(y)} \overline{k(y)}$ consists of a single orbit set-theoretically. (This implies that π is surjective.)

(3) a subset $U \subset Y$ is open if and only if $\pi^{-1}(U)$ is open,
(4) the structure sheaf $\mathcal{O}_Y$ is the subsheaf of $\mathcal{O}_X$ consisting of invariant functions.

The following proposition is Proposition 0.1 [21, pp. 4–5].

Proposition 5.5. *Suppose $\pi : X \to Y$ is a geometric quotient. Then it is a categorical quotient.*

Proof. Suppose $\psi : X \to Z$ is any G-invariant morphism. We construct a morphism $\chi : Y \to Z$ such that $\psi = \chi \circ \pi$. Let $\{V_i\}$ be any affine open covering of Z. Then for each i, $\psi^{-1}(V_i)$ is a G-invariant open subset of X. By the condition (2) of Definition 5.4, $\psi^{-1}(V_i) = \pi^{-1}(U_i)$ for some subset U_i of Y. But then by the condition (3) of Definition 5.4, U_i is an open subset.

Since π is surjective, $\{U_i\}$ is an open covering of Y, and any morphism $\chi : Y \to Z$ such that $\psi = \chi \circ \pi$ must satisfy $\chi(U_i) \subset V_i$. Since V_i is affine, morphisms $U_i, \psi^{-1}(V_i) \to V_i$ are in bijective correspondence with homomorphisms $\mathcal{O}_Z(V_i) \to \mathcal{O}_Y(U_i), \mathcal{O}_X(\psi^{-1}(V_i))$. Since ψ is G-invariant, for each i, the image of the homomorphism

$$\mathcal{O}_Z(V_i) \to \mathcal{O}_X(\psi^{-1}(V_i)) = \mathcal{O}_X(\pi^{-1}(U_i))$$

is contained in $\mathcal{O}_Y(U_i)$. Therefore, there exists a unique homomorphism $h_i : \mathcal{O}_Z(V_i) \to \mathcal{O}_Y(U_i)$ which makes the diagram

$$\begin{array}{ccc} \mathcal{O}_Z(V_i) & \xrightarrow{h_i} & \mathcal{O}_Y(U_i) \\ {\scriptstyle\psi^*}\downarrow & & \downarrow{\scriptstyle\pi^*} \\ \mathcal{O}_X(\psi^{-1}(V_i)) & = & \mathcal{O}_X(\pi^{-1}(U_i)) \end{array}$$

commutative where ψ^*, π^* are the homomorphisms corresponding to ψ, π respectively.

This h_i defines $\chi_i : U_i \to V_i$. Because of the uniqueness as above, χ_i and χ_j must coincide on $U_i \cap U_j$. This constructs χ. Since the restriction of χ to U_i is unique for all i, χ is unique. □

Because of the universality, if there exists a categorical quotient, it is unique. By the above proposition, if there exists a geometric quotient, it is unique also.

The following criterion is sometimes used to prove the existence of the categorical quotient.

Proposition 5.6. *Suppose $\pi : X \to Y$ is a morphism which satisfies the following conditions*

(1) *π is G-invariant,*
(2) $\mathcal{O}_Y = \mathcal{O}_X^G$,
(3) *if W is an invariant closed subset, then $\pi(W)$ is closed in Y. Also if $\{W_i \mid i \in I\}$ is a set of G-invariant closed subsets of X,*

$$\pi\left(\cap_{i\in I} W_i\right) = \cap_{i\in I} \pi(W_i).$$

Then the categorical quotient of X by G exists.

Proof. Note that π is dominant by (2), and so by (3), π is actually surjective.

Suppose $\psi : X \to Z$ is any G-invariant morphism. We proceed exactly as in the proof of Proposition 5.5. Choose an affine open covering $\{V_i\}$ of Z. Once we show that there is an open covering $\{U_i\}$ of Y such that $\pi^{-1}(U_i) \subset \psi^{-1}(V_i)$, we can conclude the proof as in Proposition 5.5.

To show this, let $W_i = X \setminus \psi^{-1}(V_i)$ for all i. These are G-invariant closed subsets of X. Therefore, by (3), $U_i = Y \setminus \pi(W_i)$ is open, and $\pi^{-1}(U_i) \subset \psi^{-1}(V_i)$ for all i.

Since $\cap_i W_i = \emptyset$, $\cap_i \pi(W_i) = \emptyset$ by (3). Hence, $\{U_i\}$ covers Y. $\square$

We shall define the notion of reductive groups in the next section. The following proposition is proved in Theorem 1.1, Theorem A.1.1 [21, pp. 27–29, 148–151] verifying the condition in Proposition 5.5.

Proposition 5.7. *If G is reductive,* $\operatorname{Spec} B^G$ *is the categorical quotient of X by G.*

In the above theorem, G does not have to be connected. We often have to consider quotients by subgroups. If $H \subset G$ is a subgroup, the following theorem is known (see 6.8 Theorem [2, pp. 98–99]).

Theorem 5.8. *If $H \subset G$ is a subgroup, the geometric quotient $H \backslash G$ exists and the morphism $G \to H \backslash G$ is smooth.*

Note that in the above proposition, H does not have to be connected. If H is reductive, we need the property that the quotient is affine in later sections. For that, we have to depend on Mumford's proof of the above proposition. The proof of the above proposition in characteristic $p > 0$ is based on the proof of Mumford's conjecture, proved by Haboush [5]. For the history of proofs, see [21, pp. 145–146]

Exercise 5.9. Assume that $\operatorname{ch} k \neq 2$. Express $\mathrm{PSL}(2), \mathrm{PGL}(2)$ explicitly as schemes.

6. Resume on semi-simple groups, etc.

In this section all algebraic groups are affine unless otherwise stated. The purpose of this section is to review slightly more advanced notions on algebraic groups such as semi-simple groups, reductive groups, and Borel subgroups. The main reason why we need these notions is that we have to describe automorphism groups of semi-simple groups in terms of inner automorphisms and automorphisms of Dynkin diagrams, which we shall describe later.

For that purpose we have to discuss Jordan decompositions in affine groups, which we shall do so now. Let V be a finite dimensional vector space over k regarded as a variety over k.

Definition 6.1. (1) An element $a \in \mathrm{End}(V)$ is said to be *nilpotent* if $a^n = 0$ for some $n > 0$.
(2) An element $a \in \mathrm{End}(V)$ is said to be *unipotent* if $a - \mathrm{id}_V$ is nilpotent
(3) An element $a \in \mathrm{End}(V)$ is said to be *semi-simple* if it is diagonalizable over $\bar{k}$.

It is known (see [2, pp. 79,80]) that if $a \in \mathrm{End}(V)_k$ is semi-simple, then it is diagonalizable over k^{sep}. If $p = \mathrm{ch}\, k > 0$, we put $\ell = k^{p^{-\infty}}$. The following proposition is well known (see [2, pp. 80,81]).

Proposition 6.2. *Let $a \in \mathrm{End}(V)_k$.*
(1) *There exist unique $a_s, a_n \in \mathrm{End}(V)_\ell$ such that a_s is semi-simple, a_n is nilpotent, $a_s a_n = a_n a_s$, and that $a = a_s + a_n$.*
(2) *There are polynomials $P(t), Q(t) \in \ell[t]$ such that $a_s = P(a)$, $a_n = Q(a)$.*
(3) *The elements a_s, a_n which satisfy the properties (1), (2) are unique.*

We call (1), the *additive Jordan decomposition* of a.

Corollary 6.3. *Let $g \in \mathrm{GL}(V)_k$ and $g = g_s + g_n$ be the additive Jordan decomposition of g. Put $g_u = \mathrm{id}_V + g_s^{-1} g_n$. Then $g = g_s g_u = g_u g_s$ with g_s semi-simple, g_u unipotent, and this is the unique factorization of this type.*

The above decomposition is called the *multiplicative Jordan decomposition* of g.

Let $G = \mathrm{Spec}\, A$ be an affine algebraic group over k with Lie algebra $\mathfrak{g}$. Let $g \in G_k$ and $X \in \mathfrak{g}_k$. In general, we have the following Jordan decompositions.

Theorem 6.4. (1) *There is a unique factorization $g = g_s g_u$ in G_ℓ such that if $\rho : G \to \mathrm{GL}(V)$ is any finite dimensional representation, then $\rho(g) = \rho(g_s)\rho(g_u)$ is the multiplicative Jordan decomposition of $\rho(g)$.*
(2) *There is a unique decomposition $X = X_s + X_n$ in $\mathfrak{g}_\ell$ such that if $\rho : \mathfrak{g} \to \mathfrak{gl}(V)$ is any finite dimensional Lie algebra representation, then $\rho(X) = \rho(X_s) + \rho(X_n)$ is the additive Jordan decomposition of $\rho(X)$.*

The following theorem is proved in 10.6 Theorem [2, pp. 137–140].

Theorem 6.5. *Suppose G is connected and solvable. Then the set G_u of unipotent elements of $G \times_k \bar{k}$ is a connected normal closed subgroup of $G \times_k \bar{k}$ containing $(G, G) \times_k \bar{k}$, defined over ℓ.*

Note that G_u may not be defined over k.

If G is an algebraic group over k and is isomorphic to a product of $\mathrm{GL}(1)^n$ for a certain n over $\bar{k}$, it is called an *algebraic torus*, or simply a torus. If G is an algebraic group, any homomorphism $G \to \mathrm{GL}(1)$ is called a character.

Definition 6.6. If G is an algebraic group, the set of characters of G is a group and is denoted by $X^*(G)$.

Definition 6.7. Let T be a torus.

(1) T is said to be *split* if T is isomorphic to $\mathrm{GL}(1)^n$ for a certain n over the ground field k.

(2) T is said to be *anisotropic* if $X^*(T) = \{1\}$.

It is known (see 8.11 Proposition [2, p. 117]) that if T is a torus, $T \times_k k^{\mathrm{sep}}$ is split. Moreover, for any torus T, $X^*(T) \cong \mathbb{Z}^m$ for some m (see Corollary 1 [2, p. 117]). If $T \cong \mathrm{GL}(1)^n$ over the ground field k, then $X^*(T) \cong \mathbb{Z}^n$ and any character is of the form $(t_1, \cdots, t_n) \to t_1^{p_1}, \cdots, t_n^{p_n}$. Since this is the case over $\bar{k}$ also,

$$X^*(T) \cong X^*(T \times_k \bar{k}).$$

If G is an algebraic group and a closed subgroup $T \subset G$ is isomorphic to a torus, it is called a subtorus. If T is a torus, then there exist subtori $T_a, T_d \subset T$ such that T_a is anisotropic, T_d is split, $T = T_a \cdot T_d$, and $T_a \cap T_d$ is finite. Moreover

$$T_a = \cap_{\chi \in X^*(T)} \mathrm{Ker}(\chi).$$

Also T/T_a is a split torus.

The following proposition is proved in 8.2 Proposition [2, pp. 111,112].

Proposition 6.8. (1) *If T is a torus and $H \subset T$ is a closed connected subgroup, then H is a torus.*

(2) *If $\rho : T \to \mathrm{GL}(n)$ is a finite dimensional representation, then there exists $g \in \mathrm{GL}(n)_{k^{\mathrm{sep}}}$ such that $g\rho(T)g^{-1}$ consists of diagonal matrices.*

Considering the dimension, there always exists a maximal torus. The following theorem is proved in 18.2, 19.2 Theorems [2, pp. 218–220,223].

Theorem 6.9. *Let G be connected. Then G contains a maximal torus T such that $T \times_k \bar{k} \subset G \times_k \bar{k}$ is also a maximal torus. Any two of them are conjugate by an element of G_k.*

Suppose G is connected and $S \subset G$ is a subtorus. It is known (see 11.2 Corollary [2, p. 152]) that the centralizer $Z_G(S)$ is connected. Let $T \subset G$ be a maximal torus as in Theorem 6.9. Then $Z_G(T)$ is called a *Cartan subgroup.* Also by 19.2 Theorem [2, p. 223], any two Cartan subgroups are conjugate by an element of G_k.

Definition 6.10. A maximal connected solvable closed subgroup of $G \times_k \bar{k}$ is called a *Borel subgroup.*

Note that G may not have a Borel subgroup defined over k and if it does, it is said to be *quasi-split.*

A very important property of Borel subgroups is that quotients by Borel subgroups are projective varieties. If $G = \mathrm{GL}(n)$, the subgroup B of upper triangular matrices is a Borel subgroup, and one can find an imbedding of G/B to a product of projective spaces in the following manner.

A sequence $(V_1, \cdots, V_n)$ of subspaces of Aff^n such that

$$0 \neq V_1 \subsetneqq V_2 \subset \cdots \subsetneqq V_n$$

is called a *flag*. Of course $\dim V_i = i$. If $W \subset \mathrm{Aff}^n$ is an i-dimensional subspace, it induces a map $\wedge^i W \to \wedge^i \mathrm{Aff}^n$. Its image is a line and so determines a point in $\mathbb{P}(\wedge^i \mathrm{Aff}^n)$. The set $\mathrm{Gr}(n, i)$ of points in $\mathbb{P}(\wedge^i \mathrm{Aff}^n)$ obtained in this manner is called the *Grassmann variety*. It is a smooth projective variety and points in $\mathrm{Gr}(n, i)$ are in bijective correspondence with i-dimensional subspaces of Aff^n.

Let $\mathscr{F}_n$ be the set of points

$$(V_1, \cdots, V_n) \in \mathrm{Gr}(n, 1) \times \cdots \times \mathrm{Gr}(n, n)$$

such that $V_1 \subset \cdots \subset V_n$. Then $\mathscr{F}_n$ becomes a closed subvariety of $\mathrm{Gr}(n, 1) \times \cdots \times \mathrm{Gr}(n, n)$, smooth over k. So flags in Aff^n are in bijective correspondence with points in $\mathscr{F}_n$, which is a projective variety. In particular, $\mathscr{F}_n$ is a complete variety. For details, see [2, pp. 135–137].

From now on until the end of Example 6.31, we assume that $k = \bar{k}$ unless otherwise stated. The following theorem is proved in 10.4 Theorem [2, p. 137].

Theorem 6.11. *Let G be a connected solvable group acting on a non-empty complete variety V. Then G has a fixed point in V.*

Let $G = \mathrm{GL}(n)$, $B \subset G$ be the subgroup of upper triangular matrices, and B' be another Borel subgroup. Then since G/B is complete, B' has a fixed point xB in G/B. This implies that $B'xB = xB$ or equivalently, $B' \subset xBx^{-1}$. By the maximality of Borel subgroups, $B' = xBx^{-1}$. Therefore, all Borel subgroups of $\mathrm{GL}(n)$ are conjugate.

Let G be an arbitrary connected affine group again. The above argument can be generalized to prove the following theorem. For the proof, see 11.1 Theorem [2, p. 147].

Theorem 6.12. *Let $B \subset G$ be a Borel subgroup. Then G/B is a projective variety. Moreover, all Borel subgroups of G are conjugate.*

Suppose G, G' are connected affine algebraic groups. Then the following proposition is proved in 11.14 Proposition [2, p. 152].

Proposition 6.13. (1) *Suppose $\alpha : G \to G'$ is a surjective homomorphism and $B = TB_u$ is a Borel subgroup of G with T a maximal torus. Then $\alpha(B) = \alpha(T)\alpha(B_u)$ is a Borel subgroup of G' and every such group is obtained in this way. Moreover, $\alpha(T)$ is a maximal torus and $\alpha(B_u) = \alpha(B)_u$.*

(2) *Suppose $G \subset G'$ is a subgroup and B is a Borel subgroup of G. Then there exists a Borel subgroup $B' \subset G'$ such that $B = (G \cap B')^\circ$. If G is a normal subgroup of G', then for any Borel subgroup $B \subset G'$, $B = (G \cap B')^\circ$ is a Borel subgroup of G.*

Definition 6.14. A closed subgroup $P \subset G$ is called a *parabolic subgroup* if it contains a Borel subgroup.

By Theorem 6.11, it is easy to see that P is parabolic if and only if G/P is complete. The following theorem is proved in [2, pp. 154,155].

Theorem 6.15. *If $P \subset G$ is a parabolic subgroup, it is connected and $N_G(P) = P$.*

By this theorem, in Proposition 6.13(2), we may replace $(G \cap B')^\circ$ by $G \cap B'$.

Let $\mathscr{B}$ be the set of all Borel subgroups of G. The group

$$R(G) = (\cap_{B \in \mathscr{B}} B)^\circ$$

is called the *radical* of G. It is the maximum connected solvable normal subgroup of G. Its unipotent part

$$(R(G))_u \text{ (sometimes denoted by } R_u(G))$$

is called the *unipotent radical* of G.

Definition 6.16. A connected group G is said to be *semi-simple* (resp. *reductive*) if $R(G) = \{e\}$ (resp. $R_u(G) = \{e\}$).

In general, not assuming k is algebraically closed, we say that G is semi-simple or reductive if $G^\circ \times_k \bar{k}$ is semi-simple or reductive.

Obviously, if G_1, G_2 are semi-simple (resp. reductive), $G_1 \times G_2$ is semi-simple (reductive).

There following proposition is sometimes convenient to prove that a group is semi-simple.

Proposition 6.17. *Let G be an algebraic group with Lie algebra $\mathfrak{g}$. If the bilinear form $\langle X, Y \rangle = \mathrm{tr}(\mathrm{ad}(X)\mathrm{ad}(Y))$ on $\mathfrak{g}$ is non-degenerate, G is semi-simple.*

Proof. Note that $R(G)$ is a connected normal solvable subgroup. So if $R(G) \neq \{e\}$, then the center H of $R(G)$ has a positive dimension. Then H is a normal subgroup of G. This implies that the Lie algebra $\mathfrak{h}$ of H is an abelian ideal of $\mathfrak{g}$.

If $X \in \mathfrak{h}$ and $Y, Z \in \mathfrak{g}$, then $\mathrm{ad}(X)\mathrm{ad}(Y)(Z) \in \mathfrak{h}$. So

$$\mathrm{tr}(\mathrm{ad}(X)\mathrm{ad}(Y)) = \mathrm{tr}(\mathrm{ad}(X)|_{\mathfrak{h}}\mathrm{ad}(Y)|_{\mathfrak{h}}) = \mathrm{tr}(\mathrm{ad}(Y)|_{\mathfrak{h}}\mathrm{ad}(X)|_{\mathfrak{h}}).$$

Since $\mathfrak{h}$ is abelian, this is zero. Since $\langle X, Y \rangle$ is non-degenerate, $X = 0$, which is a contradiction. Therefore, G is semi-simple. $\square$

Remark 6.18. The above bilinear form $\langle X, Y \rangle$ is called the *Killing form* of G or $\mathfrak{g}$. The group G can be semi-simple even when the Killing form is degenerate. If $\mathrm{ch}\, k = 0$, it is known that G is semi-simple if and only if the Killing form is non-degenerate.

Suppose G is reductive. It is known (see 11.21 Proposition [2, p. 158]) that $R(G) = Z(G)^\circ$ and this is a torus. We put $C = Z(G)^\circ$. Then $G = C \cdot (G, G)$, (G, G) is semi-simple, and $C \cap (G, G)$ is finite (see 14.2 Proposition [2, p. 181]). If T is a maximal torus with Lie algebra $\mathfrak{t}$, then $Z_G(T) = T$ and $\mathfrak{z}_{\mathfrak{g}}(\mathfrak{t}) = \mathfrak{t}$. This implies that Cartan subgroups of G are maximal tori (see 13.17 Corollary 2 [2, p. 175]).

Definition 6.19. We call $\dim T$ (resp. $\dim T \cap (G, G)$) the *rank* (resp. *semi-simple rank*) of G.

Let $T \to \mathrm{GL}(V)$ be a finite dimensional representation. Since $k = \bar{k}$, this representation is diagonalizable. For $\alpha \in X^*(T)$, define

$$V_\alpha = \{v \in V \mid t \cdot v = \alpha(t)v\}.$$

If $V_\alpha \neq \{0\}$, α is called a *weight* of T in V. We consider the adjoint action of T on $\mathfrak{g}$. Let Φ be the set of non-zero weights of T in $\mathfrak{g}$. Then

$$\mathfrak{g} = \mathfrak{t} \oplus \oplus_{\alpha \in \Phi} \mathfrak{g}_\alpha. \tag{6.20}$$

It is known that $\dim \mathfrak{g}_\alpha = 1$ for all $\alpha \in \Phi$.

Definition 6.21. The group $W(T,G) = N_G(T)/T$ is called the *Weyl group* of G.

Let $n \in N_G(T)$ and $\alpha \in X^*(T)$. We define $n(\alpha)(t) = \alpha(n^{-1}tn)$. This defines a left action of $W = W(T,G)$ on $X^*(T)$, and hence on $X^*(T) \otimes \mathbb{R}$. If $v \in \mathfrak{g}_\alpha$, then

$$\mathrm{Ad}(ntn^{-1})\mathrm{Ad}(n)v = \alpha(t)\mathrm{Ad}(n)v.$$

Replacing t by $n^{-1}tn$, we have

$$\mathrm{Ad}(n)\mathfrak{g}_\alpha \subset \mathfrak{g}_{n(\alpha)}.$$

So if $\alpha \in \Phi$, then $n(\alpha) \in \Phi$. Therefore, W leaves Φ stable.

Let $\alpha \in \Phi$. Then there exists a unique closed T-invariant subgroup U_α such that $L(U_\alpha) = \mathfrak{g}_\alpha$. Moreover, $U_\alpha \cong \mathbb{G}_a$. Let

$$T_\alpha = \mathrm{Ker}(\alpha)^\circ,\ G_\alpha = Z_G(T_\alpha).$$

Then G_α is a reductive subgroup of semi-simple rank one. Moreover, G_α is generated by $U_\alpha, U_{-\alpha}$, and T. Since

$$W(T,G_\alpha) = (N_G(T) \cap Z_G(T_\alpha))/T \subset W(T,G),$$

we regard $W(T,G_\alpha)$ as a subgroup of $W(T,G)$. The order of this group is two and if we denote the generator by r_α, then $r_\alpha(\alpha) = -\alpha$. For these, see 13.18 Theorem [2, p. 176].

If $\alpha, \beta \in \Phi$, it turns out (see 14.6 Corollary [2, p. 186]) that

$$r_\alpha(\beta) = \beta - n_{\beta,\alpha}\alpha$$

with $n_{\beta,\alpha} \in \mathbb{Z}$. Moreover, $n_{\alpha,\alpha} = 2$.

If V is a vector space over $\mathbb{R}$, $r \in \mathrm{GL}(V)$ is called a reflexion with respect to $\alpha \in V$ if $r(\alpha) = -\alpha$ and r fixes each point of a hyperplane.

Definition 6.22. A *root system* is a pair (V,Φ) where V is a vector space over $\mathbb{R}$, and $\Phi \subset V$ is a subset satisfying:

(1) Φ is finite, spans V, and does not contain zero.
(2) For each $\alpha \in \Phi$ there is a reflection r_α with respect to α which leaves Φ stable.
(3) If $\alpha, \beta \in \Phi$ then $r_\alpha(\beta) = \beta - n_{\beta,\alpha}\alpha$ with $n_{\beta,\alpha} \in \mathbb{Z}$. The elements of Φ are called *roots*.

The notion of isomorphisms of root systems is defined in the obvious manner. We usually denote the root system by Φ and say that "Φ is a root system in V." In particular, $\mathrm{Aut}\,(\Phi) \subset \mathrm{GL}(V)$. The subgroup $W(\Phi)$ of $\mathrm{Aut}\,(\Phi)$ generated by r_α for all $\alpha \in \Phi$ is called the *Weyl group* of Φ.

Let $\alpha \in \Phi$ be an element such that the only roots, $a\alpha$, proportional to α are such that $|a| \leq 1$. If $a\alpha$ is one such, then

$$-a\alpha = r_\alpha(a\alpha) = a\alpha - n_{n\alpha,\alpha}\alpha,$$

which implies that $2a = n_{a\alpha,\alpha} \in \mathbb{Z}$. Thus the roots proportional to α are either $\{-\alpha,\alpha\}$ or $\{-\alpha,-\alpha/2,\alpha/2,\alpha\}$. If the latter case never occurs, then the roots system is said to be *reduced.*

A basis of Φ is a subset Δ such that Δ is a basis of V, and that each root $\beta \in \Phi$ is a linear combination, $\beta = \sum_{\alpha\in\Delta} m_\alpha \alpha$ with m_α's integers of the same sign. We then define the set Φ^+ of positive roots to be the set of β for which all m_α's are non-negative. Thus Φ is a disjoint union of Φ^+ and $\Phi^- = -\Phi^+$. It is known that any root system has a basis (see 14.7 Theorem [2, p.188]).

The root system (V, Φ) is said to be irreducible if one cannot write $V = V_1 \oplus V_2$ as a non-trivial direct sum so that $\Phi = (\Phi \cap V_1) \cup (\Phi \cap V_2)$.

The following theorem is proved in 14.8 Theorem, [2, p. 189].

Theorem 6.23. *Suppose G is a connected semi-simple group and T is a maximal torus. Then $\Phi = \Phi(T, G)$ is a reduced root system in $V = X(T) \otimes \mathbb{R}$, with Weyl group $W = W(T, G)$.*

Let $B \subset G$ be a Borel subgroup containing T with Lie algebra $\mathfrak{b}$. Then $\mathfrak{t} \subset \mathfrak{b} \subset \mathfrak{g}$ and the set $\Phi(B)$ of non-zero weights of T in $\mathfrak{b}$ may be identified with a subset of Φ. Let $\Delta = \Delta(B)$ be the set of $\alpha \in \Phi(B)$ which is not a sum of two elements in $\Phi(B)$. Then the following corollary is proved in Corollary 1 [2, p. 189].

Corollary 6.24. *The subset Δ is a basis of Φ.*

We now discuss the relation between the Dynkin diagram and the automorphism group of semi-simple groups. This is what we need later in the consideration of stabilizers of generic points of prehomogeneous vector spaces.

Let (V, Φ) be a root system with Weyl group W. Let Δ be a basis. Since W leaves Φ invariant, W is a finite group. So we fix a W-invariant positive definite symmetric bilinear form $(\ ,\ )$. Then if $\alpha, \beta \in \Phi$,

$$n_{\beta,\alpha} = 2\frac{(\beta, \alpha)}{(\alpha, \alpha)}.$$

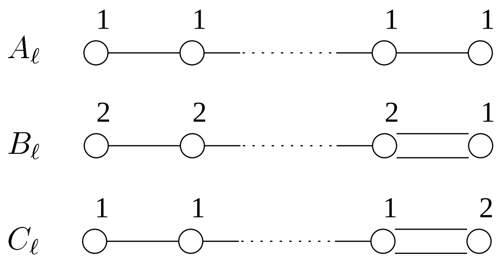
In fact, by the invariance of $(\ ,\ )$,

$$(\alpha, r_\alpha(\beta) + \beta) = (-\alpha, \beta + r_\alpha(\beta)).$$

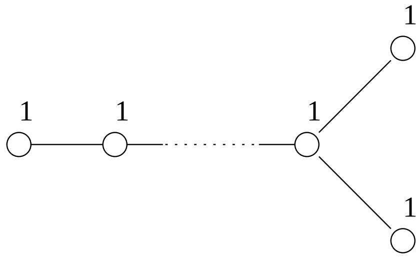
So $(\alpha, r_\alpha(\beta) + \beta) = 0$. The above relation follows easily from this equation.

We choose $(\ ,\ )$ so that the minimum of (α, α) for $\alpha \in \Delta$ is one. We associate to (V, Φ) the so called *Dynkin diagram*, which is a finite graph having Δ as its set of vertices in which $\alpha, \beta \in \Delta$ are joined by $n_{\alpha,\beta} n_{\beta,\alpha}$ edges. Moreover, each vertex α is weighted by (α, α).

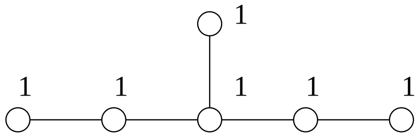
Dynkin diagrams give a complete classification of root systems. It is well known that Dynkin diagrams of irreducible reduced root systems are the following.



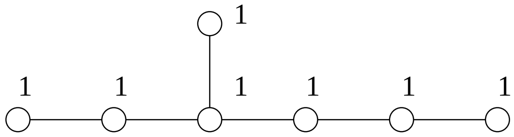
D_ℓ



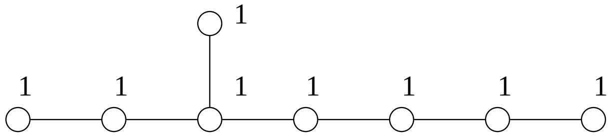
E_6



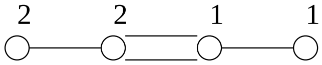
E_7



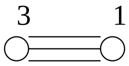
E_8



F_4



G_2



For the classification of irreducible reduced root systems and Dynkin diagrams, see Chapter X §3 [8, pp. 461–475]. It is known that $0 \leq n_{\alpha,\beta} n_{\beta,\alpha} \leq 3$ (without assuming that the root system is reduced). If $i = n_{\alpha,\beta} n_{\beta,\alpha}$ and $n_{\alpha,\beta} \geq n_{\beta,\alpha}$, then $(\alpha, \alpha) = i(\beta, \beta)$. Moreover, the angle between α, β is $\frac{2\pi}{3}, \frac{3\pi}{4}, \frac{5\pi}{6}$ for $i = 1, 2, 3$ respectively.

We give examples of semi-simple and reductive groups without proofs, except for $\mathrm{SL}(n)$, for which we shall prove later that it is semi-simple and that its Dynkin diagram is of type A_{n-1}.

Example 6.25. The following groups are semi-simple.

(1) $\mathrm{SL}(n)$ for $n \geq 2$: The Dynkin diagram is of type A_{n-1}.
(2) $\mathrm{O}(n)$ for $n \geq 3$ where $\mathrm{ch}\, k \neq 2$: The Dynkin diagram is of type $B_{(n-1)/2}$ if n is odd and $n \geq 5$, and is of type $D_{n/2}$ if n is even and $n \geq 8$.
(3) $\mathrm{Sp}(2n)$ for $n \geq 2$: The Dynkin diagram is of type C_n.

Example 6.26. All semi-simple groups are reductive. Moreover, the following groups are reductive.

(1) $\mathrm{GL}(n)$
(2) $\mathrm{GO}(n)$ where $\mathrm{ch}\, k \neq 2$
(3) $\mathrm{GSp}(2n)$

Assume G is connected semi-simple. As before, let T be a maximal torus and B a Borel subgroup containing T. In

$$A = \mathrm{Aut}\,(G),$$

let $\mathrm{Int}(G)$ be the group of inner automorphisms. Also write $A_{(B,T)}$ for the subgroup of elements of A stablizing both B and T. As we have discussed, $\Delta(B)$ is a basis of the root system $\Phi = \Phi(T, G)$. We shall write $\mathrm{Dyn}(\Phi, B)$ for the corresponding Dynkin diagram, and $\mathrm{Aut}\,(\mathrm{Dyn}(\Phi, B))$ for its automorphism group.

If $a \in A_{(B,T)}$, then since $a(T) = T$, a induces an automorphism of the root system Φ. Since $a(B) = B$, it leaves $\Delta(B)$ stable and hence defines an element $a' \in \mathrm{Aut}\,(\mathrm{Dyn}(\Phi, B))$. The following proposition is proved in 14.9 Proposition [2, p. 190].

Proposition 6.27. (1) $A = \mathrm{Int}(G) \cdot A_{(B,T)}$.

(2) $\mathrm{Int}(G) \cap A_{(B,T)}$ *is the kernel of the homomorphism*

$$A_{(B,T)} \to \mathrm{Aut}\,(\mathrm{Dyn}(\Phi, B)).$$

(3) *There is a natural injection*

$$A/\,\mathrm{Int}(G) \to \mathrm{Aut}\,(\mathrm{Dyn}(\Phi, B)).$$

In particular, $\mathrm{Int}(G)$ *has finite index in* A.

We now discuss a criterion for a connected group G to be reductive or semi-simple. Let G be a connected algebraic group, and $T \subset G$ a subtorus. We denote the Lie algebras of G, T by $\mathfrak{g}, \mathfrak{t}$.

Consider a weight decomposition of $\mathfrak{g}$ with respect to T such as (6.20). If $r \in N_G(T)$ and $\alpha \in \Phi$, then the element of $X^*(T)$ defined by $t \to \alpha(r^{-1}tr)$ is denoted by $r(\alpha)$. Note that $\mathrm{Ad}(r)\mathfrak{g}_\alpha = \mathfrak{g}_{r(\alpha)}$ and so $r(\alpha) \in \Phi$. Suppose G is imbedded in $\mathrm{GL}(n)$ for some n as a closed subgroup. Let $N^+ \subset \mathrm{GL}(n)$ (resp. $N^- \subset \mathrm{GL}(n)$) the subgroup of upper triangular matrices (resp. lower triangular matrices) with diagonal entries 1, and $\widetilde{T} \subset \mathrm{GL}(n)$ the subgroup of diagonal matrices. Then $B^+ = \widetilde{T}N^+$, $B^- = \widetilde{T}N^-$ are Borel subgroups of $\mathrm{GL}(n)$.

We consider the following assumption.

Assumption 6.28. (1) For all $\alpha \in \Phi$, $\dim \mathfrak{g}_\alpha = 1$.

(2) The set Φ does not contain 0.

(3) For any $\alpha \in \Phi$, $[\mathfrak{g}_\alpha, \mathfrak{g}_{-\alpha}] \neq 0$.

(4) For any $\alpha \in \Phi$, there exists $r_\alpha \in N_G(T)$ such that $r_\alpha(\alpha) = -\alpha$.

(5) The relation

$$(\cap_{\alpha \in \Phi} \mathrm{Ker}(\alpha))^\circ = \{e\}$$

holds.

Proposition 6.29. *If Assumption 6.28(1)–(4) is satisfied, then* T *is a maximal torus and* G *is reductive. If furthermore Assumption 6.28(5) is satisfied, then* G *is semi-simple.*

Proof. Suppose Assumption 6.28(1)–(4) is satisfied. Suppose $T \subset S$ is a maximal torus. If $T \neq S$, the Lie algebra $\mathfrak{s}$ of S strictly contains $\mathfrak{t}$. Since $S \subset Z_G(T)$, the adjoint representation of T on $\mathfrak{s}$ is trivial. Therefore, $\mathfrak{s}$ has no non-zero weights of T. Since Φ does not contain 0, this is a contradiction. Hence, T is a maximal torus.

Suppose $R_u(G) \neq \{e\}$. This is a connected, solvable, unipotent, and normal subgroup of G. Choose $n > 0$ so that $\mathscr{D}^n R_u(G) \neq \{e\}$ and $\mathscr{D}^{n+1} R_u(G) = \{e\}$. Then $H = \mathscr{D}^n R_u(G)$ is a connected, abelian, unipotent, and normal subgroup of G. Let $\mathfrak{h}$ be the Lie algebra of H. Since T is a torus, T is conjugate to a subgroup of $\widetilde{T}$. So $\mathfrak{t}$ consists of semi-simple elements. Since H is unipotent and abelian, H is conjugate to a subgroup of N^+. So $\mathfrak{h}$ consists of nilpotent elements. Therefore, $\mathfrak{t} \cap \mathfrak{h} = \{0\}$.

Since $\mathfrak{h} \neq \{0\}$, there exists $\alpha \in \Phi$ such that $\mathfrak{g}_\alpha \subset \mathfrak{h}$. Since H is a normal subgroup of G, $\mathrm{Ad}(r_\alpha)(\mathfrak{h}) = \mathfrak{h}$. Since $r_\alpha(\alpha) = -\alpha$, this implies that $\mathfrak{g}_{-\alpha} \subset \mathfrak{h}$. Since $[\mathfrak{g}_\alpha, \mathfrak{g}_{-\alpha}] \neq 0$, $\mathfrak{h}$ is not abelian, which is a contradiction. Hence, $R_u(G) = \{e\}$ and so G is reductive.

Suppose furthermore Assumption 6.28(5) is satisfied. Since G is reductive, $R(G) = Z(G)^\circ$. Since $Z(G)^\circ$ acts trivially on $\mathfrak{g}$ by the adjoint representation,

$$Z(G)^\circ \subset (\cap_{\alpha\in\Phi} \mathrm{Ker}(\alpha))^\circ = \{e\}.$$

Hence, $R(G) = \{e\}$ and so G is semi-simple. □

In the following proposition, we assume that Assumption 6.28(1)–(4) is satisfied. By the above proposition, G is reductive. So for any $\alpha \in \Phi$, there exists a subgroup $U_\alpha \cong \mathbb{G}_\mathrm{a}$ of G such that $L(U_\alpha) = \mathfrak{g}_\alpha$.

Proposition 6.30. *Suppose there exists a subset Φ^+ such that $\Phi = \Phi^+ \coprod (-\Phi^+)$. If $U_\alpha \subset B^+$ for all $\alpha \in \Phi^+$ and $T \subset \widetilde{T}$, then $G \cap B^+$ is a Borel subgroup of G (in particular, it is connected).*

Proof. Since $G \cap B^+$ contains U_α for all Φ^+ and T,

$$\mathfrak{t} \oplus \oplus_{\alpha\in\Phi^+} \mathfrak{g}_\alpha \subset L(G \cap B^+).$$

This implies that

$$\dim G \cap B^+ \geq \dim T + (1/2)(\dim G - \dim T).$$

Since G is reductive, this is the dimension of any Borel subgroup of G. Therefore, $(G \cap B^+)^\circ$ is a Borel subgroup of G. By the remark after Theorem 6.15, $G \cap B^+$ is connected. □

Example 6.31. As we promised earlier, we shall show that $\mathrm{SL}(n)$ is semi-simple using Proposition 6.28. Let $G = \mathrm{SL}(n)$. Let E_{ij} be the $n \times n$ matrix such that the (i,j)-entry is 1 and other entries are 0. We denote the diagonal matrix whose diagonal entries are $t_1, \cdots, t_n$ by $t = a_n(t_1, \cdots, t_n)$. Let T be the subgroup of G consisting of elements t such that $t_1 \cdots t_n = 1$. The group G is a subgroup of $\mathrm{GL}(n)$ in the obvious manner. Let $\mathfrak{g}, \mathfrak{t}, N^+, \widetilde{T}$, etc., be as in Propositions 6.28, 6.29. Let g_{ij} be the subspace of $\mathfrak{g}$ spanned by E_{ij}. Then

$$\mathfrak{g} = \mathfrak{t} \oplus \oplus_{i\neq j} \mathfrak{g}_{ij}.$$

Let $e_i \in X^*(T)$ be the character such that $e_i(t) = t_i$. We put $\alpha_{ij} = e_i - e_j$. Then $\mathrm{Ad}(t)(E_{ij}) = \alpha_{ij}(t) E_{ij}$. So $\mathfrak{g}_{ij} = \mathfrak{g}_{\alpha_{ij}}$. Obviously, $\mathfrak{g}_{ji} = \mathfrak{g}_{-\alpha_{ij}}$. It is easy to see that

$$[E_{ij}, E_{ji}] = E_{ii} - E_{jj} \neq 0$$

if $i \neq j$. We put

$$r_{\alpha_{ij}} = \sum_{l \neq i,j} E_{ll} + E_{ii} - E_{jj}.$$

Then $r_{\alpha_{ij}} \in N_G(T)$ and $r_{\alpha_{ij}}(\alpha_{ij}) = -\alpha_{ij}$. Since

$$\cap_{i \neq j} \mathrm{Ker}(\alpha_{ij}) = \{tI_n \mid t^n = 1\}.$$

So

$$(\cap_{i \neq j} \mathrm{Ker}(\alpha_{ij}))^\circ = \{e\}.$$

Therefore, Assumption 6.28(1)–(5) is satisfied. Hence, G is semi-simple.

Let $\Phi^+ = \{\alpha_{ij} \mid i < j\}$. Then the set of non-zero weights in $\mathfrak{g}$ is $\Phi = \Phi^+ \coprod (-\Phi^+)$. If $i < j$,

$$U_{ij} = \{I_n + uE_{ij} \mid u \in \mathbb{G}_a\}$$

is a subgroup such that $L(U_{ij}) = \mathfrak{g}_{\alpha_{ij}}$. So the condition in Proposition 6.29 is satisfied. Therefore, $B = TN^+$ is a Borel subgroup of G.

Let

$$\alpha_1 = \alpha_{12}, \cdots, \alpha_{n-1} = \alpha_{n-1\,n}.$$

Then $\Delta(B) = \{\alpha_1, \cdots, \alpha_{n-1}\}$ is a basis of the root system Φ. It is easy to see that

$$r_{\alpha_i}^{-1} t r_{\alpha_i} = a_n(t_1, \cdots, t_{i-1}, t_{i+1}, t_i, t_{i+2}, \cdots, t_n).$$

If $|j-i| \geq 2$, the j-th, and $(j+1)$-st components of $r_{\alpha_i}^{-1} t r_{\alpha_i}$ are t_j, t_{j+1}. So $r_{\alpha_i}(\alpha_j) = \alpha_j$. Since $r_{\alpha_i}(\alpha_{i+1})(t) = t_i t_{i+2}^{-1} = (\alpha_i + \alpha_{i+1})(t)$, $n_{\alpha_{i+1},\alpha_i} = -1$. Similarly, $n_{\alpha_i,\alpha_{i+1}} = -1$. So $n_{\alpha_i,\alpha_{i+1}} n_{\alpha_{i+1},\alpha_i} = 1$. This implies that the corresponding Dynkin diagram is of type A_{n-1}.

Let k be an arbitrary field again. Suppose G is a connected reductive group over k. For the rest of this section, we consider the structure of $X^*(G)$.

If G is semi-simple, then $Z(G)^\circ = R(G) = \{e\}$. So $\dim G = \dim(G, G)$. Therefore, $G = (G, G)$. This implies that $X^*(G) = \{0\}$.

In general, we put $G_1 = (G, G)$ and $T = G/G_1$. We denote the natural homomorphism $G \to T$ by π. Let $G_2 = \pi^{-1}(T_a)$. Put $\overline{T} = G/G_2 \cong T/T_a$. Then $\overline{T}$ is a split torus. If $\chi \in X^*(G)$, then it is trivial on G_2 and so it is induced by a character of $\overline{T}$. This implies that $X^*(G) \cong \mathbb{Z}^m$ for some m.

A character χ of an algebraic group is said to be *primitive* if ψ is another character and $\chi = \psi^p$ for an integer p, then $p = \pm 1$. If T is a torus, $\chi \in X^*(T)$ is primitive if and only if it is a primitive vector in $X^*(T) \cong \mathbb{Z}^m$.

Proposition 6.32. *Suppose G is connected reductive. If $\chi \in X^*(G)$ is primitive, then it is primitive in $X^*(G \times_k \bar{k})$.*

Proof. Suppose $\psi \in X^*(G \times_k \bar{k})$ and $\phi = \psi^p$. Since $\chi|_{G_2}$ is trivial, $(\psi|_{G_2 \times_k \bar{k}})^p$ is trivial. Since $X^*(G_2 \times_k \bar{k})$ is torsion free, $\psi|_{G_2 \times_k \bar{k}}$ is trivial. So ψ is induced by a character of $\overline{T}$. Since $\overline{T}$ is split,

$$X^*(\overline{T}) \cong X^*(\overline{T} \times_k \bar{k}).$$

Since χ corresponds to a primitive integer point, p must be ± 1. $\square$

Exercise 6.33. Prove that $\mathrm{SO}(n)$ is semi-simple for $n \geq 3$. Find the Dynkin diagram.

Exercise 6.34. Prove that $\mathrm{Sp}(2n)$ is semi-simple for $n \geq 2$. Find the Dynkin diagram.

Exercise 6.35. Prove that if $\mathrm{ch}\, k = 2$, the Killing form of $\mathrm{SL}(2)$ is identically zero.

7. Rational forms and Galois cohomology

In this section, we shall discuss how the Galois cohomology arises by considering rational forms of a variety, etc.

Definition 7.1. Let X/k be an algebraic object such as a variety, a scheme, an algebraic group, etc. If X, Y are two such objects and $X \times_k k^{\mathrm{sep}} \cong Y \times_k k^{\mathrm{sep}}$, we say Y is a *k-form* of X. If K/k is a separable algebraic extension, we also say that X is a k-form of $X \times_k K$.

We consider the following question.

Question 7.2. Describe k-isomorphism classes of k-forms of X.

In many cases, the answer turns out to be the following.

Answer 7.3. *The set of k-isomorphism classes of k-forms of X is in one-to-one correspondence with the first Galois cohomology set* $\mathrm{H}^1(k, \mathrm{Aut}\,(X))$.

The Galois cohomology set $\mathrm{H}^1(k, \mathrm{Aut}\,(X))$ shall be defined in Definition 7.10. We describe how $\mathrm{H}^1(k, \mathrm{Aut}\,(X))$ naturally arises by considering k-forms of X.

We assume that the action of $\mathrm{Gal}(k^{\mathrm{sep}}/k)$ on k^{sep} is a right action. In other words, if $\sigma, \tau \in \mathrm{Gal}(k^{\mathrm{sep}}/k)$ and $a \in k^{\mathrm{sep}}$, $\sigma\tau(a)$ is by definition $\tau(\sigma(a))$. We may write a^σ instead of $\sigma(a)$.

Let $Z = X \times_k k^{\mathrm{sep}}$. Then $\mathrm{Gal}(k^{\mathrm{sep}}/k)$ acts on Z. For example, if $X = \mathrm{Spec}\, R$, then $Z = \mathrm{Spec}\, R \otimes_k k^{\mathrm{sep}}$ and the action of $\sigma \in \mathrm{Gal}(k^{\mathrm{sep}}/k)$ is induced by the algebra homomorphism

$$\mu_X(\sigma) : R \otimes k^{\mathrm{sep}} \ni r \otimes a \to r \otimes a^{\sigma^{-1}} \in R \otimes k^{\mathrm{sep}}. \tag{7.4}$$

We denote the corresponding morphism $Z \to Z$ by $\nu_X(\sigma)$ $(= \mu_X(\sigma)^*)$.

Note that this is compatible with the set theoretic definition. For example, if $X = \mathrm{Spec}\, k[t]$, $Z_{k^{\mathrm{sep}}} = k^{\mathrm{sep}}$. The inverse image of the ideal $(t - a)$ by $\mu_X(\sigma)$ is $(t - a^\sigma)$. Therefore, it induces the map $Z_{k^{\mathrm{sep}}} \ni a \to a^\sigma \in Z_{k^{\mathrm{sep}}}$.

Proposition 7.5. (1) *The following diagram is commutative.*

$$\begin{array}{ccc} Z & \xrightarrow{\nu_X(\sigma)} & Z \\ \downarrow & & \downarrow \\ \mathrm{Spec}\, k^{\mathrm{sep}} & \xrightarrow{(\sigma^{-1})^*} & \mathrm{Spec}\, k^{\mathrm{sep}} \end{array}$$

(2) $\nu_X(\sigma\tau) = \nu_X(\tau) \circ \nu_X(\sigma)$.

Proof. The proof of (1) is easy. Since

$$\begin{aligned} \mu_X(\sigma)(\mu_X(\tau)(a \otimes r)) &= \mu_X(\sigma)(a \otimes r^{\tau^{-1}}) = a \otimes (r^{\tau^{-1}})^{\sigma^{-1}} = a \otimes r^{(\sigma\tau)^{-1}} \\ &= \mu_X(\sigma\tau)(a \otimes r), \end{aligned}$$

$$\nu_X(\sigma\tau) = (\mu_X(\sigma) \circ \mu_X(\tau))^* = \nu_X(\tau) \circ \nu_X(\sigma).$$

∎

Now we fix X. How do we classify k-forms Y of X? A natural idea is to compare the difference between ν_X and ν_Y. So for a k-form Y of X, we define

$$h_Y(\sigma) = \nu_Y(\sigma) \circ \nu_X(\sigma)^{-1}. \tag{7.6}$$

Note that the following diagram is commutative.

$$\begin{tikzcd}
Z \arrow[d] & Z \arrow[l, "\nu_X(\sigma)"'] \arrow[r, "\nu_Y(\sigma)"] \arrow[d] & Z \arrow[d] \\
\operatorname{Spec} k^{\mathrm{sep}} & \operatorname{Spec} k^{\mathrm{sep}} \arrow[l, "(\sigma^{-1})^*"'] \arrow[r, "(\sigma^{-1})^*"] & \operatorname{Spec} k^{\mathrm{sep}}
\end{tikzcd}$$

Therefore, the following diagram is commutative.

$$\begin{tikzcd}
Z \arrow[r, "h_Y(\sigma)"] \arrow[d] & Z \arrow[d] \\
\operatorname{Spec} k^{\mathrm{sep}} \arrow[r, equal] & \operatorname{Spec} k^{\mathrm{sep}}
\end{tikzcd}$$

So $h_Y(\sigma) \in \operatorname{Aut}_{k^{\mathrm{sep}}}(Z)$, and $h_Y(\sigma)$ is a k^{sep}-morphism.

Let's consider set theoretically now. For $z \in Z$, we write z^σ instead of $\nu_X(\sigma)(z)$. Note that ν_X is a right action. For $h \in \operatorname{Aut}_{k^{\mathrm{sep}}}(Z)$, we define

$$h^\sigma(z) = (h(z^{\sigma^{-1}}))^\sigma = \nu_X(\sigma) \circ h \circ \nu_X(\sigma^{-1})(z). \tag{7.7}$$

Then $h^\sigma \in \operatorname{Aut}_{k^{\mathrm{sep}}}(Z)$.

From now on, we may write h_1h_2 instead of $h_1 \circ h_2$ for $h_1, h_2 \in \operatorname{Aut}(Z)_{k^{\mathrm{sep}}}$.

Lemma 7.8. *For all $\sigma, \tau \in \operatorname{Gal}(k^{\mathrm{sep}}/k)$, $h_Y(\sigma\tau) = h_Y(\tau)h_Y(\sigma)^\tau$.*

Proof.

$$\begin{aligned}
h_Y(\sigma\tau) &= \nu_Y(\sigma\tau)\nu_X(\sigma\tau)^{-1} \\
&= \nu_Y(\tau)\nu_Y(\sigma)\nu_X(\sigma)^{-1}\nu_X(\tau)^{-1} \\
&= \nu_Y(\tau)h_Y(\sigma)\nu_X(\tau)^{-1} \\
&= \nu_Y(\tau)\nu_X(\tau)^{-1}\nu_X(\tau)h_Y(\sigma)\nu_X(\tau)^{-1} \\
&= h_Y(\tau)h_Y(\sigma)^\tau.
\end{aligned}$$

□

Suppose Y_1, Y_2 are k-forms of X and $g : Y_2 \to Y_1$ is a k-isomorphism. Then we extend g to a k^{sep}-autmorphism of Z and denote it by g also.

Lemma 7.9. *For all $\sigma \in \operatorname{Gal}(k^{\mathrm{sep}}/k)$, $h_{Y_2}(\sigma) = g^{-1}h_{Y_1}(\sigma)g^\sigma$.*

Proof. Since g is defined over k, the following diagram is commutative.

$$\begin{tikzcd}
Z \arrow[r, "g"] \arrow[d, "\nu_{Y_2}(\sigma)"'] & Z \arrow[d, "\nu_{Y_1}(\sigma)"] \\
Z \arrow[r, "g"'] & Z
\end{tikzcd}$$

Therefore,

$$\begin{aligned} h_{Y_2}(\sigma) &= \nu_{Y_2}(\sigma)\nu_X(\sigma)^{-1} \\ &= g^{-1}\nu_{Y_1}(\sigma)g\nu_X(\sigma)^{-1} \\ &= g^{-1}h_{Y_1}(\sigma)\nu_X(\sigma)g\nu_X(\sigma)^{-1} \\ &= g^{-1}h_{Y_1}(\sigma)g^{\sigma}. \end{aligned}$$

□

So we naturally come to the following definition.

Definition 7.10. Suppose G is a group scheme over k. We consider the discrete topology on $G_{k^{\text{sep}}}$.

(1) We define $\mathrm{H}^0(k, G) = G_k$.

(2) A continuous function $h : \mathrm{Gal}(k^{\text{sep}}/k) \to G_{k^{\text{sep}}}$ is called a *1-cocycle* if $h(\sigma\tau) = h(\tau)h(\sigma)^{\tau}$ for all σ, τ. Two 1-cocycles h_1, h_2 are equivalent if there exists $g \in G_{k^{\text{sep}}}$ such that $h_2(\sigma) = g^{-1}h_1(\sigma)g^{\sigma}$ for all σ. We denote the set of equivalence classes of 1-cocycles by $\mathrm{H}^1(k, G)$.

If $g \in G_{k^{\text{sep}}}$, $\mathrm{Gal}(k^{\text{sep}}/k) \ni \sigma \to g^{-1}g^{\sigma}$ is a 1-cocycle. Its class in $\mathrm{H}^1(k, G)$ does not depend on g and is called the *trivial class* or the trivial element.

Note that in (2), there exists an open normal subgroup H such that h factors as $\mathrm{Gal}(k^{\text{sep}}/k) \to \mathrm{Gal}(k^{\text{sep}}/k)/H \to G_{k^{\text{sep}}}$. Since $\mathrm{Gal}(k^{\text{sep}}/k)$ is compact, $[\mathrm{Gal}(k^{\text{sep}}/k) : H] < \infty$. Let K/k be the extension corresponding to H. Then K/k is a Galois extension since H is a normal subgroup.

For a finite Galois extension one can define $\mathrm{H}^1(K/k, G_K)$ similarly as in Definition 7.10(2). Then any cohomology class of $\mathrm{H}^1(k, G)$ actually comes from $\mathrm{H}^1(K/k, G_K)$ for a Galois extension K/k. This implies that

$$\mathrm{H}^1(k, G) = \varinjlim_{K} \mathrm{H}^1(K/k, G_K). \tag{7.11}$$

By Lemmas 7.8, 7.9, there is a well define map

$$\{k\text{-forms of } X\} \to \mathrm{H}^1(k, \mathrm{Aut}\,(X))$$

(it is known that $\mathrm{Aut}\,(X)$ is a group scheme). This map is bijective for many cases, for example, if X is a variety, a scheme, or an algebraic group over k.

For the rest of this course, we may use the notation $h = (h_\sigma)_{\sigma \in \mathrm{Gal}(k^{\text{sep}}/k)}$ or $h = (h_\sigma)_{\sigma \in \mathrm{Gal}(K/k)}$ for a 1-cocycle, where h_σ stands for the value of h at the Galois group element σ.

If $G_1 \to G_2$ is a homomorphism of group schemes, it obviously induces a map $\mathrm{H}^1(k, G_1) \to \mathrm{H}^1(k, G_2)$.

8. Existence of rational forms

In this section, we shall prove that the cocycle condition in the definition of the Galois cohomology guarantees the existence of rational forms. As an application, we discuss the restriction of scalar for algebraic groups.

Suppose K/k is a finite Galois extension of degree n. Let $\Gamma = \mathrm{Gal}(K/k)$. In section 7, we considered the situation where R is a k-algebra and $S = R \otimes_k K$. Then there is a natural action of $\mathrm{Gal}(K/k)$ on S by

$$R \otimes_k K \ni s = r \otimes x \to s^\sigma = r \otimes x^\sigma \in R \otimes_k K$$

for $\sigma \in \mathrm{Gal}(K/k), r \in R, x \in K$.

The above action of course satisfies the following assumption.

Assumption 8.1. There is a right action $S \ni s \to s^\sigma \in S$ of $\mathrm{Gal}(K/k)$ on S such that

$$(xs)^\sigma = x^\sigma s^\sigma.$$

for all $\sigma \in \mathrm{Gal}(K/k), s \in S, x \in K$,

Actions which satisfy Assumption 8.1 are called semi-linear actions. This notion can trivially generalized to actions on vector spaces and so we assume that V is a vector space over K with a semi-linear $\Gamma = \mathrm{Gal}(K/k)$ action. It turns out that Assumption 8.1 ensures the existence of a k-form. Therefore, we proceed with Assumption 8.1 without assuming that V has a k-form and prove that it does.

Theorem 8.2. *If Assumption 8.1 is satisfied, there exists a unique k-vector space W such that $V \cong W \otimes_k K$ and that the action of Γ induced by this k-form coincides with the given semi-linear action. Moreover, if V has a K-algebra structure and the action is compatible with the ring structure, then W has a k-algebra structure.*

Proof. We give the proof of this theorem following Borel [2, §14].

Let

$$W = V^\Gamma = \{x \in V \mid \forall \sigma \in \Gamma \; x^\sigma = x\}.$$

Note that if V has a K-algebra structure, W has the obvious k-algebra structure.

Define a K-algebra homomorphism $\phi : W \otimes_k K \to V$ by

$$\phi(x \otimes t) = tx$$

for $t \in K, \; x \in W$. Since

$$\begin{aligned} \phi(x \otimes t^\sigma) &= t^\sigma x \\ &= t^\sigma x^\sigma \\ &= (tx)^\sigma \\ &= \phi(x \otimes t)^\sigma, \end{aligned}$$

ϕ is a Γ-homomorphism. Therefore, for the existence of W, it suffices to show that ϕ is an isomorphism. The uniqueness follows from the observation that if $V = W \otimes_k K$ then $V^\Gamma = W$.

We first show that ϕ is surjective. Let $a_1, \cdots, a_n\}$ be a basis of K/k, $\Gamma = \{\sigma_1 = 1, , \cdots, \sigma_n\}$, and $x \in V$. We put

$$y_i = \sum_j (a_i x)^{\sigma_j}.$$

If $\sigma \in \Gamma$, then the set $\{\sigma_1\sigma, \cdots, \sigma_n\sigma\}$ coincides with Γ. Therefore, y_i is invariant by the action of σ for all $\sigma \in \Gamma$. This implies that $y_i \in W$.

Since $\{\sigma_1, \cdots, \sigma_n\}$ is linearly independent over K, the matrix $(a_i^{\sigma_j})$ is invertible. We put $(a_i^{\sigma_j})^{-1} = (b_{rs})$. Then

$$\begin{aligned}
\sum_i b_{ih} y_i &= \sum_{i,j} b_{ih} (a_i x)^{\sigma_j} \\
&= \sum_{i,j} b_{ih} a_i^{\sigma_j} x^{\sigma_j} \\
&= \sum_j \left(\sum_i b_{ih} a_i^{\sigma_j} \right) x^{\sigma_j} \\
&= \sum_j \delta_{jh} x^{\sigma_j} \\
&= x^{\sigma_h}.
\end{aligned}$$

Since $\sigma_1 = 1$, this shows that ϕ is surjective.

Next we show that ϕ is injective. Let $W' = \mathrm{Ker}(\phi)$. Since ϕ is a Γ-homomorphism, W' is Γ-invariant. Therefore, W' itself has a semi-linear action. By the previous step, $W'^{\Gamma} \otimes_k K \to W'$ is surjective. So

$$W'^{\Gamma} = \mathrm{Ker}(\phi) \cap W = \{0\}.$$

This shows that ϕ is injective. □

We now consider the problem of classifying rational forms. Let X be a variety over k. It is known that $\mathrm{Aut}\,(X)$ is a group scheme over k. More precisely, for any k-algebra R, $\mathrm{Aut}\,(X)_R$ is the group of R-automorphisms of $X \times_k R$.

Let K/k be a finite Galois extension and $\Gamma = \mathrm{Gal}(K/k)$. We assume that $X = \mathrm{Spec}\, A$ in the following. However, the general situation can be handled by covering X with affine open sets.

If Y is a k-form of $X \times_k K$, we denote the action of Γ on $Y \times_k K \cong X \times_k K$ induced by Y by $\nu_Y(\sigma)$. Let $\nu_Y(\sigma) = \mu_Y(\sigma)^* : A \otimes_k K \to A \otimes_k K$ be the corresponding homomorphism. We define $h_Y(\sigma)$ by (7.6) again. For any $h \in \mathrm{Aut}\,(X)_K$, we define $h^\sigma = \nu_X(\sigma) \circ h \circ \nu_X(\sigma)^{-1}$ as before. We have shown in Lemma 7.8 that $h_Y(\sigma)$ satisfies the cocycle condition in the definition of $\mathrm{H}^1(K/k, \mathrm{Aut}\,(X))$.

Conversely, let $(h_\sigma)_\sigma$ be a 1-cocycle. We put

$$\nu_h(\sigma) = h_\sigma \circ \nu_X(\sigma),\ \mu_h(\sigma) = \nu_h(\sigma^{-1})^*. \tag{8.3}$$

Proposition 8.4. (1) *For all $\sigma, \tau \in \Gamma$, $\nu_h(\sigma\tau) = \nu_h(\tau) \circ \nu_h(\sigma)$. In other words, ν_h is a right action.*

(2) *The action μ_h is semi-linear.*

Proof. Since h_σ satisfies the cocycle condition,

$$\begin{aligned}\nu_h(\sigma\tau) &= \mathrm{H}_{\sigma\tau} \circ \nu_X(\sigma\tau) \\ &= \nu_h(\tau) \circ \nu_X(\tau)^{-1} \circ \nu_X(\tau) \circ h_\sigma \circ \nu_X(\tau)^{-1} \circ \nu_X(\tau) \circ \nu_X(\sigma) \\ &= \nu_h(\tau) \circ h_\sigma \circ \nu_X(\sigma) \\ &= \nu_h(\tau) \circ \nu_h(\sigma).\end{aligned}$$

This shows (1).

Since $\nu_h(\sigma) = \nu_X(\sigma) \circ h^*_{\sigma^{-1}}$, $\nu_X(\sigma^{-1})$ is semi-linear, and $h^*_{\sigma^{-1}}$ is K-linear, $\nu_h(\sigma)$ is semi-linear. □

By the above proposition, given any 1-cocycle, there exists a unique k-form Y of $X \times_k K$ such that $\nu_Y(\sigma) = h_\sigma \circ \nu_X(\sigma)$. Taking the limit with respect to K, we obtain the following theorem.

Theorem 8.5. *By associating the 1-cocycle given by $h_Y(\sigma) = \nu_Y(\sigma) \circ \nu_X(\sigma)^{-1}$ to a k-form Y of X, k-forms of X and $\mathrm{H}^1(k, \mathrm{Aut}\,(X))$ correspond bijectively.*

Suppose L/k is a finite separable extension and K/k a Galois extension containing L. Let $X = \operatorname{Spec} S$ be an affine scheme over L, which is absolutely irreducible. Weil (see [29] for example) formulated the notion of the restriction of scalar as follows.

Let $\bar{S} = S \otimes_L K$. We express $\bar{S}$ in the form $K[x]/I$ where $x = (x_1, \cdots, x_N)$. For $\sigma \in \mathrm{Gal}(K/k)$, define $\bar{S}^\sigma = K[x]/I^\sigma$. It turns out this definition does not depend on the choice of the expression $K[x]/I$. There is an obvious map $\sigma^{-1} : \bar{S}^\sigma \to \bar{S}$, which induces a map $X \to X^\sigma = \operatorname{Spec} \bar{S}^\sigma$.

Let $H_0 = \mathrm{Gal}(K/k)$, and $H_1 \subset H_0$ be the subgroup corresponding to L. Let $\{\sigma_1 = 1, \cdots, \sigma_d\}$ be the complete set of representatives of $H_1 \backslash H_0$, and

$$A = \bar{S}^{\sigma_1} \otimes_K \cdots \otimes_K \bar{S}^{\sigma_d}. \tag{8.6}$$

We define a homomorphism $\phi : G \to \mathfrak{S}_d$ by $H_1\sigma_i\tau = H_1\sigma_{\phi(\tau)(i)}$ where the product in $\mathfrak{S}_d$ is defined by $(\tau_1\tau_2)(i) = \tau_2(\tau_1(i))$. Then ϕ is a homomorphism because if $\tau_1, \tau_2 \in H_0$,

$$\begin{aligned}H_1\sigma_{\phi(\tau_1\tau_2)(i))} &= H_1\sigma_i\tau_1\tau_2 = H_1\sigma_{\phi(\tau_1)(i)}\tau_2 \\ &= H_1\sigma_{\phi(\tau_2)(\phi(\tau_1)(i))} \\ &= H_1\sigma_{(\phi(\tau_1)\phi(\tau_2))(i)}.\end{aligned}$$

We define an action of H_0 on $A, \operatorname{Spec} A$ by

$$\begin{aligned}(s_1 \otimes \cdots \otimes s_d)^\tau &= s^\tau_{\phi(\tau)^{-1}(1)} \otimes \cdots \otimes s^\tau_{\phi(\tau)^{-1}(d)}, \\ (x_1, \cdots, x_d)^\tau &= (x^\tau_{\phi(\tau)^{-1}(1)}, \cdots, x^\tau_{\phi(\tau)^{-1}(d)}).\end{aligned}$$

for $s_1, \cdots, s_d \in \bar{S}, (x_1, \cdots, x_d) \in \operatorname{Spec} A$. It is easy to verify that this action is well defined and is a K-homomorphism. We verify that it is a right action. Since the argument is similar, we only consider the action on A.

Let $\tau_1, \tau_2 \in G$ and $s_1, \cdots, s_d \in \bar{S}$. Then if $t_i = s^{\tau_1}_{\phi(\tau_1)^{-1}(i)}$,

$$\begin{aligned}t^{\tau_2}_{\phi(\tau_2)^{-1}(i)} &= s^{\tau_1\tau_2}_{\phi(\tau_1)^{-1}(\phi(\tau_2)^{-1}(i))} = s^{\tau_1\tau_2}_{(\phi(\tau_2)^{-1}\phi(\tau_1)^{-1})(i)} \\ &= s^{\tau_1\tau_2}_{(\phi(\tau_1)\phi(\tau_2))^{-1}(i)} = s^{\tau_1\tau_2}_{\phi(\tau_1\tau_2)^{-1}(i)}.\end{aligned}$$

Therefore,

$$\begin{aligned}((s_1 \otimes \cdots \otimes s_d)^{\tau_1})^{\tau_2} &= t_{\phi(\tau_2)^{-1}(1)}^{\tau_2} \otimes \cdots \otimes t_{\phi(\tau_2)^{-1}(d)}^{\tau_2} \\ &= s_{\phi(\tau_1\tau_2)^{-1}(1)}^{\tau_1\tau_2} \cdots \otimes s_{\phi(\tau_1\tau_2)^{-1}(d)}^{\tau_1\tau_2}.\end{aligned}$$

If $x \in K, a \in A$, the relation $(xa)^\tau = x^\tau a^\tau$ is obvious. So this is an action satisfying Assumption 8.1. Therefore, A has a k-form which induces the above action. Moreover, such a k-form is unique by Theorem 8.2(2) (the 1-cocycle is determine by the Galois action).

Definition 8.7. The *restriction of scalar* $\mathrm{R}_{L/k}(X)$ of X is the unique k-scheme W such that there is an isomorphism

$$W \times_k K \cong X^{\sigma_1} \times_K \cdots \times_K X^{\sigma_d}$$

which is compatible with the Galois group actions.

Proposition 8.8. *Suppose X is an affine variety over L. Then $\mathrm{R}_{L/k}(X)_k \cong X_L$.*

Proof. Suppose $x = (x_1, \cdots, x_d) \in \mathrm{R}_{L/k}(X)_k$. We chose $\sigma_1 = 1$ and so $\phi(1) = 1$. This implies that $x_1^\tau = x_1$ for $\tau \in H_1$. So $x_1 \in X_L$. By the condition $x^{\sigma_i} = x$, it follows that $x_i = x_1^{\sigma_i}$. Therefore,

$$\mathrm{R}_{L/k}(X)_k = \{(x_1^{\sigma_1}, \cdots, x_1^{\sigma_d}) \mid x_1 \in X_L\} \cong X_L.$$

□

If X is an algebraic group, we can of course make $\mathrm{R}_{L/k}(X)$ an algebraic group over k.

Example 8.9. Let $L, \sigma_1, \cdots, \sigma_d$, etc., be as above. We regard $G = \mathrm{GL}(1) = \operatorname{Spec} L[t,s]/(ts-1) = \operatorname{Spec} L[t,t^{-1}]$ as a group over L. Let $\mathrm{N}_{L/k}$ be the norm map, and $\{a_1, \cdots, a_d\}$ a basis of L over k as a vector space. We show that

$$\mathrm{R}_{L/k}(G) \cong \operatorname{Spec} k[t_1, \cdots, t_d, s]/(s\mathrm{N}_{L/k}(a_1t_1 + \cdots + a_dt_d) - 1). \tag{8.10}$$

Note that $\mathrm{N}_{L/k}(a_1t_1 + \cdots + a_dt_d) \in k[t_1, \cdots, t_d]$.

Let K/k be the Galois closure of L. Over K, the polynomial $\mathrm{N}_{L/k}(a_1t_1 + \cdots + a_dt_d)$ factors as

$$\mathrm{N}_{L/k}(a_1t_1 + \cdots + a_dt_d) = \prod_{i=1}^d (a_1^{\sigma_i}t_1 + \cdots + a_d^{\sigma_i}t_d).$$

We show that these linear factors are linearly independent.

Let

$$A = \begin{pmatrix} a_1^{\sigma_1} & \cdots & a_d^{\sigma_1} \\ \vdots & \vdots & \vdots \\ a_1^{\sigma_d} & \cdots & a_d^{\sigma_d} \end{pmatrix}.$$

Suppose $x_1, \cdots, x_d \in K$ and $\begin{pmatrix} x_1 & \cdots & x_d \end{pmatrix} A = 0$. This means that

$$\sum_{j=1}^d x_j a_i^{\sigma_j} = 0 \tag{8.11}$$

for all i.

Define a map $\chi : L \to K$ by

$$\chi(\sum_i y_i a_i) = \sum_{i,j} x_j y_i a_i^{\sigma_j}$$

for all $y_1, \cdots, y_d \in k$ (in other words, $\chi = \sum_j x_j \sigma_j$). By the assumption (8.11), this map is identically zero. Since $\sigma_1, \cdots, \sigma_d$ are linearly independent over K, $x_1, \cdots, x_d$ must be zero. This implies that $\det A \neq 0$.

Therefore,

$$K[t_1, \cdots, t_d, s]/(s\mathrm{N}_{L/k}(a_1 t_1 + \cdots + a_d t_d) - 1) \cong K[u_1, \cdots, u_d, (u_1, \cdots, u_d)^{-1}]$$

where $u_i = a_1^{\sigma_i} t_1 + \cdots + a_d^{\sigma_i} t_d$ for $i = 1, \cdots, d$.

It is easy to see that $u_i^\sigma = u_{\phi(\sigma)(i)}$. We define a map from $K[u] \otimes \cdots \otimes K[u]$ to itself by

$$f_1 \otimes \cdots \otimes f_d \to f^\sigma_{\phi(\sigma)^{-1}(1)} \otimes \cdots \otimes f^\sigma_{\phi(\sigma)^{-1}(d)}. \tag{8.12}$$

Then u in the i-th component maps to u in the $\phi(\sigma)(i)$-th component. Since

$$\begin{aligned} K[u_1, \cdots, u_d, (u_1, \cdots, u_d)^{-1}] &= K[u_1, \cdots, u_d, u_1^{-1}, \cdots, u_d^{-1}], \\ &\cong K[u, u^{-1}] \otimes_K \cdots \otimes_K K[u, u^{-1}] \end{aligned}$$

with the Galois action defined as in (8.12). This proves (8.10).

Example 8.13. Similarly as in the previous example, if we put

$$A = k[g_{i,j\ell} \mid 1 \le i \le d,\ 1 \le j, \ell \le n],$$

$$P((g_{i,j\ell})) = \mathrm{N}_{L/k}\left(\det\left(\sum_{i=1}^d a_i g_{i,j\ell}\right)\right).$$

then one can show that

$$\mathrm{R}_{L/k}(\mathrm{GL}(n)) = \mathrm{Spec}\, A[P((g_{i,j\ell}))^{-1}].$$

Exercise 8.14. Let $k = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt{-1})$. Describe $\mathrm{R}_{L/k}(\mathrm{Sp}(2n))$ explicitly. You don't have to prove that it satisfies the properties of the restriction of scalar, but you have to show how you found the answer.

9. Properties of Galois cohomology

Let G_1, G_2, G_3 be algebraic groups over k. Then we say

$$1 \longrightarrow G_1 \xrightarrow{\phi_1} G_2 \xrightarrow{\phi_2} G_3 \longrightarrow 1 \tag{9.1}$$

is *exact* if ϕ_1, ϕ_2 are homomorphisms, $G_{1\,k^{\mathrm{sep}}}$ is a normal subgroup of $G_{2\,k^{\mathrm{sep}}}$, and $G_{2\,k^{\mathrm{sep}}}/G_{1\,k^{\mathrm{sep}}} \cong G_{3\,k^{\mathrm{sep}}}$. Moreover, if there exists a homomorphism $\psi : G_3 \to G_2$ such that $\phi_2 \circ \psi$ is the identity map id_{G_3} of G_3, the exact sequence (9.1) is said to be *split*. Given an exact sequence (9.1), we have the following natural maps

$$\begin{array}{ccccc} G_{1\,k} & \longrightarrow & G_{2\,k} & \longrightarrow & G_{3\,k}, \\ \mathrm{H}^1(k, G_1) & \longrightarrow & \mathrm{H}^1(k, G_2) & \longrightarrow & \mathrm{H}^1(k, G_3). \end{array}$$

We define an action of $G_{3\,k}$ on $\mathrm{H}^1(k, G_1)$. Suppose $g \in G_{3\,k}$. By assumption, there exists $\bar{g} \in G_{2\,k^{\mathrm{sep}}}$ such that $\phi_2(\bar{g}) = g$. If K/k is a large enough Galois extension, $\bar{g} \in G_{2\,K}$. Let $\bar{h} \in \mathrm{H}^1(k, G_1)$ be a cohomology class. We may assume that $\bar{h}$ is represented by a 1-cocycle $h = (h_\sigma)_{\sigma \in \mathrm{Gal}(K/k)}$. It is easy to see that $h' = (h'_\sigma)_{\sigma \in \mathrm{Gal}(K/k)} = (\bar{g} h_\sigma (\bar{g}^\sigma)^{-1})_{\sigma \in \mathrm{Gal}(K/k)}$ is a 1-cocycle defining an element in $\mathrm{H}^1(k, G_2)$. Since

$$\phi_2(\bar{g} h_\sigma (\bar{g}^\sigma)^{-1}) = \phi_2(\bar{g})(\phi_2(\bar{g})^\sigma)^{-1} = g(g^\sigma)^{-1} = 1,$$

$h'_\sigma \in G_{1\,K}$. Since this holds for all σ, h' actually defines an element in $\mathrm{H}^1(k, G_1)$. It is easy to verify that this cohomology class does not depend on the choice of K, $\bar{g}$, and the 1-cocycle h and so we denote this element by ${}^g\bar{h}$. By considering the action of $G_{3\,k}$ on the trivial element in $\mathrm{H}^1(k, G_1)$, we get a map $G_{3\,k} \to \mathrm{H}^1(k, G_1)$. By construction, the image of the composition of the maps $G_{3\,k} \to \mathrm{H}^1(k, G_1) \to \mathrm{H}^1(k, G_2)$ consists only of the trivial element.

Theorem 9.2. *If (9.1) is exact,*

(1)
$$\begin{array}{ccccccc} 1 \longrightarrow & G_{1\,k} & \longrightarrow & G_{2\,k} & \longrightarrow & G_{3\,k} & \\ \longrightarrow & \mathrm{H}^1(k, G_1) & \longrightarrow & \mathrm{H}^1(k, G_2) & \longrightarrow & \mathrm{H}^1(k, G_3) & \end{array}$$

is exact, and

(2) *the map $G_{3\,k} \backslash \mathrm{H}^1(k, G_1) \to \mathrm{H}^1(k, G_2)$ is injective.*

Proof. Note that the exactness in the above theorem means that classes which map to the trivial class come from the previous set.

It is enough to prove the exactness of

$$\mathrm{H}^1(k, G_1) \longrightarrow \mathrm{H}^1(k, G_2) \longrightarrow \mathrm{H}^1(k, G_3) \tag{9.3}$$

and (2).

Suppose that $\bar{h} \in \mathrm{H}^1(k, G_2)$ is represented by a 1-cocycle $h = (h_\sigma)_{\sigma \in \mathrm{Gal}(k^{\mathrm{sep}}/k)}$ and it maps to the trivial element in $\mathrm{H}^1(k, G_3)$. Then there exists $g \in G_{3\,k}$ such that $h_\sigma = g^{-1} g^\sigma$ for all σ. Choose $\bar{g} \in G_{2\,k^{\mathrm{sep}}}$ such that $\phi_2(\bar{g}) = g$. Then h is equivalent to the 1-cocycle $(\bar{g} h_\sigma (\bar{g}^\sigma)^{-1})_{\sigma \in \mathrm{Gal}(k^{\mathrm{sep}}/k)}$. It is easy to see that $\bar{g} h_\sigma (\bar{g}^\sigma)^{-1} \in G_{1\,k^{\mathrm{sep}}}$ for all σ. Therefore, $\bar{h}$ is in the image of $\mathrm{H}^1(k, G_1) \to \mathrm{H}^1(k, G_2)$.

Let $\bar{h}_1, \bar{h}_2 \in \mathrm{H}^1(k, G_1)$ be represented by 1-cocycles $h_1 = (h_{1\,\sigma})_{\sigma \in \mathrm{Gal}(k^{\mathrm{sep}}/k)}$, $h_2 = (h_{2\,\sigma})_{\sigma \in \mathrm{Gal}(k^{\mathrm{sep}}/k)}$. Suppose $\bar{h}_1, \bar{h}_2$ map to the same element in $\mathrm{H}^1(k, G_2)$. Then there exists $g \in G_{2\,k^{\mathrm{sep}}}$ such that $\phi_1(h_{1\,\sigma}) = g^{-1}\phi_1(h_{2\,\sigma})g^\sigma$ for all σ. Then

$$1 = \phi_2 \circ \phi_1(h_{1\,\sigma}) = \phi_2(g)^{-1}\phi_2 \circ \phi_1(h_{2\,\sigma})\phi_2(g)^\sigma = \phi_2(g)^{-1}\phi_2(g)^\sigma.$$

This implies that $\phi_2(g) \in G_{3\,k}$. By the definition of the action of $G_{3\,k}$ on $\mathrm{H}^1(k, G_1)$, $\bar{h}_1$ is in the orbit of $\bar{h}_2$. $\square$

If G is an algebraic group which is abelian, one can define $\mathrm{H}^i(k, G)$ for all $i \geq 0$, and $\mathrm{H}^i(k, G)$ has a structure of an abelian group for $i \geq 0$. Moreover, if (9.1) is exact and G_1, G_2, G_3 are abelian, then we get a long exact sequence.

$$\begin{aligned} \cdots \longrightarrow \ \mathrm{H}^i(k, G_1) \ &\longrightarrow \mathrm{H}^i(k, G_2) \longrightarrow \mathrm{H}^i(k, G_3) \\ \longrightarrow \mathrm{H}^{i+1}(k, G_1) \ &\longrightarrow \quad \cdots \end{aligned}$$

The following facts are known.

(1) $\mathrm{H}^1(k, \mathrm{GL}(n)) = \{1\}$.
(2) $\mathrm{H}^1(k, \mathrm{SL}(n)) = \{1\}$.
(3) $\mathrm{H}^1(k, \mathrm{Sp}(2n)) = \{1\}$.
(4) $\mathrm{H}^1(k, \mathrm{GSp}(2n)) = \{1\}$.

The statement (1) means that the only k-form of a vector space is the usual vector space structure. The statement (3) means that any two symplectic forms are equivalent over any field. The statement (2) follows from (1) and the exact sequence

$$1 \longrightarrow \mathrm{SL}(n) \longrightarrow \mathrm{GL}(n) \longrightarrow \mathrm{GL}(1) \longrightarrow 1$$

because the map $\mathrm{GL}(n)_k \to k^\times$ is surjective. The statement (4) follows from the statement (3) for the same reason.

We include the proof of (1) here following Kneser [13, pp. 16–17]. Let A be a finitely generated k-algebra. If M is an A-module, it is called a *simple* A-module if it has no submodule other than $\{0\}$ and M. An A-module is *semi-simple* if it is a direct sum of simple modules. It is known (see Lang [15, pp. 645–646]) that any submodule of a semi-simple module is semi-simple. Also simple components of a semi-simple module are unique.

Let A be a finite dimensional associated algebra over k. We define

$$\begin{aligned} A^\times &= \{x \in A \mid \exists y \in A,\ xy = yx = 1\}, \\ A_L^\times &= \{x \in A \mid \exists y \in A,\ yx = 1\}, \\ A_R^\times &= \{x \in A \mid \exists y \in A,\ xy = 1\}. \end{aligned}$$

Lemma 9.4. *If A is a finite dimensional associative algebra over k, then $A^\times = A_L^\times = A_R^\times$.*

We leave the proof of this lemma to the reader (see Exercise 9.11).

We regard $A^\times$ as an algebraic group over k.

Theorem 9.5. *Let A be a finite dimensional k-algebra which is semi-simple as a right A-module. Then $\mathrm{H}^1(k, A^\times) = \{1\}$.*

Proof. It is enough to prove $\mathrm{H}^1(K/k, A^\times) = \{1\}$ for any finite Galois extension K/k. Any automorphism of A_K as a right A_K-module is given by left multiplication by an element of $A_K^\times$. So $\mathrm{H}^1(K/k, A^\times)$ is in one-to-one correspondence with k-forms of the right A-module A. Let B be a k-form of A and $h = (h_\sigma)_\sigma$ the corresponding 1-cocycle. Then B is also an A_k-module. Note that

$$B_k = \{x \in A_K \mid h_\sigma x^\sigma = x \text{ for all } \sigma\}.$$

So if $x \in B_k,\ y \in A_k$, then $h_\sigma (xy)^\sigma = h_\sigma x^\sigma y^\sigma = xy$, which implies that $xy \in B_K$.

We only have to verify that $B_k \cong A_k$ as right A_k-modules. Since $B_K = B \otimes K \cong A_K$ as right A_K-modules and $A_k \subset A_K$, we get the A_k-isomorphism

$$[K:k]A_k \cong [K:k]B_k$$

where $[K:k]A_k$ means the direct sum of $[K:k]$ copies of A_k. By assumption, the left hand side is a semi-simple A_k-module. Therefore, B_k is semi-simple also. The above isomorphism implies that A_k and B_k have the same simple components. This implies that $A_k \cong B_k$ as right A_k-modules. $\square$

The statement $\mathrm{H}^1(k, \mathrm{GL}(n)) = \{1\}$ is an easy consequence of the above theorem by considering $A = \mathrm{M}(n,n)$. The following theorem is also well known.

Theorem 9.6. *Let L/k be a finite separable extension and G a connected algebraic group over L. Then $\mathrm{H}^1(k, \mathrm{R}_{L/k}(G)) \cong \mathrm{H}^1(L, G)$.*

Proof. It is enough to prove that for any Galois extension K/k containing L,

$$\mathrm{H}^1(K/k, \mathrm{R}_{L/k}(G)) \cong \mathrm{H}^1(K/L, G).$$

Let $H_0 = \mathrm{Gal}(K/k)$, $H_1 = \mathrm{Gal}(K/L)$, and $d = [L:k]$. We choose a set of representatives $\{\sigma_1, \cdots, \sigma_d\}$ of $H_1 \backslash H_0$. Let $\phi : H_0 \to \mathfrak{S}_d$ be the homomorphism such that $H_1\sigma_1\sigma = H_1\sigma_{\phi(\sigma)(i)}$ for all i. We express elements of $\mathrm{R}_{L/k}(G)_K$ as

$$g = (g_1, \cdots, g_d) \in G_K^{\sigma_1} \times_K \cdots \times_K G_K^{\sigma_d}. \tag{9.7}$$

Suppose $\bar{h} \in \mathrm{H}^1(K/k, \mathrm{R}_{L/k}(G))$ is an element determined by a 1-cocycle $h = (h_\sigma)_{\sigma \in H_0}$. Let $h_\sigma = (h_{\sigma,1}, \cdots, h_{\sigma,d})$. We define $\alpha(h) = (h_{\tau,1})_{\tau \in H_1}$. Then $\alpha(h)$ is obviously a 1-cocycle which defines an element in $\mathrm{H}^1(K/L, G)$. We denote this element by $\alpha(h)$ also. If $\tau \in H_1$ and g are as in (9.7), then

$$g^\tau = (g_1^\tau, \cdots)$$

because $\phi(\tau)(1) = 1$ (note that $H_1\tau = H_1$). This implies that

$$g^{-1} h_\tau g^\tau = (g^{-1} h_{\tau,1} g_1^\tau, \cdots).$$

Therefore, α induces a map $\mathrm{H}^1(K/k, \mathrm{R}_{L/k}(G)) \to \mathrm{H}^1(K/L, G)$, which we also denote by α.

If $\sigma \in H_0$, we write $\sigma_i \sigma^{-1} = \lambda_i(\sigma)\sigma_{\phi(\sigma)^{-1}(i)}$ where $\lambda_i(\sigma) \in H_1$. Suppose $\bar{h} \in \mathrm{H}^1(K/L, G)$ is an element determined by a 1-cocycle $h = (h_\tau)_{\tau \in H_1}$. Then we define $\beta(h) = (h'_\sigma)_{\sigma \in H_0}$ where

$$h'_\sigma = (h^{\sigma_1}_{\lambda_1(\sigma)^{-1}}, \cdots, h^{\sigma_d}_{\lambda_d(\sigma)^{-1}}).$$

We show that $\beta(h)$ is a 1-cocycle defining an element in $\mathrm{H}^1(K/k, \mathrm{R}_{L/k}(G))$ and induces a map $\mathrm{H}^1(K/L, G) \to \mathrm{H}^1(K/k, \mathrm{R}_{L/k}(G))$.

If $\sigma, \nu \in H_0$, then

$$\begin{aligned}\lambda_i(\sigma\nu)\sigma_{\phi(\sigma\nu)^{-1}(i)} &= \sigma_i(\sigma\nu)^{-1}\\ &= \sigma_i\nu^{-1}\sigma^{-1}\\ &= \lambda_i(\nu)\sigma_{\phi(\nu)^{-1}(i)}\sigma^{-1}\\ &= \lambda_i(\nu)\lambda_{\phi(\nu)^{-1}(i)}(\sigma)\sigma_{\phi(\sigma)^{-1}\circ\phi(\nu)^{-1}(i)}\\ &= \lambda_i(\nu)\lambda_{\phi(\nu)^{-1}(i)}(\sigma)\sigma_{\phi(\sigma\nu)^{-1}(i)}.\end{aligned}$$

Therefore, $\lambda_i(\sigma\nu) = \lambda_i(\nu)\lambda_{\phi(\nu)^{-1}(i)}(\sigma)$. This implies that

$$\begin{aligned}h^{\sigma_i}_{\lambda_i(\sigma\nu)^{-1}} &= h^{\sigma_i}_{\lambda_{\phi(\nu)^{-1}(i)}(\sigma)^{-1}\lambda_i(\nu)^{-1}}\\ &= h^{\sigma_i}_{\lambda_i(\nu)^{-1}}(h^{\lambda_i(\nu)^{-1}}_{\lambda_{\phi(\nu)^{-1}(i)}(\sigma)^{-1}})^{\sigma_i}\\ &= h^{\sigma_i}_{\lambda_i(\nu)^{-1}}h^{\lambda_i(\nu)^{-1}\sigma_i}_{\lambda_{\phi(\nu)^{-1}(i)}(\sigma)^{-1}}.\end{aligned}$$

Since $\sigma_i\nu^{-1} = \lambda_i(\nu)\sigma_{\phi(\nu)^{-1}(i)}$, $\lambda_i(\nu)^{-1}\sigma_i = \sigma_{\phi(\nu)^{-1}(i)}\nu$. So

$$h^{\sigma_i}_{\lambda_i(\sigma\nu)^{-1}} = h^{\sigma_i}_{\lambda_i(\nu)^{-1}}h^{\sigma_{\phi(\nu)^{-1}(i)}\nu}_{\lambda_{\phi(\nu)^{-1}(i)}(\sigma)^{-1}}.$$

Since $h^{\sigma_{\phi(\nu)^{-1}(i)}\nu}_{\lambda_{\phi(\nu)^{-1}(i)}(\sigma)^{-1}}$ is the i-th entry of h'^{ν}_{σ}, $\beta(h)$ is a 1-cocycle.

Let $g \in G_K$. Then $\beta((g^{-1}h_\tau g^\tau)_{\tau\in H_1}) = (h''_\sigma)_{\sigma\in H_0}$ where

$$h''_\sigma = ((g^{-1}h_{\lambda_1(\sigma)^{-1}}g^{\lambda_1(\sigma)^{-1}})^{\sigma_1}, \cdots, (g^{-1}h_{\lambda_d(\sigma)^{-1}}g^{\lambda_d(\sigma)^{-1}})^{\sigma_d}).$$

Let $g' = (g^{\sigma_1}, \cdots, g^{\sigma_d})$. Then the i-th entry of g'^σ is

$$(g^{\sigma_{\phi(\sigma)^{-1}(i)}})^\sigma = g^{\sigma_{\phi(\sigma)^{-1}(i)}\sigma} = g^{\lambda_i(\sigma)^{-1}\sigma_i}.$$

Therefore,

$$\beta((g^{-1}h_\tau g^\tau)_{\tau\in H_1}) = (g'^{-1}h'_\sigma g'^\sigma)_{\sigma\in H_0}.$$

This implies that $\beta(h)$ depends only on $\bar{h}$.

If $\tau \in H_1$, $\sigma_1\tau^{-1} = \tau^{-1} \in H_1$. So $\lambda_1(\tau)^{-1} = (\tau^{-1})^{-1} = \tau$. So $\alpha\circ\beta$ is the identity map of $\mathrm{H}^1(K/L, G)$.

We show that $\beta\circ\alpha$ is the identity map of $\mathrm{H}^1(K/k, \mathrm{R}_{L/k}(G))$. Let $h = (h_\sigma)_{\sigma\in H_0}$, where $h_\sigma = (h_{\sigma,1}, \cdots, h_{\sigma,d})$, be a 1-cocycle defining an element $\bar{h}$ in $\mathrm{H}^1(K/k, \mathrm{R}_{L/k}(G))$. We put $g = (h_{\sigma_1,1}, \cdots, h_{\sigma_d,d})$.

We fix $\sigma \in H_0$, $1 \le i \le d$ and put $\lambda = \lambda_i(\sigma)$, $j = \phi(\sigma)^{-1}(i)$. Then the i-th entry of g^σ is $h^\sigma_{\sigma_j,j}$. So the i-th entry of $g^{-1}h_\sigma g^\sigma$ is

$$h^{-1}_{\sigma_i,i}h_{\sigma,i}h^\sigma_{\sigma_j,j}. \tag{9.8}$$

Since $\sigma_i = (\sigma_i\sigma^{-1})\sigma$, $h_{\sigma_i} = h_\sigma h^\sigma_{\sigma_i\sigma^{-1}}$. So $h_{\sigma_i,i} = h_{\sigma,i}h^\sigma_{\sigma_i\sigma^{-1},j}$. Therefore, (9.8) equals

$$(h^\sigma_{\sigma_i\sigma^{-1},j})^{-1}h^\sigma_{\sigma_j,j} = (h^\sigma_{\lambda\sigma_j,j})^{-1}h^\sigma_{\sigma_j,j}. \tag{9.9}$$

By the cocycle condition, $h_{\lambda\sigma_j} = h_{\sigma_j}h^{\sigma_j}_\lambda$. Since $\sigma_i\sigma^{-1} = \lambda\sigma_j$, $\sigma_j\sigma = \lambda\sigma_i$. So

$$h^\sigma_{\lambda\sigma_j} = h^\sigma_{\sigma_j}h^{\sigma_j\sigma}_\lambda = h^\sigma_{\sigma_j}h^{\lambda^{-1}\sigma_i}_\lambda. \tag{9.10}$$

Since $\phi(\sigma_i)^{-1}(i) = 1$, the i-th entry of (9.10) equals

$$h^{\sigma}_{\lambda\sigma_j,j} = h^{\sigma}_{\sigma_j,j} h^{\lambda^{-1}\sigma_i}_{\lambda,1}.$$

Therefore, (9.9) equals

$$(h^{\lambda^{-1}\sigma_i}_{\lambda,1})^{-1} = h^{\sigma_i}_{\lambda^{-1},1}.$$

Note that $(h^{\lambda^{-1}}_{\lambda,1})^{-1} = h_{\lambda^{-1},1}$ by the cocycle condition. Therefore, h is equivalent to the 1-cocycle whose σ component is

$$(h^{\sigma_1}_{\lambda_1(\sigma)^{-1},1}, \cdots, h^{\sigma_d}_{\lambda_d(\sigma)^{-1},1}).$$

But this is the definition of $\beta \circ \alpha(h)$. $\square$

Exercise 9.11. Prove Lemma 9.4.

10. Prehomogeneous vector spaces and their classification

In this section, we define the notion of prehomogeneous vector spaces and discuss fundamental properties.

Let G be a connected reductive group, V a representation, and $\chi \in X^*(G)$ a primitive character, all defined over k. We are mainly interested in irreducible representations. However, if $\operatorname{ch} k = p > 0$, we sometimes have to consider reducible representations which are obtained by reducing irreducible representations modulo p. Those representations can be handled more or less in the same manner as irreducible representations and we consider the following condition for that purpose.

Let Z be the identity component of the center of G. Since G is reductive, Z is a torus.

Condition 10.1. There exists $\psi \in X^*(Z)$ such that if $t \in Z$, then $tv = \psi(t)v$ for all $v \in V$.

Note that because of Schur's lemma, this assumption is satisfied if V is an irreducible representation.

Now we discuss prehomogeneous vector spaces. The notion of prehomogeneous vector spaces was introduced by M. Sato in early 1960's. We first recall the definition of prehomogeneous vector spaces.

Definition 10.2. Let G be a connected reductive group, V a representation of G, and χ a non-trivial primitive character of G, all defined over k. Then (G, V, χ) is called a *prehomogeneous vector space* if it satisfies the following properties.
(1) There exists a Zariski open orbit.
(2) There exists a non-constant polynomial $\Delta(x) \in k[V]$ such that $\Delta(gx) = \chi(g)^a\Delta(x)$ for a positive integer a.

In (1) of the above definition, if $U \subset V$ is an open set, it is a single G-orbit if there exists $x \in U_{\bar{k}}$ such that $U_{\bar{k}} = G_{\bar{k}}x$. Note that a variety is, by definition, a separated k-scheme of finite type which is absolutely integral. So when we consider points, we are not restricting ourselves to k-rational points. However, since the image of the map $G \ni g \to gx \in U$ is always a locally closed set by Theorem 3.24 (since G is irreducible), it suffices to consider only closed points since the set of closed points in U is dense in U.

We explain the meaning of (2) more precisely also. Let $G = \operatorname{Spec} A$ and $V = \operatorname{Spec} B$. Let

$$\lambda, h_2 : B \to A \otimes B, \quad h_1 : A \to A \otimes B \tag{10.3}$$

be the homomorphisms which correspond to the action $G \times V \to V$, the projection to G and V respectively. Since $\mathrm{GL}(1) \subset \mathrm{Aff}^1$, we regard χ as an element of A. Then the function $(g, x) \to \chi(g)^a\Delta(x)$ may be regarded as $h_1(\chi)^a h_2(\Delta)$. Therefore, the condition (2) of Definition 10.2 is, more precisely, interpreted as

$$\lambda(\Delta) = h_1(\chi)^a h_2(\Delta).$$

Define

$$\begin{aligned} R_a &= \{\Delta \in B \mid \lambda(\Delta) = h_1(\chi)^a h_2(\Delta)\} \\ &= \{\Delta \in B \mid (\lambda - h_1(\chi)^a h_2)(\Delta) = 0\}. \end{aligned} \tag{10.4}$$

We change the base from k to $\bar{k}$ and denote everything by $\overline{A}$, $\overline{h_2}$, etc.

Lemma 10.5. *For all a, $\overline{R}_a = R_a \otimes_k \bar{k}$.*

Proof. Since $k \to \bar{k}$ is flat,

$$\begin{aligned}\overline{R}_a &= \operatorname{Ker}((\lambda - h_1(\chi)^a h_2) \otimes \mathrm{id}_{\bar{k}}) \\ &= \operatorname{Ker}(\lambda - h_1(\chi)^a h_2) \otimes \bar{k} \\ &= R_a \otimes \bar{k}.\end{aligned}$$

□

It is known that if $k = \bar{k}$ and A is an integral domain,

$$\cap\, \mathfrak{m} = \{0\} \tag{10.6}$$

where $\mathfrak{m}$ runs through all maximal ideals of A.

The polynomial Δ in Definition 10.2(2) is called a *relative invariant polynomial.* We define $V^{\mathrm{ss}} = \{x \in V \mid \Delta(x) \neq 0\}$ and call it the set of semi-stable points. We show that V^{ss} does not depend on the choice of Δ.

Proposition 10.7. *If Δ_1, Δ_2 are relative invariant polynomials, there exist positive integers a, b such that $\Delta_1(x)^a/\Delta_2(x)^b$ is a constant.*

Proof. By definition, there exist positive integers a, b such that

$$\Delta_1(gx) = \chi(g)^b \Delta_1(x),\ \Delta_2(gx) = \chi(g)^a \Delta_2(x).$$

Then $\Delta_1(x)^a/\Delta_2(x)^b$ is invariant by the action of G. Since V has an open G-orbit, $\Delta_1(x)^a/\Delta_2(x)^b$ is a constant. □

Lemma 10.8. *If $\Delta(x)$ is a relative invariant polynomial, it is a homogeneous polynomial.*

Proof. Suppose $\Delta(gx) = \chi(g)^a \Delta(x)$. Let $t \in \mathrm{GL}(1)$. Then $\Delta(tgx) = \Delta(gtx) = \chi(g)^a \Delta(tx)$. So by the proof of Proposition 10.7, there exists $c(t) \in \mathrm{GL}(1)$ such that $\Delta(tx) = c(t)\Delta(x)$. Obviously, $t \to c(t)$ is a character of $\mathrm{GL}(1)$ and so there exists an integer N such that $c(t) = t^N$. Since $\Delta(x)$ is a non-constant polynomial, $N > 0$. So $\Delta(x)$ is a homogeneous polynomial. □

Proposition 10.9. *If R is the subring of $k[V]$ generated by relative invariant polynomials, it is generated by a single element. Moreover, if $R = k[\Delta]$, Δ generates the corresponding ring over $\bar{k}$.*

Proof. Note that $k[V]$ is UFD. Choose a relative invariant polynomial $\Delta(x)$ so that $\deg \Delta(x)$ is the smallest.

Let $\Delta_1(x)$ be another relative invariant polynomial. Suppose

$$\Delta(x) = cP_1(x)^{p_1} \cdots P_i(x)^{p_i}$$

is the prime decomposition ($c \in k^\times$). Then by the uniqueness of the prime decomposition, the prime decomposition of $\Delta_1(x)$ must be of the form

$$\Delta_1(x) = c' P_1(x)^{q_1} \cdots P_i(x)^{q_i}$$

and the vectors ${}^t\begin{pmatrix} p_1 & \cdots & p_i \end{pmatrix}$ and ${}^t\begin{pmatrix} q_1 & \cdots & q_i \end{pmatrix}$ must be proportional.

Let

$$\begin{pmatrix} p_1 \\ \vdots \\ p_i \end{pmatrix} = s_1 \begin{pmatrix} r_1 \\ \vdots \\ r_i \end{pmatrix}, \quad \begin{pmatrix} q_1 \\ \vdots \\ q_i \end{pmatrix} = s_2 \begin{pmatrix} r_1 \\ \vdots \\ r_i \end{pmatrix} \tag{10.10}$$

where s_1, s_2 are positive integers and ${}^t\begin{pmatrix} r_1 & \cdots & r_i \end{pmatrix}$ is a primitive integer vector.

By assumption, $s_2 \geq s_1$. If s_1 divides s_2, $\Delta_1(x)$ belongs to the ring generated by $\Delta(x)$. Suppose s_1 does not divide s_2. Then $s_2 = \alpha s_1 + \beta$ where α, β are positive integers and $\beta < s_1$. Obviously, $\Delta_1(x)\Delta(x)^{-\alpha}$ is a relative invariant polynomial and the degree is less than s_1, which is a contradiction. Therefore, R must be generated by $\Delta(x)$.

The second assertion follows from Lemma 10.5. □

Lemma 10.11. *Suppose $F \subset V$ is a G-invariant closed subset and $F = \cup_{i=1}^N F_i$ is the irreducible decomposition. Then each F_i is G-invariant.*

Proof. Without loss of generality, it suffices to prove that F_1 is G-invariant. Let

$$U_1 = F_1 \setminus \left(\cup_{i=2}^N F_i\right).$$

Then U_1 is an open set of F_1 and so is irreducible.

Let $\mu : G \times V \to V$ be the group action, $\widetilde{U}_1 = \mu(G \times U_1)$, and $\widetilde{F}_1$ be the closure of $\widetilde{U}_1$. Since G is irreducible also, $\widetilde{U}_1, \widetilde{F}_1$ are irreducible. Since

$$U_1 \subset \widetilde{U}_1 \subset \widetilde{F}_1 \subset F,$$

$F_1 \subset \widetilde{F}_1 \subset F$. This implies that $F_1 = \widetilde{F}_1$ and so F_1 is a G-invariant subset. □

Suppose F_i in the above lemma is the zero set of an irreducible polynomial $\Delta_i(x)$ (this is the case if the codimension of F_i is one). By Hilbert's Nullstellensatz, there exists a character χ_i of G such that $\Delta_i(gx) = \chi_i(g)\Delta_i(x)$.

Next we show that if a prehomogeneous vector space (G, V, χ) satisfies Condition 10.1, the choice of χ is essentially unique.

Proposition 10.12. *Suppose that V is a representation of G satisfying Condition 10.1. If χ_1, χ_2 are primitive rational characters of G and $(G, V, \chi_1), (G, V, \chi_2)$ are prehomogeneous vector spaces, then $\chi_1 = \chi_2$.*

Proof. We may assume that $k = \bar{k}$. Let $G_1 = (G, G)$. By assumption, G_1 is semi-simple and so has no non-trivial character. Also G contains a torus T which is contained in the center of G such that $G = TG_1$.

By Condition 10.1, there exists $\psi \in X^*(T)$ such that $tv = \psi(t)v$ for all $t \in T$, $v \in V$. Suppose $\Delta_1(x), \Delta_2(x) \in k[V]$ and

$$\Delta_1(gx) = \chi_1(g)^a \Delta_1(x), \ \Delta_2(gx) = \chi_2(g)^b \Delta_2(x).$$

If $g = tg_1$ with $t \in T, g_1 \in G_1$, then

$$\begin{aligned} \Delta_1(gx) &= \chi_1(g)^a \Delta_1(x) = \chi_1(t)^a \Delta_1(x) = \Delta_1(tx) \\ &= \Delta_1(\psi(t)x) = \psi(t)^{\deg \Delta_1} \Delta_1(x). \end{aligned}$$

This implies that $\chi_1(tg_1)^a = \psi(t)^{\deg \Delta_1}$. Similarly, $\chi_2(tg_1)^b = \psi(t)^{\deg \Delta_2}$. Therefore, $\chi_1(tg_1)^{a \deg \Delta_2} = \chi_2(tg_1)^{b \deg \Delta_1}$. Since both χ_1, χ_2 are primitive, $\chi_1 = \chi_2$. □

By the above proposition, if (G, V, χ) satisfies Condition 10.1, we may use the notation (G, V) instead.

Corollary 10.13. *Let (G, V) be a prehomogeneous vector spacesatisfying Condition 10.1, and $\Delta(x)$ a relative invariant polynomial of the lowest degree. Then $\Delta(x)$ is irreducible over $\bar{k}$. Moreover, the zero set of $\Delta(x)$ is the only G-invariant irreducible codimension one closed subset of V.*

Proof. By Lemma 10.5, we may assume that $k = \bar{k}$.

Let

$$\Delta(x) = \Delta_1(x)^{p_1} \cdots \Delta_N(x)^{p_N} \tag{10.14}$$

be the prime decomposition, and

$$\begin{aligned} F &= \{x \in V \mid \Delta(x) = 0\}, \\ F_i &= \{x \in V \mid \Delta_i(x) = 0\} \end{aligned} \tag{10.15}$$

for all i. More precisely, $F = \operatorname{Spec} k[V]/(\Delta(x))$, etc. By Hilbert's Nullstellensatz, $F_i \not\subset F_j$ if $i \neq j$.

By the comment after Lemma 10.11, for each i, there exists a character χ_i of G such that $\Delta_i(gx) = \chi_i(g)\Delta_i(x)$. Suppose $\chi_i = \psi_i^{n_i}$ where ψ_i is primitive and n_i is a positive integer for all i. By Proposition 10.12, $\psi_i = \chi$ for all i. Therefore, $\Delta_i(x)$ is a relative invariant polynomial (corresponding to χ). Since the degree of $\Delta(x)$ is the smallest, $p_1 = 1$ and so $\Delta(x)$ is irreducible.

If $\overline{F} \subset V$ is any irreducible codimension one closed subset, it is the zero set of an irreducible polynomial $\overline{\Delta}(x)$. Then by Hilbert's Nullstellensatz, there exists a character $\bar{\chi}$ of G such that $\overline{\Delta}(x)(gx) = \bar{\chi}(g)\overline{\Delta}(x)$. Then by Proposition 10.12 again, $\overline{\Delta}(x)$ is a relative invariant polynomial. Since both $\Delta(x)$ and $\overline{\Delta}(x)$ are irreducible, $\overline{\Delta}(x)$ must be a constant multiple of $\Delta(x)$. $\square$

Suppose that (G, V) is a prehomogeneous vector space satisfying Condition 10.1. In general, $V^{\rm ss}_{k^{\rm sep}}$ is not a single $G_{k^{\rm sep}}$-orbit. However, if (G, V) satisfies a condition called regularity, then $V^{\rm ss}_{k^{\rm sep}}$ becomes a single $G_{k^{\rm sep}}$-orbit.

The notion of regularity was introduced by Sato and Kimura in §4 [23]. We use the property of Proposition 25 [23, p. 72] as the definition of regularity.

Proposition 10.16. *Suppose G is a connected reductive group, V a representation of G satisfying Condition 10.1 If there exists a point $w \in V_k$ such that $U = Gw$ is Zariski open and G_w is reductive (and so smooth as a group scheme), then*

(1) *U is affine,*
(2) *$U_{k^{\rm sep}}$ is a single $G_{k^{\rm sep}}$-orbit.*

Proof. We may assume that k is separably closed.

Let $G = \operatorname{Spec} A$, and $S = A^{G_w}$. Then the geometric quotient $X = G/G_w$ exists, it is affine (in fact $X = \operatorname{Spec} S$), and the map $f : G \to X$ is smooth by Proposition 5.7, Theorem 5.8. By properties of smooth morphisms, X is smooth over k. Because of the universal property of the quotient, the map $G \to U$ defined by $g \to gw$ factors through X.

Since G, V are smooth over k, $\dim T(U)_w = \dim U = \dim V$ and $\dim T(G)_e = \dim G$. Since $G \to X$ is a principal fiber bundle and the generic fiber is isomorphic to G_w, $\dim G = \dim X + \dim G_w = \dim U + \dim G_w$. Note that the map $X \to U$ is set-theoretically bijective, because X is the geometric quotient. Therefore, $\dim G_w = \dim T(G)_e - \dim T(U)_w$. Since G_w is smooth over k,

$$\dim G_w = \dim T(G_w)_e = \dim \operatorname{Ker}(T(G)_e \to T(U)_w).$$

Therefore,

$$\dim \operatorname{Ker}(T(G)_e \to T(U)_w) = \dim T(G)_e - \dim T(U)_w.$$

This proves that $T(G)_e \to T(U)_w$ is surjective.

Since the map $G \to U$ is G-equivariant, it induces surjective maps of tangent spaces. So that is the case for $X \to U$ also. Since both X, U are smooth over k, this implies that $X \to U$ is smooth. Since the map $X \to U$ is of relative dimension zero, it is etale. Since this map is set-theoretically bijective, X is isomorphic to U and U is affine. This proves (1).

Since f is smooth, for any point $x \in U_k$, the fiber $f^{-1}(x)$ over x is smooth over k. Since k is separably closed, we may choose a k-rational point $g \in f^{-1}(x)$ by Proposition 3.15. Then $gw = x$, and this proves (2). □

Assuming the above proposition, the following corollary is more elementary.

Corollary 10.17. *If the assumption of Proposition 10.16 is satisfied, there exists a relative invariant polynomial and so (G, V) is a prehomogeneous vector space. Moreover, $V^{\mathrm{ss}}_{k^{\mathrm{sep}}} = G_{k^{\mathrm{sep}}} w$.*

Proof. Let $U = Gw$, and $F_1, \cdots, F_n$ be the irreducible codimension one components of $V \backslash U$, $F = F_1 \cup \cdots \cup F_n$, and $W = V \backslash F$. Then W is affine, $U \subset W$, and the codimension of $W \backslash U$ in W is greater than one. Suppose $W = \operatorname{Spec} A$ and $U = \operatorname{Spec} B$. Then $A \subset B$ and A is a normal ring because W is smooth over k (see Theorem 36 [16, p. 121]). Since the codimension of U in W is greater than one, any regular function on U (i.e., an element of B) extends to a regular function on W (see Theorem 38 [16, p. 124]). Therefore, $A = B$ and so $W = U$.

Clearly, the orbit of the origin 0 consists of 0 itself. Since U is a single G-orbit, $0 \notin U$. This implies that $V \backslash U \neq \emptyset$. We have shown that any irreducible component of $F = V \backslash U$ is of codimension one.

Since F is a G-invariant closed subset of V, By Corollary 10.13, F is irreducible and is the zero set of a relative invariant polynomial of the lowest degree. This shows that $V^{\mathrm{ss}} = U$ and so $V^{\mathrm{ss}}_{k^{\mathrm{sep}}}$ is a single $G_{k^{\mathrm{sep}}}$-orbit by Proposition 10.16. □

Definition 10.18. A prehomogeneous vector space (G, V) satisfying Condition 10.1 is said to be *regular* if it satisfies the assumption of Proposition 10.16.

Remark 10.19. Even if Condition 10.1 is not satisfied, one can define the notion of regularity by the existence of a point w such that Gw is open and G_w is reductive. Then it is possible to show as in Corollary 10.17, that any irreducible component of $V \setminus Gw$ is of codimension one. In [23] for example, a relative invariant polynomial is the one which satisfies the condition $\Delta(gx) = \chi(g)\Delta(x)$ for an *unspecified* χ. So our definition of relative invariant polynomials is slightly different from that in [23].

Our purpose of using our formulation was to define the notion of a generic point from the viewpoint of geometric invariant theory. If we put $G' = \operatorname{Ker}(\chi)$ and π :

$V\setminus\{0\} \to \mathbb{P}(V)$ the natural map, then our definition of V^{ss} coincides with $\pi^{-1}(\mathbb{P}(V)^{\mathrm{ss}})$ where $\mathbb{P}(V)^{\mathrm{ss}}$ is the set of semi-stable points defined as in Definition 1.7 [21].

We shall prove a proposition, convenient for verifying the assumption of Proposition 10.16 for actual examples.

Proposition 10.20. *If there exists a point $w \in V$ such that*

$$\dim T(G_w)_e = \dim G - \dim V,$$

then Gw is open in V. Moreover, G_w is smooth over k.

Proof. We may assume that $k = \bar{k}$. Consider the map $G \to V$ defined by $g \to gw$. Then the image Gw is a constructible set. Since G is irreducible, $F = \overline{Gw}$ is irreducible. If $Gw = \cup_{i=1}^{l} F_i \cap U_i$ where F_i is closed and U_i is open for all i, then there must exists i such that $F_i = F$. Hence Gw contains an open set of F. Since G acts on Gw transitively, Gw itself is an open set of F. Therefore, Gw is a variety.

Note that for any $y \in Gw$, the fiber over y is isomorphic to G_w. By Theorem 3.25,

$$\begin{aligned} \dim G &= \dim G_w + \dim Gw \\ &\leq \dim T(G_w)_e + \dim Gw \\ &= \dim G - \dim V + \dim Gw. \end{aligned}$$

Therefore, $\dim Gw \geq \dim V$ and so $Gw \subset V$ is open and $\dim T(G_w)_e = \dim G_w$. This implies that G_w is smooth over k. This proves the proposition. $\square$

Next we discuss the notion of the castling transform (see [23, pp. 37–39]). If $\rho : G \to \mathrm{GL}(V)$ is a representation, we define a representation of G on the dual vector space V^* by $(\rho^*(g)f)(v) = f(\rho(g^{-1})v)$ for $g \in G,\ f \in V^*$. This is also a left action and is called the *contragredient representation* of V.

To explain the castling transform, we have to discuss the notion of the Grassmann varieties. Let $V = \mathrm{Aff}^n$ be the n-dimensional affine space, regarded as a vector space of dimension n. If $0 \leq m \leq n$, there is an algebraic variety (which is not affine) called the Grassmann variety $\mathrm{Gr}(n,m) = \mathrm{Gr}(V,m)$ of m-planes in V whose points are in one-to-one correspondence with m-dimensional subspaces of V. If $W \subset V$ is an m-dimensional subspace,

$$\widehat{W} = \{f \in V^* \mid f(v) = 0 \text{ for all } v \in W\}$$

is an $(n-m)$-dimensional subspace of V^*. Therefore, there is a map $\mathrm{Gr}(V,m) \to \mathrm{Gr}(V^*, n-m)$. It is easy to see that this set-theoretically bijective, and it is known that this map is in fact an isomorphism of algebraic varieties.

Now let $\rho : G \to \mathrm{GL}(V)$ be a representation of a reductive group G, and $\rho^* : G \to \mathrm{GL}(V^*)$ its contragredient representation. Consider the following two representations

(1) $G \times \mathrm{GL}(m)$ acting on $V \otimes \mathrm{Aff}^m$
(2) $G \times \mathrm{GL}(n-m)$ acting on $V^* \otimes \mathrm{Aff}^{n-m}$

Note that we are regarding $\mathrm{Aff}^m, \mathrm{Aff}^{n-m}$ as the set of column vectors and so $\mathrm{GL}(m), \mathrm{GL}(n-m)$ act on them respectively.

The following proposition is Proposition 7 [23, p. 37].

Proposition 10.21. *The representation (1) has an open orbit if and only if the representation (2) has an open orbit. If so, their generic stabilizers are isomorphic over $\bar{k}$.*

Proof. We may assume that k is algebraically closed. Let

$$U = \{v = (v_1, \cdots, v_m) \mid V \ni v_1, \cdots, v_m \text{ are linearly independent}\},$$
$$U^* = \{v = (v_1, \cdots, v_{n-m}) \mid V^* \ni v_1, \cdots, v_{n-m} \text{ are linearly independent}\}.$$

Note that $U \subset V \otimes \mathrm{Aff}^k$, $U^* \subset V^* \otimes \mathrm{Aff}^{n-m}$ are Zariski open subsets.

If $v = (v_1, \cdots, v_m) \in U$, let $\langle v \rangle \in \mathrm{Gr}(V, m)$ be the m-dimensional subspace spanned by $v_1, \cdots, v_m$. Then G acts on $\mathrm{Gr}(V, m)$, $\mathrm{Gr}(V^*, n-m)$ and the maps

$$\pi : U \ni v \to \langle v \rangle \in \mathrm{Gr}(V, m),\ \pi^* : U^* \ni v \to \langle v \rangle \in \mathrm{Gr}(V^*, n-m)$$

are equivariant with respect to the action of G. Moreover, points in $\mathrm{Gr}(V, m)$ (resp. $\mathrm{Gr}(V^*, n-m)$) are in one-to-one correspondence with $\mathrm{GL}(m)$-orbits in U (resp. $\mathrm{GL}(n-m)$-orbits in U^*). So there is an open orbit in U if and only if there is an open orbit in $\mathrm{Gr}(V, m) \cong \mathrm{Gr}(V^*, n-m)$. Therefore, this is the case if and only if there is an open orbit in U^*.

Suppose that the orbit of $w \in U$ is open and corresponds to the orbit of $w^* \in U^*$. Note that the action of $\mathrm{GL}(m)$ on U does not have a fixed point (in other words the action is *free*). Therefore, the stabilizer of w in $G \times \mathrm{GL}(m)$ and the stabilizer of $\pi(w)$ in G are isomorphic. Similarly, the stabilizer of w^* in $G \times \mathrm{GL}(n-m)$ and the stabilizer of $\pi^*(w^*)$ in G are isomorphic. Since the stabilizers of $\pi(w), \pi^*(w^*)$ are isomorphic, this proves the second assertion. □

The following corollary is obvious.

Corollary 10.22. *The representation (1) is a regular prehomogeneous vector space if and only if the representation (2) is a regular prehomogeneous vector space.*

Definition 10.23. Two prehomogeneous vector spaces which are related as the two prehomogeneous vector spaces (1), (2) as above are called the *castling transform* of each other. If a prehomogeneous vector space is obtained from another prehomogeneous vector space by a finite number of castling transforms, we say that those prehomogeneous vector spaces belong to the same *castling class*. If (G, V) is a prehomogeneous vector space such that $\dim V$ is the smallest among prehomogeneous vector spaces in the castling class of (G, V), then we say that (G, V) is *reduced*.

If k is an algebraically closed field of characteristic zero, by a monumental work, Sato and Kimura classified irreducible reduced regular prehomogeneous vector spaces in [23] into 29 classes as follows.

(1) $G = \mathrm{GL}(n) \times G'$, $V = \mathrm{M}(n, n)$ where $G' \subset \mathrm{GL}(n)$ is a reductive subgroup such that Aff^n is an irreducible representation of G'.
(2) $G = \mathrm{GL}(1) \times \mathrm{GL}(n)$, $V = \mathrm{Sym}^2\mathrm{Aff}^n$.
(3) $G = \mathrm{GL}(2n)$, $V = \wedge^2\mathrm{Aff}^{2n}$.
(4) $G = \mathrm{GL}(1) \times \mathrm{GL}(2)$, $V = \mathrm{Sym}^3\mathrm{Aff}^2$.
(5) $G = \mathrm{GL}(1) \times \mathrm{GL}(6)$, $V = \wedge^3\mathrm{Aff}^6$.
(6) $G = \mathrm{GL}(1) \times \mathrm{GL}(7)$, $V = \wedge^3\mathrm{Aff}^7$.
(7) $G = \mathrm{GL}(1) \times \mathrm{GL}(8)$, $V = \wedge^3\mathrm{Aff}^8$.

(8) $G = \mathrm{GL}(3) \times \mathrm{GL}(2),\ V = \mathrm{Sym}^3 \mathrm{Aff}^2 \otimes \mathrm{Aff}^2$.
(9) $G = \mathrm{GL}(6) \times \mathrm{GL}(2),\ V = \wedge^2 \mathrm{Aff}^6 \otimes \mathrm{Aff}^2$.
(10) $G = \mathrm{GL}(5) \times \mathrm{GL}(3),\ V = \wedge^2 \mathrm{Aff}^5 \otimes \mathrm{Aff}^3$.
(11) $G = \mathrm{GL}(5) \times \mathrm{GL}(4),\ V = \wedge^2 \mathrm{Aff}^5 \otimes \mathrm{Aff}^4$.
(12) $G = \mathrm{GL}(3) \times \mathrm{GL}(3) \times \mathrm{GL}(2),\ V = \mathrm{M}(3,3) \otimes \mathrm{Aff}^2$.
(13) $G = \mathrm{GSp}(2n) \times \mathrm{GL}(2m),\ V = \mathrm{Aff}^{2n} \otimes \mathrm{Aff}^{2m}$ where $n \geq 2m \geq 2$.
(14) $G = \mathrm{GSp}(6)$ and $V = \mathrm{Aff}^{14}$ corresponds to the third fundamental weight.
(15) $G = \mathrm{GO}(n) \times \mathrm{GL}(m),\ V = \mathrm{M}(n,m)$.
(16) $G = \mathrm{GSpin}(7)$ and $V = \mathrm{spin} = \mathrm{Aff}^8$ is the spin representation.
(17) $G = \mathrm{GSpin}(7) \times \mathrm{GL}(2),\ V = \mathrm{spin} \otimes \mathrm{Aff}^2$.
(18) $G = \mathrm{GSpin}(7) \times \mathrm{GL}(3),\ V = \mathrm{spin} \otimes \mathrm{Aff}^3$.
(19) $G = \mathrm{GSpin}(9),\ V = \mathrm{spin} = \mathrm{Aff}^{16}$.
(20) $G = \mathrm{GSpin}(10) \times \mathrm{GL}(2),\ V = \mathrm{halfspin} \otimes \mathrm{Aff}^2$ where $\mathrm{halfspin} = \mathrm{Aff}^{16}$ is the half spin representation.
(21) $G = \mathrm{GSpin}(10) \times \mathrm{GL}(3),\ V = \mathrm{halfspin} \otimes \mathrm{Aff}^3$ where $\mathrm{halfspin} = \mathrm{Aff}^{16}$ is the half spin representation.
(22) $G = \mathrm{GSpin}(11),\ V = \mathrm{spin} = \mathrm{Aff}^{32}$.
(23) $G = \mathrm{GSpin}(12),\ V = \mathrm{halfspin} = \mathrm{Aff}^{32}$
(24) $G = \mathrm{GSpin}(14),\ V = \mathrm{halfspin} = \mathrm{Aff}^{64}$
(25) $G = \mathrm{G}_2 \times \mathrm{GL}(1),\ V = \mathrm{Aff}^7$ where G_2 is the automorphism group of the split octonion, Aff^7 is the imaginary part of the split octonion.
(26) $G = \mathrm{G}_2 \times \mathrm{GL}(2),\ V = \mathrm{Aff}^7 \otimes \mathrm{Aff}^2$.
(27) $G = \mathrm{E}_6 \times \mathrm{GL}(1),\ V = J$ where E_6 is a semi-simple group of type E_6 and $J = \mathrm{Aff}^{27}$ is the exceptional Jordan algebra.
(28) $G = \mathrm{E}_6 \times \mathrm{GL}(2),\ V = J \otimes \mathrm{Aff}^2$.
(29) $G = \mathrm{E}_7 \times \mathrm{GL}(1),\ V = \mathrm{Aff}^1 \oplus \mathrm{Aff}^1 \oplus J \oplus J$ where E_7 is a semi-simple group of type E_7.

Exercise 10.24. Suppose that $G_k \subset G$ is Zariski dense. Then show that

$$R_a = \{\Delta \in k[V] \mid \forall g \in G_k\ \Delta(gx) = \chi(g)\Delta(x)\}.$$

11. Prehomogeneous vector spaces and Galois cohomology

In this section we shall describe the rational orbit space $G_k\backslash V_k^{\rm ss}$ of regular prehomogeneous vector spaces in terms of Galois cohomology. After discussing the correspondence, we shall consider a few easy examples.

Let (G,V) be an irreducible regular prehomogeneous vector space. We assume that there exists a rational point $w\in V_k$ such that Gw is open. If so, G_w must be reductive. Note that if U is an open orbit, U contains a k-rational point. So if k is an infinite field, such w always exists. However, in all the cases we consider in later sections, we shall find such w explicitly regardless of k being infinite or not.

Let $x\in V_k^{\rm ss}$. Then there exists $g_x\in G_{k^{\rm sep}}$ such that $x=g_xw$. Since both x and w are rational points,

$$x^\sigma=g_x^\sigma w=x=g_xw \tag{11.1}$$

for all $\sigma\in{\rm Gal}(k^{\rm sep}/k)$. Therefore, $g_x^{-1}g_x^\sigma\in G_{w\,k^{\rm sep}}$. It is easy to see that

$$h_x=(g_x^{-1}g_x^\sigma)_{\sigma\in{\rm Gal}(k^{\rm sep}/k)} \tag{11.2}$$

is a 1-cocycle. We denote its class in ${\rm H}^1(k,G_w)$ by c_x. The class c_x is apparently trivial in ${\rm H}^1(k,G)$.

Theorem 11.3. (Igusa) *The map*

$$G_k\backslash V_k^{\rm ss}\ni x\to c_x\in{\rm Ker}({\rm H}^1(k,G_w)\to{\rm H}^1(k,G))$$

is well defined and is bijective.

Proof. Since the surjectivity is easy, we only prove the injectivity here. Suppose $c_x=c_y$. Then there exists $h\in G_{w\,k^{\rm sep}}$ such that

$$g_x^{-1}g_x^\sigma=h^{-1}g_y^{-1}g_y^\sigma h^\sigma$$

for all $\sigma\in{\rm Gal}(k^{\rm sep}/k)$. So

$$g_yhg_x^{-1}=g_y^\sigma h^\sigma(g_x^{-1})^\sigma=(g_yhg_x^{-1})^\sigma$$

for all σ. This implies $g_yhg_x^{-1}\in G_k$. Clearly $g_yhg_x^{-1}x=y$. So $G_kx=G_ky$. □

We consider the prehomogeneous vector spaces (1), (2) $n=3$, (3), (13) in the Sato-Kimura classification in the previous section.

Example 11.4. $G={\rm GL}(n)\times G'$, $V={\rm M}(n,n)$ where $G'\subset{\rm GL}(n)$ is a reductive subgroup such that ${\rm Aff}^n$ is an irreducible representation of G'.

The group G acts on V by $(g_1,g_2)x=g_1x\,{}^tg_2$ for $(g_1,g_2)\in G$, $x\in V$. Let $\Delta(x)=\det x$. Then $\Delta((g_1,g_2)x)=\det g_1\det g_2\Delta(x)$. Let $U=\{x\in V\mid\Delta(x)\neq0\}$. Obviously U is an open set. Since $U_k\cong{\rm GL}(n)_k$ as sets, U_k is a single G_k-orbit. So (G,V) is a prehomogeneous vector space and $\Delta(x)$ is a relative invariant polynomial. So obviously $V_k^{\rm ss}$ is U_k above.

If $w=I_n$,

$$G_w=\{(g,{}^tg^{-1})\mid g\in G'\}\cong G'.$$

So (G,V) is regular.

Example 11.5. $\operatorname{ch} k \neq 2,\ G = \mathrm{GL}(1) \times \mathrm{GL}(3),\ V = \mathrm{Sym}^2\mathrm{Aff}^3$ (the space of ternary quadratic forms).

This case is closely related to Example 4.9 because the generic stabilizer becomes GO(3) which we defined in Example 4.9. This is the first non-trivial example. In sections 7 and 8, we showed that k-forms of a given object X are parametrized by $\mathrm{H}^1(k, \mathrm{Aut}\,(X))$. We shall use this correspondence and show that $G_k\backslash V_k^{\mathrm{ss}}$ is in bijective correspondence with k-forms of PGL(2), SL(2), $\mathbb{P}^1$, and the associative algebra M(2, 2). Note that k-forms of M(2, 2) are called quarternion algebras.

Before discussing this example, we need some preparation. Consider the action ρ_d of GL(2) on $\mathrm{Sym}^d\mathrm{Aff}^2$ (the space of binary forms of degree d). We express elements x, y of $\mathrm{Sym}^d\mathrm{Aff}^2$ as

$$\begin{aligned} x &= x_0 v_1^d + x_1 v_1^{d-1} v_2 + \cdots + x_d v_2^d, \\ y &= y_0 v_1^d + y_1 v_1^{d-1} v_2 + \cdots + y_d v_2^d, \end{aligned}$$

where v_1, v_2 are the variables. Note that regarding x as a polynomial $x(v)$ of $v = \begin{pmatrix} v_1 & v_2 \end{pmatrix}$, $g \in \mathrm{GL}(2)$ acts on $\mathrm{Sym}^d\mathrm{Aff}^2$ by $x(v) \to \rho_d(g)x(v) = x(vg)$.

Suppose $\operatorname{ch} k$ is large enough so that $\binom{d}{1}, \cdots, \binom{d}{d} \neq 0$ in k. Define

$$\langle x, y \rangle = x_0 y_d - \binom{d}{1}^{-1} x_1 y_{d-1} + \binom{d}{2}^{-1} x_2 y_{d-2} - \cdots$$

where $\binom{d}{i}$ is the binomial coefficient. It is easy to show that

$$\langle \rho_d(g)x, \rho_d(g)y \rangle = (\det g)^d \langle x, y \rangle \tag{11.6}$$

for all $g \in \mathrm{GL}(2),\ x, y \in \mathrm{Sym}^d\mathrm{Aff}^2$.

If $d = 2$, we choose $\{v_1^2, v_1v_2, v_2^2\}$ as a basis for $\mathrm{Sym}^2\mathrm{Aff}^2$. Then with respect to this basis, the matrix of the bilinear form $\langle\ ,\ \rangle$ is

$$w = \begin{pmatrix} 0 & 0 & 1 \\ 0 & -1/2 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

Regard w as an element of $\mathrm{Sym}^2\mathrm{Aff}^3$. Note that it is enough to assume $\operatorname{ch} k \neq 2$ for w to be well defined.

Consider a representation $\bar{\rho}$ of GL(2) defined by $\bar{\rho}(g) = (\det g)^{-1}\rho_2(g)$. Then by (11.6)

$$\langle \bar{\rho}(g)x, \bar{\rho}(g)y \rangle = \langle x, y \rangle$$

for all $x, y \in \mathrm{Sym}^2\mathrm{Aff}^2$. If we regard x, y as column vectors and $\bar{\rho}(g)$ as a 3×3 matrix, then since the matrix of the bilinear form $\langle\ ,\ \rangle$ is w,

$${}^t x\, {}^t \bar{\rho}(g) w \bar{\rho}(g) y = {}^t x w y$$

for all x, y. Therefore, ${}^t\bar{\rho}(g) w \bar{\rho}(g) = w$.

Regard $V = \mathrm{Sym}^2\mathrm{Aff}^3$ as the space of 3×3 symmetric matrices. We define an action of the group $G = \mathrm{GL}(1) \times \mathrm{GL}(3)$ on V by $(t, g)x = tgx\,{}^tg$ for $(t, g) \in G,\ x \in V$. Define

$$\phi : \mathrm{GL}(2) \ni g \to {}^t\bar{\rho}(g)^{-1} \in G$$

This is a homomorphism from GL(2) to GL(3). Regarding $\mathrm{GL}(3) \subset G$, the above consideration shows the following lemma.

Lemma 11.7. *We have* $\phi(\mathrm{GL}(2)) \subset G_w$.

The homomorphism ϕ induces a linear map between the tangent spaces

$$d\phi : T(\mathrm{GL}(2))_e \to T(G_w^\circ)_e.$$

We consider the image of $d\phi$.

Let

$$L_1 = \left\{ \left(0, \begin{pmatrix} a & 2b & 0 \\ c & 0 & b \\ 0 & 2c & -2a \end{pmatrix}\right) \middle| a, b, c \in k \right\},$$
$$L_2 = \{(-2t, tI_3) \mid t \in k\}.$$

Lemma 11.8. *We have* $T(G_w)_e = L_1 \oplus L_2$.

Proof. Let $A = (a_{ij}) \in \mathrm{GL}(3)_k$. Then $A \in T(G_w)_e$ if and only if $Aw + w^tA = 0$. Writing down this condition explicitly,

$$\begin{pmatrix} a_{13} & -\frac{1}{2}a_{12} & a_{11} \\ a_{23} & -\frac{1}{2}a_{22} & a_{21} \\ a_{33} & -\frac{1}{2}a_{32} & a_{31} \end{pmatrix} + \begin{pmatrix} a_{13} & a_{23} & a_{33} \\ -\frac{1}{2}a_{12} & -\frac{1}{2}a_{22} & -\frac{1}{2}a_{32} \\ a_{11} & a_{21} & a_{31} \end{pmatrix} = 0.$$

So

$$2a_{13}, 2a_{31}, -a_{22}, a_{11} + a_{33}, -\frac{1}{2}a_{12} + a_{23}, -\frac{1}{2}a_{32} + a_{21}$$

are zero.

Since $\mathrm{ch}\, k \neq 2$, this is equivalent to the condition $A \in L_1 \oplus L_2$. $\square$

Since $\dim T(G_w)_e = 4 = \dim G - \dim V$, G_w is smooth over k.

Lemma 11.9. *We have* $d\phi(T(\mathrm{GL}(2))_e) = L_1$.

Proof. Let Z be the subgroup of GL(2) consisting of scalar matrices tI_2. Then Z is the center of GL(2). It is easy to see that $Z \cong \mathrm{GL}(1) \subset \mathrm{Ker}(\bar{\rho})$. So in order to consider the image of $d\phi$, we only have to consider elements of the form

$$\begin{pmatrix} a & b \\ c & -a \end{pmatrix}. \tag{11.10}$$

Let $\{v_1, v_2\}$ be the standard basis for Aff^2. Put $e_0 = v_1^2,\ e_1 = v_1v_2,\ e_2 = v_2^2$. Then $\{e_0, e_1, e_2\}$ is a basis for $\mathrm{Sym}^2\mathrm{Aff}^2$. The $k[\epsilon]/(\epsilon^2)$-valued point of GL(2) which corresponds to (11.10) is the map

$$\begin{aligned} \begin{pmatrix} v_1 & v_2 \end{pmatrix} &\to \begin{pmatrix} v_1 & v_2 \end{pmatrix} \left(I_2 + \epsilon \begin{pmatrix} a & b \\ c & -a \end{pmatrix} \right) \\ &= \begin{pmatrix} v_1 + \epsilon(av_1 + cv_2) & v_2 + \epsilon(bv_1 - av_2) \end{pmatrix}. \end{aligned}$$

The image of this map in GL(3) is the map

$$\begin{aligned} e_0 &\to v_1^2 + 2\epsilon v_1(av_1 + cv_2) = e_0 + 2\epsilon(av_1 + cv_2), \\ e_1 &\to v_1v_2 + \epsilon(v_2(av_1 + cv_2) + v_1(bv_1 - av_2)) = e_1 + \epsilon(be_0 + ce_2), \\ e_2 &\to v_2^2 + 2\epsilon v_1(bv_1 - av_2) = e_2 + 2\epsilon(bv_1 - av_2) \end{aligned}$$

So its matrix representation is

$$I_3 + \epsilon \begin{pmatrix} 2a & b & 0 \\ 2c & 0 & 2b \\ 0 & c & -2a \end{pmatrix}.$$

Since $d\phi = -{}^t d\bar{\rho}$, this proves the lemma. $\square$

By the above lemma, $\dim T(\mathrm{Ker}(\phi))_e = 1$ and so $\mathrm{Ker}(\phi) = Z$ as schemes. Since Z is reductive, the quotient $\mathrm{PGL}(2) = \mathrm{GL}(2)/Z$ is a geometric quotient, it is affine, and $\mathrm{PGL}(2) \subset G_w^\circ$.

Let

$$\widetilde{T} = \{(t^{-2}, tI_3) \in G \mid t \in \mathrm{GL}(1)\} \cong \mathrm{GL}(1).$$

Then $\widetilde{T}$ acts on $\mathrm{Sym}^2\mathrm{Aff}^3$ trivially and so $\widetilde{T} \subset G_w$. Obviously

$$T(\widetilde{T})_e = L_2. \tag{11.11}$$

Proposition 11.12. *We have $G_w^\circ = \mathrm{PGL}(2) \times \widetilde{T}$.*

Proof. We first show that $\mathrm{PGL}(2)_{\bar{k}} \cap \widetilde{T}_{\bar{k}} = \{1\}$. Note that $\mathrm{PGL}(2)_{\bar{k}} = \mathrm{GL}(2)_{\bar{k}}/Z_{\bar{k}}$. If $A = (a_{ij}) \in \mathrm{GL}(2)_{\bar{k}}$, $\phi(A) \in \widetilde{T}_{\bar{k}}$ if and only if $\bar{\rho}(A) \in \widetilde{T}_{\bar{k}}$. The matrix representation of $\bar{\rho}(A)$ is

$$(\det A)^{-1} \begin{pmatrix} a_{11}^2 & a_{11}a_{12} & a_{12}^2 \\ 2a_{11}a_{21} & a_{11}a_{22} + a_{12}a_{21} & 2a_{12}a_{22} \\ a_{21}^2 & a_{21}a_{22} & a_{22}^2 \end{pmatrix}.$$

So if $\bar{\rho}(A) \in \widetilde{T}_{\bar{k}}$, $a_{12}^2 = a_{21}^2 = 0$. So $a_{12} = a_{21} = 0$. This implies that $a_{11}, a_{22} \in \bar{k}^\times$. Also $a_{11}^2 = a_{11}a_{22}$, which implies that $a_{11} = a_{22}$. However, scalar matrices map to the identity element by $\bar{\rho}$. Therefore,

$$\mathrm{PGL}(2)_{\bar{k}} \cap \widetilde{T}_{\bar{k}} = \{1\}.$$

Consider the homomorphism $\mathrm{PGL}(2) \times \widetilde{T} \to G_w^\circ$ defined by ϕ and the inclusion map. We have shown above that this is injective set-theoretically. By Lemma 11.9 and (11.11), it induces a bijection between the tangent spaces. Since $\mathrm{PGL}(2) \times \widetilde{T}$ and G_w° are smooth over k, this is an isomorphism. $\square$

Proposition 11.13. *We have $G_w = G_w^\circ$.*

Proof. Since G_w° stays connected by field extensions, we may assume that $k = \bar{k}$.

Suppose $g = (g_1, g_2) \in G_{w\,k}$. Since $\widetilde{T}$ is contained in the center of G, the element g induces an automorphism of $\mathrm{PGL}(2)$ by $h \to ghg^{-1}$. It is known that any automorphism of $\mathrm{PGL}(2)$ is an inner automorphism. So there exists an element $g_0 \in \mathrm{PGL}(2) \subset G_w^\circ$ such that $ghg^{-1} = g_0hg_0^{-1}$ for all $h \in \mathrm{PGL}(2)$. Replacing g by gg_0^{-1}, we may assume that g commutes with elements of $\mathrm{PGL}(2)$.

Consider the element $\mu(t) = \bar{\rho}(\mathrm{diag}(t, 1, t^{-1}))$ for $t \in k^\times$. Then regarding $\mu(t)$ as a 3×3 matrix, its eigenspaces are spanned by

$$\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}.$$

Since g commutes with $\mu(t)$, g_2 must preserve the eigenspaces and so is a diagonal matrix. If $g = (t, \mathrm{diag}(\alpha, \beta, \gamma))$, writing down the condition $gw = w$ explicitly, it is easy to show that $\alpha = \beta = \gamma$ and $t = \alpha^{-2}$. So $g \in \widetilde{T}_k$. □

Proposition 11.14. *We have*

$$\begin{aligned} \mathrm{PGL}(2) &\cong \mathrm{Aut}\,(\mathrm{SL}(2)) \\ &\cong \mathrm{Aut}\,(\mathrm{PGL}(2)) \\ &\cong \mathrm{Aut}\,(\mathbb{P}^1) \\ &\cong \mathrm{Aut}\,(\mathrm{M}(2,2)). \end{aligned}$$

Proof. By Proposition 6.27 and Example 6.31, SL(2) is semi-simple and all automorphisms are inner. Since conjugation by elements of GL(2) also induce isomorphisms of SL(2), we have a homomorphism $\mathrm{GL}(2) \to \mathrm{Aut}\,(\mathrm{SL}(2))$. If $g \in \mathrm{GL}(2)$ is in the kernel of the homomorphism, g commutes with all elements of SL(2) and so g is a scalar matrix. Therefore, set-theoretically, $\mathrm{PGL}(2) \cong \mathrm{Aut}\,(\mathrm{SL}(2))$. If a tangent vector $I_2 + \epsilon A$ of GL(2) is in the kernel of this homomorphism, one can easily show that A is a scalar matrix also. Therefore, the homomorphism $\mathrm{PGL}(2) \cong \mathrm{Aut}\,(\mathrm{SL}(2))$ is an isomorphism of schemes. Note that we could have used PSL(2) instead because $\mathrm{PSL}(2) \cong \mathrm{PGL}(2)$. Once again we should probably point out that $\mathrm{PSL}(2)_k$ may not be $\mathrm{SL}(2)_k/\{\pm 1\}$.

It is easy to show the same thing for Aut (PGL(2)). The isomorphism $\mathrm{PGL}(2) \cong \mathrm{Aut}\,(\mathbb{P}^1)$ is well known. One can find the proof of this fact in 10.8 [2, pp. 141–144] for example (it shows a scheme-theoretic isomorphism). In Example 7.1.1 [6, p. 151], this isomorphism is proved set-theoretically but the proof can be modified to show a scheme-theoretic isomorphism. If $\phi \in \mathrm{Aut}\,(\mathrm{M}(2,2))$, it leaves the set of invertible elements $\mathrm{GL}(n)$ stable. Since ϕ is an isomorphism of k-algebras, it fixes any scalar matrix. Therefore, ϕ induces an automorphism of PGL(2) and ϕ is determined by this automorphism because GL(2) is dense in M(2,2). Therefore, $\mathrm{Aut}\,(\mathrm{M}(2,2)) \cong \mathrm{PGL}(2)$ also. □

By Propositions 11.12, 11.13, 11.14, we get the following theorem.

Theorem 11.15. *The representation (G, V) is a regular prehomogeneous vector space. Moreover,*

$$\begin{aligned} G_k \backslash V_k^{\mathrm{ss}} &\cong \{k\text{-forms of } \mathrm{PGL}(2)\}, \\ &\cong \{k\text{-forms of } \mathrm{SL}(2)\}, \\ &\cong \{k\text{-forms of } \mathbb{P}^1\}, \\ &\cong \{k\text{-forms of } \mathrm{M}(2,2)\}. \end{aligned}$$

Remark 11.16. It is possible to show that if $Q \in V_k^{\mathrm{ss}}$, then the corresponding k-form of $\mathbb{P}^1$ is the zero set of Q in $\mathbb{P}^2$. Also the corresponding quarternion algebra is the Clifford algebra of Q.

Example 11.17. $G = \mathrm{GL}(2n),\ V = \wedge^2 \mathrm{Aff}^{2n}$.

We regard $x \in V$ as a skew-symmetric matrix of dimension $2n$ with zero diagonal entries. Note that the last condition is necessary if $\mathrm{ch}\, k = 2$.

The group G acts on V by $x \to g\cdot x = gx^tg$ for $g \in G,\ x \in V$. It is known that there exists a polynomial $\mathrm{Pfaff}(x)$ called the Pfaffian of $x \in V$ such that $\det x = \mathrm{Pfaff}(x)^2$. This implies that

$$\mathrm{Pfaff}(g \cdot x)^2 = (\det g)^2 \mathrm{Pfaff}(x)^2.$$

Therefore, $\mathrm{Pfaff}(g \cdot x) = \pm \det g \mathrm{Pfaff}(x)$.

We show that $\mathrm{Pfaff}(g\cdot x) = \det g \mathrm{Pfaff}(x)$. If $\mathrm{ch}\, k = 2$, this is obvious. So we assume that $\mathrm{ch}\, k \neq 2$. We may assume that $k = \bar{k}$. The group G is connected (as a scheme). Since $U = \{x \in V \mid \mathrm{Pfaff}(x) \neq 0\}$ is an open subset of V, it is connected (since it is dense in V). Define

$$\begin{aligned} U_+ &= \{(g,x) \in G \times U \mid \mathrm{Pfaff}(g\cdot x) = \det g \mathrm{Pfaff}(x)\}, \\ U_- &= \{(g,x) \in G \times U \mid \mathrm{Pfaff}(g\cdot x) = -\det g \mathrm{Pfaff}(x)\}. \end{aligned}$$

Then since $U_\pm = U \setminus U_\mp$, U_+, U_- are both open and $U = U_+ \coprod U_-$. Since U is connected and $U_+ \neq \emptyset$, $U = U_+$. Therefore,

$$\mathrm{Pfaff}(g \cdot x) = \det g \mathrm{Pfaff}(x). \tag{11.18}$$

Let $w = \left(\begin{smallmatrix} 0 & I_n \\ -I_n & 0 \end{smallmatrix}\right)$. Then $G_w = \mathrm{Sp}(2n)$ (see Example 4.12). By an explicit computation, the tangent space at the unit element e of the stabilizer G_w is

$$T(G_w)_e = \left\{ \begin{pmatrix} A & B \\ C & -{}^tA \end{pmatrix} \,\middle|\, {}^tB = B,\ {}^tC = C \right\} \tag{11.19}$$

Therefore,

$$\dim \mathrm{Sp}(2n) = n^2 + 2 \cdot (n(n+1)/2) = 2n^2 + n$$

Since $2n^2 + n = \dim G - \dim V$, Gw is open and G_w is smooth over k. It is well known that $G_w = \mathrm{Sp}(2n)$ is a semi-simple group. So (G,V) is a regular prehomogeneous vector space.

It is well known that for any k, the set

$$\{x \in V_k \mid \det x \neq 0\}.$$

is a single G_k-orbit. Since $\mathrm{H}^1(k,G) = \{1\}$, $G_k \backslash V_k^{\mathrm{ss}}$ is in one-to-one correspondence with $\mathrm{H}^1(k, \mathrm{Sp}(2n))$. Therefore, $\mathrm{H}^1(k, \mathrm{Sp}(2n)) = \{1\}$.

Example 11.20. $G = \mathrm{Sp}(2n) \times \mathrm{GL}(2m),\ V = \mathrm{M}(2n, 2m)$ where $n \geq 2m \geq 2$.

The group G acts on V by $(g_1, g_2)x = g_1 x^t g_2$ for $(g_1, g_2) \in G\ x \in V$. Let $J_n = \left(\begin{smallmatrix} 0 & I_n \\ -I_n & 0 \end{smallmatrix}\right)$. We define J_m similarly. Define

$$\Phi(x) = {}^tx J_n x \in \mathrm{M}(2m, 2m)$$

for $x \in V$.

Note that $J_n J_n = -I_{2n}$. So if $g \in \mathrm{Sp}(2n)$,

$$\begin{aligned} gJ_n{}^tg = J_n &\Longrightarrow {}^tg^{-1} J_n^{-1} g^{-1} = J_n^{-1} \\ &\Longrightarrow -{}^tg^{-1} J_n g^{-1} = -J_n \\ &\Longrightarrow {}^tg^{-1} J_n g^{-1} = J_n. \end{aligned}$$

This implies that for all $g \in \mathrm{Sp}(2n)$, ${}^tg^{-1} \in \mathrm{Sp}(2n)$. Replacing g by g^{-1}, ${}^tg \in \mathrm{Sp}(2n)$.

If $(g_1, g_2) \in G$ and $x \in V$, then

$$
\begin{aligned}
\Phi((g_1,g_2)x) &= {}^t(g_1 x {}^t g_2) J_n (g_1 x {}^t g_2) \\
&= g_2 {}^t x ({}^t g_1 J_n g_1) x {}^t g_2 \\
&= g_2 {}^t x J_n x {}^t g_2 \\
&= g_2 \Phi(x) {}^t g_2.
\end{aligned} \tag{11.21}
$$

We let the first factor of G act on $\mathrm{M}(2m, 2m)$ trivially. Since the second factor of G acts on $\mathrm{M}(2m, 2m)$ naturally, we have an action of G on $\mathrm{M}(2m, 2m)$. The map Φ is equivariant with respect to the actions of G on V and $\mathrm{M}(2m, 2m)$.

Let

$$
w = \begin{pmatrix} I_m & 0 \\ 0 & 0 \\ 0 & I_m \\ 0 & 0 \end{pmatrix}.
$$

Then by an easy computation, $\Phi(w) = J_m$.

Define

$$
\Delta(x) = \mathrm{Pfaff}(\Phi(x)).
$$

This is a polynomial on V. By (11.18) and (11.21),

$$
\Delta((g_1, g_2)x) = \mathrm{Pfaff}(g_2 \Phi(x)) = \det g_2 \mathrm{Pfaff}(\Phi(x)) = \det g_2 \Delta(x).
$$

Since $\Delta(w) = \mathrm{Pfaff}(J_m) \neq 0$, $\Delta(x)$ is a relative invariant polynomial.

It is an interesting exercise problem to finish this example and prove that (G, V) is a regular prehomogeneous vector space and V_k^{ss} is a single G_k-orbit for any k. We leave this to the reader.

Exercise 11.22. Prove (11.6).

Exercise 11.23. Prove that (G, V) of Example 11.20 is a regular prehomogeneous vector space and V_k^{ss} is a single G_k-orbit for any k in the following order.

(1) Compute the tangent space at the unit element e of the stabilizer G_w.
(2) Prove that $G_w^\circ \cong \mathrm{Sp}(2m) \times \mathrm{Sp}(2(n-m))$.
(3) Prove that $G_w = G_w^\circ$.

12. Prehomogeneous vector spaces and field extensions

In this section we discuss the formulation to relate the rational orbit space $G_k \backslash V_k^{\text{ss}}$ with field extensions of the ground field k following [31], [11], [33].

We make the following assumption.

Assumption 12.1. There exists a point $w \in V_k^{\text{ss}}$ and a natural number i such that

(1) $\mathrm{Gal}(k^{\text{sep}}/k)$ acts trivially on G_w/G_w°,
(2) $G_w/G_w^\circ \cong \mathfrak{S}_i$,
(3) the following sequence is exact and split.

$$1 \longrightarrow G_w^\circ \longrightarrow G_w \longrightarrow \mathfrak{S}_i \longrightarrow 1 \tag{12.2}$$

Since (12.2) is a split exact sequence, there is a natural surjective map $\mathrm{H}^1(k, G_w) \to \mathrm{H}^1(k, \mathfrak{S}_i)$. Therefore, we have a natural map

$$\gamma_V : G_k \backslash V_k^{\text{ss}} \to \mathrm{H}^1(k, \mathfrak{S}_i). \tag{12.3}$$

We consider the set $\mathrm{H}^1(k, \mathfrak{S}_i)$ now. Let $h = (h_\sigma)_\sigma$ be a 1-cocycle. The cocycle condition becomes

$$h_{\sigma\tau} = h_\tau h_\sigma^\tau = h_\tau h_\sigma.$$

Therefore, h is an anti-homomorphism. So the map

$$\lambda_h : \mathrm{Gal}(k^{\text{sep}}/k) \ni \sigma \to h_\sigma^{-1} \in \mathfrak{S}_i \tag{12.4}$$

is a homomorphism.

Suppose $h_1 = (h_{1\,\sigma})_\sigma, h_2 = (h_{2\,\sigma})_\sigma : \mathrm{Gal}(k^{\text{sep}}/k) \to \mathfrak{S}_i$ are 1-cocycles. If they are equivalent, there exists an element $g \in \mathfrak{S}_i$ such that

$$h_{1\,\sigma} = g^{-1} h_{2\,\sigma} g^\sigma = g^{-1} h_{2\,\sigma} g$$

for all σ. So

$$\lambda_{h_1}(\sigma) = g^{-1} \lambda_{h_1}(\sigma) g$$

also. Therefore, $\mathrm{H}^1(k, \mathfrak{S}_i)$ is in bijective correspondence with conjugacy classes of homomorphisms from $\mathrm{Gal}(k^{\text{sep}}/k)$ to $\mathfrak{S}_i$. So $\mathrm{Ker}(\lambda_h)$ depends only on the cohomology class of h.

Definition 12.5. If $h = (h_\sigma)_\sigma$ is a 1-cocycle, then $N_h = \mathrm{Ker}(\lambda_h)$, F_h/k is the corresponding Galois extension, and $\Gamma_h = \mathrm{Gal}(F_h/k)$.

By the above remark, N_h, F_h, Γ_h depend only on the cohomology class of h.

Definition 12.6. We define $\mathfrak{Ex}_i$ to be the set of isomorphism classes of Galois extensions of k which are splitting fields of degree i equations without multiple roots.

If $x \in V_k^{\text{ss}}$, we denote the field which corresponds to the cohomology class $\gamma_V(x) \in \mathrm{H}^1(k, \mathfrak{S}_i)$ by $\alpha_V(x)$ or simply, $k(x)$. This does *not* mean the residue field of $x \in V$, because that is k since x is a k-rational point.

Remark 12.7. It is known that fields of the form F_h always belong to $\mathfrak{Ex}_i$.

We describe the fibers of the map γ_V now. Let $x \in V_k^{\mathrm{ss}}$. We choose an element $g_x \in G_{k^{\mathrm{sep}}}$ so that $x = g_x w$. Then for each element $c \in \mathrm{H}^1(k, G_w)$ defined by a 1-cocycle $(h_\sigma)_\sigma$, we can associate an element ${}^{g_x}c \in \mathrm{H}^1(k, G_x)$ defined by the 1-cocycle $(g_x h_\sigma (g_x^\sigma)^{-1})_\sigma$. Note that since $(g_x^\sigma)^{-1} g_x \in G_{w\,k^{\mathrm{sep}}}$ (but may not be in $G^\circ_{w\,k^{\mathrm{sep}}}$),

$$g_x h_\sigma (g_x^\sigma)^{-1} = g_x (h_\sigma (g_x^\sigma)^{-1} g_x) g_x^{-1} \in G_{x\,k^{\mathrm{sep}}}.$$

It is easy to see that the map $\mathrm{H}^1(k, G_w) \ni c \to {}^{g_x}c \in \mathrm{H}^1(k, G_x)$ is well defined and does not depend on the choice of g_x. Also a similar construction using g_x^{-1} defines a map from $\mathrm{H}^1(k, G_x)$ to $\mathrm{H}^1(k, G_w)$. So we have the following lemma.

Lemma 12.8. *The map*

$$\mathrm{H}^1(k, G_w) \ni c \to {}^{g_x}c \in \mathrm{H}^1(k, G_x)$$

is bijective.

Let $x \in V_k^{\mathrm{ss}}$. By the exact sequence

$$(12.9) \qquad 1 \longrightarrow G_x^\circ \longrightarrow G_x \longrightarrow G_x/G_x^\circ \longrightarrow 1$$

and Theorem 9.2, $(G_x/G_x^\circ)_k \backslash \mathrm{H}^1(k, G_x^\circ)$ can be regarded as a subset of $\mathrm{H}^1(k, G_x)$, which is in bijective correspondence with $\mathrm{H}^1(k, G_w)$. It is easy to see that $c \in \mathrm{H}^1(k, G_w)$ maps to the trivial element of $\mathrm{H}^1(k, G)$ if and only if ${}^{g_x}c \in \mathrm{H}^1(k, G_x)$ maps to the trivial element of $\mathrm{H}^1(k, G)$ by the imbedding $G_x \subset G$. So cohomology classes in $(G_x/G_x^\circ)_k \backslash \mathrm{H}^1(k, G_x^\circ)$ which correspond to rational orbits are those in

$$\mathrm{Ker}((G_x/G_x^\circ)_k \backslash \mathrm{H}^1(k, G_x^\circ) \to \mathrm{H}^1(k, G)).$$

Theorem 12.10. (1) *If $x \in V_k^{\mathrm{ss}}$,*

$$\gamma_V^{-1}(\gamma_V(G_k x)) \cong \mathrm{Ker}((G_x/G_x^\circ)_k \backslash \mathrm{H}^1(k, G_x^\circ) \to \mathrm{H}^1(k, G)).$$

(2) *By this identification, the cohomology class $(g^{-1} g^\sigma)_\sigma \in \mathrm{H}^1(k, G_x^\circ)$ ($g \in G_{k^{\mathrm{sep}}}$) corresponds to the orbit $G_k g x$.*

Proof. Let $x = g_x w$ and $y \in V_k^{\mathrm{ss}}$. Then $y = gx$ for some $g \in G_{k^{\mathrm{sep}}}$. So $y = g g_x w$, which implies that y corresponds to the cohomology class $c = ((g g_x)^{-1} (g g_x)^\sigma)_\sigma$. Therefore, by the identification in Lemma 12.8,

$${}^{g_x}c = (g_x (g g_x)^{-1} (g g_x)^\sigma (g_x^\sigma)^{-1})_\sigma = (g^{-1} g^\sigma)_\sigma.$$

So if we identify $G_x \backslash V_k^{\mathrm{ss}}$ with $\mathrm{H}^1(k, G_x)$, the orbit of y corresponds to the cohomology class $c_{x,y} = (g^{-1} g^\sigma)_\sigma$. Because of Theorem 9.2, we only have to prove that $\gamma_V(y) = \gamma_V(x)$ if and only if $c_{x,y}$ comes from $\mathrm{H}^1(k, G_x^\circ)$.

Since both x and w are rational elements, $x = g_x^\sigma w$ for all σ. Therefore,

$$G_{x\,k^{\mathrm{sep}}} = g_x G_{w\,k^{\mathrm{sep}}} g_x^{-1} = g_x^\sigma G_{w\,k^{\mathrm{sep}}} (g_x^\sigma)^{-1},$$
$$G^\circ_{x\,k^{\mathrm{sep}}} = g_x G^\circ_{w\,k^{\mathrm{sep}}} g_x^{-1} = g_x^\sigma G^\circ_{w\,k^{\mathrm{sep}}} (g_x^\sigma)^{-1}.$$

Since the sequence (12.2) is split, we regard $\mathfrak{S}_i$ as a subgroup of G_w. Suppose $y = gx = g g_x w$ satisfies the condition $\gamma_V(y) = \gamma_V(x)$. Then $(g_x^{-1} g^{-1} g^\sigma g_x^\sigma)_\sigma$ and $(g_x^{-1} g_x^\sigma)_\sigma$ map to the same element in $\mathrm{H}^1(k, \mathfrak{S}_i)$. So there exist $r \in \mathfrak{S}_i$ and $n_\sigma \in G^\circ_{w\,k^{\mathrm{sep}}}$ such that

$$g_x^{-1} g^{-1} g^\sigma g_x^\sigma = r^{-1} g_x^{-1} g_x^\sigma r n_\sigma.$$

We can modify the above equation as

$$(g_x r^{-1} g_x^{-1})^{-1}(g^{-1}g^\sigma)(g_x r^{-1} g_x^{-1})^\sigma = g_x^\sigma r n_\sigma r^{-1}(g_x^\sigma)^{-1}.$$

The left hand side defines the same cohomology class as $(g^{-1}g^\sigma)_\sigma$ in $\mathrm{H}^1(k, G_x)$ and the right hand side belongs to $G^\circ_{x\,k^{\mathrm{sep}}}$. Therefore, this cohomology class comes from $\mathrm{H}^1(k, G_x^\circ)$.

Conversely, if $(g^{-1}g^\sigma)_\sigma$ comes from $\mathrm{H}^1(k, G_x^\circ)$, by changing g is necessary, we may assume that $g^{-1}g^\sigma \in G^\circ_{x\,k^{\mathrm{sep}}}$ for all σ. Then

$$g_x^{-1}g^{-1}g^\sigma g_x^\sigma = g_x^{-1}g_x^\sigma(g_x^\sigma)^{-1}g^{-1}g^\sigma g_x^\sigma,$$

and

$$(g_x^\sigma)^{-1}g^{-1}g^\sigma g_x^\sigma \in G^\circ_{w\,k^{\mathrm{sep}}}$$

for all η. Therefore, $\gamma_V(y) = \gamma_V(x)$. This proves the theorem. □

If $k = \mathbb{F}_q$ (the finite field with q-elements), the following theorem is known (see [14]).

Theorem 12.11. (**Lang**) *Let G be a connected algebraic group over $\mathbb{F}_q$, then $\mathrm{H}^1(\mathbb{F}_q, G) = \{1\}$.*

So Theorem 12.10 immediately implies the following corrolary.

Corollary 12.12. *Suppose $k = \mathbb{F}_q$ and Assumption 12.1 is satisfied. Then γ_V gives a bijection between $G_k\backslash V_k^{\mathrm{ss}}$ and $\mathrm{H}^1(k, \mathfrak{S}_i)$.*

In the subsequent sections, we determine the orbit space $G_k\backslash V_k^{\mathrm{ss}}$ and interpret its meaning for various prehomogeneous vector spaces. Many of these examples arise from maximal parabolic subgroups of exceptional groups. Mizuno (see [17], [18]) classified unipotent orbits of exceptional groups E_6, E_7, E_8 over finite fields, thus giving representatives of the orbit space $G_k\backslash V_k^{\mathrm{ss}}$ (for example, the quintic case in section 16). However, the meaning of the orbit space cannot easily be read from his results.

13. Binary quadratic and cubic forms

In this section we determine $G_k\backslash V_k^{\mathrm{ss}}$ for the following representations

(1) $G = \mathrm{GL}(1) \times \mathrm{GL}(2),\ V = \mathrm{Sym}^2\mathrm{Aff}^2$,
(2) $G = \mathrm{GL}(1) \times \mathrm{GL}(2),\ V = \mathrm{Sym}^3\mathrm{Aff}^2$.

These are the cases (2) $n = 2$, (4) in the Sato-Kimura classification in section 10. We follow [31], [11] in sections 13–17

We regard V as the space of homogeneous polynomials in two variables $v = (v_1, v_2)$ of degree two or three. We regard v as a row vector. We express elements of V as

$$x = x(v) = \begin{cases} x_0v_1^2 + x_1v_1v_2 + x_2v_2^2 & (1), \\ x_0v_1^3 + x_1v_1^2v_2 + x_2v_1v_2^2 + x_3v_2^3 & (2). \end{cases} \tag{13.1}$$

The group G acts on V by $(t, g_1)x(v) = tx(vg_1)$ for $g = (t, g_1) \in G,\ x(v) \in V$. These are irreducible representations unless $\mathrm{ch}\, k = 2$ in the case (1). However, it is obvious that Condition 10.1 is satisfied.

Define

$$\widetilde{T} = \begin{cases} \{(t^{-2}, tI_2) \mid t \in \mathrm{GL}(1)\} & (1), \\ \{(t^{-3}, tI_2) \mid t \in \mathrm{GL}(1)\} & (2). \end{cases} \tag{13.2}$$

Then $\widetilde{T} = \mathrm{Ker}(G \to \mathrm{GL}(V)) \cong \mathrm{GL}(1)$ in both cases. We put

$$w = \begin{cases} v_1v_2 & (1), \\ v_1v_2(v_1 - v_2) & (2). \end{cases} \tag{13.3}$$

If $V_k \ni x(v) \neq 0$ factors as

$$x = x(v) = \begin{cases} (v_1 - \alpha_1v_2)(v_1 - \alpha_2v_2) & (1), \\ (v_1 - \alpha_1v_2)(v_1 - \alpha_2v_2)(v_1 - \alpha_3v_2) & (2), \end{cases}$$

then we define a subset $\mathrm{Zero}(x) \subset \mathbb{P}^1$ called the *zero set* of x by

$$\mathrm{Zero}(x) = \begin{cases} \{(1, \alpha_1), (1, \alpha_2)\} & (1), \\ \{(1, \alpha_1), (1, \alpha_2), (1, \alpha_3)\} & (2). \end{cases} \tag{13.4}$$

Note that we allow α_i to be ∞.

Suppose $x, y \in V_{k^{\mathrm{sep}}},\ g = (t, g_1) \in G_{k^{\mathrm{sep}}}$, and $y = gx$. Regard $\mathrm{Zero}(x)$ as a set of row vectors. Then

$$\begin{aligned} v \in \mathrm{Zero}(y) &\Longleftrightarrow y(v) = 0 \\ &\Longleftrightarrow tx(vg_1) = 0 \\ &\Longleftrightarrow vg_1 \in \mathrm{Zero}(x) \\ &\Longleftrightarrow v \in \mathrm{Zero}(x)g_1^{-1}. \end{aligned} \tag{13.5}$$

Proposition 13.6. *In both cases (G, V) is a regular prehomogeneous vector space. Moreover,*

$$G_w^\circ \cong \begin{cases} \mathrm{GL}(1)^2 & (1), \\ \mathrm{GL}(1) & (2). \end{cases}$$

Proof. We first determine $T(G_w)_e$. Consider the action of

$$\left(1+\epsilon t, I_2+\epsilon\begin{pmatrix} a & b \\ c & d\end{pmatrix}\right)$$

where $k[\epsilon]/(\epsilon^2)$ is the ring of dual numbers. We write w as $w(v)$. Since v is replaced by (av_1+cv_2, bv_1+dv_2),

$$w(v) \to \epsilon t w(v) + w\left(v_1+\epsilon(av_1+cv_2) \quad v_2+\epsilon(bv_1+dv_2)\right). \tag{13.7}$$

In the case (1), (13.7) equals

$$w(v)+\epsilon(bv_1^2+(t+a+d)v_1v_2+cv_2^2).$$

So if this is $w(v)$, $b=c=0,\ t=-(a+d)$. This implies that $T(G_w)_e$ consists of elements of the form

$$\left(-(a+d), \begin{pmatrix} a & 0 \\ 0 & d\end{pmatrix}\right).$$

Therefore, $\dim T(G_w)_e = 2 = \dim G - \dim V$. So Gw is open and G_w is smooth over k.

Let

$$H=\left\{\left((t_1t_2)^{-1}, \begin{pmatrix} t_1 & 0 \\ 0 & t_2\end{pmatrix}\right) \middle| t_1,t_2\in \mathrm{GL}(1)\right\}.$$

Then obviously $H\cong \mathrm{GL}(1)^2$ is contained in G_w. Since we have already shown that $\dim G_w=2$, $G_w^\circ = H$. So G_w is reductive and this proves the proposition for the case (1).

In the case (2), (13.7) equals

$$w(v)+\epsilon(bv_1^3+(t+2a+2b+d)v_1^2v_2+(t+a+2c+2d)v_1v_2^2+cv_2^3).$$

So if this is $w(v)$, $b=c=0,\ a=d,\ t=-3a$. This implies that $T(G_w)_e$ consists of elements of the form

$$(-3a, aI_3).$$

Therefore, $\dim T(G_w)_e = 1 = \dim G - \dim V$. So Gw is open and G_w is smooth over k.

Obviously, $\widetilde{T}\subset G_w$. Since $\dim G_w=1$, $G_w^\circ=\widetilde{T}$. This proves the proposition for the case (2). $\square$

Remark 13.8. In both cases, the discriminant $\Delta(x)$ of $x(v)$ is a relative invariant polynomial. Explicitly,

$$\Delta(x)=\begin{cases} x_1^2-4x_0x_2 & (1), \\ x_1^2x_2^2+18x_0x_1x_2x_3-4x_0x_2^3-4x_1^3x_3-27x_0^2x_3^2 & (2). \end{cases}$$

It is easy to see that this $\Delta(x)$ satisfies the relation $\Delta((t,g_1)x)=\chi(t,g_1)\Delta(x)$ where

$$\chi(t,g_1)=\begin{cases} t^2(\det g_1)^2 & (1), \\ t^4(\det g_1)^6 & (2). \end{cases}$$

Let $i = 2, 3$ for the cases (1), (2) respectively. Put

$$p_1 = (1,0),\ p_2 = (0,1),\ p_3 = (1,1) \in \mathbb{P}^1. \tag{13.9}$$

Then it is easy to see that

$$\mathrm{Zero}(w) = \{p_1, p_2\} \text{ or } \{p_1, p_2, p_3\} \tag{13.10}$$

Since V^{ss} is a single orbit over k^{sep}, if $x \in V^{\mathrm{ss}}_{k^{\mathrm{sep}}}$, Zero$(x)$ consists of i points in $\mathbb{P}^1$.

Let $x \in V^{\mathrm{ss}}_{\bar{k}}$ and

$$\mathrm{Zero}(x) = \{p_{x\,1}, p_{x\,2}\} \text{ or } \{p_{x\,1}, p_{x\,2}, p_{x\,3}\}. \tag{13.11}$$

If $(t, g_1) \in G_{x\,\bar{k}}$ then $\mathrm{Zero}(x)g_1^{-1} = \mathrm{Zero}(x)$ by (13.5).

If $x \in V^{\mathrm{ss}}_k$, then Zero(x) can be regarded as a scheme over k and the map $\pi_x(g)$: $\mathrm{Zero}(x) \ni q \to qg_1 \in \mathrm{Zero}(x)$ for $g = (t, g_1) \in G_x$ is a homomorphism $G_x \to \mathrm{Aut}\,(\mathrm{Zero}(x))$ of group schemes over k. Note that we define the product of $\phi_1, \phi_2 \in \mathrm{Aut}\,(\mathrm{Zero}(x))$ by $\phi_1\phi_2 = \phi_2 \circ \phi_1$. If $x = w$ then Zero(w) is a set of discrete points and so $\mathrm{Aut}\,(\mathrm{Zero}(w)) \cong \mathfrak{S}_i$. Since $\mathrm{Aut}\,(\mathrm{Zero}(x))$ is isomorphic to $\mathrm{Aut}\,(\mathrm{Zero}(w))$ over $\bar{k}$, it is an algebraic group.

Over $\bar{k}$, we consider π_x set-theoretically and identify π_x with a homomorphism $\pi_x : G_{x\,\bar{k}} \to \mathfrak{S}_i$ defined by

$$p_{x\,j}g_1 = p_{x\,\pi_x(g)(j)} \quad \text{for all } j. \tag{13.12}$$

Note that the above definition of π_x depends on the choice of the order of Zero(x). However, changing the order of Zero(x) corresponds to taking a conjugate of π_x and so its conjugacy class does not depend on the choice of the order of Zero(x).

Let

$$\tau_1 = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix},\ \tau_2 = \begin{pmatrix} -1 & 0 \\ 1 & 1 \end{pmatrix}. \tag{13.13}$$

The following lemma is easy to verify and the proof is left to the reader.

Lemma 13.14. *The element τ_1 belongs to G_w in both cases and the element τ_2 belongs to G_w in the case (2).*

Obviously, τ_1 generates a subgroup of order two for the case (1). Moreover, τ_1 maps to the transposition (12) by the homomorphism π_w.

Lemma 13.15. *The elements τ_1, τ_2 generate a subgroup of* GL(2) *which maps to $\mathfrak{S}_3$ bijectively by the homomorphism π_w.*

Proof. Let $\nu = \tau_1\tau_2$. Then $\langle \tau_1, \tau_2 \rangle = \langle \tau_1, \nu \rangle$. By easy computations, $\tau_1^2 = \nu^3 = 1$, $\tau_1\nu\tau_1 = \nu^{-1}$. Therefore, there is a surjective homomorphism $\mathfrak{S}_3 \to \langle \tau_1, \tau_2 \rangle$ and so the order of $\langle \tau_1, \tau_2 \rangle$ is at most six.

By the homomorphism π_w, τ_1, τ_2 map to the transpositions (12), (23) respectively. Therefore, π_w is surjective. Since the order of $\langle \tau_1, \tau_2 \rangle$ is at most six, it must be exactly six and π_w is an isomorphism. □

Now we are ready to prove the following proposition.

Proposition 13.16. *In both cases, Assumption 12.1 is satisfied.*

Proof. Lemma 13.15 and the comment before it implies that π_w is a surjective homomorphism from G_w to $\mathfrak{S}_i$. Since $\mathfrak{S}_i$ is a finite group, we only have to show that $\mathrm{Ker}(\pi_w) = G_w^\circ$ set-theoretically.

Let $g = (t, g_1) \in \mathrm{Ker}(\pi_w)_{\bar{k}}$. Then g_1 fixes the set $\{p_1, p_2\}$ or $\{p_1, p_2, p_3\}$ pointwise. This implies that in the case (1), g_1 is a diagonal matrix and that in the case (2), g_1 is a scalar matrix. The condition $g \in G_w$ then implies that $g \in G_w^\circ$. $\square$

Let i be an arbitrary positive integer. Let β_i be the natural map $\mathrm{H}^1(k, \mathfrak{S}_i) \to \mathfrak{Ex}_i$. we consider the fiber structure of β_i.

Let $h = (h_\sigma)_\sigma$ be a 1-cocycle which defines an element in $\mathrm{H}^1(k, \mathfrak{S}_i)$. Let λ_h, N_h, F_h be as in (12.4), (12.5).

We fix a field $F \in \mathfrak{Ex}_i$. Let $N \subset \mathrm{Gal}(k^{\mathrm{sep}}/k)$ be the corresponding subgroup and $\Gamma = \mathrm{Gal}(F/k) \subset \mathfrak{S}_i$. Then

$$\beta_i^{-1}(F) = \{h \in \mathrm{H}^1(k, \mathfrak{S}_i) \mid \Gamma_h \cong \Gamma\}. \tag{13.17}$$

Moreover, λ_h induces this isomorphism.

If $h_1 = (h_{1\,\sigma})_\sigma, h_2 = (h_{2\,\sigma})_\sigma$ are 1-cocycles, then they define the same element in $\mathrm{H}^1(k, \mathfrak{S}_i)$ if and only if there exists $\nu \in \mathfrak{S}_i$ such that $h_{1\,\sigma}^{-1} = \nu^{-1} h_{2\,\sigma}^{-1} \nu$. So the subgroups $\mathrm{Im}(\lambda_{h_1}), \mathrm{Im}(\lambda_{h_2}) \subset \mathfrak{S}_i$ are conjugate.

Let $\Gamma_1, \cdots, \Gamma_{j_F}$ be the conjugacy classes of subgroups in $\mathfrak{S}_i$ which are isomorphic to Γ. Suppose both $\mathrm{Im}(\lambda_{h_1}), \mathrm{Im}(\lambda_{h_2})$ are conjugate to Γ_j. By taking conjugates if necessary, we may assume that $\mathrm{Im}(\lambda_{h_1}) = \mathrm{Im}(\lambda_{h_2}) = \Gamma_j$. Then $\lambda_{h_1}, \lambda_{h_2}$ can be regarded as automorphisms of Γ_j.

Therefore, if we define an equivalence relation on $\mathrm{Aut}\,(\Gamma_j)$ by

$$f_1 \sim f_2 \Longleftrightarrow \exists \nu \in \mathfrak{S}_i\ \forall \sigma \in \Gamma_j\ f_1(\sigma) = \nu^{-1} f_2(\sigma) \nu \tag{13.18}$$

for $f_1, f_2 \in \mathrm{Aut}\,(\Gamma_j)$, we obtain the following lemma.

Lemma 13.19. *We have* $\beta_i^{-1}(F) \cong \coprod_{j=1}^{j_F} \mathrm{Aut}\,(\Gamma_j)/\sim$.

Proposition 13.20. *The map* $\beta_i : \mathrm{H}^1(k, \mathfrak{S}_i) \to \mathfrak{Ex}_i$ *is bijective for* $i = 2, 3$.

Proof. Let F, N, Γ be as before. If $\Gamma = \{1\}$ or $\mathbb{Z}/2\mathbb{Z}$, $\mathrm{Aut}\,(\Gamma)$ consists of the identity map. This implies that $\beta_i^{-1}(F)$ is a single point.

If $\Gamma = \mathfrak{S}_3$, the proposition follows from the following fact.

Theorem 13.21. *Suppose $i \neq 6$. Then all automorphisms of $\mathfrak{S}_i$ are inner. Moreover, they coincide with automorphisms of A_i.*

For the proof of the above theorem, see (2.18) [26, p. 300].

If $\Gamma \cong \mathbb{Z}/3\mathbb{Z}$, $\Gamma = A_3$. So by Theorem 13.21 again, $\beta_i^{-1}(F)$ is a single point. $\square$

Let $x \in V_k^{\mathrm{ss}}$. We choose $g_x \in G_{k^{\mathrm{sep}}}$ so that $x = g_x w$. Then $(g_x^{-1} g_x^\sigma)_\sigma$ is the corresponding cohomology class in $\mathrm{H}^1(k, G_w)$. Let $\mathrm{Zero}(x)$ be as in (13.11). Define a map $\phi : \mathrm{Gal}(k^{\mathrm{sep}}/k) \to \mathfrak{S}_i$ by

$$p_{x\,j}^\sigma = p_{x\,\phi(\sigma)(j)} \text{ for all } j. \tag{13.22}$$

It is easy to verify that ϕ is a homomorphism. Also define a homomorphism $\psi : \mathrm{Gal}(k^{\mathrm{sep}}/k) \to \mathfrak{S}_i$ by

$$\psi(\sigma) = \pi_w (g_x^{-1} g_x^\sigma)^{-1}. \tag{13.23}$$

Proposition 13.24. *There exists $\nu \in \mathfrak{S}_i$ such that $\phi(\sigma) = \nu^{-1}\psi(\sigma)\nu$.*

Proof. Since we are allowed to take conjugates, we may assume that $p_{x\,j} = p_j g_{x\,1}^{-1}$ for all j. So

$$\begin{aligned} p_{x\,j}^{\sigma} &= p_j (g_{x\,1}^{\sigma})^{-1} \\ &= p_j (g_{x\,1}^{\sigma})^{-1} g_{x\,1} g_{x\,1}^{-1} \\ &= p_{\psi(\sigma)(j)} g_{x\,1}^{-1} \\ &= p_{x\,\psi(\sigma)(j)}. \end{aligned}$$

Therefore, $\phi(\sigma) = \psi(\sigma)$. □

This proposition implies that in order to determine the conjugacy class of the homomorphism from $\mathrm{Gal}(k^{\mathrm{sep}}/k)$ to $\mathfrak{S}_i$ which corresponds to the orbit of x, it suffices to consider the action of $\mathrm{Gal}(k^{\mathrm{sep}}/k)$ on $\mathrm{Zero}(x)$.

We shall construct an element w_α in the fiber of γ_V for each cohomology class in $\mathrm{H}^1(k, \mathfrak{S}_i)$. Let F, N, Γ be as before.

We consider the case (1) first. Let $\alpha = (\alpha_1, \alpha_2)$ be the roots of a quadratic polynomial

$$w_\alpha(v) = v_1^2 + a_1 v_1 v_2 + a_2 v_2^2 \tag{13.25}$$

where $a_1, a_2 \in k$. We assume that $\alpha_1 \neq \alpha_2$. We denote $k(\alpha) = k(\alpha_1, \alpha_2)$.

If $F = k$ then we may choose either w or w_α where $\alpha = (0, 1)$ as a point which corresponds to F. If $F = k(\alpha)$ is a quadratic extension of k, then by Proposition 13.24, w_α corresponds to the natural homomorphism $\mathrm{Gal}(k^{\mathrm{sep}}/k) \to \mathrm{Gal}(k(\alpha)/k)$. Since β_2 is one-to-one, we may choose w_α as a point which corresponds to F.

We shall find $g_\alpha \in G_{k^{\mathrm{sep}}}$ such that $w_\alpha = g_\alpha w$. Let

$$g_\alpha = \left(-1, \begin{pmatrix} 1 & -1 \\ -\alpha_1 & \alpha_2 \end{pmatrix}\right). \tag{13.26}$$

If σ is the non-trivial element of $\mathrm{Gal}(k(\alpha)/k)$, then $g_\alpha^{-1} g_\alpha^{\sigma} = \tau_1$. It is easy to verify

$$w_\alpha = g_\alpha w. \tag{13.27}$$

Next we consider the case (2). Let $\alpha = (\alpha_1, \alpha_2, \alpha_3)$ be the roots of a cubic polynomial

$$w_\alpha(v) = v_1^3 + a_1 v_1^2 v_2 + a_2 v_1 v_2^2 + a_3 v_2^3 \tag{13.28}$$

where $a_1, a_2, a_3 \in k$. We assume that $\alpha_1, \alpha_2, \alpha_3$ are distinct. We denote $k(\alpha) = k(\alpha_1, \alpha_2, \alpha_3)$. Then by Proposition 13.24 again, w_α corresponds to the natural homomorphism $\mathrm{Gal}(k^{\mathrm{sep}}/k) \to \mathrm{Gal}(k_\alpha/k)$.

If $F = k$, we choose w as a point which corresponds to F. Note that if $F = \mathbb{F}_2$, we cannot choose a representative of the form w_α.

If F is a quadratic extension of k, consider $\alpha = (\alpha_1, \alpha_2, 0)$ where α_1, α_2 are conjugate and $F = k(\alpha)$. For other cases, F is the splitting field of a cubic polynomial w_α of the form (13.28) which is irreducible. In both cases, we may choose w_α as a point which corresponds to F.

We shall find $g_\alpha \in G_{k^{\mathrm{sep}}}$ such that $w_\alpha = g_\alpha w$. Let

$$D_\alpha = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3),$$

(13.29)
$$g_\alpha(v) = \left(1, D_\alpha^{-1}\begin{pmatrix} -(\alpha_3-\alpha_1) & -(\alpha_3-\alpha_2) \\ \alpha_2(\alpha_3-\alpha_1) & \alpha_1(\alpha_3-\alpha_2) \end{pmatrix}\right).$$

Then if σ_1, σ_2 are the elements of $\mathrm{Gal}(k_\alpha/k)$ which correspond to the transpositions $(12), (13)$, then $g_\alpha^{-1} g_\alpha^\sigma = \tau_1, \tau_2$ respectively. Straightforward computations show that

(13.30)
$$w_\alpha = g_\alpha w.$$

Let $\alpha_V : G_k \backslash V_k^{\mathrm{ss}} \to \mathfrak{Ex}_i$ be the map defined after Definition 12.6.

Theorem 13.31. *The map α_V is bijective in both cases. If $x \in V_k^{\mathrm{ss}}$, $\alpha_V(x)$ is generated by coordinates of points in* $\mathrm{Zero}(x)$. *In the case (2), $G_x^\circ \cong \widetilde{T}$ for all $x \in V_k^{\mathrm{ss}}$. In the case (1), if $x \in V_k^{\mathrm{ss}}$ and $k(x)/k$ is a quadratic field, then*

$$G_x^\circ \cong \mathrm{R}_{k(x)/k}(\mathrm{GL}(1)).$$

Proof. By Theorem 9.5, $\mathrm{H}^1(k, G) == \{1\}$ in both cases. In the case (2), $\mathrm{H}^1(k, \widetilde{T}) = \{1\}$. In the case (1), if $k(x)/k$ is a quadratic extension,

$$\mathrm{H}^1(k, \mathrm{R}_{k(x)/k}(\mathrm{GL}(1))) = \{1\}$$

by Theorems 9.5, 9.6. Therefore, by Theorem 12.10, and Propositions 13.6, 13.20, it suffices to determine $G_{w_\alpha}^\circ$ for points of the form w_α.

In the case (2), $G_w^\circ = \widetilde{T}$ and $\widetilde{T}$ is contained in the center of G. So if $x = g_x w$ then $G_x^\circ = g_x G_w^\circ g_x^{-1} = \widetilde{T} \cong \mathrm{GL}(1)$.

Consider the case (1). In order to prove an isomorphism between schemes, the following theorem is sometimes convenient. Recall that if X is a scheme and R is a k-algebra, X_R is the set of R-rational points.

Theorem 13.32. *Let X, Y be schemes over k. Suppose there exists a map $f_R : X_R \to Y_R$ for each k-algebra R such that if $i : R_1 \to R_2$ is a homomorphism of k-algebras, then the diagram*

$$\begin{array}{ccc} X_{R_1} & \xrightarrow{f_{R_1}} & Y_{R_1} \\ \downarrow & & \downarrow \\ X_{R_2} & \xrightarrow{f_{R_2}} & Y_{R_2} \end{array}$$

is commutative. Then there exists a morphism $f : X \to Y$ such that f_R is the induced map for all R.

For the proof of the above theorem, see Theorem [19, p. 17]. In order to prove an isomorphism between affine schemes for example, one has to prove an isomorphism between k-algebras. However, the above theorem states that it suffices to prove isomorphisms more or less set-theoretically as long as the isomorphisms are "natural" in some sense.

We continue the proof of Theorem 13.31. Consider $x = w_\alpha$ in (13.25) and g_α in (13.26).

Let R be a k-algebra. Define $R(x) = R \otimes_k k(x)$. Let $\sigma \in \mathrm{Gal}(k(x)/k)$ be the non-trivial element. We may regard g_α has entries in $R(x)$. Let

$$s(t_1, t_2) = \left((t_1 t_2)^{-1}, \begin{pmatrix} t_1 & 0 \\ 0 & t_2 \end{pmatrix} \right)$$

for $t_1, t_2 \in R(x)^\times$. By (13.27),

$$\begin{aligned} G^\circ_{w_\alpha\, R(x)} &= g_\alpha G^\circ_{w\, R(x)} g_\alpha^{-1} \\ &= g_\alpha \{ s(t_1, t_2) \mid t_1, t_2 \in R(x)^\times \} g_\alpha^{-1}. \end{aligned}$$

The element $g_\alpha s(t_1, t_2) g_\alpha^{-1}$ is invariant by the action of σ if and only if

$$\begin{aligned} g_\alpha s(t_1, t_2) g_\alpha^{-1} &= g_\alpha^\sigma s(t_1^\sigma, t_2^\sigma)(g_\alpha^\sigma)^{-1} \\ &= g_\alpha \tau_1 s(t_1^\sigma, t_2^\sigma) \tau_1 g_\alpha^{-1} \\ &= g_\alpha s(t_2^\sigma, t_1^\sigma) g_\alpha^{-1}. \end{aligned}$$

Therefore, $t_2 = t_1^\sigma$. So

$$G^\circ_{w_\alpha\, R} = g_\alpha \{ s(t, t^\sigma) \mid t \in R(x)^\times \} g_\alpha^{-1}.$$

This set can naturally be identified with the set of R-rational points of $\mathrm{R}_{k(x)/k}(\mathrm{GL}(1))$. Theorem 13.32 now implies that $G^\circ_x \cong \mathrm{R}_{k(x)/k}(\mathrm{GL}(1))$. In all the cases, $k(\alpha)$ is generated by coordinates of points in $\mathrm{Zero}(w_\alpha)$. This proves the theorem.

$\square$

14. Pairs of ternary quadratic forms

In this section we consider the prehomogeneous vector space (8) in the Sato-Kimura classification in section 10. This is the space of pairs of ternary quadratic forms, which we shall describe as below.

Let $G_1 = \mathrm{GL}(3)$, $G_2 = \mathrm{GL}(2)$, $G = G_1 \times G_2$, and $V = \mathrm{Sym}^2\mathrm{Aff}^3 \otimes \mathrm{Aff}^2$. We regard elements of V either as pairs $x = (x_1, x_2)$ of ternary quadratic forms or as forms $x(v, u)$ in two sets of variables which are quadratic in $v = (v_1, v_2, v_3)$ and linear in $u = (u_1, u_2)$ where u, v are regarded as row vectors. The action of $g = (g_1, g_2) \in G$, where $g_2 = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, is given either as

$$(x_1(v), x_2(v)) \to (ax_1(vg_1) + bx_2(vg_1), cx_1(vg_1) + dx_2(vg_1))$$

or by $x(v, u) \to x(vg_1, ug_2)$. This action is compatible with the actin of $\mathrm{GL}(3)$ on $\mathrm{Sym}^2\mathrm{Aff}^3$ which we defined in Example 11.5. This is an irreducible representation unless $\mathrm{ch}\, k = 2$, and even so, it is obvious that Condition 10.1 is satisfied.

We express a ternary quadratic form as

$$x(v) = x_{11}v_1^2 + x_{12}v_1v_2 + x_{13}v_1v_3 + x_{22}v_2^2 + x_{23}v_2v_3 + x_{33}v_3^2. \tag{14.1}$$

If $\mathrm{ch}\, k \neq 2$, we identify $\mathrm{Sym}^2\mathrm{Aff}^3$ with the space of symmetric 3×3 matrices by the map

$$x(v) \to S_x = \begin{pmatrix} 2x_{11} & x_{12} & x_{13} \\ x_{12} & 2x_{22} & x_{23} \\ x_{13} & x_{23} & 2x_{33} \end{pmatrix}.$$

Then the action of $g \in \mathrm{GL}(3)$ is given by $M \to gM{}^tg$.

For $x(v)$, define

$$P(x) = 4x_{11}x_{22}x_{33} + x_{12}x_{13}x_{23} - x_{11}x_{23}^2 - x_{12}^2x_{33} - x_{13}^2x_{22} \tag{14.2}$$

Proposition 14.3. *If $g \in \mathrm{GL}(3)$ and $x \in \mathrm{Sym}^2\mathrm{Aff}^3$, then $P(gx) = (\det g)^2 P(x)$.*

Proof. We first assume that $k = \mathbb{Q}$. Easy computations show that

$$P(x) = (1/2)\det S_x.$$

Therefore,

$$P(gx) = (1/2)\det(gS_x{}^tg) = (1/2)(\det g)^2 \det S_x = (\det g)^2 P(x).$$

Note that $P(x) \in \mathbb{Z}[x_{11}, \cdots, x_{33}]$ and if $g = (g_{ij})$, $\det g \in \mathbb{Z}[g_{11}, \cdots, g_{33}]$. Therefore, $P(gx) = (\det g)^2 P(x)$ as integral polynomials.

If k is an arbitrary field, there is a homomorphism $\mathbb{Z} \to k$ which maps 1 to 1. This induces a homomorphism

$$\mathbb{Z}[x_{11}, \cdots, x_{33}, g_{11}, \cdots, g_{33}] \to k[x_{11}, \cdots, x_{33}, g_{11}, \cdots, g_{33}].$$

Applying this homomorphism to both sides of the equation $P(gx) = (\det g)^2 P(x)$, we obtain this equation over k. □

Note that we cannot use the equation $P(x) = (1/2)\det S_x$ if $\mathrm{ch}\, k = 2$ and so we had to reduce the problem to the case $\mathrm{ch}\, k = 0$. This argument can be generalized as follows and shall be used later.

Let G be an algebraic group, and $\rho_i : G \to \mathrm{GL}(V_i)$ a representation for $i = 1, 2$, all defined over $\mathbb{Z}$. Let k be any field, and $\pi : \mathbb{Z} \to k$ the unique homomorphism sending 1 to 1. Let $\overline{G} = G \times_{\mathbb{Z}} k$, etc.

Proposition 14.4. *Suppose $\Phi : V_1 \to V_2$ is a non-zero equivariant map defined over $\mathbb{Q}$. Then there exists a non-zero equivariant map $\overline{\Phi} : \overline{V}_1 \to \overline{V}_2$. Moreover, if Φ is defined by homogeneous polynomials of degree d, so is $\overline{\Phi}$.*

Proof. We choose coordinate systems $x = (x_1, \cdots, x_n)$, $y = (y_1, \cdots, y_m)$ for V_1, V_2 respectively. Suppose $\Phi(x) = (\Phi_1(x), \cdots, \Phi_m(x))$ and

$$\Phi_i(x) = \sum_I a_{i,I} y^I,$$

where I is a multi-index and $a_{i,I} \in \mathbb{Q}$ for all i, I. There exists $q \in \mathbb{Q}$ such that $qa_{i,I} \in \mathbb{Z}$ for all i, I and the GCD of all $qa_{i,I}$ is 1.

Define $\Psi(x) = q\Phi(x)$. Then

$$\Psi(\rho_1(g)x) = q\Phi(\rho_1(g)x) = q\rho_2(g)\Phi(x) = \rho_2(g)\Psi(x).$$

So Ψ is a G-equivariant map.

By π, Ψ induces an equivariant map

$$\overline{\Phi} : \overline{V}_1 \to \overline{V}_2.$$

If $\operatorname{ch} k = p > 0$, there exist i and I such that p does not divide $N^{-1}a_{i,I}$. Therefore, $\overline{\Phi} \neq 0$. □

Remark 14.5. If $V_2 = \mathrm{Aff}^1$, an equivariant map $V_1 \to V_2$ is a polynomial, say $\Delta(x)$, such that $\Delta(\rho_1(g)x) = \rho_2(g)\Delta(x)$. So it is a relative invariant polynomial.

Now we go back to pairs of ternary quadratic forms. We use the coordinate system $x = (x_1, x_2) = (x_{i,jk})$ where $(x_{i,jk})_{jk}$ is the coordinate of the ternary quadratic form x_i as in (14.1) for $i = 1, 2$.

For $x \in V$, we define a binary cubic form $F_x(u)$ by the map

$$x \to F_x(u) = -P(u_1x_1 + u_2x_2). \tag{14.6}$$

This map was considered in [23, p. 91]. It is easy to see that if $g = (g_1, g_2)$,

$$F_{gx}(u) = (\det g_1)^2 F_x(ug_2). \tag{14.7}$$

Let $\Delta(x)$ be the discriminant of F_x. Then $\Delta(x)$ is a polynomial of degree 12 and it satisfies a relation $P(gx) = \chi(g)P(x)$ where

$$\chi(g) = (\det g_1)^8(\det g_2)^6. \tag{14.8}$$

For $x = (x_1, x_2)$, we consider the zero set of x_1, x_2 in $\mathbb{P}^2$ and denote it by $\mathrm{Zero}(x)$. As in (13.5), if $g = (g_1, g_2) \in G$,

$$\mathrm{Zero}(gx) = \mathrm{Zero}(x)g_1^{-1}. \tag{14.9}$$

We define $w = (w_1, w_2)$ where

$$w_1 = v_2v_3 - v_1v_3,\ w_2 = v_1v_2 - v_2v_3. \tag{14.10}$$

By the definition of $F_w(u)$ and (13.8),

$$F_w(u) = u_1u_2(u_1 - u_2),\ \Delta(w) = 1 \neq 0.$$

So $\Delta(x)$ is a relative invariant polynomial.

Let

$$p_1 = (1,0,0),\ p_2 = (0,1,0),\ p_3 = (0,0,1),\ p_4 = (1,1,1). \tag{14.11}$$

Then $\mathrm{Zero}(w) = \{p_1, \cdots, p_4\}$. As before, we regard $\mathrm{Zero}(x)$ as a set of row vectors.

Let $\widetilde{T} = \mathrm{Ker}(G \to \mathrm{GL}(V))$. Then it is easy to see that

$$\widetilde{T} \cong \mathrm{GL}(1) = \{(tI_3, t^{-2}I_2) \mid t \in \mathrm{GL}(1)\} \tag{14.12}$$

If $S \subset \mathbb{P}^2$ consists of four points and no three of them are on the same line, we say that S is in general position. The following lemma is easy to verify and we leave it to the reader.

Lemma 14.13. *If $S \subset \mathbb{P}^2_{\bar{k}}$ consists of four points in general position, there exists $g_1 \in \mathrm{GL}(3)_{\bar{k}}$ such that $Sg_1 = \{p_1, p_2, p_3, p_4\}$.*

Obviously, $\mathrm{Zero}(w)$ is in general position.

Proposition 14.14. *The representation (G, V) is a regular prehomogeneous vector space. Moreover, $x \in V^{\mathrm{ss}}$ if and only if $\mathrm{Zero}(x)$ consists of four points in $\mathbb{P}^2$. If so, $\mathrm{Zero}(x)$ is in general position.*

Proof. We start with the following lemma.

Lemma 14.15. *The stabilizer G_w is smooth and $G_w^\circ = \widetilde{T}$.*

Proof. Let

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix},\ B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}.$$

Suppose $g(A,B) = (I_3 + \epsilon A, I_2 + \epsilon B)$ fixes w where $k[\epsilon]/(\epsilon^2)$ is the ring of dual numbers. Then

$$F_{g(A,B)w}(u) = (\det(I_3 + \epsilon A))^2 F_w(u(I_2 + \epsilon B)) = (1 + \epsilon\,\mathrm{tr}(A)) F_w(u(I_2 + \epsilon B)).$$

Note that $F_w = u_1 u_2 (u_1 - u_2)$ and we have determined the stabilizer of this element in $\mathrm{GL}(1) \times \mathrm{GL}(2)$ in the proof of Proposition 13.6 and in Theorem 13.31. So B must be a scalar matrix of the form bI_2 and $2(a_{11} + a_{22} + a_{33}) = -3b$.

Writing down the action explicitly,

$$g(A, bI_2)(w_1, w_2) = ((1+\epsilon b) w_1(v(I_3 + \epsilon A)), (1+\epsilon b) w_2(v(I_3 + \epsilon A))).$$

If this is w,

$$(1+\epsilon b) w_i(v(I_3 + \epsilon A)) = w_i$$

for $i = 1, 2$.

We simplify the above equation for $i = 1$ as follows

$$\begin{aligned}(1+\epsilon b)w_1(v(I_3+\epsilon A)) &= w_1 + \epsilon b(v_2v_3 - v_1v_3)\\ &\quad + \epsilon(v_3(a_{12}v_1 + a_{22}v_2 + a_{32}v_3))\\ &\quad + \epsilon(v_2(a_{13}v_1 + a_{23}v_2 + a_{33}v_3))\\ &\quad - \epsilon(v_3(a_{11}v_1 + a_{21}v_2 + a_{31}v_3))\\ &\quad - \epsilon(v_1(a_{13}v_1 + a_{23}v_2 + a_{33}v_3))\\ &= w_1 + \epsilon(a_{13}v_1^2 + (a_{13} - a_{23})v_1v_2)\\ &\quad + \epsilon((-a_{11} + a_{12} - a_{33} - b)v_1v_3 + a_{23}v_2^2)\\ &\quad + \epsilon((-a_{21} + a_{22} + a_{33} + b)v_2v_3 + (-a_{31} + a_{32})v_3^2).\end{aligned}$$

Similarly,

$$\begin{aligned}(1+\epsilon b)w_2(v(I_3+\epsilon A)) &= w_2 + \epsilon b(v_1v_2 - v_2v_3)\\ &\quad - \epsilon(v_3(a_{12}v_1 + a_{22}v_2 + a_{32}v_3))\\ &\quad - \epsilon(v_2(a_{13}v_1 + a_{23}v_2 + a_{33}v_3))\\ &\quad + \epsilon(v_2(a_{11}v_1 + a_{21}v_2 + a_{31}v_3))\\ &\quad + \epsilon(v_1(a_{12}v_1 + a_{22}v_2 + a_{32}v_3))\\ &= w_2 + \epsilon(a_{12}v_1^2 + (a_{11} - a_{13} + a_{22} + b)v_1v_2)\\ &\quad + \epsilon((-a_{12} + a_{32})v_1v_3 + (a_{21} - a_{23})v_2^2)\\ &\quad - \epsilon((a_{22} - a_{31} + a_{33} + b)v_2v_3 + a_{32}v_3^2).\end{aligned}$$

So we get the following system of linear equations

$$\begin{aligned}&a_{13} = a_{13} - a_{23} = a_{11} - a_{12} + a_{33} + b = 0,\\ &a_{23} = -a_{21} + a_{22} + a_{33} + b = a_{31} - a_{32} = 0,\\ &a_{12} = a_{11} - a_{13} + a_{22} + b = a_{12} - a_{32} = 0,\\ &a_{21} - a_{23} = a_{22} - a_{31} + a_{33} + b = a_{32} = 0.\end{aligned}$$

Solving these equations, $a_{ij} = 0$ if $i \neq j$, $a_{11} = a_{22} = a_{33}$, and $b = -2a_{11}$. Therefore,

$$T(G_w)_e = \{(tI_3, -2tI_2) \mid t \in k\}.$$

Since $\widetilde{T} \subset G_w^\circ$ and $\dim G_w \leq \dim T(G_w)_e = 1$, G_w must be smooth over k and $G_w^\circ = \widetilde{T} \cong \mathrm{GL}(1)$. $\square$

We continue the proof of Proposition 14.14. Since $\dim T(G_w)_e = 1 = \dim G - \dim V$, (G, V) is a regular prehomogeneous vector space.

Since (G, V) is regular, $V_{\bar{k}}^{\mathrm{ss}} = G_{\bar{k}}w$. Suppose $x = (x_1(v), x_2(v)) \in V_{\bar{k}}$. If $x \in G_{\bar{k}}w$, by (14.9), $\mathrm{Zero}(x)$ consists of four points.

Conversely, suppose $\mathrm{Zero}(x)$ consists of four points. We show that $x \in G_{\bar{k}}w$. Note that if a conic in $\mathbb{P}^2$ contains three points on a line, it contains the entire line. So if three points of $\mathrm{Zero}(x)$ are on a line, both $x_1(v) = 0$, $x_2(v) = 0$ contains the line. Therefore, $\mathrm{Zero}(x)$ is an infinite set, which is a contradiction.

By Lemma 14.13, if $\mathrm{Zero}(x)$ consists of four points, there exists $g_1 \in \mathrm{GL}(3)_{\bar{k}}$ such that $\mathrm{Zero}(x)g_1 = \mathrm{Zero}(w)$. Replacing x by $(g_1^{-1}, 1)x$, we may assume that $\mathrm{Zero}(x) = \mathrm{Zero}(w)$. It is easy to verify that if $f(v) \in \mathrm{Sym}^2\bar{k}^3$ is a ternary quadratic form such that $f(p_i) = 0$ for $i = 1, 2, 3, 4$, then f is a linear combination of w_1, w_2. So x_1, x_2 belong to the span of w_1, w_2. If x_1, x_2 are proportional, $\mathrm{Zero}(x)$ is an infinite set, which is a contradiction. This implies that $\{x_1, x_2\}$ is a basis for the span of $\{w_1, w_2\}$. Therefore, there exists $g_2 \in \mathrm{GL}(2)_{\bar{k}}$ such that $x = (1, g_2)w \in G_{\bar{k}}w = V_{\bar{k}}^{\mathrm{ss}}$. □

Remark 14.16. In the proof of the above proposition, we used the equivariant map $F : V \to \mathrm{Sym}^3\mathrm{Aff}^2$ to show $\dim T(G_w)_e = 1$. However, it is not much more difficult to compute $T(G_w)_e$ directly without using this equivariant map. However, F is an interesting equivariant map, and that is why we chose this method in this case. In later sections, we usually compute $T(G_w)_e$ directly.

Let $x \in V_k^{\mathrm{ss}}$. We choose $g_x \in G_{k^{\mathrm{sep}}}$ so that $x = g_x w$. Let

$$\mathrm{Zero}(x) = \{p_{x\,1}, p_{x\,2}, p_{x\,3}, p_{x\,4}\}.$$

As in section 13, $\mathrm{Zero}(x)$ can be regarded as a scheme over k, $\mathrm{Aut}\,(\mathrm{Zero}(x))$ is an algebraic group, and the map $\pi_x(g) : \mathrm{Zero}(x) \ni q \to qg_1 \in \mathrm{Zero}(x)$ for $g = (g_1, g_2) \in G_x$ is a homomorphism $G_x \to \mathrm{Aut}\,(\mathrm{Zero}(x))$ of algebraic groups over k.

Over $\bar{k}$, we consider π_x set-theoretically and identify π_x with the homomorphism $G^{\circ}_{x\,\bar{k}} \to \mathfrak{S}_4$ defined by

$$p_{x\,j}g_1 = p_{x\,\pi_x(g)(j)} \quad \text{for all } j.$$

We also define homomorphisms $\phi, \psi : \mathrm{Gal}(k^{\mathrm{sep}}/k) \to \mathfrak{S}_4$ similarly as in (13.22) (13.23).

Define

$$\begin{aligned} \tau_{11} &= \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, & \tau_{12} &= \begin{pmatrix} -1 & 0 \\ 1 & 1 \end{pmatrix}, \\ \tau_{21} &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, & \tau_{22} &= \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}, \\ \tau_{31} &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -1 & -1 & -1 \end{pmatrix}, & \tau_{32} &= \begin{pmatrix} -1 & 0 \\ 1 & 1 \end{pmatrix}. \end{aligned} \tag{14.17}$$

Let $\tau_i = (\tau_{i1}, \tau_{i2})$ for $i = 1, 2, 3$. Then by explicit computations, $\tau_i \in G_w$. Let $H \subset G_w$ be the subgroup generated by τ_1, τ_2, τ_3.

Proposition 14.18. *The subgroup H is isomorphic to $\mathfrak{S}_4$ by π_w.*

Proof. Let H' be the subgroup generated by $(-\tau_{11}, \tau_{12}), (-\tau_{21}, \tau_{22}), (-\tau_{31}, \tau_{32})$. We first prove the above statement for H'.

Suppose $k = \mathbb{Q}$. By π_w, the above elements and τ_1, τ_2, τ_3 map to transpositions $(12), (23), (34)$ respectively. Since $\mathfrak{S}_4$ is generated by $(12), (23), (34)$, the image of H' is $\mathfrak{S}_4$. Note that $\det(-\tau_{11}) = \det(-\tau_{21}) = \det(-\tau_{31}) = 1$. So if $\nu = (\nu_1, \nu_2) \in H'$, $\det \nu_1 = 1$. If $\nu \in \mathrm{Ker}(\pi_w)$ then ν_1 fixes any point in $\mathrm{Zero}(w)$ and so is a scalar matrix. Also $\nu_1 \in \mathrm{GL}(3)_{\mathbb{Q}}$. Since $\det \nu_1 = 1$, $\nu_1 = I_3$. Then ν_2 fixes two linearly independent polynomials. So $\nu_2 = I_2$. This proves that H' is isomorphic to $\mathfrak{S}_4$.

The sign of a permutation is a character of $\mathfrak{S}_4$. Therefore, multiplying the sign of the permutation to the first component, we still have a group isomorphic to $\mathfrak{S}_4$. Note that τ_1, τ_2, τ_3 are integral elements. Since H is a finite group, any element in H must be an element of $\mathrm{GL}(3)_{\mathbb{Z}} \times \mathrm{GL}(2)_{\mathbb{Z}}$.

We now assume that k is an arbitrary field. Consider the homomorphism $\mathbb{Z} \to k$ which sends 1 to 1. This homomorphism induces a homomorphism between abstract groups $\mathrm{GL}(3)_{\mathbb{Z}} \times \mathrm{GL}(2)_{\mathbb{Z}} \to G_k$. So the image of H is a subgroup of $G_{w\,k}$ containing τ_1, τ_2, τ_3. This shows that τ_1, τ_2, τ_3 generate a subgroup of order at most 24. However, by π_w, they map to $(12), (23), (34)$ respectively. Therefore, H (which is defined for k) is isomorphic to $\mathfrak{S}_4$ by π_w. $\square$

Proposition 14.19. *Assumption 12.1 is satisfied with $i = 4$.*

Proof. We have shown that π_w is surjective and that $G_w^\circ = \widetilde{T}$. Since $\mathfrak{S}_4$ is a finite group, we only have to show $\mathrm{Ker}(\pi_w) = \widetilde{T}$ set-theoretically.

Let $g = (g_1, g_2) \in \mathrm{Ker}(\pi_w)_{\bar{k}}$. This implies that g_1 fixes four points in general position in $\mathbb{P}^2$. So g_1 is a scalar matrix. Applying an element of $\widetilde{T}_{\bar{k}}$, we may assume that $g_1 = I_3$. Then g_2 fixes w_1, w_2 which are linearly independent. So $g_2 = I_2$. $\square$

Note that $G_w^\circ = \widetilde{T}$ is contained in the center of G. If $x = g_x w$ then

$$G_{x\,\bar{k}}^\circ = g_x G_{w\,\bar{k}}^\circ g_x^{-1} = \widetilde{T}_{\bar{k}}.$$

Therefore, $G_x^\circ = \widetilde{T}$ for all $x \in V_k^{\mathrm{ss}}$.

Let γ_V be the map defined in (12.3). Since $\mathrm{H}^1(k, G) = \mathrm{H}^1(k, \widetilde{T}) = \{1\}$, Theorem 12.10 implies the following theorem.

Theorem 14.20. *The map γ_V is bijective. Moreover, $G_x^\circ = \widetilde{T}$ for all $x \in V_k^{\mathrm{ss}}$.*

We shall find explicit representatives of the orbit space $G_k \backslash V_k^{\mathrm{ss}}$. Note that by exactly the same proof, the statement of Proposition 13.24 holds for the present situation. Therefore, in order to construct a representative $x \in G_k \backslash V_k^{\mathrm{ss}}$ which corresponds to a given homomorphism $\mathrm{Gal}(k^{\mathrm{sep}}/k) \to \mathfrak{S}_4$, it is enough to choose x so that the action of $\mathrm{Gal}(k^{\mathrm{sep}}/k)$ on $\mathrm{Zero}(x)$ is given by the above homomorphism.

We first consider the fibers of $\beta_4 : \mathrm{H}^1(k, \mathfrak{S}_4) \to \mathfrak{Ex}_4$. Up to isomorphisms, subgroups of $\mathfrak{S}_4$ are isomorphic to

$$\{1\},\ \mathbb{Z}/2\mathbb{Z},\ \mathbb{Z}/3\mathbb{Z},\ \mathbb{Z}/4\mathbb{Z},\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},\ \mathfrak{S}_3,\ D_4,\ A_4,\ \mathfrak{S}_4.$$

In almost all the cases, if Γ_1, Γ_2 are isomorphic subgroups of $\mathfrak{S}_4$, then Γ_1, Γ_2 are conjugate in $\mathfrak{S}_4$. The only exceptions are $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and D_4.

So we first consider subgroups Γ which are not isomorphic to $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or D_4. If $\Gamma \cong \{1\}$, the only automorphism is the identity map. If $\Gamma \cong \mathbb{Z}/3\mathbb{Z}, \mathfrak{S}_3$, any automorphism of Γ is induced by an inner automorphism of $\mathfrak{S}_3 \subset \mathfrak{S}_4$ by Theorem 13.21. If $\Gamma \cong A_4$ or $\mathfrak{S}_4$, any automorphism of Γ is induced by an inner automorphism of $\mathfrak{S}_4$ again by Theorem 13.21.

If $\Gamma \cong \mathbb{Z}/4\mathbb{Z}$, identify Γ with $\langle (1234) \rangle$. Then automorphisms of Γ are given by

$$(1234) \to (1234) \text{ or } (1432).$$

Since $(1432) = (24)(1234)(24)$, these automorphisms are conjugate by an element of $\mathfrak{S}_4$.

If $\Gamma \cong \mathbb{Z}/2\mathbb{Z}$, its imbedding to $\mathfrak{S}_4$ is determined by an order two element in $\mathfrak{S}_4$. Conjugacy classes of order two elements in $\mathfrak{S}_4$ are represented by (12), $(12)(34)$.

Therefore, there are exactly two conjugacy classes of imbeddings $\rho_1, \rho_2 : \mathbb{Z}/2\mathbb{Z} \to \mathfrak{S}_4$. If x is the non-trivial element of $\mathbb{Z}/2\mathbb{Z}$, then they are given by

$$\rho_1(x) = (12), \quad \rho_2(x) = (12)(34) \tag{14.21}$$

respectively.

Suppose $\Gamma = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Let $\{x, y\}$ be a set of generators of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Then there are exactly four conjugacy classes of imbeddings of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ to $\mathfrak{S}_4$. They are given by

$$\begin{aligned} &\rho_1(x) = (12),\ \rho_1(y) = (34), \\ &\rho_2(x) = (12),\ \rho_2(y) = (12)(34), \\ &\rho_3(x) = (12)(34),\ \rho_3(y) = (12), \\ &\rho_4(x) = (12)(34),\ \rho_4(y) = (13)(24). \end{aligned} \tag{14.22}$$

Note that the images of ρ_1, ρ_2, ρ_3 in $\mathfrak{S}_4$ are the same, but they are not conjugate as homomorphisms to $\mathfrak{S}_4$. Also the kernels of $\rho_1, \cdots, \rho_4$ are the same and so they correspond to the same biquadratic field.

Suppose $\Gamma = D_4$. We identify D_4 with the group

$$\langle x, y \mid x^4 = 1, y^2 = 1, yxy = x^{-1} \rangle.$$

We leave the following proposition to the reader (see Exercise 14.33).

Proposition 14.23. *There are exactly two conjugacy classes of imbeddings ρ_1, ρ_2 of D_4 to $\mathfrak{S}_4$ and that they are given by*

$$\begin{aligned} &\rho_1(x) = (1234),\ \rho_1(y) = (14)(23), \\ &\rho_2(x) = (1234),\ \rho_2(y) = (24). \end{aligned}$$

The above consideration shows the following proposition.

Proposition 14.24. *If $F \in \mathfrak{Ex}_4$ and $\Gamma = \mathrm{Gal}(F/k)$, then $\beta_4^{-1}(F)$ consists of a single element unless $\Gamma \cong \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or D_4. If $\Gamma \cong \mathbb{Z}/2\mathbb{Z}$ or D_4 then $\beta_4^{-1}(F)$ consists of two elements. If $\Gamma \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ then $\beta_4^{-1}(F)$ consists of four elements.*

If $F = k$ is the trivial extension, we choose $x = w$ as the representative of the corresponding orbit.

Suppose $F \neq k$. We assume that the corresponding homomorphism $\mathrm{Gal}(F/k) \to \mathfrak{S}_4$ is not ρ_2 in (14.21) if $\mathrm{Gal}(F/k) \cong \mathbb{Z}/2\mathbb{Z}$ and that it is not ρ_1, ρ_2, ρ_3 in (14.22) if $\mathrm{Gal}(F/k) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Let $a = (a_1, \cdots, a_4)$ where $a_1, \cdots, a_4 \in k$, and

$$f_a(t) = t^4 + a_1 t^3 + a_2 t^2 + a_3 t + a_4. \tag{14.25}$$

Suppose roots $\alpha = (\alpha_1, \cdots, \alpha_4)$ of this polynomial are distinct. Note that we are allowing the polynomial $f_a(t)$ to be reducible over k. We define

$$\begin{aligned} &x_{a,1}(v) = v_1 v_3 - v_2^2, \\ &x_{a,2}(v) = v_1^2 + a_1 v_1 v_2 + a_2 v_2^2 + a_3 v_2 v_3 + a_4 v_3^2 \\ &x_a = (x_{a,1}, x_{a,2}). \end{aligned} \tag{14.26}$$

Note that if $\mathrm{ch}\, k \neq 2$, then

$$S_{x_{a,1}} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & -2 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \tag{14.27}$$
$$S_{x_{a,2}} = \begin{pmatrix} 2 & a_1 & 0 \\ a_1 & 2a_2 & a_3 \\ 0 & a_3 & 2a_4 \end{pmatrix}.$$

The equation $x_{a,1}(v) = 0$ defines the conic $(t^2, t, 1)$ in inhomogeneous form in $\mathbb{P}^2$. If we restrict the equation $x_{a,2}(v) = 0$ to this conic, we get the equation $f_a(t) = 0$. So $\mathrm{Zero}(x_a) = \{(\alpha_i^2, \alpha_i, 1) \mid i = 1, \cdots, 4\}$. Therefore, points in $\mathrm{Zero}(x_{4,a})$ correspond bijectively with roots of $f_a(t)$.

So given a field $F \in \mathfrak{Ex}_4$ and an element in $\beta_4^{-1}(F)$, in order to choose the corresponding representative of the orbit in V_k^{ss}, it is enough to choose a polynomial of the form $f_a(t)$ whose roots are permuted by the given Galois group action. Note that if $F = k = \mathbb{F}_2$ or $\mathbb{F}_3$, one cannot choose a polynomial with four roots in k and that's why we chose w as the corresponding representative.

If $\Gamma \cong \mathbb{Z}/2\mathbb{Z}$ then let α_1, α_2 be a pair of conjugate elements which generate F. In this case we may choose

$$(t-\alpha_1)(t-\alpha_2)t(t-1), \text{ or}$$

as $f_a(t)$, the roots are permuted by ρ_2 in (14.21).

If $\Gamma \cong \mathbb{Z}/3\mathbb{Z}$ or $\mathfrak{S}_3$, choose $\alpha \in F$ so that its conjugates $\alpha_1 = \alpha, \alpha_2, \alpha_3$ generate F. Since there is exactly one conjugacy class of homomorphisms $\Gamma \to \mathfrak{S}_3$, by renumbering if necessary, we may assume that $\{\alpha_1, \alpha_2, \alpha_3\}$ are permuted by the given Galois group action. Then we may choose

$$f_a(t) = (t-\alpha_1)(t-\alpha_2)(t-\alpha_3)t$$

If $\Gamma \cong \mathbb{Z}/4\mathbb{Z}$, A_4, or $\mathfrak{S}_4$, choose $\alpha \in F$ so that its conjugates $\alpha_1 = \alpha, \alpha_2, \alpha_3, \alpha_4$ generate F. Then similarly as in the previous case, we may choose

$$f_a(t) = (t-\alpha_1)(t-\alpha_2)(t-\alpha_3)(t-\alpha_4).$$

Suppose $\Gamma \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Then F is in the form $k(\alpha, \beta)$ where $[k(\alpha) : k] = [k(\beta) : k] = 2$. Let $\alpha_1 = \alpha$ and α_2 be the conjugate of α. Define β_1, β_2 similarly. If we choose

$$(t-\alpha_1-\beta_1)(t-\alpha_1-\beta_2)(t-\alpha_2-\beta_2)(t-\alpha_2-\beta_2)$$

as $f_a(t)$, the roots are permuted by ρ_4 in (14.22).

The construction of $f_a(t)$ for D_4-extensions is an interesting exercise problem and we leave it to the reader (see Exercise 14.32).

We finally consider orbits which correspond to ρ_2 in (14.21) or ρ_1, ρ_2, ρ_3 in (14.22). Let $a = (a_1, a_2)$, $b = (b_1, b_2) \in k^2$ and assume that the roots (
$al_1, \alpha_2)$, (β_1, β_2) of $f_a(t) = t^2 + a_1 t + a_2$, $f_b(t) = t^2 + b_1 t + b_2$ generate quadratic Galois extensions of k. We allow $a = b$.

Define $x_{a,b} = (x_{a,b,1}, x_{a,b,2})$ where

$$x_{a,b,1} = v_2 v_3, \; x_{a,b,2} = v_1^2 + a_1 v_1 v_2 + b_1 v_1 v_3 + a_2 v_2^2 + b_2 v_3^2. \tag{14.28}$$

Then easy computations show that

$$\mathrm{Zero}(x_{a,b}) = \{(\alpha_1, 1, 0), (\alpha_2, 1, 0), (\beta_1, 0, 1), (\beta_2, 0, 1)\}.$$

If $a = b$, then $\mathrm{Zero}(x_{a,b})$ is permuted by ρ_2 in (14.21). Note that if $k = \mathbb{F}_2$, then we cannot choose a representative of the form (14.26) for orbits which correspond to ρ_2 in (14.21).

Suppose $k(\alpha_1, \alpha_2) \neq k(\beta_1, \beta_2)$. Let

$$\begin{aligned}
&f_{a^{(1)}} = (t-\alpha_1)(t-\alpha_2),\ f_{b^{(1)}} = (t-\beta_1)(t-\beta_2),\\
&f_{a^{(2)}} = (t-(\alpha_1\beta_1+\alpha_2\beta_2))(t-(\alpha_1\beta_2+\alpha_2\beta_1)),\ f_{b^{(2)}} = (t-\beta_1)(t-\beta_2),\\
&f_{a^{(3)}} = (t-(\alpha_1\beta_1+\alpha_2\beta_2))(t-(\alpha_1\beta_2+\alpha_2\beta_1)),\ f_{b^{(3)}} = (t-\alpha_1)(t-\alpha_2).
\end{aligned}$$

Then $x_{a^{(1)},b^{(1)}}, x_{a^{(2)},b^{(2)}}, x_{a^{(3)},b^{(3)}}$ correspond to ρ_1, ρ_2, ρ_3 in (14.22).

This exhausts representatives of $G_k \backslash V_k^{\mathrm{ss}}$.

Proposition 14.29. *If $x \in V_k^{\mathrm{ss}}$, then $k(x)$ is generated by coordinates of points in* $\mathrm{Zero}(x)$.

Proof. Let $F(x)$ be the field generated by coordinates of points in $\mathrm{Zero}(x)$. Then it is obvious that if $g \in G_k$ then $F(gx) = F(x)$. So we only have to verify this proposition for representatives of the orbit space $G_k \backslash V_k^{\mathrm{ss}}$.

If $x = w$ then $p_1, \cdots, p_4 \in \mathbb{P}_k^2$ and so $k(w) = F(w) = k$. For other orbits, we can choose representatives of the form x_a as in (14.26) where $f_a(t)$ is as in (14.25) with roots $\alpha_1, \cdots, \alpha_4$. Since $\mathrm{Zero}(x_a)$ consists of $\{(\alpha_i^2, \alpha_i, 1) \mid i = 1, \cdots, 4\}$, $k(x_a) = F(x_a) = k(\alpha_1, \cdots, \alpha_4)$. $\square$

Remark 14.30. The idea of expressing a quartic equation as an intersection of two conics goes back more than 900 years to the work of a medieval Persian mathematician Omar Khayyam. He expressed cubic equations as intersections of conics, but the argument was exactly the same as above. The reader can find a description of his works in [27].

The notion of the zero set $\mathrm{Zero}(x)$ for the present case and the quintic case in the next section appears in the paper of De Contini, Lusztig, Procesi [4]

Exercise 14.31. Prove Lemma 14.13.

Exercise 14.32. If F/k is a D_4-extension, construct polynomials whose roots are permuted according as ρ_1, ρ_2.

Exercise 14.33. Prove Proposition 14.23.

15. Symmetric and wedge products

In this section, we fix various normalizations regarding symmetric products and discuss fundamental equivariant maps concerning symmetric and wedge products.

We first consider normalizations regarding symmetric products. Let W be a vector space and W^* its dual space. For $a_1, \cdots, a_d \in W$, we define

$$[a_1, \cdots, a_d]_d = \frac{1}{d!} \sum_{\sigma \in \mathfrak{S}_d} a_{\sigma(1)} \otimes \cdots \otimes a_{\sigma(d)}.$$

Note that we have to assume that $\mathrm{ch}\, k$ does not divide $d!$ for the above definition to make sense. So we assume this whenever we consider $[a_1, \cdots, a_d]_d$. In later sections, we sometimes have to assume that $\mathrm{ch}\, k \neq 2, 3$ for this reason.

We identify $\mathrm{Sym}^d W$ with the subspace of $W^{\otimes d}$ spanned by elements of the form $[a_1, \cdots, a_d]_d$. Similarly, we identify $\mathrm{Sym}^d W^*$ with a subspace of $(W^*)^{\otimes d}$. For

$$a_1, \cdots, a_{d_1}, a_{d_1+1}, \cdots, a_{d_1+d_2} \in W,$$

we define

$$[a_1, \cdots, a_{d_1}]_{d_1} [a_{d_1+1}, \cdots, a_{d_1+d_2}]_{d_2} = [a_1, \cdots, a_{d_1+d_2}]_{d_1+d_2}.$$

By this product, $\oplus \mathrm{Sym}^* W$ becomes an associative algebra. Since $[a_1, \cdots, a_d]_d = a_1 \cdots a_d$, we use this usual notation of product from now on.

Since $(W^*)^{\otimes d}$ and $W^{\otimes d}$ are dual spaces of each other, there is a natural pairing between $\mathrm{Sym}^d W$ and $\mathrm{Sym}^d W^*$. If $a = a_1 \cdots a_d \in \mathrm{Sym}^d W$, $b = b_1 \cdots b_d \in \mathrm{Sym}^d W^*$, we normalize this pairing by

$$(a, b)_d = (b, a)_d = \frac{1}{d!} \sum_{\sigma \in \mathfrak{S}_d} b_1(a_{\sigma(1)}) \cdots b_d(a_{\sigma(d)}).$$

Then if $i_1 + \cdots + i_n = d$,

$$(e_1^{i_1} \cdots e_n^{i_n}, f_1^{i_1} \cdots f_n^{i_n})_d = \frac{i_1! \cdots i_n!}{d!}.$$

Therefore, $\mathrm{Sym}^d W^*$ may be identified with the dual space of $\mathrm{Sym}^d W$. Note that we shall only consider $\mathrm{Sym}^d W$ up to $d = 4$ and that we assumed that $\mathrm{ch}\, k \neq 2, 3$. So the above notions are well defined.

The map

$$W \ni a \to i_d(a) = a \otimes a \otimes \cdots \otimes a \in \mathrm{Sym}^d W$$

is a polynomial map. So if $f \in \mathrm{Sym}^d W^*$, $f(a) = f(i_d(a))$ is a polynomial map from W to k and is homogeneous of degree d. We may identify $\mathrm{Sym}^d W^*$ with the space of degree k forms on W by this correspondence. If $a = \sum_{i=1}^n a_i e_i$,

$$i_d(a) = \sum \frac{d!}{i_1! \cdots i_n!} a_1^{i_1} \cdots a_n^{i_n} e_1^{i_1} \cdots e_n^{i_n},$$

where the sum is over all $(i_1, \cdots, i_n)$ such that $i_1 + \cdots + i_n = d$. So if $f = f_1^{i_1} \cdots f_n^{i_n}$, $f(a) = a_1^{i_1} \cdots a_n^{i_n}$. Therefore, f corresponds to the monomial $a_1^{i_1} \cdots a_n^{i_n}$.

We now consider two equivariant maps regarding wedge products. Let V be a vector space. Define

$$D : \wedge^n V \to \wedge^{n-1} V \otimes V$$

by

$$D(v_1 \wedge \cdots \wedge v_n) = v_1 \wedge \cdots \wedge v_{n-1} \otimes v_n - v_1 \wedge \cdots \wedge v_{n-2} \wedge v_n \otimes v_{n-1} + \cdots . \tag{15.1}$$

It is easy to verify that D is well defined. Moreover it satisfies the relation $D \circ D = 0$. However, we do not need this relation.

The group $\mathrm{GL}(V)$ acts on both $\wedge^n V$ and $\wedge^{n-1} V \otimes V$. It is easy to see that D is equivariant with respect to the actions of $\mathrm{GL}(V)$.

Another equivariant map which we shall need later is a map

$$S : \wedge^n(\wedge^2 V) \to \wedge^n V \otimes \mathrm{Sym}^n V.$$

In order to define this map, we have to distinguish two wedge products and so use the notation

$$(v_{11} \wedge v_{12}) \bigtriangleup \cdots \bigtriangleup (v_{n1} \wedge v_{n2}) \tag{15.2}$$

for elements of $\wedge^n(\wedge^2 V)$.

Now S is defined to be the map which maps the element (15.2) to the following element

$$\sum_{\sigma_1, \cdots, \sigma_n \in \mathfrak{S}_2} \mathrm{sgn}(\sigma_1) \cdots \mathrm{sgn}(\sigma_n) v_{1\,\sigma_1(1)} \wedge \cdots \wedge v_{n\,\sigma_n(1)} \otimes v_{1\,\sigma_1(2)} \cdots v_{n\,\sigma_n(2)}. \tag{15.3}$$

If we exchange v_{i1} and v_{i2} for any i, then (15.3) changes the sign. Also if we exchange the pairs $(v_{i1}, v_{i2}), (v_{j1}, v_{j2})$, then (15.3) changes the sign also. Therefore, S is well defined.

The group $\mathrm{GL}(V)$ acts on both $\wedge^n(\wedge^2 V)$ and $\wedge^n V \otimes \mathrm{Sym}^n V$. It is easy to see that S is equivariant with respect to the actions of $\mathrm{GL}(V)$.

16. The quintic case

In this section we consider the case (11) in the Sato-Kimura classification. We call this case the "quintic case" because it parametrizes quintic extensions of a given field.

Let $G_1 = \mathrm{GL}(5)$, $G_2 = \mathrm{GL}(4)$, $G = G_1 \times G_2$, and $V = \wedge^2 \mathrm{Aff}^5 \otimes \mathrm{Aff}^4$. We identify $\wedge^2 \mathrm{Aff}^5$ with the space of alternating matrices with zero diagonal entries (this assumption is necessary if $\mathrm{ch}\, k = 2$). Let

$$x = x(v) = (x_{jk}(v)) = v_1 x_1 + v_2 x_2 + v_3 x_3 + v_4 x_4$$

where $v_1, \cdots, v_4$ are variables and $x_i = (x_{i,jk}) \in \wedge^2 \mathrm{Aff}^5$ for $i = 1, \cdots, 4$. The group G acts on V by $gx(v) = g_1 x(vg_2)^t g_1$ for $g = (g_1, g_2) \in G$.

Let $\widetilde{T} = \mathrm{Ker}(G \to \mathrm{GL}(V))$. Then it is easy to see that

$$\widetilde{T} = \{(tI_5, t^{-2} I_4) \mid t \in \mathrm{GL}(1)\} \cong \mathrm{GL}(1).$$

We put $w = v_1 w_1 + v_2 w_2 + v_3 w_3 + v_4 w_4$ where

$$w_1 = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \quad w_2 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

$$w_3 = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ -1 & 0 & -1 & 0 & 0 \end{pmatrix}, \quad w_4 = \begin{pmatrix} 0 & -1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ -1 & -1 & 0 & 0 & -1 \\ 0 & -1 & 0 & 1 & 0 \end{pmatrix}.$$

We first show the following proposition.

Proposition 16.1. *The representation (G, V) is a regular prehomogeneous vector space. Moreover, $G_w^\circ = \widetilde{T}$.*

Proof. We first determine $T(G_w)_e$. Let $A = (a_{ij})$ be a 5×5 matrix, $B = (b_{ij})$ a 4×4 matrix, and $g(A, B) = (I_5 + \epsilon A, I_4 + \epsilon B)$ where $k[\epsilon]/(\epsilon^2)$ is the ring of dual numbers. Then

$$g(A, B) w(v) = w(v) + \epsilon (A w(v) + w(v)^t A + w(vB)).$$

Therefore, $g(A, B) \in T(G_w)_e$ if and only if

$$Aw(v) + w(v)^t A + w(vB) = 0. \tag{16.2}$$

If we express the left hand side of (16.2) as $v_1C_1 + v_2C_2 + v_3C_3 + v_4C_4$, then $C_1, \cdots, C_4$ are as follows

$$
C_1 = \begin{pmatrix} 0 & a_{11}+a_{22} & a_{32} & a_{42} & a_{52} \\ & 0 & -a_{31} & -a_{41} & -a_{51} \\ & & 0 & 0 & 0 \\ & * & & 0 & 0 \\ & & & & 0 \end{pmatrix} + \begin{pmatrix} 0 & b_{11}-b_{14} & 0 & b_{14} & b_{13} \\ & 0 & 0 & b_{14} & b_{14} \\ & & 0 & b_{12} & b_{13} \\ & * & & 0 & -b_{14} \\ & & & & 0 \end{pmatrix},
$$

$$
C_2 = \begin{pmatrix} 0 & 0 & -a_{14} & a_{13} & 0 \\ & 0 & -a_{24} & a_{23} & 0 \\ & & 0 & a_{33}+a_{44} & a_{54} \\ & * & & 0 & -a_{53} \\ & & & & 0 \end{pmatrix} + \begin{pmatrix} 0 & b_{21}-b_{24} & 0 & b_{24} & b_{23} \\ & 0 & 0 & b_{24} & b_{24} \\ & & 0 & b_{22} & b_{23} \\ & * & & 0 & -b_{24} \\ & & & & 0 \end{pmatrix},
$$

$$
C_3 = \begin{pmatrix} 0 & a_{25} & a_{35}-a_{15} & a_{45} & a_{11}+a_{13}+a_{55} \\ & 0 & -a_{25} & 0 & a_{21}+a_{23} \\ & & 0 & a_{45} & a_{31}+a_{33}+a_{55} \\ & * & & 0 & a_{41}+a_{43} \\ & & & & 0 \end{pmatrix} + \begin{pmatrix} 0 & b_{31}-b_{34} & 0 & b_{34} & b_{33} \\ & 0 & 0 & b_{34} & b_{34} \\ & & 0 & b_{32} & b_{33} \\ & * & & 0 & -b_{34} \\ & & & & 0 \end{pmatrix},
$$

$$
C_4 = \begin{pmatrix} 0 & \begin{array}{c} -a_{11}-a_{14}-a_{15} \\ -a_{22}+a_{24} \end{array} & -a_{32}+a_{34} & \begin{array}{c} a_{11}+a_{12}+a_{15} \\ -a_{42}+a_{44} \end{array} & \begin{array}{c} a_{12}-a_{14} \\ -a_{52}+a_{54} \end{array} \\ & 0 & a_{31}+a_{34}+a_{35} & \begin{array}{c} a_{21}+a_{22}+a_{25} \\ +a_{41}+a_{44}+a_{45} \end{array} & \begin{array}{c} a_{22}-a_{24} \\ +a_{51}+a_{54}+a_{55} \end{array} \\ & & 0 & a_{31}+a_{32}+a_{35} & a_{32}-a_{34} \\ & * & & 0 & \begin{array}{c} a_{42}-a_{44} \\ -a_{51}-a_{52}-a_{55} \end{array} \\ & & & & 0 \end{pmatrix}
$$

$$
+ \begin{pmatrix} 0 & b_{41}-b_{44} & 0 & b_{44} & b_{43} \\ & 0 & 0 & b_{44} & b_{44} \\ & & 0 & b_{42} & b_{43} \\ & * & & 0 & -b_{44} \\ & & & & 0 \end{pmatrix}.
$$

So we obtain the following system of linear equations

$$
\begin{aligned}
&a_{11}+a_{22}+b_{11}-b_{14}=a_{32}=a_{42}+b_{14}=a_{52}+b_{13}=a_{31}=0,\\
&a_{41}-b_{14}=a_{51}-b_{14}=b_{12}=b_{13}=b_{14}=0,\\
&b_{21}-b_{24}=a_{14}=a_{13}+b_{24}=b_{23}=a_{24}=0,\\
&a_{23}+b_{24}=b_{24}=a_{33}+a_{44}+b_{22}=a_{54}+b_{23}=a_{53}+b_{24}=0,\\
&a_{25}+b_{31}-b_{34}=a_{35}-a_{15}=a_{45}+b_{34}=a_{11}+a_{13}+a_{55}+b_{33}=-a_{25}=0,\\
&b_{34}=a_{21}+a_{23}+b_{34}=a_{45}+b_{32}=a_{31}+a_{33}+a_{55}+b_{33}=a_{41}+a_{43}-b_{34}=0\\
&a_{11}+a_{14}+a_{15}+a_{22}-a_{24}-b_{41}+b_{44}=a_{32}-a_{34}=0,\\
&a_{11}+a_{12}+a_{15}-a_{42}+a_{44}+b_{44}=a_{12}-a_{14}-a_{52}+a_{54}+b_{43}=0,\\
&a_{31}+a_{34}+a_{35}=a_{21}+a_{22}+a_{25}+a_{41}+a_{44}+a_{45}+b_{44}=0,\\
&a_{22}-a_{24}+a_{51}+a_{54}+a_{55}+b_{44}=a_{31}+a_{32}+a_{35}+b_{42}=0,\\
&a_{32}-a_{34}+b_{43}=a_{42}-a_{44}-a_{51}-a_{52}-a_{55}-b_{44}=0.
\end{aligned}
$$

Solving this system of linear equations,

$$a_{ij}=b_{ij}=0 \text{ for } i\neq j,\ a_{11}=\cdots=a_{55},\ b_{11}=\cdots=b_{44},\ 2a_{11}+b_{11}=0.$$

Therefore,

$$T(G_w)_e=\{(tI_5,-2tI_4)\mid t\in k\}.$$

Since $\dim T(G_w)_e=1=\dim G-\dim V$, Gw is open and G_w is smooth over k. Since $\widetilde{T}\subset G_w^\circ$ and $\dim\widetilde{T}=1$, $G_w^\circ=\widetilde{T}\cong \mathrm{GL}(1)$. Since this is reductive, (G,V) is a regular prehomogeneous vector space. $\square$

Let $V_1=\mathrm{Aff}^5$ and $V_2=\mathrm{Aff}^4$. We identify V_2 with the space of linear forms in $v=\begin{pmatrix}v_1 & v_2 & v_3 & v_4\end{pmatrix}$. Choosing the standard basis for V_1 and considering its dual basis, we identify V_1 and V_1^* with the space of 5-dimensional column vectors. We identify Sym^2V_2 with the space of quadratic forms.

Define a linear map

$$\phi_1: V\to \wedge^4V_1\otimes \mathrm{Sym}^2V_2\cong V_1^*\otimes\mathrm{Sym}^2V_2$$

by

$$x=(x_{jk}(v))\to \mathrm{Pfaff}(x)(v)=\begin{pmatrix}\mathrm{Pfaff}_1(x)(v)\\ \vdots\\ \mathrm{Pfaff}_5(x)(v)\end{pmatrix} \tag{16.3}$$

where

$$
\begin{aligned}
\mathrm{Pfaff}_1(x)&=x_{23}x_{45}-x_{24}x_{35}+x_{25}x_{34},\\
\mathrm{Pfaff}_2(x)&=-(x_{13}x_{45}-x_{14}x_{35}+x_{15}x_{34}),\\
\mathrm{Pfaff}_3(x)&=x_{12}x_{45}-x_{14}x_{25}+x_{15}x_{24},\\
\mathrm{Pfaff}_4(x)&=-(x_{12}x_{35}-x_{13}x_{25}+x_{15}x_{23}),\\
\mathrm{Pfaff}_5(x)&=x_{12}x_{34}-x_{13}x_{24}+x_{14}x_{23}.
\end{aligned} \tag{16.4}
$$

Note that $\mathrm{Pfaff}_1(x),\cdots,\mathrm{Pfaff}_5(x)$ are the Pfaffians of 4×4 minors of diagonal entries of x and so they are quadratic forms of v.

Lemma 16.5. *If* $g = (g_1, g_2) \in G$ *then* $\mathrm{Pfaff}(gx)(v) = (\det g_1)^t g_1^{-1} \mathrm{Pfaff}(x)(vg_2)$.

Proof. Note that both sides of the above equation are integral polynomials if $k = \mathbb{Q}$. So as in the proof of Proposition 14.3, we may assume that $k = \mathbb{Q}$.

Since $\mathrm{ch}\, \mathbb{Q} = 0$, we define a map $V \to \wedge^4 V_1 \otimes \mathrm{Sym}^2 V_2$ by

$$V \ni \sum_{i=1}^{N} p_i \otimes q_i \to (1/2) \sum_{i,j=1}^{N} p_i \wedge p_j \otimes q_i q_j. \tag{16.6}$$

We identify $\wedge^4 V_1$ with the dual space of V_1 by the pairing

$$V_1 \times \wedge^4 V_1 \ni (a, b) \to a \wedge b.$$

If $g_1 \in G_1$ then $g_1 a \wedge g_1 b = (\det g_1) a \wedge b$ and so

$$a \wedge g_1 b = (\det g_1)(g_1^{-1} a) \wedge b.$$

Therefore, if we regard elements $b \in \wedge^4 V_1$ as elements of V_1^*, the action of G_1 is $\det g_1$ times the contragredient representation.

It is easy to verify that the maps (16.3), (16.6) coincide. Since the bases we chose for V_1, V_1^* are dual to each other, the action of $g_1 \in G_1$ on $\wedge^4 V_1$ can be regarded as $(\det g_1)^t g_1^{-1}$. Lemma 16.5 now follows easily from the alternative definition (16.6). $\square$

Definition 16.7. We define $\mathrm{Zero}(x)$ to be the subset of $\mathbb{P}^3$ defined by equations $\mathrm{Pfaff}_1(x)(v) = \cdots = \mathrm{Pfaff}_5(x)(v) = 0$.

By Lemma 16.5, If $g = (g_1, g_2) \in G$ then

$$\mathrm{Zero}(gx) = \mathrm{Zero}(x) g_2^{-1}. \tag{16.8}$$

Easy computations show that

$$\mathrm{Pfaff}(w) = \begin{pmatrix} v_4(v_2 - v_3) \\ v_3(v_4 - v_2) \\ v_4(v_3 - v_1) \\ v_3(v_4 - v_1) \\ v_2(v_1 - v_4) \end{pmatrix}, \tag{16.9}$$
$$\mathrm{Zero}(w) = \{(1,0,0,0), (0,1,0,0), (0,0,1,0), (0,0,0,1), (1,1,1,1)\}.$$

If $S \subset \mathbb{P}^3$, we say that S is in general position if no four points in S are on a plane. This of course implies that no three points of S are on a line.

Proposition 16.10. (1) *If* $x \in V_k$ *and* $\mathrm{Zero}(x) = \mathrm{Zero}(w)$, *there exists an element* $g \in G_k$ *such that* $gw = x$.

(2) *Suppose that* $\mathrm{Zero}(x)$ *consists of five points. Then* $\mathrm{Zero}(x)$ *is in general position.*

Proof. We first show (1). The assumption implies that $\mathrm{rk}(x_i) \le 2$ for $i = 1, \cdots, 4$ and $\mathrm{rk}(x_1 + \cdots + x_4) \le 2$. If $x_i = 0$ for any $1 \le i \le 4$, then $\mathrm{Zero}(x)$ does not depend on the i-th coordinate. So if it is not empty, then it is an infinite set, which is a contradiction. If $x_1 + \cdots + x_4 = 0$, then by changing the coordinate system of Aff^4, one can also show that $\mathrm{Zero}(x)$ is either empty or an infinite set, which is a contradiction. Therefore, $\mathrm{rk}(x_i) = 2$ for all i and $\mathrm{rk}(x_1 + \cdots + x_4) = 2$.

Since $\mathrm{rk}(x_1) = 2$, applying an element of $\mathrm{GL}(5)_k$, we may assume that $x_1 = w_1$. The matrix x_1 is fixed by the following matrices

$$d_1(A, B) = \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}, \; n_1(u) = \begin{pmatrix} I_2 & u \\ 0 & I_3 \end{pmatrix},$$

where $A \in \mathrm{GL}(2)_k, B \in \mathrm{GL}(3)_k, u \in \mathrm{M}(2,3)_k$.

Suppose that x_2, x_3, x_4 are of the form

$$\begin{pmatrix} B_i & {}^tC_i \\ -C_i & 0 \end{pmatrix},$$

where $B_i \in \mathrm{M}(2,2)_k, C_i \in \mathrm{M}(2,3)_k$ for $i = 1,2,3$. The matrices C_2, C_3, C_4 are of rank 1, for otherwise the rank of either x_2, x_3 or x_4 becomes 4.

By applying an element of the form $d_1(A, B)$, we may assume that

$$C_2 = \begin{pmatrix} * & * \\ 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Then $\mathrm{Zero}(x)$ contains the line $v_3 = v_4 = 0$. This is a contradiction. Therefore, we may assume that an (i, j)-entry of x_2 for some $3 \le i, j \le 5$ is non-zero.

By applying an element of the form $d_1(I_2, B)$, we may assume that x_2 is of the form

$$x_2 = \begin{pmatrix} * & & * & & \\ & & 0 & 1 & 0 \\ * & & -1 & 0 & 0 \\ & & 0 & 0 & 0 \end{pmatrix}.$$

By applying an element of the form $n_1(u)$, we can make the (i, j)-entry of x_2 for $i = 3, 4, \; j = 1, 2$ zero. Since $\mathrm{rk}(x_2) = 2$, considering the minors of $(5,5), \; (2,2), \; (1,1)$-entries of x_2 in this order, the $(1,2), \; (1,5), \; (2,5)$-entries of x_2 are zero. So $x_2 = w_2$.

Next, we consider x_3. If the fifth rows of x_3, x_4 are zero, $\mathrm{Zero}(x)$ contains the hypersurface

$$\{v \mid \mathrm{Pfaff}_5(x)(v) = 0\},$$

which is an infinite set. Therefore, we may assume that the fifth row of x_3 is non-zero. The points x_1, x_2 are fixed by matrices of the form

$$d_2(A, B) = \begin{pmatrix} A & & \\ & B & \\ & & 1 \end{pmatrix}, \; n_2(u) = \begin{pmatrix} I_4 & u \\ 0 & 1 \end{pmatrix},$$

where $A, B, \in \mathrm{GL}(2)_k, u \in \mathrm{M}(4,1)_k$. By applying elements of the form $d_2(A, B)$ and $n_2(u)$, we may assume that the fifth row of x_3 is either

$$\begin{pmatrix} -1 & 0 & -1 & 0 & 0 \end{pmatrix}, \; \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \end{pmatrix}, \text{ or } \begin{pmatrix} 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

We show that the last two possibilities do not happen. Consider the second case. Since $\mathrm{rk}(x_3) = 2$, the (i, j)-entries of x_3 for $i, j = 3, 4$ are zero. The $(3,2), (4,2)$-entries of x_3 are zero for the same reason. Then the $(3,1), (4,1)$-entries of x_3 become zero after applying $n_2(u)$ for some u. This implies that $\mathrm{Zero}(x)$ contains the line $v_2 = v_4 = 0$, which is a contradiction. The argument is the same for the third case.

Therefore, we may assume that the fifth row of x_3 is $\begin{pmatrix}1 & 0 & 1 & 0 & 0\end{pmatrix}$. By a similar argument as before, we may assume that $x_3 = w_3$.

Next we consider x_4. Suppose $x_4 = z(a, \cdots, j)$ where

$$z(a,\cdots,j) = \begin{pmatrix} 0 & a & b & c & d \\ -a & 0 & e & f & g \\ -b & -e & 0 & h & i \\ -c & -f & -h & 0 & j \\ -d & -g & -i & -j & 0 \end{pmatrix}. \tag{16.11}$$

Since $\mathrm{rk}(x_4) = 2$ and $\mathrm{rk}(x_1 + x_2 + x_3 + x_4) = 2$, 4×4 minors of diagonal elements of $x_4, x_1 + x_2 + x_3 + x_4$ are zero. This implies that

$$\begin{aligned} &ah + ce - bf = 0, \\ &ai + de - bg = 0, \\ &aj + df - cg = 0, \\ &bj + dh - ci = 0, \\ &ej + gh - fi = 0, \end{aligned} \tag{16.12}$$

$$\begin{aligned} &(a+1)(h+1) + ce - bf = 0, \\ &(a+1)(i+1) + (d+1)e - bg = 0, \\ &(a+1)j + (d+1)f - cg = 0, \\ &bj + (d+1)(h+1) - c(i+1) = 0, \\ &ej + g(h+1) - f(i+1) = 0. \end{aligned} \tag{16.13}$$

This is equivalent to (16.12) and

$$\begin{aligned} &a + h + 1 = 0, \\ &a + i + e + 1 = 0, \\ &j + f = 0, \\ &d + h - c + 1 = 0, \\ &g - f = 0. \end{aligned} \tag{16.14}$$

Therefore, $g = f = -j$.

The matrices x_1, x_2, x_3 are fixed by matrices of the form

$$d_3(t) = \left(\begin{pmatrix} t^{-1} & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & t^{-1} & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} t & 0 & 0 & 0 \\ 0 & t & 0 & 0 \\ 0 & 0 & t & 0 \\ 0 & 0 & 0 & t \end{pmatrix} \right),$$

$$n_3(u_1,u_2,u_3) = \begin{pmatrix} 1 & u_1 & 0 & 0 & u_3 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & u_2 & u_3 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

where $u_1, u_2, u_3 \in k, t \in k^\times$.

Suppose $g, j \neq 0$. Applying an element of the form $n_3(u_1, u_2, 0)$, we may assume that $d = i = 0$. Then by the second equation of (16.12), $b = 0$. Applying an element of the form $n_3(0, 0, u_3)$, we may assume $e = 0$.

In the following, note that the same rows of three of $x_1, \cdots, x_4$ cannot become zero simultaneously. For example, if the second rows of x_2, x_3, x_4 are zero, then $\mathrm{Zero}(x)$ contains the curve

$$\{v \mid v_1 = 0,\ \mathrm{Pfaff}_2(x)(v) = 0\}, \tag{16.15}$$

which is an infinite set. From the first equation of (16.12), $a = 0$ or $h = 0$. If $a = 0$ then the second rows of x_2, x_3, x_4. This is a contradiction and so we may assume that $h = 0$. By the first and the fourth equations in (16.14), $a = -1, c = 1$. Applying an element of the form $d_3(t)$, we may assume that $j = -1$. This implies that $g = f = 1$. Therefore, $x_4 = w_4$.

Suppose that $g = f = j = 0$. If $d = i = 0$ then the fifth rows of x_1, x_2, x_4 are zero, which is a contradiction. If $d = i$, $\mathrm{Zero}(x)$ contains the curve

$$\{v \mid v_4 = dv_2,\ \mathrm{Pfaff}_5(x)(v) = 0\}.$$

This is a contradiction. Therefore, by applying an element of the form $n_3(0, 0, u_3)$, we may assume that $b = 0$.

By the first equations of (16.12), (16.14), $a(a+1) = ce$. So if $a = 0$, then (16.12), (16.14) becomes

$$\begin{aligned}
&ce = 0,\\
&de = 0,\\
&d + ci = 0,\\
&h + 1 = 0,\\
&i + e + 1 = 0,\\
&d - c = 0.
\end{aligned}$$

If $e = 0$ then the second rows of x_2, x_3, x_4 are zero, which is a contradiction. So $e \neq 0$. This implies that $c = 0, d = 0$ and $h = -1$. Then if $v_2 = v_3$ then the forth row is zero. Therefore, $\mathrm{Zero}(x)$ contains the curve

$$\{v \mid v_2 = v_3,\ \mathrm{Pfaff}_4(x)(v) = 0\},$$

which is a contradiction. So $a \neq 0$.

By the fourth equation of (16.14), $h = c - d - 1$. Applying an element of the form $d_3(t)$, h changes to $tc - d - 1$. Therefore, if $c \neq 0$, we can make $h = -1, a = 0$ which is a contradiction. Therefore, $c = 0$. This implies that $a = -1, h = 0$. Hence, the fourth rows of x_1, x_3, x_4 are zero, which is a contradiction. This proves (1).

We show (2) next. Suppose a quadratic hypersurface Q contains three points on a line ℓ. Then choosing a plane P which contains ℓ and taking the intersection of Q and P, $Q \cap P$ contains ℓ. Therefore, Q contains ℓ.

If three points of $\mathrm{Zero}(x)$ are on a line, then quadratic hypersurfaces $\mathrm{Pfaff}_1(x)(v) = 0, \cdots, \mathrm{Pfaff}_5(x)(v) = 0$ all contain the line containing those three points. Therefore, $\mathrm{Zero}(x)$ is an infinite set, which is a contradiction. Therefore, no three points of $\mathrm{Zero}(x)$ are on a line.

Assuming $\mathrm{Zero}(x)$ is on a plane, we deduce a contradiction. We may assume that $\mathrm{Zero}(x)$ consists of p_1, p_2, p_3, $(1,1,1,0)$ and a point of the form $(y_1, y_2, y_3, 0)$ where not all of y_1, y_2, y_3 are the same.

As we pointed out after Lemma 14.13, if a conic on the plane $v_4 = 0$ contains p_1, p_2, p_3, and $(1,1,1,0)$, then it is in the span of w_1, w_2 in (14.10). It is easy to show that there is a unique conic in this span which contains the point $(y_1, y_2, y_3, 0)$.

Since $\mathrm{Pfaff}_1(x)(v) = 0, \cdots, \mathrm{Pfaff}_5(x)(v) = 0$ all contain these points, they must define the same conic. This implies that $\mathrm{Zero}(x)$ is an infinite set, which is a contradiction.

The above argument shows that we may assume that there are four points in $\mathrm{Zero}(x)$ which are on a plane, but the fifth point is not on this plane. Applying an element of $G_{2\,k}$, we may assume that

$$\mathrm{Zero}(x) = \{(1,0,0,0), (0,1,0,0), (0,0,1,0), (0,0,0,1), (1,1,1,0)\}. \tag{16.16}$$

Note that in the proof of (1), we did not use the assumption $\mathrm{rk}(x_1+x_2+x_3+x_4) = 2$ until the consideration of x_4.

The condition (16.16) implies that $\mathrm{rk}(x_i) = 2$ for $i = 1, \cdots, 4$, and $\mathrm{rk}(x_1+x_2+x_3) = 2$. Since the present condition $\mathrm{rk}(x_1 + x_2 + x_3) = 2$ is symmetric with respect to x_1, x_2, x_3, we apply the argument of the proof of (1) to x_4, x_1, x_2, x_3 in this order. Then we may assume that $x_1 = w_2, x_2 = w_3, x_3 = z(a, \cdots, j), x_4 = w_1$, where $z(a, \cdots, j)$ is as in (16.11).

The above condition is equivalent to (16.12) and

$$\begin{aligned}
&a(h+1) + ce - bf = 0, \\
&a(i+1) + (d+1)e - bg = 0, \\
&aj + (d+1)f - cg = 0, \\
&bj + (d+1)(h+1) - c(i+1) = 0, \\
&ej + g(h+1) - f(i+1) = 0.
\end{aligned}$$

This implies that $a = e = g = f = 0$. Therefore, the second rows of x_2, x_3, x_4 are zero, which is a contradiction.

This completes the proof of Proposition 16.10. $\square$

Proposition 16.17. *Let $x \in V_{\bar{k}}$. Then $x \in V_{\bar{k}}^{\mathrm{ss}}$ if and only if* $\mathrm{Zero}(x)$ *consists of five points. If so,* $\mathrm{Zero}(x)$ *is in general position.*

Proof. Note that since (G, V) is a regular prehomogeneous vector space, V^{ss} is a single G-orbit. By (16.8) and (16.9), if $x \in V^{\mathrm{ss}}$ then $\mathrm{Zero}(x)$ consists of five points in general position.

The converse follows from Proposition 16.10 (replacing k by $\bar{k}$). $\square$

Let $x \in V_k^{\mathrm{ss}}$. We choose $g_x \in G_{k^{\mathrm{sep}}}$ so that $x = g_x w$. Let

$$\mathrm{Zero}(x) = \{p_{x\,1}, p_{x\,2}, p_{x\,3}, p_{x\,4}, p_{x\,5}\}.$$

As in sections 13, 14, $\mathrm{Zero}(x)$ can be regarded as a scheme over k, $\mathrm{Aut}\,(\mathrm{Zero}(x))$ is an algebraic group, and the map $\pi_x(g) : \mathrm{Zero}(x) \ni q \to qg_2 \in \mathrm{Zero}(x)$ for $g = (g_1, g_2) \in G_x$ is a homomorphism $G_x \to \mathrm{Aut}\,(\mathrm{Zero}(x))$ of algebraic groups over k.

Over $\bar{k}$, we consider π_x set-theoretically and identify π_x with the homomorphism $G^\circ_{x\,\bar{k}} \to \mathfrak{S}_5$ defined by

$$p_{x\,j}g_2 = p_{x\,\pi_x(g)(j)} \quad \text{for all } j.$$

We also define homomorphisms $\phi, \psi : \mathrm{Gal}(k^{\mathrm{sep}}/k) \to \mathfrak{S}_5$ similarly as in (13.22) (13.23).

Define

$$\tau_1 = \left(\begin{pmatrix} 0 & 0 & -1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ -1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \right),$$

$$\tau_2 = \left(\begin{pmatrix} 1 & -1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & -1 \\ 1 & -1 & -1 & -1 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & -1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \right),$$

$$\tau_3 = \left(\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & -1 & -1 & -1 & 0 \\ 1 & 0 & 0 & 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix} \right),$$

$$\tau_4 = \left(\begin{pmatrix} 0 & 1 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & -1 \\ -1 & 0 & 1 & 0 & 0 \\ -1 & 1 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \right).$$

Then $\tau_i \in G_{w\,k}$. for $i = 1, 2, 3, 4$. Explicit computations show that $\tau_1, \cdots, \tau_4$ map to $(12), (13), (14), (15)$ by π_w respectively.

Let H be the subgroup of G_w generated by $\tau_1, \cdots, \tau_4$. By the same proof as that in Proposition 14.18, one can show the following proposition and we leave the proof to the reader.

Proposition 16.18. *The subgroup H is isomorphic to $\mathfrak{S}_5$ by π_w.*

Proposition 16.19. *Assumption 12.1 is satisfied with $i = 5$.*

Proof. As in Propositions 13.16, 14.19, we only have to show $\mathrm{Ker}(\pi_w) = \widetilde{T}$ set-theoretically.

Let $g = (g_1, g_2) \in \mathrm{Ker}(\pi_w)_{\bar{k}}$. This implies that g_2 fixes five points in general position in $\mathbb{P}^3$. So g_2 is a scalar matrix. Then by Lemma 16.5, g_1 fixes the quadratic forms $\mathrm{Pfaff}_1(w)(v), \cdots, \mathrm{Pfaff}_5(w)(v)$ up to scalar. Since they are linearly independent, g_1 is a scalar matrix. If $g = tI_5,\ g_2 = sI_4$, then clearly, $s = t^{-2}$ and so $g \in \widetilde{T}_{\bar{k}}$. $\square$

Note that $G^\circ_w = \widetilde{T}$ is contained in the center of G in this case also. So if $x = \in V^{\mathrm{ss}}_k$ then $G^\circ_x = \widetilde{T}$.

Let γ_V be the map defined in (12.3). Since $\mathrm{H}^1(k,G)=\mathrm{H}^1(k,\widetilde{T})=\{1\}$, Theorem 12.10 implies the following theorem.

Theorem 16.20. *The map γ_V is bijective. Moreover, $G_x^\circ=\widetilde{T}$ for all $x\in V_k^{\mathrm{ss}}$.*

We shall find explicit representatives of the orbit space $G_k\backslash V_k^{\mathrm{ss}}$. Note that the statement of Proposition 13.24 holds for the present situation also. So we construct representatives $x\in G_k\backslash V_k^{\mathrm{ss}}$ so that the action of $\mathrm{Gal}(k^{\mathrm{sep}}/k)$ on $\mathrm{Zero}(x)$ is given by homomorphisms corresponding to elements in $\mathrm{H}^1(k,\mathfrak{S}_5)$.

We first consider the fibers of $\beta_5:\mathrm{H}^1(k,\mathfrak{S}_5)\to\mathfrak{Ex}_5$. Let F,N,Γ be as before. The possible orders of subgroups of $\mathfrak{S}_5$ are

$$1,2,3,4,5,6,8,10,12,15,20,24,30,40,60,120.$$

However, as in Exercise 7 [26, p. 308], there is no subgroup of order 30 or 40.

Let $H_1,H_2,H_2\subset\mathfrak{S}_5$ be the subgroups generated by (123),(1234),(12345) respectively. Easy considerations show

$$\begin{aligned}N_{\mathfrak{S}_5}(H_1)&=\langle(123),(45)\rangle,\\ N_{\mathfrak{S}_5}(H_2)&=\langle(1234),(14)(23)\rangle,\\ N_{\mathfrak{S}_5}(H_3)&=\langle(12345),(2354)\rangle.\end{aligned}$$

Also by Corollary [26, p. 297], $C_{\mathfrak{S}_5}(H_3)=H_3$.

(1) Order 2, 3 subgroups are similar as in the case of $\mathfrak{S}_4$.

(2) Any finite group of order 4 is abelian. They are conjugate to subgroups of $\mathfrak{S}_4$.

(4) Order 5 groups are generated by 5-cycles. They are all conjugate.

(5) Suppose that $\#\Gamma=6$. Then $\Gamma\cong\mathfrak{S}_3$ or $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$. We identify $\mathfrak{S}_3$ with permutations of $\{1,2,3\}$. We define $\mu(x)=1$ if x is an odd permutation, and $\mu(x)=0$ if x is an even permutation. Let

$$\rho_1(x)=x,\quad \rho_2(x)=x(4,5)^{\mu(x)}. \tag{16.21}$$

We show that conjugacy classes of imbeddings of $\mathfrak{S}_3$ to $\mathfrak{S}_5$ are represented by ρ_1,ρ_2. Suppose $\rho:\mathfrak{S}_3\to\mathfrak{S}_5$ is an imbedding. Then $\rho_1((123))$ is an order three element and so it is conjugate to (123). Therefore, we may assume that $\rho((123))=(123)$. The normalizer of the subgroup generated by (123) is generated by $(12),(23),(45)$. Since $(12),(23)$ are conjugate by (123), we may assume that $\rho((12))=(12)$ or (45). This shows that $\rho=\rho_1$ or ρ_2.

We identify $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ with the subgroup generated by (123) and (45). We show that any imbedding of $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ in $\mathfrak{S}_5$ is conjugate to the natural imbedding. Let $\rho:\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\to\mathfrak{S}_5$ be an imbedding. As we showed above, we may assume that $\rho((123))=(123)$. The centralizer of (123) is generated by (123) and (45), So $\rho((45))$ must be (45). This shows that ρ is conjugate to the natural imbedding.

(6) Order 8 subgroups of $\mathfrak{S}_5$ are Sylow 2 subgroups of $\mathfrak{S}_5$, therefore, they are all conjugate to D_4.

(7) Suppose that $\#\Gamma=10$. Since $2\not\equiv 1 \mod 5$, the Sylow 5 subgroup is a normal subgroup, and therefore Γ is isomorphic to either D_5 or $\mathbb{Z}/5\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$. However since the centralizer of a 5-cycle is a power of that 5-cycle, the second case does not occur.

Automorphisms of D_5 are induced by inner automorphisms of $\mathfrak{S}_5$.

(8) Suppose that $\#\Gamma = 12$. The Sylow 3 subgroup is generated by a 3-cycle, say (123). Suppose that H_1 is a normal subgroup of Γ. Then $\Gamma = \langle (123), (45) \rangle \cong \mathfrak{S}_3 \times \mathbb{Z}/2\mathbb{Z}$.

Suppose that H_1 is not a normal subgroup of Γ. Since $2 \not\equiv 1 \mod 3$, there are four conjugates of H_1 in Γ. Therefore, there are eight order 3 elements in Γ. Since $\#\Gamma = 12$, there are exactly three elements of order divisible by 2. Suppose that the Sylow 2 subgroup of Γ is isomorphic to $\mathbb{Z}/4\mathbb{Z}$. Then it is generated by a 4-cycle. Since the normalizer is D_4, (123) can not normalize the Sylow 2 subgroup. Therefore, there are more than one conjugate of the Sylow 2 subgroup. This contradicts to the above statement. Therefore, the Sylow 2 subgroup is a normal subgroup of Γ, and is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Easy consideration shows that Γ is conjugate to A_4.

All the automorphisms of A_4 are induced by inner automorphisms of $\mathfrak{S}_4$. However $\mathfrak{S}_3 \times \mathbb{Z}/2\mathbb{Z}$ has an outer automorphism. Let $\mathfrak{S}_3, \mu$ be as in (5). Let y be the generator of $\mathbb{Z}/2\mathbb{Z}$, $x \in \mathfrak{S}_3$, and μ be as in 16.21. Define

$$\begin{aligned} &\rho_1(x) = x, \ \rho_1(y) = (45), \\ &\rho_2(x) = x(4,5)^{\mu(x)}, \ \rho_2(y) = (45). \end{aligned} \tag{16.22}$$

Then ρ_1, ρ_2 extend to automorphisms of $\mathfrak{S}_3 \times \mathbb{Z}/2\mathbb{Z}$. The conjugacy classes of imbeddings of $\mathfrak{S}_3 \times \mathbb{Z}/2\mathbb{Z}$ to $\mathfrak{S}_5$ are represented by ρ_1, ρ_2.

(9) Suppose that $\#\Gamma = 15$. Since $3 \not\equiv 1 \mod 5$, $5 \not\equiv 1 \mod 3$, Γ is abelian. By the same reason as in (7), this case does not occur.

(10) Suppose that $\#\Gamma = 20$. Since $2, 4 \not\equiv 1 \mod 5$, the Sylow 5 subgroup is a normal subgroup, and therefore Γ is the normalizer of a subgroup of order 5. Since all the 5-cycles are conjugate, all the subgroups of order 20 are conjugate. $N_{\mathfrak{S}_5}(H_3)$ is given by two generators x, y with relations $x^5 = y^4 = 1, yxy^{-1} = x^2$.

Lemma 16.23. *All automorphisms of* $\Gamma = N_{\mathfrak{S}_5}(H_3)$ *are inner.*

Proof. Easy computations show that the center of Γ is trivial. Therefore, there are precisely 20 inner automorphisms. Let ρ be an automorphism of Γ. Suppose that $\rho(x) = x, \rho(y) = x^a y^b$. The group Γ is generated by $x, \rho(y)$ if and only if b is an odd number. Since ρ is a homomorphism, $(x^a y^b)^4 = 1, x^a y^b x y^{-b} x^{-a} = x^2$. Conversely, if this condition is satisfied for a pair (a, b), there exists an automorphism ρ of Γ of the above form. The above condition is equivalent to the condition $a(1 + 2^b + 2^{2b} + 2^{3b}) \equiv 0 \mod 5$, $2^b \equiv 2 \mod 5$. This is equivariant to the condition $b \equiv 1 \mod 4$. Therefore, there are precisely 5 automorphisms ρ with $\rho(x) = x$. The inner automorphism $i_y : z \to yzy^{-1}$ satisfies $i_y(x) = x^2$. Therefore, there are precisely 20 automorphisms. □

(11) Suppose that $\#\Gamma = 24$. By (2.19) [26, p. 300], Γ is conjugate to $\mathfrak{S}_4$.

(12) There is only one subgroup of order 60 which is A_5.

The above consideration shows the following proposition.

Proposition 16.24. *If* $F \in \mathfrak{Ex}_5$ *and* $\Gamma = \mathrm{Gal}(F/k)$, *then* $\beta_5^{-1}(F)$ *consists of a single element unless* $\Gamma \cong \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, D_4, $\mathfrak{S}_3$ *or* $\mathfrak{S}_3 \times \mathbb{Z}/2\mathbb{Z}$. *If* $\Gamma \cong \mathbb{Z}/2\mathbb{Z}$, D_4, $\mathfrak{S}_3$ *or* $\mathfrak{S}_3 \times \mathbb{Z}/2\mathbb{Z}$, *then* $\beta_5^{-1}(F)$ *consists of two elements. If* $\Gamma \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, *then* $\beta_5^{-1}(F)$ *consists of four elements.*

If $F = k$ is the trivial extension, we choose $x = w$ as the representative of the corresponding orbit.

Let F be a separable quadratic extension generated by roots $\alpha = (\alpha_1, \alpha_2)$ of a quadratic equation $t^2 + a_1 t + a_2 = 0$ where $a_1, a_2 \in k$. Define

$$w_\alpha = \begin{pmatrix} 0 & v_2 & 0 & -v_4 + v_1 & 0 \\ -v_2 & 0 & -v_1 & -v_4 & 0 \\ 0 & v_1 & 0 & -a_1 v_1 - a_2 v_2 & v_3 \\ v_4 - v_1 & v_4 & a_1 v_1 + a_2 v_2 & 0 & v_4 \\ 0 & 0 & -v_3 & -v_4 & 0 \end{pmatrix}.$$

By explicit computations,

$$\mathrm{Pfaff}(x) = \begin{pmatrix} v_2 v_4 + v_3 v_4 \\ v_3(v_1 - v_4) \\ v_2 v_4 \\ v_2 v_3 \\ -v_2(a_1 v_1 + a_2 v_2) - v_1(v_1 - v_4) \end{pmatrix},$$
$$\mathrm{Zero}(w_\alpha) = \{(\alpha_1, 1, 0, 0), (\alpha_2, 1, 0, 0), p_3, p_4, (0, 1, 0, 1)\}.$$

So this orbit corresponds to ρ_1 in (14.21).

Let $a_1, a_2, b_1, b_2 \in k$. Suppose the roots $\alpha = (\alpha_1, \alpha_2)$, $\beta = (\beta_1, \beta_2)$ of the equations $t^2 + a_1 t + a_2 = 0$, $t^2 + b_1 t + b_2 = 0$ generate separable quadratic extensions of k. We allow the case $\alpha = \beta$. Define

$$w_\alpha = \begin{pmatrix} 0 & 0 & v_2 & v_1 & 0 \\ 0 & 0 & v_1 - v_3 & -(a_1 v_1 + a_2 v_2) & v_4 \\ -v_2 & -(v_1 - v_3) & 0 & -(b_1 v_3 + b_2 v_4) & 0 \\ -v_1 & a_1 v_1 + a_2 v_2 & b_1 v_3 + b_2 v_4 & 0 & v_3 \\ 0 & -v_4 & 0 & -v_3 & 0 \end{pmatrix}.$$

By explicit computations,

$$\mathrm{Pfaff}(x) = \begin{pmatrix} v_3(v_1 - v_3) - v_4(b_1 v_3 + b_2 v_4) \\ -v_2 v_3 \\ -v_1 v_4 \\ v_2 v_4 \\ v_1(v_1 - v_3) + v_2(a_1 v_1 + a_2 v_2) \end{pmatrix},$$
$$\mathrm{Zero}(w_\alpha) = \{(\alpha_1, 1, 0, 0), (\alpha_2, 1, 0, 0), (0, 0, \beta_1, 1), (0, 0, \beta_2, 1), (1, 0, 1, 0)\}.$$

So this orbit corresponds to ρ_2 in (14.21) or ρ_1, ρ_2, ρ_3 in (14.22).

Let $f_a(t) = t^5 + a_1t^4 + a_2t^3 + a_3t^2 + a_4t + a_5$ be a polynomial with distinct roots $\alpha = (\alpha_1, \cdots, \alpha_5)$ such that $a_1, \cdots, a_5 \in k$. Define

$$x_{a\,1} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{pmatrix},$$

$$x_{a\,2} = \begin{pmatrix} 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & a_1 & 0 \\ 0 & -1 & -a_1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix},$$

(16.25)

$$x_{a\,3} = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ 0 & 1 & 0 & a_2 & 0 \\ -1 & 0 & -a_2 & 0 & a_4 \\ 0 & 0 & 0 & -a_4 & 0 \end{pmatrix},$$

$$x_{a\,4} = \begin{pmatrix} 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & a_3 & 0 \\ 0 & 0 & -a_3 & 0 & a_5 \\ 0 & 0 & 0 & -a_5 & 0 \end{pmatrix},$$

and $x_a = \sum_{i=1}^4 v_i x_{a\,i}$. Then

$$\mathrm{Pfaff}(x_a) = \begin{pmatrix} -v_1(v_1 + a_1v_2 + a_2v_3 + a_3v_4) - v_3(a_4v_3 + a_5v_4) \\ v_2(v_1 + a_1v_2 + a_2v_3 + a_3v_4) + v_4(a_4v_3 + a_5v_4) \\ v_1v_3 - v_2^2 \\ v_1v_4 - v_2v_3 \\ v_2v_4 - v_3^2 \end{pmatrix}. \tag{16.26}$$

The last three entries define the twisted cubic $(t^3, t^2, t, 1)$. If we restrict the first two entries to this twisted cubic, we get the equation $f_a(t) = 0$. So

$$\mathrm{Zero}(x_a) = \{(\alpha_i^3, \alpha_i^2, \alpha_i, 1) \mid i = 1, \cdots, 5\}. \tag{16.27}$$

An alternative way of verifying (16.27) is the following. The hypersurface defined by the equation $v_1v_4 - v_2v_3 = 0$ is isomorphic to $\mathbb{P}^1 \times \mathbb{P}^1$. If $(t_1, t_2), (s_1, s_2)$ are homogeneous coordinates of these two $\mathbb{P}^1$'s, the above hypersurface is parametrized as

$$(t_1s_1, t_1s_2, t_2s_1, t_2s_2).$$

If we restrict the equations $v_1v_3 - v_2^2 = v_2v_4 - v_3^2 = 0$ to $\mathbb{P}^1 \times \mathbb{P}^1$,

$$t_1(t_2s_1^2 - t_1s_2^2) = t_2(t_2s_1^2 - t_1s_2^2) = 0.$$

Since $(t_1, t_2) \neq (0, 0)$, this is equivalent to $t_2s_1^2 - t_1s_2^2 = 0$.

If we restrict the remaining two equations to $\mathbb{P}^1 \times \mathbb{P}^1$,

$$s_i(t_1^2 s_1 + a_1 t_1^2 s_2 + a_2 t_1 t_2 s_1 + a_3 t_1 t_2 s_2 + a_4 t_2^2 s_1 + a_5 t_2^2 s_2) = 0$$

for $i = 1, 2$. Since $(s_1, s_2) \neq (0, 0)$, this is equivalent to

$$t_1^2 s_1 + a_1 t_1^2 s_2 + a_2 t_1 t_2 s_1 + a_3 t_1 t_2 s_2 + a_4 t_2^2 s_1 + a_5 t_2^2 s_2 = 0.$$

The set of solutions to $t_2 s_1^2 - t_1 s_2^2 = 0$ is parametrized as $t_1 = s_1^2,\ t_2 = s_2^2$. If we restrict the above equation to this set, we get the equation

$$s_1^5 + a_1 s_1^4 s_2 + a_2 s_1^3 s_2^2 + a_3 s_1^2 s_2^3 + a_4 s_1 s_2^4 + a_5 s_2^5 = 0.$$

Thus, we get the same result. The point is that $\mathrm{Zero}(x)$ becomes an intersection of a degree $(1,2), (2,1)$ divisors on $\mathbb{P}^1 \times \mathbb{P}^1$. Since the intersection number of those divisors is $2 \cdot 2 + 1 \cdot 1 = 5$, we get a quintic equation.

Except for the cases where $F = k$, F/k is quadratic, or F/k is biquadratic and and the cohomology class corresponds to ρ_1, ρ_2, ρ_3 in (14.22), we may choose representatives of the form x_a. Note that we cannot choose a representative of the form x_a if the cohomology class corresponds to ρ_1 in (14.21) and $k = \mathbb{F}_2$ for example.

If $g(t)$ is a quartic polynomial over k, without multiple roots or roots in k, then $f_a(t) = g(t)t$ is a quintic polynomial over k without multiple roots. This construction works for ρ_2 in (14.21) and for cases where

$$\Gamma \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},\ \mathbb{Z}/4\mathbb{Z},\ A_4, \text{ or } \mathfrak{S}_4.$$

Let $g(t) = t^3 + b_1 t^2 + b_2 t + b_3$ be a polynomial with distinct roots $\alpha = (\alpha_1, \alpha_2, \alpha_3)$ such that $b_1, b_2, b_3 \in k$. If the orbit corresponds to ρ_1 in (16.21), we choose

$$f_a(t) = g(t)t(t-1).$$

Suppose the orbit corresponds to ρ_2 in (16.21). Then it is well known that the unique quadratic field contained in F is generated by roots γ_1, γ_2 of the quadratic equation $t^2 - At + B = 0$ where

$$A = 9b_1 b_2 - 2b_1^3 - 27b_3,\ B = b_1^2 - 3b_2.$$

If we choose

$$f_a(t) = g(t)(t^2 - At + B),$$

the roots are permuted according as ρ_2 in (16.21).

For all other cases, the fiber of β_5 consists of a single element. Therefore, if we choose $\alpha \in F$ so that $[k(\alpha) : k] = 5$ and F is generated by conjugates $\alpha_1 = \alpha, \cdots, \alpha_5$ of α, then we may choose the polynomial

$$f_a(t) = (t - \alpha_1)(t - \alpha_2)(t - \alpha_3)(t - \alpha_4)(t - \alpha_5).$$

In all the cases, the field generated by coordinates of points in $\mathrm{Zero}(x)$ coincides with $k(x)$. Therefore, we have the following proposition.

Proposition 16.28. *If $x \in V_k^{\mathrm{ss}}$, $k(x)$ is generated by coordinates of points in* $\mathrm{Zero}(x)$.

Remark 16.29. In the mid-nineteenth century, many mathematicians, including Hermite, Kronecker, Brioschi, and Klein, studied quintic fields essentially from the viewpoint of group theory, but their work is difficult to understand within this modern context. The group theoretic aspect of the subject is clearest in Klein's works, for example [12], and an excellent modern interpretation of Klein's works can be found in Serre's letter [24]. However, Klein's viewpoint seems slightly different from ours.

The interpretation of Zero(x) as an intersection of degree (2,1) and (1,2) divisors on $\mathbb{P}^1 \times \mathbb{P}^1$ appears in the work of both Brioschi [3, p. 337] and Klein [12].

Exercise 16.30. Prove that there exists a relative invariant polynomial of degree 40 in the following manner. Since we may use Proposition 14.4, we assume that $k = \mathbb{Q}$ in the following.

(1) Regard $V_1^* \otimes \mathrm{Sym}^2 V_2$ as the space of symmetric matrices with entries in V_1^*. Then the determinant of this matrix is an element of $\mathrm{Sym}^4 V_1^*$. Let $\Phi_1(x)$ be the composition of the following maps.

$$V = \wedge^2 V_1 \otimes V_2 \xrightarrow{\phi} V_1^* \otimes \mathrm{Sym}^2 V_2 \longrightarrow \mathrm{Sym}^4 V_1^*$$

Describe $\Phi_1((g_1, g_2)x)$ in terms of $\Phi_1(x)$. Find $\Phi_1(w)$.

(2) Consider the map

$$\phi_2 : V \ni x = (x_1, x_2, x_3, x_4) \to x_1 \wedge x_2 \wedge x_3 \wedge x_4 \in \wedge^4(\wedge^2 V_1),$$

for $x_1, \cdots, x_4 \in V_1$. Let $\Phi_2(x)$ be the composition of the following maps.

$$V \longrightarrow \wedge^4(\wedge^2 V_1) \xrightarrow{S} \wedge^4 V_1 \otimes \mathrm{Sym}^4 V_1 \cong V_1^* \otimes \mathrm{Sym}^4 V_1$$

where S is the map defined in (15.3). Describe $\Phi_2((g_1, g_2)x)$ in terms of $\Phi_2(x)$. Find $\Phi_2(w)$.

(3) Let $\Phi_3(x)$ be the composition of the following maps.

$$\begin{aligned} V &\longrightarrow \wedge^4(\wedge^2 V_1) \xrightarrow{D} \wedge^3(\wedge^2 V_1) \otimes (\wedge^2 V_1) \\ &\xrightarrow{S \otimes \mathrm{id}_{\wedge^2 V_1}} \wedge^3 V_1 \otimes \mathrm{Sym}^3 V_1 \otimes \wedge^2 V_1 \longrightarrow \mathrm{Sym}^3 V_1 \end{aligned}$$

Note that the map

$$\wedge^3 V_1 \otimes \mathrm{Sym}^3 V_1 \otimes \wedge^2 V_1 \to \mathrm{Sym}^3 V_1$$

is given so that if $a \in \wedge^3 V_1, b \in \mathrm{Sym}^3 V_1, c \in \wedge^2 V_1$ and $a \wedge c = f(a, c) e_1 \wedge \cdots \wedge e_5$, then $a \otimes b \otimes c$ maps to $f(a, c)b$. Describe $\Phi_3((g_1, g_2)x)$ in terms of $\Phi_3(x)$. Find $\Phi_3(w)$.

(4) There is a natural pairing $(\ ,\ )$ between $\mathrm{Sym}^4 V_1^*$ and $\mathrm{Sym}^4 V_1$ (see section 15). Let $\Phi_4(x) = (\Phi_1(x), \Phi_2(x)) \in V_1^*$. Describe $\Phi_4((g_1, g_2)x)$ in terms of $\Phi_4(x)$. Find $\Phi_4(w)$.

(5) Regarding $\Phi_4(x) \in V_1^* \subset \mathrm{Sym}^* V_1^*$, define $\Delta(x) = (\Phi_4(x)^3, \Phi_3(x))$. Show that $\Delta(w) \neq 0$ and $\Delta(x)$ is a relative invariant polynomial of degree 40.

17. Types (9), (12)

In this section we consider the cases (9), (11) in the Sato-Kimura classification. These are the following representations

(1) $G = \mathrm{GL}(3)\times\mathrm{GL}(3)\times\mathrm{GL}(2),\ V = \mathrm{M}(3,3)\otimes\mathrm{Aff}^2$,
(2) $G = \mathrm{GL}(6)\times\mathrm{GL}(2),\ V = \wedge^2\mathrm{Aff}^6\otimes\mathrm{Aff}^2$.

In the case (1), we identify V with the space of 3×3 matrices $x(v)$ with entries in the space of linear forms in two variables $v=(v_1,v_2)$. We regard v as a row vector. The group G acts on V by $gx(v) = g_1M(vg_3)^tg_2$ for $g=(g_1,g_2,g_3)\in G,\ x(v)\in V$.

In the case (2), we identify V with the space of 6×6 alternating matrices $x(v)$ with entries in the space of linear forms in two variables $v=(v_1,v_2)$. The group G acts on V by $gx(v) = g_1M(vg_2)^tg_1$ for $g=(g_1,g_2)\in G,\ x(v)\in V$.

Let $J_2 = \left(\begin{smallmatrix} 0 & 1\\ -1 & 0\end{smallmatrix}\right)$. Define

$$w = \begin{cases} v_1\begin{pmatrix} 0 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & -1\end{pmatrix} + v_2\begin{pmatrix} -1 & 0 & 0\\ 0 & 0 & 0\\ 0 & 0 & 1\end{pmatrix} & (1),\\[2ex] v_1\begin{pmatrix} 0 & 0 & 0\\ 0 & J_2 & 0\\ 0 & 0 & -J_2\end{pmatrix} + v_2\begin{pmatrix} -J_2 & 0 & 0\\ 0 & 0 & 0\\ 0 & 0 & J_2\end{pmatrix} & (2).\end{cases}$$

We leave the verification of the following proposition to the reader (see Exercise 17.22

Proposition 17.1. *We have* $\dim T(G_w)_e = 4, 10$ *in the cases (1), (2) respectively.*

The above proposition implies that $\dim T(G_w)_e = \dim G - \dim V$. Therefore, Gw is open and G_w is smooth over k. We now determine G_w°. We first consider the case (1). Let $a_n(t_1,\cdots,t_n)$ be the $n\times n$ diagonal matrix whose diagonal entries are $t_1,\cdots,t_n$. We put

$$t = (a_3(t_{11},t_{12},t_{13}), a_3(t_{21},t_{22},t_{23}), t_3I_2). \tag{17.2}$$

Proposition 17.3. *We have*

$$G_w^\circ = \{t \mid t_{11}t_{21}t_3 = t_{12}t_{22}t_3 = t_{13}t_{23}t_3 = 1\}. \tag{17.4}$$

Proof. Let H be the right hand side of (17.4). It is easy to verify that $H\cong \mathrm{GL}(1)^4$ and that H is contained in G_w°. Since

$$4 = \dim H \le \dim G_w^\circ = \dim T(G_w)_e = 4,$$

H must coincides with G_w°. $\square$

Next we consider the case (2). The proof of the following proposition is similar to that in Proposition 17.3 and is left to the reader.

Proposition 17.5. *We have*

$$G_w^\circ = \left\{ \left(\begin{pmatrix} g_1 & 0 & 0\\ 0 & g_2 & 0\\ 0 & 0 & g_3\end{pmatrix}, tI_2\right) \,\middle|\, \begin{matrix} g_1,g_2,g_3\in\mathrm{GL}(2),\ t\in\mathrm{GL}(1),\\ t\det g_1 = t\det g_2 = t\det g_3 = 1\end{matrix}\right\}. \tag{17.6}$$

By Propositions 17.3, 17.5, G_w is reductive in both cases. Therefore, we get the following proposition.

Proposition 17.7. *In both cases, (G, V) is a regular prehomogeneous vector space.*

As before, $\widetilde{T} \subset G$ is the kernel of the homomorphism $G \to \mathrm{GL}(V)$. Then

$$\widetilde{T} = \begin{cases} \{(t_1 I_3, t_2 I_3, (t_1 t_2)^{-1} I_2) \mid t_1, t_2 \in \mathrm{GL}(1)\} \cong \mathrm{GL}(1)^2 & (1), \\ \{(t I_6, t^{-2} I_2) \mid t \in \mathrm{GL}(1)\} \cong \mathrm{GL}(1) & (2). \end{cases}$$

In the case (1), we consider the map

$$x(v) \to F_x(v) = \det x(v) \in \mathrm{Sym}^3 \mathrm{Aff}^2.$$

In the case (2), we consider the map

$$x(v) \to F_x(v) = \mathrm{Pfaff}(x(v)) \in \mathrm{Sym}^3 \mathrm{Aff}^2,$$

where $\mathrm{Pfaff}(x(v))$ is the Pfaffian of the alternating matrix $x(v)$. The following lemma is obvious.

Lemma 17.8. (1) *In the case (1), $F_{(g_1,g_2,g_3)x}(v) = \det g_1 \det g_2 F_x(v g_3)$.*
(2) *In the case (2), $F_{(g_1,g_2)x}(v) = \det g_1 F_x(v g_2)$.*

Let $\Delta(x)$ be the discriminant of $F_x(v)$. By explicit computations,

$$F_w(v) = v_1 v_2 (v_1 - v_2).$$

So $\Delta(x)$ is a non-zero polynomial. Moreover, it is easy to see that $\Delta(gx) = \chi(g)\Delta(x)$ where

$$\chi((g_1, g_2, g_3)) = (\det g_1)^4 (\det g_2)^4 (\det g_3)^6$$

in the case (1), and

$$\chi((g_1, g_2)) = (\det g_1)^4 (\det g_2)^6$$

in the case (2). So $\Delta(x)$ is a relative invariant polynomial.

For $x \in V$, we define $\mathrm{Zero}(x)$ to be the subset of $\mathbb{P}^1$ defined by the equation $F_x(v) = 0$. Let

$$p_1 = (1, 0),\ p_2 = (0, 1),\ p_3 = (1, 1) \in \mathbb{P}^1.$$

It is easy to see that $\mathrm{Zero}(w) = \{p_1, p_2, p_3\}$. Considering the above $\Delta(x)$, we get the following proposition.

Proposition 17.9. *A point $x \in V$ belongs to V^{ss} if and only if* $\mathrm{Zero}(x)$ *consists of three points.*

As before, $\mathrm{Zero}(x)$ may be regarded as a scheme over k and $\mathrm{Aut}\,(\mathrm{Zero}(x))$ is an algebraic group. In the case (1), the map $\pi_x(g) : \mathrm{Zero}(x) \ni q \to q g_3 \in \mathrm{Zero}(x)$ for $g = (g_1, g_2, g_3) \in G_x$ is a homomorphism $G_x \to \mathrm{Aut}\,(\mathrm{Zero}(x))$. In the case (2), the map $\pi_x(g) : \mathrm{Zero}(x) \ni q \to q g_2 \in \mathrm{Zero}(x)$ for $g = (g_1, g_2) \in G_x$ is a homomorphism $G_x \to \mathrm{Aut}\,(\mathrm{Zero}(x))$. Over $\bar{k}$, we consider π_x set-theoretically and identify π_x with the homomorphism $G^{\circ}_{x\,\bar{k}} \to \mathfrak{S}_3$ defined similarly as in previous sections. In the case (1), define

$$\tau_1 = \left(\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} \right), \tau_2 = \left(\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 1 & 1 \end{pmatrix} \right).$$

In the case (2), define

$$\tau_1 = \left(\begin{pmatrix} 0 & I_2 & 0 \\ I_2 & 0 & 0 \\ 0 & 0 & I_2 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} \right), \tau_2 = \left(\begin{pmatrix} I_2 & 0 & 0 \\ 0 & 0 & I_2 \\ 0 & I_2 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 1 & 1 \end{pmatrix} \right).$$

It is easy to verify that

$$\pi_w(\tau_1) = (12),\ \pi_w(\tau_2) = (23)$$

in both cases.

By the same proof as that in Proposition 14.18, one can show the following proposition and we leave the proof to the reader.

Proposition 17.10. *The elements τ_1, τ_2 generate a subgroup of G_w which is isomorphic to $\mathfrak{S}_3$ by π_w.*

As before, Assumption 12.1 is satisfied with $i = 3$. In the case (1), $G^{\circ}_w \cong \mathrm{GL}(1)^4$. In the case (2), there is an exact sequence

$$1 \longrightarrow \mathrm{SL}(2)^3 \longrightarrow G^{\circ}_w \longrightarrow \mathrm{GL}(1)^2 \longrightarrow 1.$$

Therefore,

$$\mathrm{H}^1(k, G) = \mathrm{H}^1(k, G^{\circ}_w) = \{1\} \tag{17.11}$$

in both cases.

We now choose a point in the fiber of each cohomology class in $\mathrm{H}^1(k, \mathfrak{S}_3)$.

We define homomorphisms $\phi, \psi : \mathrm{Gal}(k^{\mathrm{sep}}/k) \to \mathfrak{S}_3$ similarly as in previous sections. Then the statement of Proposition 13.24 holds also. So as before, if $x \in V^{\mathrm{ss}}_k$, the homomorphism $\mathrm{Gal}(k^{\mathrm{sep}}/k) \to \mathfrak{S}_3$ which corresponds to the orbit of x may be identified with the action of the Galois group on $\mathrm{Zero}(x)$.

We have shown in section 13 that $\mathrm{H}^1(k, \mathfrak{S}_3)$ is in bijective correspondence with $\mathfrak{Ex}_3$. So if $F \in \mathfrak{Ex}_3$, to choose a point which corresponds to F, we only have to give a point x so that the splitting field of $F_x(v)$ is F.

If $F = k$, we choose $x = w$. Otherwise, we proceed as follows.

Let

$$f_\alpha(v) = v_1^3 + a_1 v_1^2 v_2 + a_2 v_1 v_2^2 + a_3 v_2^3 \in k[V] \tag{17.12}$$

be a cubic polynomial without a multiple factor and $\alpha_1, \alpha_2, \alpha_3$ the roots of $f_\alpha(v)$.

In the case (1), we define

$$
(17.13)\quad
\begin{aligned}
D_\alpha &= (\alpha_1-\alpha_2)(\alpha_1-\alpha_3)(\alpha_2-\alpha_3),\\
Q_\alpha &= \frac{1}{D_\alpha}\begin{pmatrix} -(\alpha_3-\alpha_1) & -(\alpha_3-\alpha_2)\\ \alpha_2(\alpha_3-\alpha_1) & \alpha_1(\alpha_3-\alpha_2)\end{pmatrix},\\
P_\alpha &= \begin{pmatrix} 1 & 1 & 1\\ \alpha_1 & \alpha_2 & \alpha_3\\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2\end{pmatrix},\\
w_\alpha &= v_1\begin{pmatrix} 0 & 0 & -1\\ 0 & -1 & a_1\\ -1 & a_1 & -a_1^2+a_2\end{pmatrix}\\
&\quad + v_2\begin{pmatrix} 0 & 1 & -a_1\\ 1 & -a_1 & a_1^2-a_2\\ -a_1 & a_1^2-a_2 & -a_1^3+2a_1a_2-a_3\end{pmatrix}.
\end{aligned}
$$

In the case (2), we define D_α, Q_α as above and

$$
(17.14)\quad
\begin{aligned}
P_\alpha &= \begin{pmatrix} I_2 & I_2 & I_2\\ \alpha_1 I_2 & \alpha_2 I_2 & \alpha_3 I_2\\ \alpha_1^2 I_2 & \alpha_2^2 I_2 & \alpha_3^2 I_2\end{pmatrix},\\
w_\alpha &= v_1\begin{pmatrix} 0 & 0 & -J_2\\ 0 & -J_2 & a_1 J_2\\ -J_2 & a_1 J_2 & (-a_1^2+a_2)J_2\end{pmatrix}\\
&\quad + v_2\begin{pmatrix} 0 & J_2 & -a_1 J_2\\ J_2 & -a_1 J_2 & (a_1^2-a_2)J_2\\ -a_1 J_2 & (a_1^2-a_2)J_2 & (-a_1^3+2a_1a_2-a_3)J_2\end{pmatrix}.
\end{aligned}
$$

By easy computations,

$$
\begin{aligned}
\det Q_\alpha &= D_\alpha^{-1},\\
\det P_\alpha &= \begin{cases} D_\alpha & (1),\\ D_\alpha^2 & (2),\end{cases}\\
F_{w_\alpha} &= f_\alpha(v).
\end{aligned}
$$

We define $g_\alpha \in G_{k^{\mathrm{sep}}}$ by

$$
g_\alpha = \begin{cases} (P_\alpha, P_\alpha, Q_\alpha) & (1),\\ (P_\alpha, Q_\alpha) & (2).\end{cases}
$$

Lemma 17.15. *We have $w_\alpha = g_\alpha w$.*

Proof. Since the argument is similar, we only consider the case (1). Let

$$
A_i(\alpha) = \alpha_1^i(\alpha_2-\alpha_3) + \alpha_2^i(\alpha_3-\alpha_1) + \alpha_3^i(\alpha_1-\alpha_2)
$$

for $i = 2, 3, 4, 5$. We define

$$W_1(\alpha) = \begin{pmatrix} -(\alpha_2 - \alpha_3) & 0 & 0 \\ 0 & -(\alpha_3 - \alpha_1) & 0 \\ 0 & 0 & -(\alpha_1 - \alpha_2) \end{pmatrix},$$

$$W_2(\alpha) = \begin{pmatrix} \alpha_1(\alpha_2 - \alpha_3) & 0 & 0 \\ 0 & \alpha_2(\alpha_3 - \alpha_1) & 0 \\ 0 & 0 & \alpha_3(\alpha_1 - \alpha_2) \end{pmatrix},$$

$$W_3(\alpha) = \begin{pmatrix} 0 & 0 & -A_2(\alpha) \\ 0 & -A_2(\alpha) & -A_3(\alpha) \\ -A_2(\alpha) & -A_3(\alpha) & -A_4(\alpha) \end{pmatrix},$$

$$W_4(\alpha) = \begin{pmatrix} 0 & A_2(\alpha) & A_3(\alpha) \\ A_2(\alpha) & A_3(\alpha) & A_4(\alpha) \\ A_3(\alpha) & A_4(\alpha) & A_5(\alpha) \end{pmatrix}.$$

Then

$$\begin{aligned} g_\alpha w &= \frac{1}{D_\alpha} P_\alpha (v_1 W_1(\alpha) + v_2 W_2(\alpha)) {}^t P_\alpha \\ &= \frac{1}{D_\alpha}(v_1 W_3(\alpha) + v_2 W_4(\alpha)). \end{aligned}$$

Now the lemma follows from the relations

$$\begin{aligned} A_2(\alpha) &= D_\alpha, \\ A_3(\alpha) &= -D_\alpha a_1, \\ A_4(\alpha) &= D_\alpha(a_1^2 - a_2), \\ A_5(\alpha) &= D_\alpha(-a_1^3 + 2a_1a_2 - a_3). \end{aligned}$$

□

Now we choose a point which corresponds to F when $F \neq k$.

If F/k is quadratic, then choose a pair $\alpha = (\alpha_1, \alpha_2)$ of conjugate elements of F so that $F = k(\alpha) = k(\alpha_1, \alpha_2)$. Then we consider $f_\alpha(v)$ in (17.12) with $\alpha_3 = 0$. If $\mathrm{Gal}(F/k) \cong \mathbb{Z}/3\mathbb{Z}$ or $\mathfrak{S}_3$, then we choose three conjugate elements $\alpha = (\alpha_1, \alpha_2, \alpha_3)$ of F so that $F = k(\alpha) = k(\alpha_1, \alpha_2, \alpha_3)$. Then we consider $f_\alpha(v)$. Let $x = w_\alpha$ be the point defined in (17.13), (17.14) for the above cases. Then $F_x(v) = f_\alpha(v)$ and so w_α corresponds to F.

We have chosen a point for each point in $\mathrm{H}^1(k, \mathfrak{S}_3)$. We now determine $G^\circ_{w_\alpha}$. In the following proposition, we consider the case (1) and w_α defined in (17.13).

Proposition 17.16. (1) *If $k(\alpha)/k$ is a quadratic extension, then*

$$G^\circ_{w_\alpha} \cong \mathrm{R}_{k(\alpha)/k}(\mathrm{GL}(1)) \times \mathrm{GL}(1)^2.$$

(2) *If $k(\alpha_1)/k$ is a cubic extension, then $G^\circ_{w_\alpha} \cong \mathrm{R}_{k(\alpha_1)/k}(\mathrm{GL}(1)) \times \mathrm{GL}(1)$.*

Proof. Suppose that $k(\alpha)/k$ is a quadratic extension. We denote the non-trivial element of $\mathrm{Gal}(k(\alpha)/k)$ by σ. We use Theorem 13.32 again. Let R be any k-algebra.

We use the notation $R(\alpha) = R \otimes_k k(\alpha)$. Consider elements of the form t in (17.2) where $t_{11}, \cdots, t_{23}, t_3 \in R(\alpha)^\times$ and

$$t_{11}t_{21}t_3 = t_{12}t_{22}t_3 = t_{13}t_{23}t_3 = 1. \tag{17.17}$$

Define

$$\bar{t} = g_\alpha t g_\alpha^{-1}. \tag{17.18}$$

Then $G^\circ_{w_\alpha\, R(\alpha)}$ consists of elements of the form $\bar{t}$.

Since $g_\alpha^\sigma = g_\alpha \tau_1$,

$$\begin{aligned} \bar{t}^\sigma &= g_\alpha^\sigma t^\sigma (g_\alpha^\sigma)^{-1} \\ &= g_\alpha \tau_1 t^\sigma \tau_1 g_\alpha^{-1} \\ &= (a_3(t_{12}^\sigma, t_{11}^\sigma, t_{13}^\sigma), a_3(t_{22}^\sigma, t_{21}^\sigma, t_{23}^\sigma), t_3^\sigma I_2). \end{aligned}$$

So $\bar{t}^\sigma = \bar{t}$ if and only if

$$t_{12} = t_{11}^\sigma,\ t_{22} = t_{21}^\sigma,\ t_{13}, t_{23}, t_3 \in R^\times.$$

Note that since $k \to k(\alpha)$ is faithfully flat, multiplying an element $r \in R$ induces a bijection $R \to R$ if and only if it induces a bijection $R(\alpha) \to R(\alpha)$. This implies that $R(\alpha)^\times \cap R = R^\times$.

The above argument implies that $G^\circ_{w_\alpha\, R}$ consists of elements of the form $\bar{t}$ where

$$t = (a_3(t_{11}, t_{11}^\sigma, t_{13}), t_3^{-1} a_3(t_{11}, t_{11}^\sigma, t_{13})^{-1}, t_3)$$

with $t_{11} \in R(\alpha)^\times,\ t_{13}, t_3 \in R^\times$. Therefore,

$$G^\circ_{w_\alpha\, R} \cong (\mathrm{R}_{k(\alpha)/k}(\mathrm{GL}(1)) \times \mathrm{GL}(1)^2)_R.$$

Since this holds for all R, this proves (1).

Suppose $k(\alpha_1)/k$ is a cubic extension. Let $\sigma = (123) \in \mathrm{Gal}(k(\alpha)/k)$. If $\mathrm{Gal}(k(\alpha)/k) \cong \mathfrak{S}_3$, then let $\nu = (23)$. Let R be any k-algebra. We use the notation $R(\alpha) = R \otimes_k k(\alpha)$, $R(\alpha_1) = R \otimes_k k(\alpha_1)$. Consider $t, \bar{t}$ as above with the condition (17.17).

Suppose $\mathrm{Gal}(k(\alpha)/k) \cong \mathfrak{S}_3$. Since $g_\alpha^\nu = g_\alpha \tau_2$,

$$\begin{aligned} \bar{t}^\nu &= g_\alpha^\nu t^\nu (g_\alpha^\nu)^{-1} \\ &= g_\alpha \tau_1 t^\nu \tau_1 g_\alpha^{-1} \\ &= (a_3(t_{11}^\nu, t_{13}^\nu, t_{12}^\nu), a_3(t_{21}^\nu, t_{23}^\nu, t_{22}^\nu), t_3^\nu I_2). \end{aligned}$$

So $\bar{t}^\nu = \bar{t}$ if and only if

$$t_{11}, t_{21} \in R(\alpha_1)^\times,\ t_{13} = t_{12}^\nu,\ t_{23} = t_{22}^\nu.$$

Since $\sigma = (23)(12)$,

$$g_\alpha^\sigma = (g_\alpha \tau_2)^{(12)} = g_\alpha^{(12)} \tau_2 = g_\alpha \tau_1 \tau_2.$$

This implies that

$$\begin{aligned} \bar{t}^\sigma &= g_\alpha^\sigma t^\sigma (g_\alpha^\sigma)^{-1} \\ &= g_\alpha \tau_1 \tau_2 t^\sigma (\tau_1 \tau_2)^{-1} g_\alpha^{-1} \\ &= (a_3(t_{13}^\sigma, t_{11}^\sigma, t_{12}^\sigma), a_3(t_{23}^\sigma, t_{21}^\sigma, t_{22}^\sigma), t_3^\sigma I_2). \end{aligned}$$

This implies that assuming $\bar{t}^{\nu} = \bar{t}$, $\bar{t}^{\sigma} = \bar{t}$ if and only if

$$t_{i2} = t_{i1}^{\sigma},\ t_{i3} = t_{i1}^{\sigma^2},\ \text{for } i = 1, 2,\ t_3 \in R^{\times}.$$

The above argument shows that $G^{\circ}_{w_\alpha\, R}$ consists of elements of the form $\bar{t}$ where

$$t = (a_3(t_{11}, t_{11}^{\sigma}, t_{11}^{\sigma}), t_3^{-1} a_3(t_{11}, t_{11}^{\sigma}, t_{11}^{\sigma^2})^{-1}, t_3)$$

with $t_{11} \in R(\alpha_1)^{\times},\ t_3 \in R^{\times}$. Therefore,

$$G^{\circ}_{w_\alpha\, R} \cong (\mathrm{R}_{k(\alpha_1)/k}(\mathrm{GL}(1)) \times \mathrm{GL}(1))_R.$$

Since this holds for all R, this proves (2) if $\mathrm{Gal}(k(\alpha)/k) \cong \mathfrak{S}_3$. The proof for the case $\mathrm{Gal}(k(\alpha)/k) \cong \mathbb{Z}/3\mathbb{Z}$ is similar. $\square$

Theorems 9.5, 9.6 imply that

$$\mathrm{H}^1(k, G_{w_\alpha}) = \{1\} \tag{17.19}$$

in the case (1).

In the following proposition, we consider the case (2) and w_α defined in (17.14).

Proposition 17.20. (1) *If $k(\alpha)/k$ is a quadratic extension, then*

$$G^{\circ}_{w_\alpha} \cong \{(g_1, g_2) \in \mathrm{R}_{k(\alpha)/k}(\mathrm{GL}(2)) \times \mathrm{GL}(2) \mid \det g_1 = \det g_2\}.$$

(2) *If $k(\alpha_1)/k$ is a cubic extension, then*

$$G^{\circ}_{w_\alpha} \cong \{g \in \mathrm{R}_{k(\alpha_1)/k}(\mathrm{GL}(2)) \mid \det g \in \mathrm{GL}(1)\}.$$

The proof of the above proposition is similar to that of Proposition 17.16 and is left to the reader.

In the situation of Proposition 17.20(1), we have an exact sequence

$$1 \longrightarrow \mathrm{R}_{k(\alpha)/k}(\mathrm{SL}(2)) \times \mathrm{SL}(2) \longrightarrow G^{\circ}_{w_\alpha} \longrightarrow \mathrm{GL}(1) \longrightarrow 1.$$

In the situation of Proposition 17.20(2), we have an exact sequence

$$1 \longrightarrow \mathrm{R}_{k(\alpha_1)/k}(\mathrm{SL}(2)) \longrightarrow G^{\circ}_{w_\alpha} \longrightarrow \mathrm{GL}(1) \longrightarrow 1.$$

So $\mathrm{H}^1(k, G^{\circ}_{w_\alpha}) = \{1\}$ as before. Let γ_V be the map defined in (12.3). By Proposition 13.20, this map may be identified with $\alpha_V : G_k \backslash V_k^{\mathrm{ss}} \to \mathfrak{Ex}_i$, which was defined after Definition 12.6.

Theorem 17.21. *The map α_V is bijective in both cases. Moreover, if $x \in V_k^{\mathrm{ss}}$, then $k(x)$ is generated by coordinates of points in* $\mathrm{Zero}(x)$.

Proof. The bijectivity of γ_V follows from Theorem 12.10, Propositions 17.3, 17.5, 17.10, and (17.11), (17.19). Therefore, α_V is bijective also. For points of the form w_α, $k(\alpha)$ is generated by coordinates of points in $\mathrm{Zero}(w_\alpha)$. If $g \in rg$ and $x = gw_\alpha$, then $k(x) = k(w_\alpha)$ and the fields generated by coordinates of points in $\mathrm{Zero}(x)$, $\mathrm{Zero}(w_\alpha)$ are the same. So the second part of the theorem follows. $\square$

Exercise 17.22. Prove Proposition 17.1

Exercise 17.23. Let $f(t) = t^3 + a_1t^2 + a_2t + a_3 \in k[t]$ be a polynomial with three distinct roots $\alpha = (\alpha_1, \alpha_2, \alpha_3)$. Define

$$x_\alpha = \left(I_3, \begin{pmatrix} 0 & -1 & 0 \\ 0 & 0 & -1 \\ a_3 & a_2 & a_1 \end{pmatrix} \right).$$

Find $g \in G_k$ such that $x_\alpha = gw_\alpha$ where w_α is given in (17.13).

18. Type (10)

In this section we consider the case (10) in the Sato-Kimura classification. There is a similarity between this case and the quintic case (the case (11) in the classification) which we discussed in section 16. This case was investigated extensively in [34], [22].

Throughout this section, we assume that $\mathrm{ch}\, k \neq 2, 3$. We shall prove that the rational orbit space $G_k \backslash V_k^{\mathrm{ss}}$ in this case is in bijective correspondence with that in Example 11.5. Recall that $G_k \backslash V_k^{\mathrm{ss}}$ in Example 11.5 is in bijective correspondence with k-forms of $\mathrm{PGL}(2)$. In the present case, in addition to parametrizing k-forms of $\mathrm{PGL}(2)$, we can naturally obtain the irreducible 5-dimensional representations of these k-forms and their invariant polynomials. We shall construct these invariant polynomials using the present case.

Let $W = \mathrm{Aff}^2$ be the space of two dimensional column vectors, and $\{e_1, e_2\}$ the standard basis for W. Consider the usual action of $\mathrm{GL}(2)$ on W. This induces an action of $\mathrm{GL}(2)$ on $\mathrm{Sym}^d W$ and $\mathrm{Sym}^d W^*$ for any d. We define new actions of $\mathrm{GL}(2)$ on $\mathrm{Sym}^2 W, \mathrm{Sym}^4 W$ by $g \cdot x = (\det g)^{-1} gx, (\det g)^{-2} gx$ where $g \cdot x$ is the new action and gx is the usual action. Note that scalar matrices act trivially and therefore, this defines an action of $\mathrm{PGL}(2)$ on $\mathrm{Sym}^2 W, \mathrm{Sym}^4 W$.

Let $V_1 = \mathrm{Sym}^4 W$, $V_2 = \mathrm{Sym}^2 W$, $V = \wedge^2 V_1 \otimes V_2$ and $G_1 = \mathrm{GL}(V_1) \cong \mathrm{GL}(5)$, $G_2 = \mathrm{GL}(V_2) \cong \mathrm{GL}(3)$, $G = G_1 \times G_2$. Then G acts on V in the usual manner. By the construction, there is a homomorphism $\mathrm{PGL}(2) \to G$.

Generally speaking, to understand a given prehomogeneous vector space (G, V), it helps to consider various G-equivariant maps from V^{ss} to other G-varieties. In the present case, we consider equivariant maps in the following manner.

$$
\begin{array}{ccccc}
V^{\mathrm{ss}} & \longrightarrow & V_1^* \otimes \mathrm{Sym}^2 V_2 & \longrightarrow & \wedge^5 V_1^* \otimes \wedge^5 \mathrm{Sym}^2 V_2 \cong \mathrm{Sym}^2 V_2^* \\
 & & \downarrow & & \\
 & & V_1^* \otimes \mathrm{Hom}(V_2, V_2) & \longrightarrow & \mathrm{Sym}^2 V_1^* \\
 & & \downarrow & & \\
 & & \mathrm{Sym}^3 V_1^* & &
\end{array}
\tag{18.1}
$$

Let W^* be the dual space of W with the dual basis $\{f_1, f_2\}$. We follow the normalization regarding $\mathrm{Sym}^d W$ and $\mathrm{Sym}^d W^*$, which we defined in section 15. Note that we shall only consider $\mathrm{Sym}^d W$ up to $d = 4$. Since we assumed that $\mathrm{ch}\, k \neq 2, 3$, $\mathrm{ch}\, k$ does not divide d and so we are justified to use the normalizations in section 15.

If $G \subset \mathrm{GL}(W)$ is a subgroup, G acts on W^* by $(gf)(v) = f(g^{-1}v)$ for $g \in G, f \in W^*$. Whenever we consider the dual space of a given representation we consider a similar action.

We shall proceed in the following order. (1) We first prove that $\mathrm{PGL}(2)$ fixes a particular point $w \in V_k$, and determine the stabilizer G_w. (2) Next we construct various equivariant maps. (3) Then we evaluate those equivariant maps at w and construct invariant polynomials on 5-dimensional representations of the stabilizers. (4) Finally we determine the orbit space $G_k \backslash V_k^{\mathrm{ss}}$.

We now find a point w fixed by $\mathrm{PGL}(2)$. By Schur's lemma, the homomorphism $\mathrm{PGL}(2) \to G$ is an imbedding. In fact,

$$\mathrm{Ker}(\mathrm{PGL}(2) \to G_1) = \{1\}.$$

So we regard $\mathrm{PGL}(2)$ as a subgroup of G. Note that by applying the argument of Schur's lemma to $k[\epsilon]/(\epsilon^2)$-valued points, we get the above statement scheme-theoretically. Let $\widetilde{T} = \mathrm{Ker}(G \to \mathrm{GL}(V))$. By Schur's lemma again,

$$\widetilde{T} = \{(tI_5, t^{-2}I_3) \mid t \in \mathrm{GL}(1)\} \cong \mathrm{GL}(1). \tag{18.2}$$

If $(tI_5, t^{-2}I_3) \in \mathrm{PGL}(2)$, it acts trivially on V_1, V_2. So $t = 1$. Therefore, $\mathrm{PGL}(2) \cap \widetilde{T} = \{1\}$. Note by considering the Lie algebras, this is true as schemes.

Let $l_1 = e_1^2, l_2 = e_1e_2, l_3 = e_2^2$ and $m_1 = e_1^4, \cdots, m_5 = e_2^4$. Then $\{l_1, l_2, l_3\}$, $\{m_1, \cdots, m_5\}$ are bases of V_2, V_1 respectively. Let $\{p_1, p_2, p_3\}$ be the dual basis of $\{l_1, l_2, l_3\}$.

We identify $\mathrm{Sym}^4 W^*$ with the space of homogeneous polynomials of degree four in two variables $v = {}^t\begin{pmatrix} v_1 & v_2 \end{pmatrix}$ (v corresponds to $v_1e_1 + v_2e_2$). We identify $a = a(v) = a_1v_1^4 + \cdots + a_5v_2^4$ with $(a_1, \cdots, a_5)$. The group $\mathrm{PGL}(2)$ acts on $\mathrm{Sym}^4 W^*$ also.

Let $\mathfrak{h}$ be the Lie algebra of $\mathrm{PGL}(2)$. Then $\mathfrak{h}$ is the Lie algebra of $\mathrm{SL}(2)$ also. Let

$$H_1 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},\ H_2 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},\ H_3 = \begin{pmatrix} 0 & 0 \\ -1 & 0 \end{pmatrix}$$

regarded as elements of $\mathfrak{h}$. They may be regarded as $k[\epsilon]/(\epsilon^2)$-valued points of $\mathrm{PGL}(2)$. If U is any representation of $\mathrm{PGL}(2)$, $H \in \mathfrak{h}$, and $v \in U$, then we use the notation Hv for the element in U such that

$$(1 + \epsilon H) \cdot v = v + \epsilon(Hv).$$

Let

$$\begin{aligned} A_1 &= \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 0 & 4 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix},\ A_1' = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix}, \\ A_2 &= \begin{pmatrix} 4 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -2 & 0 \\ 0 & 0 & 0 & 0 & -4 \end{pmatrix},\ A_2' = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -2 \end{pmatrix}, \\ A_3 &= \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 4 & 0 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix},\ A_3' = \begin{pmatrix} 0 & 0 & 0 \\ 2 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}. \end{aligned} \tag{18.3}$$

Then the actions of $\mathfrak{h}$ on V_1, V_2 are easy to describe and with respect to the bases $\{e_1, \cdots, e_5\}, \{l_1, l_2, l_3\}$, H_1, H_2, H_3 correspond to

$$(A_1, A_1'), (A_2, A_2'), -(A_3, A_3')$$

respectively.

Since the action of $g \in \mathrm{PGL}(2)$ on $a(v) \in \mathrm{Sym}^4 W^*$ is $(\det g)^2 a(g^{-1} \cdot v)$, the action of $H \in \mathfrak{h}$ on $a = a(v)$ is given by

$$a((1-\epsilon H)\cdot v) = a(v) + \epsilon (Ha)(v).$$

Then easy computations show that

$$\begin{aligned} H_1 a &= (0, -4a_1, -3a_2, -2a_3, -a_4), \\ H_2 a &= (-4a_1, -2a_2, 0, 2a_4, 4a_5), \\ H_3 a &= (a_2, 2a_3, 3a_4, 4a_5, 0). \end{aligned} \tag{18.4}$$

For $a = (a_1, \cdots, a_5), b = (b_1, \cdots, b_5)$, we define

$$Q(a,b) = a_1 b_5 - \frac{1}{4} a_2 b_4 + \frac{1}{6} a_3 b_3 - \frac{1}{4} a_4 b_2 + a_5 b_1. \tag{18.5}$$

Then by (11.6), Q is a non-degenerate symmetric bilinear form, invariant under the action of $\mathrm{PGL}(2)$. This implies that $Q(Ha, b)$ is an alternating form for any $H \in \mathfrak{h}$. We regard this alternating form as an element of $\wedge^2(\mathrm{Sym}^4 W^*)^* \cong \wedge^2 \mathrm{Sym}^4 W$. Consider the adjoint action of $\mathrm{PGL}(2)$ on $\mathfrak{h}$.

Lemma 18.6. *The map $H \to f_H(a,b) = Q(Ha,b)$ is a $\mathrm{PGL}(2)$-homomorphism from $\mathfrak{h}$ to $\wedge^2 \mathrm{Sym}^4 W$.*

Proof. Since the bilinear form Q is PGL(2)-invariant,

$$Q(gHg^{-1}a, b) = Q(Hg^{-1}, g^{-1}b).$$

The lemma follows. □

This defines an PGL(2)-homomorphism $\mathfrak{h} \to \wedge^2 V_1$. Regarding this homomorphism as an element of $\wedge^2 V_1 \otimes \mathfrak{h}^* \cong \wedge^2 V_1 \otimes V_2 = V$, we get a fixed point of V by the action of PGL(2). We compute this element explicitly.

Note that the linear map defined by

$$H_1 \to \frac{1}{2} v_2^2, \ H_2 \to v_1 v_2, \ H_3 \to \frac{1}{2} v_1^2.$$

is a PGL(2)-homomorphism.

By (18.4), (18.5),

$$\begin{aligned} Q(H_0 a, b) &= a_0 b_3 - \frac{1}{2} a_1 b_2 + \frac{1}{2} a_2 b_1 - a_3 b_0, \\ Q(H_1 a, b) &= -4 a_0 b_4 + \frac{1}{2} a_1 b_3 - \frac{1}{2} a_3 b_1 + 4 a_4 b_0, \\ Q(H_2 a, b) &= a_1 b_4 - \frac{1}{2} a_2 b_3 + \frac{1}{2} a_3 b_2 - a_4 b_1. \end{aligned}$$

Note that $\{e_1^2, 2e_1e_2, e_2^2\}$ is the dual basis of $\{v_1^2, v_1v_2, v_2^2\}$, and

$$(m_1, v_1^4)_4 = 1, \ (m_2, v_1^3 v_2)_4 = \frac{1}{4},$$

etc. We identify $\wedge^2 V_1$ with the space of alternating bilinear forms on V_1^* by assuming

$$m \wedge m'(a,b) = (m,a)_1 (m',b)_1 - (m,b)_1 (m',a)_1$$

for $m, m' \in V_1,\ a, b \in V_1^*$. So by the correspondence $H \to f_H$,

$$\begin{aligned} H_1 &\to 4m_1 \wedge m_4 - 12m_2 \wedge m_3, \\ H_2 &\to -4m_1 \wedge m_5 + 8m_2 \wedge m_4, \\ H_3 &\to 4m_2 \wedge m_5 - 12m_3 \wedge m_4. \end{aligned}$$

Since $\{H_1, H_2, H_3\}$ corresponds to $\{(1/2)v_2^2, v_1v_2, (1/2)v_1^2\}$ and $\{2l_3, 2l_2, 2l_1\}$ is its dual basis, this correspondence may be regarded as the element $8w$ where

$$\begin{aligned} w = {} & (m_1 \wedge m_4 - 3m_2 \wedge m_3) \otimes l_3 + (-m_1 \wedge m_5 + 2m_2 \wedge m_4) \otimes l_2 \\ & + (m_2 \wedge m_5 - 3m_3 \wedge m_4) \otimes l_1. \end{aligned}$$

These considerations show the following proposition.

Proposition 18.7. *The element $w \in V$ is fixed by* $\mathrm{PGL}(2)$.

We now compute $T(G_w)_e$.

Lemma 18.8. *Let A_1, A_1' etc. be as in (18.3). Then*

$$T(G_w)_e = \langle (A_1, A_1'), (A_2, A_2'), (A_3, A_3'), (I_5, -2I_3) \rangle$$

and so $\dim T(G_w)_e = 4$.

Proof. Using bases $\{e_1, \cdots, e_5\}$, $\{l_1, l_2, l_3\}$, we identify V with the space of 5×5 alternating matrices with entries in linear forms in three variables $v = (v_1, v_2, v_3)$. We regard v as a row vector. Let

$$w_1 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & -3 & 0 \\ 0 & 0 & 3 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \end{pmatrix}, \quad w_2 = \begin{pmatrix} 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & -2 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix},$$

$$w_3 = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & -3 & 0 & 0 \\ 0 & 3 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Then $w = v_1w_1 + v_2w_2 + v_3w_3$

Let $A = (a_{ij})$ be a 5×5 matrix, $B = (b_{ij})$ a 3×3 matrix, and $g(A, B) = (I_5 + \epsilon A, I_4 + \epsilon B)$ where $k[\epsilon]/(\epsilon^2)$ is the ring of dual numbers. Then as in (16.2), $g(A, B) \in T(G_w)_e$ if and only if the condition

$$Aw(v) + w(v)^t A + w(vB) = 0 \tag{18.9}$$

is satisfied.

If we express the left hand side of (18.9) as $v_1C_1 + v_2C_2 + v_3C_3$, then C_1, C_2, C_3 are as follows

$$
C_1 = \begin{pmatrix}
0 & -a_{15} & 3a_{14} & -3a_{13} & a_{12} \\
 & 0 & 3a_{24}+a_{35} & -3a_{23}+a_{45} & a_{22}+a_{55} \\
 & & 0 & -3a_{33}-3a_{44} & a_{32}-3a_{54} \\
 & * & & 0 & a_{42}+3a_{53} \\
 & & & & 0
\end{pmatrix}
+ \begin{pmatrix}
0 & 0 & 0 & b_{13} & -b_{12} \\
0 & 0 & -3b_{13} & 2b_{12} & b_{11} \\
0 & 3b_{13} & 0 & -3b_{11} & 0 \\
-b_{13} & -2b_{12} & 3b_{11} & 0 & 0 \\
b_{12} & -b_{11} & 0 & 0 & 0
\end{pmatrix},
$$

$$
C_2 = \begin{pmatrix}
0 & -2a_{14}-a_{25} & -a_{35} & 2a_{12}-a_{45} & -a_{11}-a_{55} \\
 & 0 & 2a_{34} & 2a_{22}+2a_{44} & -a_{21}+2a_{54} \\
 & & 0 & 2a_{32} & -a_{32} \\
 & * & & 0 & -a_{41}-2a_{52} \\
 & & & & 0
\end{pmatrix}
+ \begin{pmatrix}
0 & 0 & 0 & b_{23} & -b_{22} \\
0 & 0 & -3b_{23} & 2b_{22} & b_{21} \\
0 & 3b_{23} & 0 & -3b_{21} & 0 \\
-b_{23} & -2b_{22} & 3b_{21} & 0 & 0 \\
b_{22} & -b_{21} & 0 & 0 & 0
\end{pmatrix},
$$

$$
C_3 = \begin{pmatrix}
0 & 3a_{13}+a_{24} & -3a_{12}+a_{34} & a_{11}+a_{44} & a_{54} \\
 & 0 & -3a_{22}-3a_{33} & a_{21}-3a_{43} & -3a_{53} \\
 & & 0 & a_{31}+3a_{42} & 3a_{52} \\
 & * & & 0 & -a_{51} \\
 & & & & 0
\end{pmatrix}
+ \begin{pmatrix}
0 & 0 & 0 & b_{33} & -b_{32} \\
0 & 0 & -3b_{33} & 2b_{32} & b_{31} \\
0 & 3b_{33} & 0 & -3b_{31} & 0 \\
-b_{33} & -2b_{32} & 3b_{31} & 0 & 0 \\
b_{32} & -b_{31} & 0 & 0 & 0
\end{pmatrix}.
$$

So we get

$$
\begin{aligned}
& a_{15} = 3a_{14} = 3a_{13} - b_{13} = a_{12} - b_{12} = 3a_{24} + a_{35} - 3b_{13} = -3a_{23} + a_{45} + 2b_{12} = 0, \\
& a_{22} + a_{55} + b_{11} = 3a_{33} + 3a_{44} + 3b_{11} = a_{32} - 3a_{54} = a_{42} + 3a_{53} = 0, \\
& 2a_{14} + a_{25} = a_{35} = 2a_{12} - a_{45} + b_{23} = a_{11} + a_{55} + b_{22} = 2a_{34} - 3b_{23} = 0, \\
& 2a_{22} + 2a_{44} + 2b_{22} = -a_{21} + 2a_{54} + b_{21} = 2a_{32} - 3b_{21} = a_{31} = a_{41} + 2a_{52} = 0, \\
& 3a_{13} + a_{24} = -3a_{12} + a_{34} = a_{11} + a_{44} + b_{33} = a_{54} - b_{32} = 3a_{22} + 3a_{33} + 3b_{33} = 0, \\
& a_{21} - 3a_{43} + 2b_{32} = -3a_{53} + b_{31}a_{31} + 3a_{42} - 3b_{31} = 3a_{52} = a_{51} = 0.
\end{aligned}
$$

Since

$$(A_1, A_1'), (A_2, A_2'), (A_3, A_3'), (I_5, -2I_3) \in T(G_w)_e,$$

we assume that $b_{11} = b_{12} = b_{21} = b_{22} = 0$ and prove that $A = B = 0$.

It is easy to see that

$$a_{12} = a_{14} = a_{15} = a_{25} = a_{31} = a_{35} = a_{51} = a_{52} = 0.$$

By the 2nd equation in the 5th line, $a_{34} = 0$. By the 5th equation in the 3rd line, $b_{23} = 0$. By the 3rd equation in the 3rd line, $a_{45} = 0$. By the 6th equation in the 1st line, $a_{23} = 0$. By the 3rd equation in the 3rd line, $a_{45} = 0$. By the 3rd equation in the 2nd line, $a_{54} = 0$. By the 4th equation in the 5th line, $b_{32} = 0$. By the 2nd equation in the 4th line, $a_{21} = 0$. By the 5th equation in the 4rd line, $a_{41} = 0$. By the 1st equation in the 2nd line, the 2nd equation in the 2nd line, the 4th equation in the 3rd line, the 1st equation in the 4th line, the 3rd equation in the 5th line, and the 5th equation in the 5th line,

$$a_{11} = a_{22} = a_{33} = a_{44} = a_{55} = b_{33} = 0.$$

The rest follows from the remaining equations. □

Since $\dim T(G_w)_e = 4 = \dim G - \dim V$, Gw is open and G_w is smooth. We have shown that $\mathrm{PGL}(2) \subset G_w$. Obviously, $\widetilde{T} \subset G_w$. By Schur's lemma again, $\mathrm{PGL}(2) \cap \widetilde{T} = \{1\}$ set-theoretically. By Lemma 18.8 and (18.2), $T(\mathrm{PGL}(2))_e \cap T(\widetilde{T})_e = \{0\}$. Therefore, $\mathrm{PGL}(2) \cap \widetilde{T} = \{1\}$ as schemes. This implies that $\mathrm{PGL}(2) \times \widetilde{T} \subset G_w^\circ$.

Proposition 18.10. *The representation (G, V) is a regular prehomogeneous vector space. Moreover, we have $G_w = \mathrm{PGL}(2) \times \widetilde{T}$.*

Proof. Since

$$4 = \dim \mathrm{PGL}(2) \times \widetilde{T} \leq \dim G_w \leq \dim T(G_w)_e = 4,$$

$G_w^\circ = \mathrm{PGL}(2) \times \widetilde{T}$. Since $4 = \dim G - \dim V$, (G, V) is a regular prehomogeneous vector space.

We show that $G_w = G_w^\circ$. We may assume that k is algebraically closed. Suppose $g \in G_k/\widetilde{T}_k$. The identity component of the stabilizer of w in $G/\widetilde{T}$ is isomorphic to $\mathrm{PGL}(2)$. The conjugation by g induces an automorphism of $\mathrm{PGL}(2)$. Since all automorphisms of $\mathrm{PGL}(2)$ are inner, by changing g if necessary, we may assume that g commutes with elements of $\mathrm{PGL}(2)$. Since V_1, V_2 are irreducible representations, by Schur's lemma, g is represented by an element of the form $(t_1 I_5, t_2 I_3)$. This element fixes w if and only if $t_1^2 t_2 = 1$. So $g = 1$ (in $G/\widetilde{T}$). This proves the proposition. □

We now define equivariant maps we stated in (18.1). Define a linear map

$$\phi_1 : V \to \wedge^4 V_1 \otimes \mathrm{Sym}^2 V_2 \cong V_1^* \otimes \mathrm{Sym}^2 V_2$$

by the same formula as in (16.3). Then it has an alternative definition (16.6) also. Moreover, if we regard V_2 as the dual space of V_2^*, the statement of Lemma 16.5 holds. Regarding $\mathrm{Sym}^2 V_2$ as a subspace of $V_2 \otimes V_2$, we denote the element of $V_1^* \otimes V_2 \otimes V_2$ which corresponds to $\phi_1(x)$ by $\overline{\phi}_1(x)$.

Let $m_1^*, \cdots, m_5^* \in \wedge^4 V_1$ be elements such that $m_i \wedge m_j^* = \delta_{ij} m_1 \wedge \cdots \wedge m_5$ (δ_{ij} is Kronecker's delta). Explicitly,

$$m_1 = m_2 \wedge m_3 \wedge m_4 \wedge m_5,\ m_2 = -m_1 \wedge m_3 \wedge m_4 \wedge m_5,\ \text{etc.}$$

We identify $\wedge^4 V_1$ with the dual space of V_1 by the pairing

$$V_1 \times \wedge^4 V_1 \ni (a, b) \to a \wedge b$$

and by choosing $m_1 \wedge \cdots \wedge m_5$ as the basis element of $\wedge^5 V_1$. Then $\{m_1^*, \cdots, m_5^*\}$ may be regarded as the dual basis of $\{m_1, \cdots, m_5\}$.

Next we consider a linear map $\phi_2 : V_1^* \otimes \mathrm{Sym}^2 V_2 \to \wedge^5 \mathrm{Sym}^2 V_2 \cong \mathrm{Sym}^2 V_2^*$ defined by

$$V_1^* \otimes \mathrm{Sym}^2 V_2 \ni \sum_{i=1}^{5} m_i^* \otimes p_i \to p_1 \wedge \cdots \wedge p_5 \in \wedge^5 \mathrm{Sym}^2 V_2 \cong \mathrm{Sym}^2 V_2^*.$$

Note that ϕ_2 is the Castling transform which we discussed in section 10.

Definition 18.11. We define $\Phi_1 = \frac{1}{3^4} \phi_2 \circ \phi_1$.

Φ_1 is a map from V to $\mathrm{Sym}^2 V_2^*$. The proof of the following lemma is easy and is left to the reader.

Lemma 18.12. *We have* $\Phi_1(gx) = (\det g_1)^4 (\det g_2) g_2 \Phi_1(x)$.

For $x \in V$, let $\overline{\Phi}_1(x)(\alpha, \beta)$ be the symmetric bilinear form on V_2 associated with $\Phi_1(x)$. In other words,

$$\overline{\Phi}_1(x)(\alpha, \beta) = (1/2)(\Phi_1(x)(\alpha + \beta) - \Phi_1(x)(\alpha) - \Phi_1(x)(\beta))$$

for $\alpha, \beta \in V_2$.

We define a linear map $j_x : V_1^* \otimes V_2 \otimes V_2 \to \mathrm{Hom}(V_2, V_1^* \otimes V_2)$ by

$$j_x(a \otimes \alpha \otimes \beta)(\gamma) = \overline{\Phi}_1(x)(\alpha, \gamma) a \otimes \beta$$

for $a \in V_1^*,\ \alpha, \beta, \gamma \in V_2$. If $f \in \mathrm{Hom}(V_2, V_1^* \otimes V_2)$, we define $gf \in \mathrm{Hom}(V_2, V_1^* \otimes V_2)$ by

$$(gf)(\alpha) = gf(g_2^{-1}\alpha)$$

where we consider the action of g on the element $f(g_2^{-1}\alpha)$.

Lemma 18.13. *We have* $j_{gx}(g(a \otimes \alpha \otimes \beta)) = (\det g_1)^4 (\det g_2) g j_x(a \otimes \alpha \otimes \beta)$ *for all* $a \in V_1^*, \alpha, \beta \in V_2$.

Proof. Let $\gamma \in V_2$. Then by Lemma 18.12,

$$\begin{aligned}
j_{gx}(g(a \otimes \alpha \otimes \beta))(\gamma) &= \overline{\Phi}_1(gx)(g_2\alpha, \gamma) g_1 a \otimes g_2 \beta \\
&= (\det g_1)^4 (\det g_2)(g_2 \overline{\Phi}_1(x))(g_2\alpha, \gamma) g_1 a \otimes g_2 \beta \\
&= (\det g_1)^4 (\det g_2) \overline{\Phi}_1(x)(\alpha, g_2^{-1}\gamma) g_1 a \otimes g_2 \beta \\
&= (\det g_1)^4 (\det g_2) g(\overline{\Phi}_1(x)(\alpha, g_2^{-1}\gamma) a \otimes \beta) \\
&= (\det g_1)^4 (\det g_2) g(j_x(a \otimes \alpha \otimes \beta)(g_2^{-1}\gamma)) \\
&= (\det g_1)^4 (\det g_2)(g(j_x(a \otimes \alpha \otimes \beta)))(\gamma).
\end{aligned}$$

This proves the lemma. □

Definition 18.14. We define $\phi_3(x) = j_x(\overline{\phi}_1(x))$.

Apparently, ϕ_3 is a map from V to $\mathrm{Hom}(V_2, V_1^* \otimes V_2)$.

Lemma 18.15. *We have* $\phi_3(gx) = (\det g_1)^5(\det g_2)g\phi_3(x)$.

Proof.

$$\begin{aligned}\phi_3(gx) &= j_{gx}(\overline{\phi}_1(gx)) \\ &= \det g_1 j_{gx}(g\overline{\phi}_1(x)) \\ &= (\det g_1)^5(\det g_2)gj_x(\overline{\phi}_1(x)) \\ &= (\det g_1)^5(\det g_2)g\phi_3(x).\end{aligned}$$

□

By the basis $\{l_1, l_2, l_3\}$ for V_2, we may regard $\phi_3(x)$ as a 3×3 matrix with entries in V_1^*. Then the action of $g = (g_1, g_2) \in \mathrm{GL}(V_1) \times \mathrm{GL}(3)$ is obtained by considering $g_2\phi_3(x)g_2^{-1}$ and then applying g_1 entry-wise. Therefore,

$$\Phi_2(x) = \mathrm{tr}(\phi_3(x)^2) \in \mathrm{Sym}^2 V_1^*, \ F_x = \det \phi_3(x) \in \mathrm{Sym}^3 V_1^* \tag{18.16}$$

define maps $x \to \Phi_2(x), F_x$ from V to $\mathrm{Sym}^2 V_1^*, \mathrm{Sym}^3 V_1^*$ respectively.
The following lemma is an easy corollary of Lemma 18.13.

Lemma 18.17. *We have*
(1) $\Phi_2(gx) = (\det g_1)^{10}(\det g_2)^2 g_1 \Phi_2(x)$,
(2) $F_{gx}(a) = (\det g_1)^{15}(\det g_2)^3 F_x(g_1^{-1}a)$ *for all* $a \in V_1$.

We shall describe how to compute $\Phi_2(x), F_x$. Suppose

$$\overline{\phi}_1(x) = \sum_{i,j=1}^{3} a_{ij} \otimes l_i \otimes l_j, \ \overline{\Phi_1}(x) = \sum_{t,s=1}^{3} b_{ts} p_t \otimes p_s$$

with $a_{ij} \in V_1^*, \ b_{ts} \in k$ for all i, j, t, s and $a_{ij} = a_{ji}, \ b_{ts} = b_{st}$. We denote the matrices $(a_{ij}), (b_{ts})$ also by $\overline{\phi}_1(x), \overline{\Phi}_1(x)$. Let $\gamma = \sum_{s=1}^{3} \gamma_s l_s$. Then

$$\begin{aligned}\phi_3(x)(\gamma) &= j_x(\overline{\phi}_1(x))(\gamma) \\ &= \sum_{i,j,s=1}^{3} j_x(a_{ij} \otimes l_i \otimes l_j)(\gamma_s l_s) \\ &= \sum_{i,j,s=1}^{3} \overline{\Phi}_1(x)(l_i \otimes l_s) a_{ij}\gamma_s \otimes l_j \\ &= \sum_{i,j,s=1}^{3} a_{ij} b_{is}\gamma_s \otimes l_j \\ &= \sum_{i,j,s=1}^{3} a_{ji} b_{is}\gamma_s \otimes l_j.\end{aligned}$$

Note that $\sum_{i=1}^3 a_{ji}b_{is}$ is the (j,s)-entry of the matrix product $\overline{\phi}_1(x)\overline{\Phi}_1(x)$. So if we regard $\phi_3(x)$ as a 3×3 matrix with entries in V_1^*, we get the following relation

$$\phi_3(x) = \overline{\phi}_1(x)\overline{\Phi}_1(x).$$

Since this is a matrix representation of ϕ_3, one can easily compute $\Phi_2(x)$, F_x. We now evaluate the above equivariant maps at w. By the basis $\{e_1,\cdots,e_5\}$, we regard V as the space of 5×5 alternating matrices with entries in V_2. Then

$$w = \begin{pmatrix} 0 & 0 & 0 & l_3 & -l_2 \\ 0 & 0 & -3l_3 & 2l_2 & l_1 \\ 0 & 3l_3 & 0 & -3l_1 & 0 \\ -l_3 & -2l_2 & 3l_1 & 0 & 0 \\ l_2 & -l_1 & 0 & 0 & 0 \end{pmatrix}.$$

By the definition (16.4),

$$\begin{aligned} &\mathrm{Pfaff}_1(w) = -3l_1^2,\ \mathrm{Pfaff}_2(w) = -3l_1l_2,\ \mathrm{Pfaff}_3(w) = -2l_2^2 - l_1l_3, \\ &\mathrm{Pfaff}_4(w) = -3l_2l_3,\ \mathrm{Pfaff}_5(w) = -3l_3^2. \end{aligned}$$

Note that we are regarding them as elements of Sym^2V_2 and not of Sym^4W.

By the basis $\{l_1,l_2,l_3\}$, we regard $\overline{\phi}_1(w)$ as a 3×3 matrix with entries in V_1^* as before. Then

$$\overline{\phi}_1(w) = -\begin{pmatrix} 3m_1^* & \frac{3}{2}m_2^* & \frac{1}{2}m_3^* \\ \frac{3}{2}m_2^* & 2m_3^* & \frac{3}{2}m_4^* \\ \frac{1}{2}m_3^* & \frac{3}{2}m_4^* & 3m_5^* \end{pmatrix}.$$

Let

$$n_1 = l_1^2,\ n_2 = l_2^2,\ n_3 = l_3^2,\ n_4 = l_1l_2,\ n_5 = l_2l_3,\ n_6 = l_1l_3 \in \mathrm{Sym}^2V_2.$$

Then $\{n_1,\cdots,n_6\}$ is a basis of Sym^2V_2. Let $n_1^*,\cdots,n_6^*$ be elements of $\wedge^5\mathrm{Sym}^2V_2 \cong \mathrm{Sym}^2V_2^*$ such that $n_i\wedge n_j^* = \delta_{ij}n_1\wedge\cdots\wedge n_6$. Then

$$\begin{aligned} &\mathrm{Pfaff}_1(w)\wedge\mathrm{Pfaff}_2(w)\wedge\mathrm{Pfaff}_3(w)\wedge\mathrm{Pfaff}_4(w)\wedge\mathrm{Pfaff}_5(w) \\ &= (-3n_1)\wedge(-3n_4)\wedge(-2n_2-n_6)\wedge(-3n_5)\wedge(-3n_3) \\ &= -3^4 n_1\wedge n_4\wedge(2n_2+n_6)\wedge n_5\wedge n_3 \\ &= -3^4(2n_1\wedge n_4\wedge n_2\wedge n_5\wedge n_3 + n_1\wedge n_4\wedge n_6\wedge n_5\wedge n_3) \\ &= 3^4(n_2^* - 2n_6^*). \end{aligned}$$

Therefore,

$$\Phi_1(w) = n_2^* - 2n_6^*.$$

We identify $\mathrm{Sym}^2V_2^*$ with the dual space of Sym^2V_2. Then with respect to the basis $\{p_1,p_2,p_3\}$, n_2^*, n_6^* correspond to $p_2^2, 2p_1p_3$. Therefore, $\Phi_1(w) = p_2^2 - 4p_1p_3$. We regard $\overline{\Phi}_1(w)$ as a 3×3 matrix as in as before. Then

$$\overline{\Phi}_1(w) = \begin{pmatrix} 0 & 0 & -2 \\ 0 & 1 & 0 \\ -2 & 0 & 0 \end{pmatrix}. \qquad (18.18)$$

Therefore,

$$\phi_3(w) = \overline{\phi}_1(w)\overline{\Phi}_1(w) = \begin{pmatrix} m_3^* & -\frac{3}{2}m_2^* & 6m_1^* \\ 3m_4^* & -2m_3^* & 3m_2^* \\ 6m_5^* & -\frac{3}{2}m_4^* & m_3^* \end{pmatrix}.$$

So, we get the following proposition easily.

Proposition 18.19. *Let $a = a_1m_1 + \cdots + a_5m_5$. Then*

(1) $\Phi_2(w)(a) = (\mathrm{tr}(\phi_3(w)^2))(a) = 72(a_1a_5 - \frac{1}{4}a_2a_4 + \frac{1}{12}a_3^2)$,
(2) $F_w(a) = (\det \phi_3(w))(a) = 72a_1a_3a_5 + 9a_2a_3a_4 - 2a_3^3 - 27a_1a_4^2 - 27a_2^2a_5$.

If $g \in G_x$ then by Lemma 18.17, $\Phi_2(gx), F_{gx}$ are scalar multiples of $\Phi_2(x)$, F_x respectively. By these considerations, Φ_1, Φ_2 are non-trivial maps. By (18.18), the discriminant $\Delta_1(x)$ of $\Phi_1(x)$ is a non-zero polynomial. By Lemma (18.12), $\Delta_1(x)$ is a non-constant polynomial. Therefore, it is a relative invariant polynomial, and it is easy to see that its degree is 30. Since we have shown (G, V) is a regular prehomogeneous vector space, $V_{\bar{k}}^{\mathrm{ss}}$ is a single $G_{\bar{k}}$-orbit. Therefore, V^{ss} consists of points x such that $\Phi_1(x)$ is non-degenerate.

Since $\Phi_2(w)$ is non-degenerate, $\Phi_2(x)$ is non-degenerate for all $x \in V^{\mathrm{ss}}$.

We finally determine the orbit space $G_k \backslash V_k^{\mathrm{ss}}$.

Proposition 18.20. *The map $\Phi_1 : V \to V_3 = \mathrm{Sym}^2 V_2^*$ induces a bijection $G_k \backslash V_k^{\mathrm{ss}} \cong \mathrm{GL}(1)_k \times \mathrm{GL}(3)_k \backslash V_{3\,k}^{\mathrm{ss}}$.*

Proof. Let $H = \mathrm{SL}(5) \times \mathrm{SL}(3)$. Note that $G_w \subset H$. Let $c \in \mathrm{H}^1(k, G_w)$. Then c becomes trivial in $\mathrm{H}^1(k, H)$ also. Let $g = (g_1, g_2) \in H_{k^{\mathrm{sep}}}$ be the element such that c is represented by $(g^{-1}g^{\sigma})_{\sigma \in \mathrm{Gal}(k^{\mathrm{sep}}/k)}$. Then the orbit in V_k^{ss} corresponding to c is gw. By Lemma (18.12), $\Phi_1(gw) = g_2\Phi_1(w)$.

Since $\mathrm{H}^1(k, G_w) \cong \mathrm{H}^1(k, \mathrm{PGL}(2))$ and the projection of $\mathrm{PGL}(2)$ to G_2 is an isomorphism to its image,

$$\mathrm{H}^1(k, G_w) \ni (g^{-1}g^{\sigma})_{\sigma \in \mathrm{Gal}(k^{\mathrm{sep}}/k)} \to (g_2^{-1}g_2^{\sigma})_{\sigma \in \mathrm{Gal}(k^{\mathrm{sep}}/k)} \in \mathrm{H}^1(k, \mathrm{PGL}(2))$$

is a bijection. Since $(\mathrm{GL}(1)_k \times \mathrm{GL}(3)_k) \backslash V_{3\,k}^{\mathrm{ss}} \cong \mathrm{H}^1(k, \mathrm{PGL}(2))$, this proves the proposition. □

Exercise 18.21. Prove that there exists a relative invariant polynomial of degree 15 in the following manner. Since we may use Proposition 14.4, we assume that $k = \mathbb{Q}$ in the following.

(1) Let $\phi_4 : V \to \wedge^3(\wedge^2 V_1)$ be the map defined by

$$\phi_4(x_1 \otimes l_1 + x_2 \otimes l_2 + x_3 \otimes l_3) = x_1 \wedge x_2 \wedge x_3$$

for $x_1, x_2, x_3 \in \wedge^2 V_1$. Sow that ϕ_4 is G-equivariant. Note that G_1 acts naturally on $\wedge^3(\wedge^2 V_1)$ and G_2 acts on it by multiplication by the determinant.

(2) Let

$$D : \wedge^3 (\wedge^2 V_1) \to \wedge^2(\wedge^2 V_1) \otimes (\wedge^2 V_1),$$
$$S : \wedge^2 (\wedge^2 V_1) \to \wedge^2 V_1 \otimes \mathrm{Sym}^2 V_1$$

be the equivariant maps defined in (15.1), (15.3). Let $\Phi_3 : V \to V_1^* \otimes \mathrm{Sym}^2 V_1$ be the composition of the following maps.

$$\begin{aligned} V &\xrightarrow{\phi} \wedge^3(\wedge^2 V_1) \xrightarrow{D} \wedge^2(\wedge^2 V_1) \otimes \wedge^2 V_1 \\ &\xrightarrow{S \otimes \mathrm{id}_{\wedge^2 V_1}} \wedge^2 V_1 \otimes \mathrm{Sym}^2 V_1 \otimes \wedge^2 V_1 \longrightarrow \wedge^4 V_1 \otimes \mathrm{Sym}^2 V_1 \\ &\longrightarrow V_1^* \otimes \mathrm{Sym}^2 V_1 \end{aligned}$$

Note that we identify $\wedge^4 V_1$ with V_1^* so that if $a \in \wedge^4 V_1, b \in V_1$, and $a \wedge b = f(a)(b) m_1 \wedge \cdots \wedge m_5$, then $f(a) \in V_1^*$ is the corresponding element. Express $\Phi_3((g_1, g_2)x)$ in terms of $\Phi_3(x)$.

(3) For $x \in V$, regard $\Phi_3(x) \in V_1^* \otimes V_1 \otimes V_1 \cong \mathrm{Hom}(V_1, V_1) \otimes V_1$. Note that $ab \in \mathrm{Sym}^2 V_1$ corresponds to $(1/2)(a \otimes b + b \otimes a) \in V_1 \otimes V_1$. Let

$$\Phi_4(x) = \mathrm{tr}(\Phi_3(x) \circ \Phi_3(x) \circ \Phi_3(x)) \in \mathrm{Sym}^3 V_1.$$

There is a natural pairing (,) between $\mathrm{Sym}^3 V_1$ and $\mathrm{Sym}^3 V_1^*$ (see section 15). Let $\Delta_2(x) = (\Phi_4(x), F_x)$ where F_x is defined in (18.16). Express $\Delta_2((g_1, g_2)x)$ in terms of $\Delta_2(x)$.

(4) Find $\Delta_2(w)$ assuming $k = \mathbb{Q}$, and show that $\Delta_2(x)$ is a relative invariant polynomial of degree 45.

19. Type (5)

In this section we consider the case (5) in the Sato-Kimura classification following [23] and [30]. We assume that $\operatorname{ch} k \neq 2$ in this section. Let $G = \mathrm{GL}(6)$, $W = \mathrm{Aff}^6$, and $V = \wedge^3 W$. We denote the standard basis for W by $\{e_1, \cdots, e_6\}$. We use the notation $e_{i_1 \cdots i_k} = e_{i_1} \wedge \cdots \wedge e_{i_k}$.

Let

$$w = e_{123} + e_{456}$$

Proposition 19.1. *The representation (G, V) is a regular prehomogeneous vector space. Moreover, $G_w^\circ \cong \mathrm{SL}(3) \times \mathrm{SL}(3)$.*

Proof. By Exercise 4.24,

$$T(G_w)_e = \left\{ \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} \middle| \operatorname{tr}(A) = \operatorname{tr}(B) = 0 \right\}.$$

It is easy to see that elements of the form $\left(\begin{smallmatrix} A & 0 \\ 0 & B \end{smallmatrix}\right)$, where $A, B \in \mathrm{SL}(3)$, belong to G_w. Therefore, $\mathrm{SL}(3) \times \mathrm{SL}(3) \subset G_w^\circ$.

Since

$$16 = \dim \mathrm{SL}(3) \times \mathrm{SL}(3) \leq \dim G_w \leq \dim T(G_w) = 16,$$

G_w is smooth over k and $G_w^\circ \cong \mathrm{SL}(3) \times \mathrm{SL}(3)$. Since $16 = \dim G - \dim V$, Gw is open. Moreover, G_w is reductive and so (G, V) is a regular prehomogeneous vector space. $\square$

Let $D : \wedge^3 W \to \wedge^2 W \otimes W$ be the equivariant map defined in (15.1). We choose an isomorphism $\phi : \wedge^6 W \otimes W \to W$ so that $e_{123456} \otimes v$ maps to v. For $x \in V_k$, we define $S_x : W \to W$ by

$$S_x(v) = \phi(v \wedge D(x) \wedge x).$$

We define an action of G on $\mathrm{Hom}(W, W)$ by $(gh)(v) = g(h(g^{-1}v))$.

Proposition 19.2. *We have $S_{gx} = \det g(gS_x)$ for all $g \in G$ and $x \in V$.*

Proof.

$$\begin{aligned} S_{gx}(v) &= \phi(v \wedge D(gx) \wedge gx) \\ &= \phi(g(g^{-1}v \wedge D(x) \wedge x)) \\ &= \det g g(\phi(g^{-1}v \wedge D(x) \wedge x)) \\ &= \det g(gS_x)(v). \end{aligned}$$

$\square$

Lemma 19.3. *We have $S_w(e_i) = e_i$ for $i = 1, 2, 3$ and $S_w(e_i) = -e_i$ for $i = 4, 5, 6$.*

Proof.

$$D(w) = e_{23} \otimes e_1 - e_{13} \otimes e_2 + e_{12} \otimes e_3 + e_{56} \otimes e_4 - e_{46} \otimes e_5 + e_{45} \otimes e_6.$$

So

$$\begin{aligned} D(w) \wedge w = {} & e_{23456} \otimes e_1 - e_{13456} \otimes e_2 + e_{12456} \otimes e_3 \\ & + e_{56123} \otimes e_4 - e_{46123} \otimes e_5 + e_{45123} \otimes e_6. \end{aligned}$$

Therefore, $S_w(e_1) = e_1$. Since $e_4 \wedge e_{56123} = -e_{123456}$, $S_w(e_4) = -e_4$. Other cases are similar. □

Let

$$\tau = \begin{pmatrix} 0 & I_3 \\ I_3 & 0 \end{pmatrix}.$$

Clearly, $\tau \in G_w$.

Proposition 19.4. (1) *There exists a relative invariant polynomial $\Delta(x)$ such that $S_x^2 = \Delta(x)\mathrm{id}_W$.*

(2) *The assumption 12.1 is satisfied with $i = 2$, and G_w/G_w° is generated by τ.*

Proof. We first prove (1). We may assume that $k = \bar{k}$. Let

$$E_{w\,1} = \langle e_1, e_2, e_3 \rangle,\ E_{w\,2} = \langle e_4, e_5, e_6 \rangle.$$

Both of these are 3-dimensional subspaces of W. Then S_w has eigenvalues ± 1 and E_{w1}, E_{w2} are the eigenspaces. Note that $1 \neq -1$ because we assumed that $\mathrm{ch}\, k \neq 2$. Let $g \in G_k$. Since $S_{gw} = \det g(gS_w)$, S_{gw} has eigenvalues $\pm \det g$ with eigenspaces $gE_{w\,1}, gE_{w\,2}$. So if $x \in Gw$, then S_x^2 is a scalar matrix. Since this holds for $x \in Gw \subset V$ which is open in V, S_x^2 must be a scalar matrix, say $\Delta(x)\,\mathrm{id}_W$, for all $x \in V$.

By Proposition 19.2,

$$S_{gx}^2 = (\det g)^2 S_x^2.$$

So $\Delta(gx) = (\det g)^2 \Delta(x)$. Since $\Delta(w) = 1 \neq 0$, $\Delta(x)$ is a relative invariant polynomial. This proves (1).

We now consider (2). We still assume that $k = \bar{k}$. If $g \in G_{w\,k}$, then

$$\{gE_{w\,1}, gE_{w\,2}\} = \{E_{w\,1}, E_{w\,2}\}.$$

So by applying τ if necessary, we may assume that $gE_{w\,i} = E_{w\,i}$ for $i = 1, 2$. Therefore, g must be in the form

$$g = \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix},$$

where $A, B \in \mathrm{GL}(3)$. Since this element fixes w, A, B must belong to $\mathrm{SL}(3)$. □

Let γ_V be the map defined in (12.3). Since we are going to use Theorem 12.10, we shall choose a point in the fiber of γ_V at each cohomology class in $\mathrm{H}^1(k, \mathfrak{S}_2) \cong \mathfrak{Ex}_2$.

If $F = k$, we choose w as a representative of the corresponding orbit. Let F/k be a quadratic extension generated by a pair of conjugate elements $\alpha = (\alpha_1, \alpha_2)$. Suppose α_1, α_2 are the roots of the equation $t^2 + a_1 t + a_2 = 0$ where $a_1, a_2 \in k$. We define $w_\alpha = g_\alpha w$ where

$$g_\alpha = \begin{pmatrix} I_3 & I_3 \\ \alpha_1 I_3 & \alpha_2 I_3 \end{pmatrix}.$$

Suppose $\sigma \in \mathrm{Gal}(k(\alpha)/k)$ is the non-trivial element. It is easy to see that $g_\alpha^\sigma = g_\alpha \tau$. This implies that $(g_\alpha w)^\sigma = g_\alpha \tau w = g_\alpha w$. So $w_\alpha \in V_k^{\mathrm{ss}}$ corresponds to the natural homomorphism $\mathrm{Gal}(k^{\mathrm{sep}}/k) \to \mathrm{Gal}(F/k)$. Easy computations show that

$$\begin{aligned} w_\alpha = {} & 2e_{123} - a_1(e_{126} - e_{135} + e_{234}) \\ & + (a_1^2 - 2a_2)(e_{156} - e_{246} + e_{345}) + (-a_1^3 + 3a_1 a_2)e_{456}. \end{aligned}$$

We now determine $G^\circ_{w_\alpha}$.

Proposition 19.5. *We have*

$$\begin{aligned} G^\circ_{w_\alpha} &= g_\alpha \left\{ d(A, A^\sigma) \mid A \in \mathrm{SL}(3)_{k(\alpha)} \right\} g_\alpha^{-1} \\ &\cong \mathrm{R}_{k(\alpha)/k}(\mathrm{SL}(3)). \end{aligned}$$

Proof. Let R be any k-algebra. We define $R(\alpha) = R \otimes k(\alpha)$. Then

$$G^\circ_{w_\alpha R} = \{g \in G^\circ_{w_\alpha R(\alpha)} \mid g^\sigma = g\}.$$

Over $R(\alpha)$, we can express elements of $G^\circ_{w_\alpha R}$ as

$$g_\alpha d(A, B) g_\alpha^{-1},$$

where $A, B \in \mathrm{SL}(3)_{R(\alpha)}$. The above element belongs to $G^\circ_{w_\alpha R}$ if and only if

$$\begin{aligned} g_\alpha d(A, B) g_\alpha^{-1} &= g_\alpha^\sigma d(A^\sigma, B^\sigma)(g_\alpha^\sigma)^{-1} \\ &= g_\alpha \tau d(A^\sigma, B^\sigma) \tau g_\alpha^{-1} \\ &= g_\alpha d(B^\sigma, A^\sigma) g_\alpha^{-1}. \end{aligned}$$

This condition is satisfied if and only if $B = A^\sigma$. This proves the proposition. □

Theorem 19.6. *The map γ_V is bijective. Moreover, if $x \in V_k^{\mathrm{ss}}$, then $k(x)$ is generated by eigenvalues of S_x.*

Proof. The first part of the theorem follows from Theorems 9.5, 9.6, Propositions 19.1, 19.5

For the second part of the theorem, we can use a similar argument as before, and we only have to show it for points of the form $x = w_\alpha$. By Proposition 19.2, eigenvalues of S_x are $\pm(\det g_\alpha) = \pm(\alpha_2 - \alpha_1)^3$. Since $\mathrm{ch}\, k \neq 2$, they generate $k(\alpha)$. □

20. Type (6)

In this section we consider the case (6) in the Sato-Kimura classification following [30].

Since this case is closely related to octonion algebras, we briefly recall the Cayley–Dickson process following [7, pp. 101–110]. We assume that $\mathrm{ch}\, k \neq 2, 3$. Note that even though [7] assumes $k = \mathbb{R}$, the argument for the Cayley–Dickson process works as long as $\mathrm{ch}\, k \neq 2, 3$. Octonian algebras are often referred to as Cayley algebras also.

Definition 20.1. A *normed k-algebra* is a not necessarily associative finite dimensional k-algebra A with multiplicative unit 1, equipped with a non-degenerate symmetric bilinear form $\langle x, y\rangle$ for $x, y \in A$ such that the associated square norm $\|x\| = \langle x, x\rangle$ satisfies the multiplicative property

$$\|xy\| = \|x\|\|y\|.$$

If A is a normed k-algebra, then we denote the span of 1 by $\mathrm{Re}(A)$ and its orthogonal complement $\{x \in A \mid \langle 1, x\rangle = 0\}$ by $\mathrm{Im}(A)$. Any $x \in A$ has a unique decomposition $x = x_1 + x_2$ with $x_1 \in \mathrm{Re}(A), x_2 \in \mathrm{Im}(A)$. We denote $\mathrm{Re}(x) = x_1, \mathrm{Im}(x) = x_2$. We define the conjugation by $\bar{x} = x_1 - x_2$. So $\mathrm{Re}(x) = \frac{1}{2}(x + \bar{x})$.

Given a normed k-algebra A, we make two new normed k-algebras $A(\pm)$ as follows. As a vector space,

$$A(\pm) = A \oplus A.$$

We define the multiplication and the norm by

$$\begin{aligned} &(a, b)(c, d) = (ac \mp \bar{d}b, da + b\bar{c}),\\ &\|(a, b)\| = \|a\| \pm \|b\|. \end{aligned}$$

Then we define

$$\langle (a, b), (c, d)\rangle = \frac{1}{2}(\|(a, b) + (c, d)\| - \|(a, b)\| - \|(c, d)\|).$$

We use the notation $a + b\eta$ for (a, b). Note that if k contains $\sqrt{-1}$, $\eta \to \sqrt{-1}\eta$ induces an isomorphism $A(+) \to A(-)$.

For a normed k-algebra A, we define $[x, y, z] = (xy)z - x(yz)$ for $x, y, z \in A$. This is called the associator. If the associator is alternating, A is called an alternative algebra. It is known that if A is commutative, $A(\pm)$ is associative, and if A is associative, $A(\pm)$ is alternative. It is known that the norm of $A(\pm)$ is compatible with the product if and only if A is associative. The above process is called the Cayley–Dickson process. It is easy to see that

$$\mathrm{Im}(a + b\eta) = \mathrm{Im}(a) + b\eta,\ \overline{a + b\eta} = \bar{a} - b\eta.$$

The following lemma is proved in [7].

Lemma 20.2. *We have*

(1) $\overline{xy} = \bar{y}\bar{x}$,
(2) $\langle x, y\rangle = \mathrm{Re}(x\bar{y})$,
(3) $\|x\| = x\bar{x}$.

If A, B are normed k-algebras, a homomorphism $\phi : A \to B$ is a k-linear map such that $\phi(1) = 1$, $\phi(xy) = \phi(x)\phi(y)$, and $\|\phi(x)\| = \|x\|$. The third condition implies $\langle \phi(x), \phi(y) \rangle = \langle x, y \rangle$. So $\phi(\mathrm{Im}(A)) \subset \mathrm{Im}(B)$. Suppose $x, y \in \mathrm{Im}(A)$. Then $\langle x, y \rangle = \mathrm{Re}(x\bar{y}) = -\mathrm{Re}(xy)$. So

$$\begin{aligned} -\mathrm{Re}(\phi(x)\phi(y)) &= \langle \phi(x), \phi(y) \rangle = \langle x, y \rangle = -\mathrm{Re}(xy), \\ \phi(\mathrm{Im}(xy)) &= \phi(xy - \mathrm{Re}(xy)) = \phi(x)\phi(y) - \mathrm{Re}(xy) \\ &= \phi(x)\phi(y) - \mathrm{Re}(\phi(x)\phi(y)) = \mathrm{Im}(\phi(x)\phi(y)). \end{aligned}$$

Conversely, ϕ is a homomorphism if the above conditions are satisfied. So we have proved the following proposition.

Proposition 20.3. *A k-linear map $\phi : A \to B$ is a homomorphism if and only if*

$$\phi(1) = 1,\ \phi(\mathrm{Im}(xy)) = \mathrm{Im}(\phi(x)\phi(y)),\ \langle \phi(x), \phi(y) \rangle = \langle x, y \rangle$$

for all $x, y \in \mathrm{Im}(A)$.

It is easy to see that

$$\begin{aligned} k(+) &\cong \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \middle| a, b \in k \right\}, \\ k(+)(-) &\cong \mathrm{M}(2,2)_k. \end{aligned}$$

For $k(+)$, $\eta = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, and the conjugation is

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \to \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

For $k(+)(-)$, $\eta = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, and the conjugation is

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \to \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

Therefore, $\mathrm{Re}(x) = \frac{1}{2}\mathrm{tr}(x)$ in both cases and the norm is the determinant.

We define $\mathbb{H} = k(+)(+)$, $\mathbb{O} = \mathbb{H}(+)$, and $\widetilde{\mathbb{O}} = \mathrm{M}(2,2)(+)$. The normed k-algebra $\mathbb{O}$ is called the non-split octonion algebra (if k does not contain $\sqrt{-1}$), and $\widetilde{\mathbb{O}}$ is called the split octonion algebra.

We consider properties of the split octonion algebra $\widetilde{\mathbb{O}}$. Let

$$C(x, y, z) = \langle x, yz \rangle$$

for $x, y, z \in \widetilde{\mathbb{O}}$.

Lemma 20.4. *If $g \in \mathrm{Aut}\,(\widetilde{\mathbb{O}})$ then $C(gx, gy, gz) = C(x, y, z)$ for all x, y, z.*

Proof. Since g preserves the product and the norm,

$$C(gx, gy, gz) = \langle gx, (gy)(gz) \rangle = \langle gx, g(yz) \rangle = \langle x, yz \rangle = C(x, y, z).$$

□

Suppose $x = x_1 + x_2\eta$, $y = y_1 + y_2\eta$, and $z = z_1 + z_2\eta$.

Lemma 20.5. *We have*

$$C(x, y, z) = \frac{1}{2}\,\mathrm{tr}(x_1(\bar{z}_1\bar{y}_1 - \bar{y}_2 z_2) + (\bar{y}_1\bar{z}_2 + z_1\bar{y}_2)x_2).$$

Proof. Since $yz = y_1z_1 - \bar{z}_2y_2 + (z_2y_1 + y_2\bar{z}_1)\eta$,

$$\begin{aligned}\overline{yz} &= \bar{z}_1\bar{y}_1 - \bar{y}_2z_2 - (z_2y_1 + y_2\bar{z}_1)\eta,\\ x(\overline{yz}) &= x_1(\bar{z}_1\bar{y}_1 - \bar{y}_2z_2) + (\bar{y}_1\bar{z}_2 + z_1\bar{y}_2)x_2\\ &\quad + (-(z_2y_1 + y_2\bar{z}_1)x_1 + x_2(y_1z_1 - \bar{z}_2y_2))\eta.\end{aligned}$$

Therefore,

$$\begin{aligned}C(x,y,z) &= \mathrm{Re}(x(\overline{yz}))\\ &= \mathrm{Re}(x_1(\bar{z}_1\bar{y}_1 - \bar{y}_2z_2) + (\bar{y}_1\bar{z}_2 + z_1\bar{y}_2)x_2)\\ &= \frac{1}{2}\,\mathrm{tr}(x_1(\bar{z}_1\bar{y}_1 - \bar{y}_2z_2) + (\bar{y}_1\bar{z}_2 + z_1\bar{y}_2)x_2).\end{aligned}$$

□

Note that $\mathrm{tr}(x) = \mathrm{tr}(\bar{x})$ for $x \in \mathrm{M}(2,2)$. Also if $x,y,z \in \mathrm{Im}(\widetilde{\mathbb{O}})$, $x_1 + \bar{x}_1 = y_1 + \bar{y}_1 = z_1 + \bar{z}_1 = 0$. Therefore, the above lemma and a straightforward argument shows that $C(x,y,z)$ is an element of $\wedge^3\mathrm{Im}(\widetilde{\mathbb{O}})^*$ (see (6.60) [7, p. 113] also).

Let E_{ij} be the 2×2 matrix whose (i,j)-entry is 1 and other entries are zero. Let

$$\begin{aligned}&f_1 = \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix},\ f_2 = E_{12},\ f_3 = E_{11}\eta,\ f_4 = -E_{21}\eta,\\ &f_5 = -E_{21},\ f_6 = E_{22}\eta,\ f_7 = E_{12}\eta.\end{aligned}$$

Then $\{f_1,\cdots,f_7\}$ is a basis for $\mathrm{Im}(\widetilde{\mathbb{O}})$. Let $e_1,\cdots,e_7$ be the dual basis. Straightforward computations (35 computations for (2)) using the above lemma shows the following proposition and the proof is left to the reader.

Proposition 20.6. (1) *Suppose*

$$x = \sum_{i=1}^{7} x_if_i = \begin{pmatrix}x_1 & x_2\\ -x_5 & -x_1\end{pmatrix} + \begin{pmatrix}x_3 & x_7\\ -x_4 & x_6\end{pmatrix}\eta.$$

Then $\|x\| = -x_1^2 + x_2x_5 + x_3x_6 + x_4x_7$.

(2) *We have* $C = \frac{1}{2}(e_{234} + e_{567} + e_{125} + e_{136} + e_{147})$.

We now assume $\mathrm{ch}\,k \neq 3$ (allowing $\mathrm{ch}\,k = 2$). Let $W = \mathrm{Im}(\widetilde{\mathbb{O}})^*$. We choose the above basis $\{e_1,\cdots,e_7\}$. Let $G = \mathrm{GL}(1)\times\mathrm{GL}(W)$ and $V = \wedge^3 W$. The GL(1)-factor acts by the usual multiplication. We need this factor for number theoretic reasons unlike the case in section 19.

Let

$$w = e_{234} + e_{567} + e_{125} + e_{136} + e_{147}.$$

We shall show that Gw is open and G_w is reductive.

Let

$$
(20.7) \qquad A(a,\cdots,f,X) = \begin{pmatrix} 0 & 2d & 2e & 2f & 2a & 2b & 2c \\ a & & & & 0 & f & -e \\ b & & X & & -f & 0 & d \\ c & & & & e & -d & 0 \\ d & 0 & -c & b & & & \\ e & c & 0 & -a & & -{}^tX & \\ f & -b & a & 0 & & & \end{pmatrix},
$$

where $a,\cdots,f \in k,\ X \in \mathrm{SL}(3)_k$. Define

$$
\begin{aligned}
L_1 &= \{(0, A(a,\cdots,f,X)) \mid a,\cdots,f \in k,\ \mathrm{Tr}(X)=0\}, \\
L_2 &= \{(-3t, tI_7) \mid t \in k\}.
\end{aligned}
$$

Define

$$
\widetilde{T} = \{(t^{-3}, tI_7) \mid t \in \mathrm{GL}(1)\} \cong \mathrm{GL}(1).
$$

Obviously, $\widetilde{T} \subset \mathrm{Ker}(G \to \mathrm{GL}(V))$.

Lemma 20.8. *We have* $T(G_w)_e = L_1 \oplus L_2$ *and so* $\dim T(G_w) = 15$.

Proof. Let $A = (a_{ij})$ be a 7×7 matrix. Let $k[\epsilon]/(\epsilon^2)$ be the ring of dual numbers as before. Straightforward computations show that elements of the $(I_7 + \epsilon A(a,\cdots,f,X))$ fix the points w. Since L_2 is the Lie algebra of $\widetilde{T}$, it fixes w. So it is enough to show that if $I_7 + \epsilon A$ fixes and

$$
a_{21} = \cdots = a_{71} = a_{22} = a_{23} = a_{24} = a_{32} = a_{33} = a_{34} = a_{42} = a_{43} = 0,
$$

then $A = 0$.

By $I_7 + \epsilon A$,

$$
\begin{aligned}
&e_1 \to e_1 + \epsilon a_{11} e_1, \\
&e_2 \to e_2 + \epsilon(a_{12}e_1 + a_{52}e_5 + a_{62}e_6 + e_{72}e_7), \\
&e_3 \to e_3 + \epsilon(a_{13}e_1 + a_{53}e_5 + a_{63}e_6 + e_{73}e_7), \\
&e_4 \to e_4 + \epsilon(a_{14}e_1 + a_{44}e_4 + a_{54}e_5 + a_{64}e_6 + e_{74}e_7), \\
&e_5 \to e_5 + \epsilon(a_{15}e_1 + a_{25}e_2 + a_{35}e_3 + a_{45}e_4 + a_{55}e_5 + a_{65}e_6 + e_{75}e_7), \\
&e_6 \to e_6 + \epsilon(a_{16}e_1 + a_{26}e_2 + a_{36}e_3 + a_{46}e_4 + a_{56}e_5 + a_{66}e_6 + e_{76}e_7), \\
&e_7 \to e_7 + \epsilon(a_{17}e_1 + a_{27}e_2 + a_{37}e_3 + a_{47}e_4 + a_{57}e_5 + a_{67}e_6 + e_{77}e_7).
\end{aligned}
$$

So

$$\begin{aligned}(I_7+\epsilon A)w = w &+ (a_{14}-a_{26}+a_{35})e_{123} + (-a_{13}-a_{27}+a_{45})e_{124} + (a_{11}+a_{55})e_{125} \\ &+ a_{65}e_{126} + a_{75}e_{127} + (a_{12}-a_{37}+a_{46})e_{134} \\ &+ a_{56}e_{135} + (a_{11}+a_{66})e_{136} + a_{76}e_{137} \\ &+ a_{57}e_{145} + a_{67}e_{146} + (a_{11}+a_{44}+a_{77})e_{147} \\ &+ (-a_{16}+a_{17}+a_{53}-a_{62})e_{156} + (-a_{16}+a_{54}-a_{72})e_{157} \\ &+ (a_{15}+a_{64}-a_{73})e_{167} + a_{44}e_{234} + a_{54}e_{235} + a_{64}e_{236} + a_{74}e_{237} \\ &- a_{53}e_{245} - a_{63}e_{246} - a_{73}e_{247} + a_{27}e_{256} - a_{26}e_{257} + a_{25}e_{267} \\ &+ a_{52}e_{345} + a_{62}e_{346} + a_{72}e_{347} + a_{37}e_{356} - a_{36}e_{357} + a_{35}e_{367} \\ &+ a_{47}e_{456} - a_{46}e_{457} + a_{45}e_{467} + (a_{55}+a_{66}+a_{77})e_{567}.\end{aligned}$$

The above condition immediately implies that $a_{ij}=0$ for $i \neq j$, $a_{44}=0$, and that

$$a_{11}+a_{55} = a_{11}+a_{66} = a_{11}+a_{77} = a_{55}+a_{66}+a_{77} = 0.$$

Since $\operatorname{ch} k \neq 3$, $a_{11}=a_{55}=a_{66}=a_{77}=0$ also. $\square$

Since $15 = \dim G - \dim V$, Gw is open and G_w is smooth over k. Note that this does not hold if $\operatorname{ch} k = 3$.

Proposition 20.9. *The group $(G_w \cap \mathrm{SL}(7))^\circ$ is semi-simple and its Dynkin diagram is of type G_2.*

Proof. Let

$$a(t_1,t_2) = \begin{pmatrix} 1 &&&&&& \\ & t_1 &&&&& \\ && t_2 &&&& \\ &&& (t_1t_2)^{-1} &&& \\ &&&& t_1^{-1} && \\ &&&&& t_2^{-1} & \\ &&&&&& t_1t_2 \end{pmatrix},$$

$$H(s_1,s_2) = \begin{pmatrix} 0 &&&&&& \\ & s_1 &&&&& \\ && s_2 &&&& \\ &&& -s_1-s_2 &&& \\ &&&& -s_1 && \\ &&&&& -s_2 & \\ &&&&&& s_1+s_2 \end{pmatrix}.$$

Its is easy to see that $a(t_1,t_2) \in G_w$. We put

$$T = \{a(t_1,t_2) \mid t_1,t_2 \in \mathrm{GL}(1)\}.$$

We use the notation "+" for the multiplication in $X^*(T)$. Define $e_1,e_2 \in X^*(T)$ by

$$e_1(a(t_1,t_2)) = t_1,\ e_2(a(t_1,t_2)) = t_2.$$

Expressing

$$X = \begin{pmatrix} s_1 & u_1 & u_2 \\ v_1 & s_2 & u_3 \\ v_2 & v_3 & -s_1 - s_2 \end{pmatrix},$$

we may use the notation $A(a, \cdots, f, s_1, s_2, u_1, \cdots, v_3)$ instead of $A(a, \cdots, f, X)$. If $a = 1, b = \cdots = 0$, we denote the matrix $A(a, \cdots, f, X)$ by X_a. We define X_{u_1}, etc., similarly. Then the weights of X_a, etc., are as follows.

element	weight	element	weight
X_a	e_1	X_{u_1}	$e_1 - e_2$
X_b	e_2	X_{u_2}	$2e_1 + e_2$
X_c	$-(e_1 + e_2)$	X_{u_3}	$e_1 + 2e_2$
X_d	$-e_1$	X_{v_1}	$-e_1 + e_2$
X_e	$-e_2$	X_{v_2}	$-2e_1 - e_2$
X_f	$e_1 + e_2$	X_{v_3}	$-e_1 - 2e_2$

Let $\alpha_1 = e_1 - e_2$ and $\alpha_2 = e_2$. Then

$$e_1 = \alpha_1 + \alpha_2,\ e_1 + e_2 = \alpha_1 + 2\alpha_2,\ e_1 + 2e_2 = \alpha_1 + 3\alpha_2,\ 2e_1 + e_2 = 2\alpha_1 + 3\alpha_2.$$

So the weights are

$$\Phi = \{\pm\alpha_1, \pm\alpha_2,\ \pm(\alpha_1 + \alpha_2),\ \pm(\alpha_1 + 2\alpha_2),\ \pm(\alpha_1 + 3\alpha_2),\ \pm(2\alpha_1 + 3\alpha_2)\}.$$

By easy computations,

$$[X_a, X_d] = H(2, -1),\ [X_b, X_e] = H(-1, 2),\ [X_c, X_f] = H(-1, 2),$$
$$[X_{u_1}, X_{v_1}] = H(1, -1),\ [X_{u_2}, X_{v_2}] = H(1, 0),\ [X_{u_3}, X_{v_3}] = H(0, 1).$$

So for any $\alpha \in \Phi$, $[\mathfrak{g}_\alpha, \mathfrak{g}_{-\alpha}] \neq 0$.

Let

$$r_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & \Lambda_1 \\ 0 & \Lambda_1 & 0 \end{pmatrix}, \quad r_2 = -\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & \Lambda_2 \\ 0 & \Lambda_2 & 0 \end{pmatrix},$$

where

$$\Lambda_1 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \quad \Lambda_2 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

Then

$$\mathrm{Ad}(r_1)(X_{u_1}) = X_{v_1},\ \mathrm{Ad}(r_2)(X_b) = X_e.$$

Define

$$r_3 = r_1 r_2 r_1,\ r_4 = r_2 r_1 r_2,\ r_5 = (r_1 r_2 r_1) r_2 (r_1 r_2 r_1),\ r_6 = (r_2 r_1 r_2) r_1 (r_2 r_1 r_2).$$

Then

$$r_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & \Lambda_3 \\ 0 & \Lambda_3 & 0 \end{pmatrix}, \quad r_4 = -\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & \Lambda_1 \\ 0 & \Lambda_1 & 0 \end{pmatrix},$$
$$r_5 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \Lambda_3 & 0 \\ 0 & 0 & \Lambda_3 \end{pmatrix}, \quad r_6 = -\begin{pmatrix} 1 & 0 & 0 \\ 0 & \Lambda_2 & 0 \\ 0 & 0 & \Lambda_2 \end{pmatrix},$$

where

$$\Lambda_3 = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

Then

$$\mathrm{Ad}(r_3)(X_a) = X_d,\ \mathrm{Ad}(r_4)(X_c) = -X_f,\ \mathrm{Ad}(r_5)(X_{u_3}) = X_{v_3},\ \mathrm{Ad}(r_6)(X_{u_2}) = X_{v_2}.$$

If $a(t_1, t_2) \in \mathrm{Ker}(\alpha_1) \cap \mathrm{Ker}(\alpha_2)$, then $t_1 t_2^{-1} = t_2 = 1$. This implies that $t_1 = t_2 = 1$ and so

$$\cap_{\alpha \in \Phi} \mathrm{Ker}(\alpha) = \{e\}.$$

Therefore, by Proposition 6.28, $(G_w \cap \mathrm{SL}(7))^\circ$ is semi-simple.

We shall consider the root system now. Let $\sigma \in \mathrm{GL}(7)$ be the permutation matrix which corresponds to the permutation

$$\sigma = \binom{1234567}{4237651}$$

(the $(i, \sigma(i))$ entry is 1 for all i and other entries are 0).

We put

$$
\begin{aligned}
d(A) &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & A & 0 \\ 0 & 0 & {}^tA^{-1} \end{pmatrix}, \\
u_1(a,b,c) &= \exp\left(\begin{pmatrix} 0 & 0 & 0 & 0 & 2a & 2b & 2c \\ a & 0 & 0 & 0 & 0 & 0 & 0 \\ b & 0 & 0 & 0 & 0 & 0 & 0 \\ c & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -c & b & 0 & 0 & 0 \\ 0 & c & 0 & -a & 0 & 0 & 0 \\ 0 & -b & a & 0 & 0 & 0 & 0 \end{pmatrix}\right) \\
&= \begin{pmatrix} 1 & 0 & 0 & 0 & 2a & 2b & 2c \\ a & 1 & 0 & 0 & a^2 & ab & ac \\ b & 0 & 1 & 0 & ab & b^2 & bc \\ c & 0 & 0 & 1 & ac & bc & c^2 \\ 0 & 0 & -c & b & 1 & 0 & 0 \\ 0 & c & 0 & -a & 0 & 1 & 0 \\ 0 & -b & a & 0 & 0 & 0 & 1 \end{pmatrix}, \\
u_2(d,e,f) &= \exp\left(\begin{pmatrix} 0 & 2d & 2e & 2f & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & f & -e \\ 0 & 0 & 0 & 0 & -f & 0 & d \\ 0 & 0 & 0 & 0 & e & -d & 0 \\ d & 0 & 0 & 0 & 0 & 0 & 0 \\ e & 0 & 0 & 0 & 0 & 0 & 0 \\ f & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}\right) \\
&= \begin{pmatrix} 1 & 2d & 2e & 2f & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & f & -e \\ 0 & 0 & 1 & 0 & -f & 0 & d \\ 0 & 0 & 0 & 1 & e & -d & 0 \\ d & d^2 & de & df & 1 & 0 & 0 \\ e & de & e^2 & ef & 0 & 1 & 0 \\ f & df & ef & f^2 & 0 & 0 & 1 \end{pmatrix}.
\end{aligned}
\tag{20.10}
$$

for $A \in \mathrm{SL}(3)$ and $a, \cdots, f \in \mathrm{Aff}^1$. These are elements of $G_1 \cap \mathrm{SL}(7)$. Note that we assumed $\operatorname{ch} k \neq 3$, but we did not assume $\operatorname{ch} k \neq 2$. Even though

$$u_1(a,b,c) = I_7 + A(a,b,c,0,\cdots,0) + (1/2)A(a,b,c,0,\cdots,0)^2,$$

and $1/2$ appears in the formula, the entries of the resulting matrix are integral polynomials of a, b, c. So by the argument of Proposition 14.4, one can prove that $\{u_1(a,0,0) \mid a \in \mathbb{G}_\mathrm{a}\}$, etc., are subgroups of G even if $\operatorname{ch} k = 2$ (Note that $u_1(a,0,0)$ and $u_1(0,b,0)$ do not commute and so we have to consider each parameter separately). We use the notation U_a, etc., for the subgroup which corresponds to the parameter a, etc.

By easy computations,

$$\sigma^{-1}u_1(a,b,0)\sigma = \begin{pmatrix} 1 & -b & a & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & a & ab & a^2 & 0 \\ 0 & 0 & 1 & b & b^2 & ab & 0 \\ 0 & 0 & 0 & 1 & 2b & 2a & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & -a \\ 0 & 0 & 0 & 0 & 0 & 1 & b \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

$$\sigma^{-1}u_2(0,0,f)\sigma = \begin{pmatrix} 1 & 0 & 0 & f & 0 & 0 & f^2 \\ 0 & 1 & 0 & 0 & f & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & -f & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 2f \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

It is easy to see that $U_{u_i} = \{I_7 + u_i X_{u_i} \mid u_i \in \mathbb{G}_a\}$ is a subgroup of G for $i = 1,2,3$. By easy computations,

$$\sigma^{-1}(I_7 + A(0,\cdots,0,u_1,u_2,u_3,0,0,0))\sigma = \begin{pmatrix} 1 & 0 & 0 & 0 & -u_3 & -u_2 & 0 \\ 0 & 1 & u_1 & 0 & 0 & 0 & u_2 \\ 0 & 0 & 1 & 0 & 0 & 0 & u_3 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -u_1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

So the condition of Proposition 6.29 is satisfied. Therefore, the groups

$$T, U_a, U_b, U_f, U_{u_1}, U_{u_2}, U_{u_3}$$

generate a Borel subgroup B of $(G_w \cap \mathrm{SL}(7))^\circ$.

It is easy to see that $\Delta(B) = \{\alpha_1, \alpha_2\}$ is a basis of the root system Φ.

Lemma 20.11. *We have* $r_{\alpha_1}(\alpha_2) = \alpha_2 + \alpha_1$ *and* $r_{\alpha_2}(\alpha_1) = \alpha_1 + 3\alpha_2$ *and so* $n_{\alpha_2,\alpha_1} = -1$, $n_{\alpha_1,\alpha_2} = -3$.

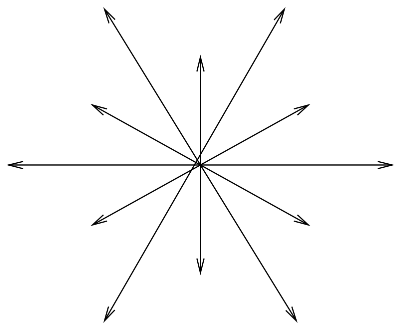
Proof. The statement follows from the following computations

$$\alpha_2(r_1 a(t_1,t_2) r_1) = \alpha_2(a(t_2,t_1)) = t_1 = (\alpha_2+\alpha_1)(a(t_1,t_2)),$$
$$\alpha_1(r_2 a(t_1,t_2) r_2) = \alpha_1(a(t_1t_2,t_2^{-1})) = t_1t_2^2 = (\alpha_1+3\alpha_2)(a(t_1,t_2)).$$

□

By the above consideration, in the Dynkin diagram, we assign 3 to the root α_1 and 1 to the root α_2. Therefore, the Dynkin diagram is of type G_2. This completes the proof of Proposition 20.9 □

The picture of weights is as follows.



1 α_1 2 $\alpha_1+\alpha_2$ 3 $2\alpha_1+3\alpha_2$ 4 $\alpha_1+2\alpha_2$ 5 $\alpha_1+3\alpha_2$ 6 α_2

It is known that the smallest non-trivial representation is the seven dimensional representation and the weights are the short weights of the above picture plus the zero weight.

The above consideration implies that G_w° is generated by $(G_w \cap \mathrm{SL}(7))^\circ$ and $\widetilde{T}$. Since $\widetilde{T}$ is contained in the center of G and is isomorphic to $\mathrm{GL}(1)$, G_w is reductive. Therefore, we get the following proposition.

Proposition 20.12. *The representation (G,V) is a regular prehomogeneous vector space.*

For the rest of this section, we assume that $\mathrm{ch}\, k \neq 2,3$. We use the operation D defined in (15.1) again. For $x \in V$, we define

$$S_x = x(\wedge,\otimes)D(x)(\wedge,\otimes)D(x) \in \wedge^7 W \otimes W \otimes W \cong W \otimes W,$$

where $(\wedge,\otimes)$ means the wedge product for the first factor and the tensor product for the second factor. Let $\phi : W \otimes W \to \mathrm{Sym}^2 W$ be the canonical map.

Definition 20.13. We define $Q_x = \phi(S_x)$.

We regard Q_x and x as elements of $\mathrm{Sym}^2(W^*)^* \cong \mathrm{Sym}^2\mathrm{Im}(\widetilde{\mathbb{O}})^*$ and $\wedge^3(W^*)^*$ respectively. So Q_x is a quadratic polynomial on W^* and x is an alternating tri-linear form on W^*. We use the same notation Q_x for the associated bilinear form on W^*. We define the action of $\mathrm{GL}(W)$ on W^* by $\iota(g)f(v) = f(g^{-1}v)$. In this way, we identify $\mathrm{GL}(W)$ and $\mathrm{GL}(W^*)$. Note that if we use bases for W, W^* which are dual to each other and identify $\mathrm{GL}(W), \mathrm{GL}(W^*)$ with the set of 7×7 matrices, $\iota(g) \in \mathrm{GL}(7)$ corresponds to ${}^t g^{-1}$ by this identification. In particular, $\iota((tI_7)g)v = t^{-1}\iota(g)v$.

It is easy to see that

$$Q_{(t,g)x} = t^3(\det g) g Q_x \tag{20.14}$$

(we are taking the determinant regarding $g \in \mathrm{GL}(W)$).

One can compute Q_x for $x = w$ by rather long and tedious computations, and the result is

$$Q_w = 6(-e_1^2 + e_2e_5 + e_3e_6 + e_4e_7). \tag{20.15}$$

We verified the above computation by the software "MAPLE" [28] also. To do so, we associate a differential form $dx_2 \wedge dx_3 \wedge dx_4 + \cdots$ to w and the input is as follows.

```
> with(difforms);
```

```
> defform(x1=0,x2=0,x3=0,x4=0,x5=0,x6=0,x7=0);
> w:= &^(d(x2),d(x3),d(x4))+&^(d(x5),d(x6),d(x7))
  +&^(d(x1),d(x2),d(x5))+&^(d(x1),d(x3),d(x5))
  +&^(d(x1),d(x4),d(x7));
> v:= x2*d(x3)&^d(x4)-x3*d(x2)&^d(x4)+x4*d(x2)&^d(x3)
  +x5*d(x6)&^d(x7)-x6*d(x5)&^d(x7)+x7*d(x5)&^d(x6)
  +x1*d(x2)&^d(x5)-x2*d(x1)&^d(x5)+x5*d(x1)&^d(x2)
  +x1*d(x3)&^d(x6)-x3*d(x1)&^d(x6)+x6*d(x1)&^d(x3)
  +x1*d(x4)&^d(x7)-x4*d(x1)&^d(x7)+x7*d(x1)&^d(x4);
> w&^v&^v;
```

Let $\Delta_1(x)$ be the discriminant of Q_x regarding Q_x as a quadratic polynomial on W^*. Since Q_w is non-degenerate, by (20.14), $\Delta_1(x)$ is a relative invariant polynomial of degree 21, and satisfies the relation

$$\Delta_1((t,g)x) = t^{21}(\det g)^9\Delta_1(x). \tag{20.16}$$

Since Q_w is irreducible, Q_x is irreducible as a polynomial of $v \in W^*$.

Let $j_x : W \to W^*$ be the map defined by

$$Q_x(v_1^*, j_x(v_2)) = 3^{-6}\Delta_1(x)v_1^*(v_2) \tag{20.17}$$

for $v_1^* \in W^*,\ v_2 \in W$.

Lemma 20.18. *The map j_x is holomorphic.*

Proof. Let $q_x = (q_{x\,ij})$ be the matrix of Q_x, i.e., $Q_x = \sum_{ij} q_{x\,ij}e_i \otimes e_j$. Then $\Delta_1(x) = \det(q_x)$. Let h_x be the matrix representation of j_x with respect to the bases $\{e_1, \cdots, e_7\}, \{f_1, \cdots, f_7\}$. Then $q_x h_x = 3^{-6}\Delta_1(x)I_7$. Therefore, h_x is a constant multiple of the adjoint matrix of q_x. □

Lemma 20.19. *We have $j_{(t,g)x}(gv) = t^{18}(\det g)^8 g(j_x(v))$ for $(t,g) \in G,\ x \in V$, and $v \in W$.*

Proof. If $(t,g) \in G,\ x \in V$ and $v \in W, v^* \in W^*$, then

$$\begin{aligned} t^{21}(\det g)^9\Delta_1(x)v^*(v) &= \Delta_1((t,g)x)v^*(v) \\ &= Q_{(t,g)x}(v^*, j_{(t,g)x}(v)) \\ &= (t^3\det g)gQ_x(v^*, j_{(t,g)x}(v)) \\ &= (t^3\det g)Q_x(g^{-1}v^*, g^{-1}j_{(t,g)x}(v)). \end{aligned}$$

Substituting $v^* = g\bar{v}^*,\ v = g\bar{v}$,

$$\begin{aligned} t^{21}(\det g)^9\Delta_1(x)\bar{v}^*(\bar{v}) &= t^{21}(\det g)^9\Delta_1(x)\bar{v}^*(\bar{v}) \\ &= (t^3\det g)Q_x(\bar{v}^*, g^{-1}j_{(t,g)x}(g\bar{v})) \\ &= t^{21}(\det g)^9 Q_x(\bar{v}^*, j_x(\bar{v})). \end{aligned}$$

Therefore,

$$g^{-1}j_{(t,g)x}(g\bar{v}) = t^{18}(\det g)^8 j_x(\bar{v}).$$

Replacing $\bar{v}$ by v, we get the lemma. □

By (20.15), the matrix representation of Q_w is

$$3\begin{pmatrix} -2 & 0 & 0 \\ 0 & 0 & I_3 \\ 0 & I_3 & 0 \end{pmatrix}.$$

So $\Delta_2(w) = 2 \cdot 3^7$. The adjoint matrix of the above matrix is

$$3^6\begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 2I_3 \\ 0 & 2I_3 & 0 \end{pmatrix}.$$

This implies that by j_w,

$$\begin{aligned} &e_1 \to -f_1,\ e_2 \to 2f_5,\ e_3 \to 2f_6,\ e_4 \to 2f_7, \\ &e_5 \to 2f_2,\ e_6 \to 2f_3,\ e_7 \to 2f_4. \end{aligned} \tag{20.20}$$

Proposition 20.21. *There exists a relative invariant polynomial of degree* 7.

Proof. By Proposition 10.9, it suffices to show the existence of a relative invariant polynomial of degree 56. By Proposition 14.4, we may assume that $k = \mathbb{Q}$.

Let $\wedge^3(j_x)$ be the map $\wedge^3 W \to \wedge^3 W^*$ induced by j_x, and $(\ ,\ )$ the natural pairing between $\wedge^3 W$ and $\wedge^3 W^*$. Define $\Delta_2(x) = (x, \wedge^3(j_x)(x))$.

Lemma 20.22. *We have* $\Delta_2((t,g)x) = t^{56}(\det g)^{24}\Delta_2(x)$.

Proof. Since

$$\wedge^3(j_{(t,g)x})(gw) = t^{54}(\det g)^{24} g \wedge^3 (j_x)(w),$$

we have

$$\wedge^3(j_{(t,g)x})((t,g)x) = t^{55}(\det g)^{24} g \wedge^3 (j_x)(x).$$

Therefore,

$$\begin{aligned} \Delta_2((t,g)x) &= (tgx, t^{55}(\det g)^{24} g \wedge^3 (j_x)(x)) \\ &= t^{56}(\det g)^{24}(x, \wedge^3(j_x)(x)) \\ &= t^{56}(\det g)^{24}\Delta_2(x). \end{aligned}$$

□

We show that $\Delta_2(w) \neq 0$. By (20.20),

$$\wedge^3(j_w)(w) = 8f_{567} + 8f_{234} + 4f_1 \wedge (f_{25} + f_{36} + f_{47}).$$

So $(w, \wedge^3(j_w)(w)) = 28 \neq 0$. Hence $\Delta_2(x)$ is a relative invariant polynomial of degree 56.

Since the GCD of $21, 56$ is 7, there exists a relative invariant polynomial of degree 7. □

For later purposes, we describe the dual of Q_x. Define

$$Q_x^*(v_1, v_2) = Q_x(j_x(v_1), j_x(v_2)) \tag{20.23}$$

for $v_1, v_2 \in W$. This is a quadratic form on W and is non-degenerate if $x \in V^{\mathrm{ss}}$. The following proposition follows from (20.14) and Lemma 20.19.

Proposition 20.24. *We have* $Q^*_{(t,g)x} = t^{39}(\det g)^{17} g Q_x^*$.

By (20.20),

$$Q^*_w(\sum_i x_i e_i) = 6(-x_1^2 + 4(x_2x_5 + x_3x_6 + x_4x_7)). \tag{20.25}$$

If A is a normed k-algebra, $\mathrm{Re}(A)$ is contained in the center of A. So the structure of A is determined by its restriction to $\mathrm{Im}(A)$. On W^*, we define a product structure $(\,\cdot\,)_x$ depending on x by the equation

$$3x(v_1, v_2, v_3) = Q_x(v_1, (v_2 \cdot v_3)_x) \tag{20.26}$$

for all $v_1, v_2, v_3 \in W^*$.

Let $\Delta(x)$ be the relative invariant polynomial of degree 7 such that $\Delta(w) = 6$. It is easy to verify that $\Delta((t,g)x) = t^7(\det g)^3\Delta(x)$. For $x \in V_k^{\mathrm{ss}}$ and $v \in W_k^*$, we define

$$\|v\|_x = \Delta(x)^{-1}Q_x(v). \tag{20.27}$$

Definition 20.28. We define $\mathbb{O}_x$ to be the algebra $k \oplus W^*$ such that $W^* = \mathrm{Im}(\mathbb{O}_x)$. The norm is defined by $\|v\|_x$ for $v \in W^*$, and the product v_1v_2 for $v_1, v_2 \in W^*$ is defined by

$$\mathrm{Re}(v_1v_2) = -\Delta(x)^{-1}Q_x(v_1, v_2),\ \mathrm{Im}(v_1v_2) = (v_1 \cdot v_2)_x.$$

If $x = w$, the product structure and the norm of $\mathbb{O}_w$ coincide with those of $\widetilde{\mathbb{O}}$ by Proposition 20.6. Therefore, $\mathbb{O}_w \cong \widetilde{\mathbb{O}}$ and is a normed k-algebra. Suppose $x, y \in V_k^{\mathrm{ss}}$, $(t,g) \in G_{\bar{k}}$, and $y = (t,g)x$. Then we define $m_{x,y,(t,g)} : W^* \to W^*$ by

$$m_{x,y,(t,g)}(v) = t^2 \det g\,\iota(g)v \tag{20.29}$$

for $v \in W^*$. Note that we are taking the determinant of g regarding $g \in \mathrm{GL}(W)$.

Proposition 20.30. (1) *For all $x \in V_k^{\mathrm{ss}}$, $\mathbb{O}_x$ is a normed k-algebra and is a k-form of $\widetilde{\mathbb{O}}$.*

(2) *If $x, y \in V_k^{\mathrm{ss}}$, $(t,g) \in G_{\bar{k}}$, and $y = (t,g)x$, $m_{x,y,(t,g)}$ is an isomorphism of normed $\bar{k}$-algebras from $\mathbb{O}_{x\,\bar{k}}$ to $\mathbb{O}_{y\,\bar{k}}$.*

Proof. Let $m = m_{x,y,(t,g)}$. Then

$$\begin{aligned}
Q_y(\iota(g)v_1, (m(v_2) \cdot m(v_3))_y) &= t^4(\det g)^2 Q_y(\iota(g)v_1, (\iota(g)v_2 \cdot \iota(g)v_3)_y) \\
&= 3t^4(\det g)^2 y(\iota(g)v_1, \iota(g)v_2, \iota(g)v_3) \\
&= 3t^4(\det g)^2 g^{-1}y(v_1, v_2, v_3) \\
&= 3t^5(\det g)^2 x(v_1, v_2, v_3) \\
&= t^5(\det g)^2 Q_x(v_1, (v_2 \cdot v_3)_x) \\
&= t^2 \det g Q_y(\iota(g)v_1, \iota(g)(v_2 \cdot v_3)_x) \\
&= Q_y(\iota(g)v_1, m((v_2 \cdot v_3)_x))
\end{aligned}$$

for all $v_1, v_2, v_3 \in W^*$.

Therefore, $(m(v_2) \cdot m(v_3))_y = m(v_2 \cdot v_3)_x$. Since

$$\begin{aligned}
\Delta(y)^{-1}Q_y(m(v_1), m(v_2)) &= t^{-7}(\det g)^{-3}t^4(\det g)^2\Delta(x)^{-1}Q_y(\iota(g)v_1, \iota(g)v_2) \\
&= t^{-3}(\det g)^{-1}t^3 \det g\Delta(x)^{-1}Q_x(v_1, v_2) \\
&= \Delta(x)^{-1}Q_x(v_1, v_2)
\end{aligned}$$

for all $v_1, v_2 \in W^*$, m preserves the norm also.

Since $\mathbb{O}_w$ is a normed k-algebra, this proves both (1), (2). $\square$

By the above proof, one can see that if $x = (t,g)w \in V_k^{\mathrm{ss}}$, the imaginary part of the k-form of $\widetilde{\mathbb{O}}$ which corresponds to $\mathbb{O}_x$ is

$$\{v \in \mathrm{Im}(\widetilde{\mathbb{O}})_{\bar{k}} \mid m_{w,x,(t,g)}(v) \in \mathrm{Im}(\widetilde{\mathbb{O}})_k\}.$$

Let $\mathfrak{O}$ be the set of k-isomorphism classes of k-forms of $\widetilde{\mathbb{O}}$. We regard $\mathrm{Aut}\,(\widetilde{\mathbb{O}}) \subset \mathrm{GL}(\mathrm{Im}(\widetilde{\mathbb{O}}))$.

Lemma 20.31. *If* $g \in G_w \cap \mathrm{GL}(7)$, *then* $(\det g)^3 = 1$.

Proof. We may assume that $k = \bar{k}$. Note that

$$G_w \cap \mathrm{GL}(7) = (G_w \cap \mathrm{SL}(7)) \cdot (\widetilde{T} \cap \mathrm{GL}(7)).$$

So if $(1, tI_7) \in \widetilde{T} \cap \mathrm{GL}(7)$, then $(\det(tI_7))^3 = t^{21} = 1$, because $t^3 = 1$. $\square$

Lemma 20.32. *We have* $\mathrm{Aut}\,(\widetilde{\mathbb{O}}) = \iota(G_w \cap \mathrm{SL}(7))$.

Proof. Suppose $g \in \mathrm{Aut}\,(\widetilde{\mathbb{O}})$. Since $Q_w(gv_1, gv_2) = Q_w(v_1, v_2)$ for all $v_1, v_2 \in W^*$, $(\det g)^2 = 1$. Since $g(v_1 \cdot v_2)_w = (gv_1 \cdot gv_2)_w$, $\iota^{-1}(g)w = w$ by (20.26). By the above lemma, $(\det g)^{-3} = 1$. This implies $\det g = (\det g)^3/(\det g)^2 = 1$. Therefore, $\mathrm{Aut}\,(\widetilde{\mathbb{O}}) \subset G_w \cap \mathrm{SL}(7)$.

Suppose $(1, g) \in G_w \cap \mathrm{SL}(7)$. Then $m_{w,w,(1,g)} = \iota(g)$ belongs to $\mathrm{Aut}\,(\widetilde{\mathbb{O}})$ by Proposition 20.30 This proves the proposition. $\square$

We shall prove in section 22 (Proposition 22.1) that $G_w \cap \mathrm{SL}(7)$ is connected. For the moment, we assume this fact.

Proposition 20.33. *We have* $G_w \cong (G_w \cap \mathrm{SL}(7)) \times \widetilde{T}$. *Moreover, the center of* $G_w \cap \mathrm{SL}(7)$ *is trivial.*

Proof. Set-theoretically, if $g \in G_w \cap \mathrm{SL}(7) \cap \widetilde{T}$, then $g = (1, tI_7)$ and $t^3 = t^7 = 1$. Therefore, $t = 1$. It is easy to see that

$$T(G_w \cap \mathrm{SL}(7))_e = L_1,\ T(\widetilde{T})_e = L_2,\ L_1 \cap L_2 = \{0\}.$$

Therefore, $G_w \cap \mathrm{SL}(7) \cap \widetilde{T} = \{e\}$ as schemes.

This implies that $(G_w \cap \mathrm{SL}(7)) \times \widetilde{T} \subset G_w$. Since

$$15 = \dim T(G_w) = T(G_w \cap \mathrm{SL}(7)) + 1 \le \dim G_w \le \dim T(G_w) = 15,$$

$G_w, G_w \cap \mathrm{SL}(7)$ are smooth over k, and $G_w^\circ = (G_w \cap \mathrm{SL}(7)) \times \widetilde{T}$. Note that $G_w \cap \mathrm{SL}(7)$ is a connected simple group of type G_2 and so has no outer automorphisms.

To show that $G_w = G_w^\circ$, we may assume that $k = \bar{k}$. If $g \in G_w$, the conjugation by g fixes elements of $\widetilde{T}$ and so induces an automorphism of $G_w \cap \mathrm{SL}(7)$. Since all automorphisms of $G_w \cap \mathrm{SL}(7)$ are inner, by changing g if necessary, we may assume that g commutes with elements of $G_w \cap \mathrm{SL}(7)$. Since

$$\begin{pmatrix} 1 & & & & & & \\ & t_1 & & & & 0 & \\ & & t_2 & & & & \\ & & & (t_1t_2)^{-1} & & & \\ & & & & t_1^{-1} & & \\ & 0 & & & & t_2^{-1} & \\ & & & & & & t_1t_2 \end{pmatrix} \in G_w \cap \mathrm{SL}(7),$$

g fixes eigenspaces of the above element. Therefore, g is in the form $g = (t_1, g_1)$ where g_1 is diagonal. Since g fixes w, $g_1 = t_2 I_7$ for some t_2 and $t_1 = t_2^{-3}$. So $g \in \widetilde{T}$.

If $(1, g)$ belongs to the center of $G_w \cap \mathrm{SL}(7)$, g is a diagonal element by the same argument as above. Since $\mathrm{Ad}(g)$ is trivial, g must be a scalar matrix tI_7. Since $(1, tI_7) \in G_w \cap \mathrm{SL}(7)$, $t^3 = t^7 = 1$ and so $t = 1$. This proves the proposition. □

By the above proposition, $G_w \cap \mathrm{SL}(7) \cong \mathrm{Aut}\,(\widetilde{\mathbb{O}})$. Therefore,

$$\mathrm{H}^1(k, G_w) \cong \mathrm{H}^1(k, \mathrm{Aut}\,(\widetilde{\mathbb{O}})) \times \mathrm{H}^1(k, \widetilde{T}) \cong \mathrm{H}^1(k, \mathrm{Aut}\,(\widetilde{\mathbb{O}})).$$

Hence, $G_k \backslash V_k^{\mathrm{ss}}$ is in bijective correspondence with k-forms of $\widetilde{\mathbb{O}}$. This was proved by Sato-Kimura [23] and Igusa [10]. We make this correspondence more explicit. For that purpose, we shall prove the following theorem.

Theorem 20.34. *The map*

$$\alpha_V : G_k \backslash V_k^{\mathrm{ss}} \ni x \to \mathbb{O}_x \in \mathfrak{O}$$

is well defined and is bijective.

Proof. If $x, y \in V_k^{\mathrm{ss}}$, $(t, g) \in G_k$, and $y = (t, g)x$, then $m_{x,y,(t,g)}$ is a k-isomorphism. Therefore, the above map is well defined. Suppose $x, y \in V_k^{\mathrm{ss}}$ and $g' : \mathbb{O}_x \to \mathbb{O}_y$ is a k-isomorphism. Let $g \in \mathrm{GL}(W)_k$ be the element such that $\iota(g^{-1}) = g'$. Then for all $v_1, v_2, v_3 \in W^*$,

$$\begin{aligned} 3g^{-1}y(v_1, v_2, v_3) &= 3y(g'v_1, g'v_2, g'v_3) \\ &= Q_y(g'v_1, (g'v_2 \cdot g'v_3)_y) \\ &= Q_y(g'v_1, g'(v_2 \cdot v_3)_x) \\ &= \Delta(y)\Delta(y)^{-1} Q_y(g'v_1, g'(v_2 \cdot v_3)_x) \\ &= \Delta(y)\Delta(x)^{-1} Q_x(v_1, (v_2 \cdot v_3)_x) \\ &= 3\Delta(y)\Delta(x)^{-1} x(v_1, v_2, v_3). \end{aligned}$$

Therefore, $y = (\Delta(x)^{-1}\Delta(y), g)x \in G_k x$. This implies that α_V is injective.

Let A be a k-form of $\widetilde{\mathbb{O}}$ corresponding to a cohomology class $c \in \mathrm{H}^1(k, \mathrm{Aut}\,(\widetilde{\mathbb{O}}))$. Suppose $c = (h_\sigma)_\sigma$. Then

$$\mathrm{Im}(A)_k = \{v \in \mathrm{Im}(\widetilde{\mathbb{O}})_{k^{\mathrm{sep}}} \mid h_\sigma v^\sigma = v \text{ for all } \sigma \in \mathrm{Gal}(k^{\mathrm{sep}}/k)\}.$$

Since Aut $(\widetilde{\mathbb{O}}) \subset \mathrm{GL}(\mathrm{Im}(\widetilde{\mathbb{O}}))$ and $\mathrm{H}^1(k, \mathrm{GL}(\mathrm{Im}(\widetilde{\mathbb{O}})))$ is trivial, there exists $g' \in \mathrm{GL}(\widetilde{\mathbb{O}})_{k^{\mathrm{sep}}}$ such that $c = (g'^{-1} g'^{\sigma})_{\sigma}$. Then

$$\begin{aligned}\mathrm{Im}(A)_k &= \{v \in \mathrm{Im}(\widetilde{\mathbb{O}})_{k^{\mathrm{sep}}} \mid g'^{-1} g'^{\sigma} v^{\sigma} = v \text{ for all } \sigma \in \mathrm{Gal}(k^{\mathrm{sep}}/k)\} \\ &= \{v \in \mathrm{Im}(\widetilde{\mathbb{O}})_{k^{\mathrm{sep}}} \mid g'^{\sigma} v^{\sigma} = g' v \text{ for all } \sigma \in \mathrm{Gal}(k^{\mathrm{sep}}/k)\} \\ &= \{v \in \mathrm{Im}(\widetilde{\mathbb{O}})_{k^{\mathrm{sep}}} \mid g' v \in \mathrm{Im}(\widetilde{\mathbb{O}})_k\}.\end{aligned}$$

Since $g'^{-1} g'^{\sigma} \in \mathrm{Aut}\,(\widetilde{\mathbb{O}})$, $\det g' \in k^{\times}$ by Lemma 20.32. Let $g \in G_{\bar{k}}$ be the element such that $\iota(g) = g'$. Then $x = (1, g)w \in V_k^{\mathrm{ss}}$. Let $m = m_{w,x,(1,g)}$. Then $m(v) = (\det g) g' v$. The k-form of $\mathrm{Im}(\widetilde{\mathbb{O}})$ which corresponds to x is

$$\begin{aligned}&\{v \in \mathrm{Im}(\widetilde{\mathbb{O}})_{k^{\mathrm{sep}}} \mid (\det g) g' v \in \mathrm{Im}(\widetilde{\mathbb{O}})_k\} \\ &= \{v \in \mathrm{Im}(\widetilde{\mathbb{O}})_{k^{\mathrm{sep}}} \mid g' v \in \mathrm{Im}(\widetilde{\mathbb{O}})_k\} \\ &= \mathrm{Im}(A)_k.\end{aligned}$$

Therefore, $A \cong \mathbb{O}_x$. □

Exercise 20.35. Find an explicit isomorphism $k(-)(+)(+) \cong k(+)(+)(-)$.

Exercise 20.36. Let $A = A(a, \cdots, f, X)$ and $A' = A(a', \cdots, f', X')$. Prove that the Killing form of is

$$\langle A, A' \rangle = 24(ad' + a'd + be' + b'e + cf' + c'f) + 8\,\mathrm{tr}(XX') = 4\,\mathrm{tr}(AA').$$

Exercise 20.37. Construct a G-equivariant map $V \to \mathrm{Sym}^2 W^*$ defined by degree four polynomials in the following manner. Since we may use Proposition 14.4, we assume $k = \mathbb{Q}$ in the following.

(1) Let $w' = e_{234} + e_{567} + e_1 \wedge (e_{36} + e_{47})$. Show that $\dim T(G_{w'})_e = 16$.
(2) Show that $V \setminus V^{\mathrm{ss}} = \overline{Gw'}$.
(3) Let $x_t = e_{234} + e_{567} + e_1 \wedge (te_{25} + e_{36} + e_{47})$ for $t \in \mathrm{Aff}^1$. Find Q_{x_t}.
(4) Consider $j_x : W \to W^*$ which we constructed in (20.17). Let $\mathrm{Sym}^2(j_x) : \mathrm{Sym}^2 W \to \mathrm{Sym}^2 W^*$ be the induced map. Define $\Phi(x) = \mathrm{Sym}^2(j_x)(Q_x)$. Express $\Phi((t, g)x)$ in terms of $\Phi(x)$.
(5) Find $\Phi(x_t)$, $\Delta(x_t)$. (Find $g \in G_{\overline{k(t)}}$ such that $x_t = gw$. You may not be above to choose this g in $G_{k(t)}$.)
(6) Prove that $\Delta(x)$ is irreducible.
(7) Prove that $\Delta(x)^{-5}\Phi(x)$ is holomorphic on V and is defined by homogeneous polynomials of degree four.

21. Type (7)

In this section we consider the case (7) in the Sato-Kimura classification following [32] We assume that $\operatorname{ch} k \neq 2,3$ in this section. Throughout this section we identify Aff^8 with the Lie algebra $W = L(\mathrm{PGL}(3))$. If $X, Y \in W$, the Killing form is

$$Q(X,Y) = \mathrm{tr}(\mathrm{ad}(X)\mathrm{ad}(Y)) = 6\mathrm{tr}(XY).$$

This is a non-degenerate symmetric bilinear form since $\operatorname{ch} k \neq 2,3$. Define

$$C(X,Y,Z) = Q([X,Y],Z) \tag{21.1}$$

for $X, Y, Z \in W$.

Lemma 21.2. *The trilinear form $C(X,Y,Z)$ is an element of $\wedge^3 W^*$. Moreover, it is invariant by the adjoint action of* $\mathrm{PGL}(3)$.

Proof. Since Q is invariant by the action of $\mathrm{PGL}(3)$,

$$Q([X,Y],Z) + Q(Y,[X,Z]) = 0$$

for all $X, Y, Z \in W$. So

$$C(X,Y,Z) = Q([X,Y],Z) = -Q(Y,[X,Z]) = -Q([X,Z],Y) = C(X,Z,Y).$$

Obviously $C(X,Y,Z) = -C(Y,X,Z)$. So $C(X,Y,Z)$ is an element of $\wedge^3 W^*$.

If $g \in \mathrm{PGL}(3)$ then

$$\begin{aligned} C(\mathrm{Ad}(g)(X), \mathrm{Ad}(g)(Y), \mathrm{Ad}(g)(Z)) &= Q([\mathrm{Ad}(g)(X), \mathrm{Ad}(g)(Y)], \mathrm{Ad}(g)(Z)) \\ &= Q(\mathrm{Ad}(g)([X,Y]), \mathrm{Ad}(g)(Z)) \\ &= Q([X,Y],Z) \\ &= C(X,Y,Z). \end{aligned}$$

This proves the lemma. $\square$

We shall express $C(X,Y,Z)$ explicitly by choosing a basis for W. Let E_{ij} be the matrix whose only non-zero entry is the (i,j)-entry and is 1. We define

$$H_1 = \frac{1}{3}\begin{pmatrix} 2 & & \\ & -1 & \\ & & -1 \end{pmatrix}, \; H_2 = \frac{1}{3}\begin{pmatrix} 1 & & \\ & 1 & \\ & & -2 \end{pmatrix},$$

$$e_1 = E_{12}, \; e_2 = E_{23}, \; e_3 = -E_{31}, \; e_4 = -E_{21}, \; e_5 = -E_{32}, \; e_6 = E_{13},$$

$$e_7 = H_1 - 2H_2 = \begin{pmatrix} 0 & & \\ & -1 & \\ & & 1 \end{pmatrix}, \; e_8 = H_1 + H_2 = \begin{pmatrix} 1 & & \\ & 0 & \\ & & -1 \end{pmatrix}.$$

We choose $\{e_1, \cdots, e_8\}$ as a basis for W.

Let $\alpha_i, \beta_i, \gamma_i \in k$ for $i = 1,2,3$, and $\alpha_1 + \alpha_2 + \alpha_3 = 0$. We put

$$\alpha = (\alpha_1, \alpha_2, \alpha_3), \; \beta = (\beta_1, \beta_2, \beta_3), \; \gamma = (\gamma_1, \gamma_2, \gamma_3).$$

We define $H = H(\alpha),\ X = X(\alpha, \beta, \gamma),\ A = A(\alpha, \beta, \gamma)$ by

$$\begin{aligned}
&H = \alpha_1 H_1 + \alpha_2 H_2, \\
&X = H - \beta_1 E_{12} - \beta_2 E_{23} - \beta_3 E_{31} - \gamma_1 E_{21} - \gamma_2 E_{32} - \gamma_3 E_{13}, \\
&A = \begin{pmatrix} \alpha_1 & 0 & 0 & 0 & \gamma_3 & \gamma_2 & \beta_1 & \beta_1 \\ 0 & \alpha_2 & 0 & -\gamma_3 & 0 & -\gamma_1 & -2\beta_2 & \beta_2 \\ 0 & 0 & \alpha_3 & -\gamma_2 & \gamma_1 & 0 & -\beta_3 & 2\beta_3 \\ 0 & -\beta_3 & -\beta_2 & -\alpha_1 & 0 & 0 & \gamma_1 & \gamma_1 \\ \beta_3 & 0 & \beta_1 & 0 & -\alpha_2 & 0 & -2\gamma_2 & \gamma_2 \\ \beta_2 & -\beta_1 & 0 & 0 & 0 & -\alpha_3 & -\gamma_3 & 2\gamma_3 \\ \gamma_1 & -\gamma_2 & 0 & \beta_1 & -\beta_2 & 0 & 0 & 0 \\ \gamma_1 & 0 & \gamma_3 & \beta_1 & 0 & \beta_3 & 0 & 0 \end{pmatrix}.
\end{aligned} \tag{21.3}$$

Then easy computations show that

$$(\mathrm{ad}(X)(e_1), \cdots, \mathrm{ad}(X)(e_8)) = (e_1, \cdots, e_8)A. \tag{21.4}$$

Let $\{f_1, \cdots, f_8\}$ be the dual basis of $\{e_1, \cdots, e_8\}$. We use the notation $e_{i_1 \cdots i_k}, f_{i_1 \cdots i_k}$ as before.

Proposition 21.5. *We have*

(1)

$$C = -6(f_{123} + f_{456} + f_7 \wedge (f_{14} - 2f_{25} + f_{36}) + f_8 \wedge (f_{14} + f_{25} - 2f_{36})),$$

(2)

$$Q(\sum_i x_i e_i, \sum_i x_i e_i) = 12(-x_1 x_4 - x_2 x_5 - x_3 x_6 + x_7^2 - x_7 x_8 + x_8^2).$$

Proof. Let $C = \sum_{i<j<k} a_{ijk} f_{ijk}$. By the definition (21.1), $a_{ijk} = 0$ if $[e_i, e_j] = 0,\ [e_i, e_k] = 0$, or $[e_j, e_k] = 0$. Since

$$[e_1, e_5] = [e_1, e_6] = [e_2, e_4] = [e_2, e_6] = [e_3, e_4] = [e_3, e_5] = [e_7, e_8] = 0,$$

we do not have to consider a_{i78}, etc.

By (21.4),

$$\begin{aligned}
a_{123} &= 6\mathrm{tr}([e_1, e_2]e_3) = 6\mathrm{tr}(e_6 e_3) = -6,\\
a_{127} &= 6\mathrm{tr}([e_1, e_2]e_7) = 6\mathrm{tr}(e_6 e_7) = 0,\\
a_{128} &= 6\mathrm{tr}([e_1, e_2]e_8) = 6\mathrm{tr}(e_6 e_8) = 0,\\
a_{137} &= 6\mathrm{tr}([e_1, e_3]e_7) = -6\mathrm{tr}(e_5 e_7) = 0,\\
a_{138} &= 6\mathrm{tr}([e_1, e_3]e_8) = -6\mathrm{tr}(e_5 e_8) = 0,\\
a_{147} &= 6\mathrm{tr}([e_1, e_4]e_7) = -6\mathrm{tr}((e_7 + e_8)e_7) = -6,\\
a_{148} &= 6\mathrm{tr}([e_1, e_4]e_8) = -6\mathrm{tr}((e_7 + e_8)e_8) = -6,\\
a_{236} &= 6\mathrm{tr}([e_2, e_3]e_6) = 6\mathrm{tr}(e_4 e_6) = 0,\\
a_{237} &= 6\mathrm{tr}([e_2, e_3]e_7) = 6\mathrm{tr}(e_4 e_7) = 0,\\
a_{238} &= 6\mathrm{tr}([e_2, e_3]e_8) = 6\mathrm{tr}(e_4 e_8) = 0,\\
a_{257} &= 6\mathrm{tr}([e_2, e_5]e_7) = 6\mathrm{tr}(e_7 e_7) = 12,\\
a_{258} &= 6\mathrm{tr}([e_2, e_5]e_8) = 6\mathrm{tr}(e_7 e_8) = -6,\\
a_{367} &= 6\mathrm{tr}([e_3, e_6]e_7) = 6\mathrm{tr}(e_8 e_7) = -6,\\
a_{368} &= 6\mathrm{tr}([e_3, e_6]e_8) = 6\mathrm{tr}(e_8 e_8) = 12,\\
a_{456} &= 6\mathrm{tr}([e_4, e_5]e_6) = 6\mathrm{tr}(e_3 e_6) = -6,\\
a_{457} &= 6\mathrm{tr}([e_4, e_5]e_7) = 6\mathrm{tr}(e_3 e_7) = 0,\\
a_{458} &= 6\mathrm{tr}([e_4, e_5]e_8) = 6\mathrm{tr}(e_3 e_8) = 0,\\
a_{467} &= 6\mathrm{tr}([e_4, e_6]e_7) = -6\mathrm{tr}(e_2 e_7) = 0,\\
a_{468} &= 6\mathrm{tr}([e_4, e_6]e_8) = -6\mathrm{tr}(e_2 e_8) = 0,\\
a_{567} &= 6\mathrm{tr}([e_5, e_6]e_7) = 6\mathrm{tr}(e_1 e_7) = 0,\\
a_{568} &= 6\mathrm{tr}([e_5, e_6]e_8) = 6\mathrm{tr}(e_1 e_8) = 0.
\end{aligned}$$

The statement (1) follows from the above relations.

The statement (2) is easier to verify by computing $\mathrm{tr}(e_1 e_1) = 0$, etc. We leave the details to the reader. □

Let $j : W \to W^*$ be a map such that $j(X)(Y) = (1/6)Q(X, Y)$. Since Q is non-degenerate, j is an isomorphism. Since Q is invariant by the action of PGL(3),

$$j(\mathrm{Ad}(g)(X))(Y) = j(X)(\mathrm{Ad}(g)^{-1}(Y)) = (gj(X))(Y). \tag{21.6}$$

The map j induces an isomorphism $\wedge^3(j) : \wedge^3 W \to \wedge^3 W^*$. By (21.6), the following proposition follows.

Proposition 21.7. *The element* $\wedge^3(j)^{-1}(C)$ *is invariant by the action of* PGL(3).

We now describe $\wedge^3(j)^{-1}(C)$ explicitly.

Proposition 21.8. *We have*

$$\wedge^3(j)^{-1}(C) = 6(e_{123} + e_{456} + e_7 \wedge (e_{14} - e_{25}) + e_8 \wedge (e_{14} - e_{36})).$$

Proof. By the map j,

$$\begin{aligned}&e_1 \to -f_4,\ e_2 \to -f_5,\ e_3 \to -f_6,\\ &e_4 \to -f_1,\ e_5 \to -f_2,\ e_6 \to -f_3,\\ &e_7 \to 2f_7 - f_8,\ e_8 \to -f_7 + 2f_8.\end{aligned}$$

So by j^{-1},

$$\begin{aligned}&f_1 \to -e_4,\ f_2 \to -e_5,\ f_3 \to -e_6,\\ &f_4 \to -e_1,\ f_5 \to -e_2,\ f_6 \to -e_3,\\ &f_7 \to \frac{1}{3}(2e_7 + e_8),\ f_8 \to \frac{1}{3}(e_7 + 2e_8).\end{aligned}$$

Therefore,

$$\begin{aligned}\wedge^3(j)^{-1}(C) &= 6(e_{456} + e_{123})\\ &\quad + 2(2e_7 + e_8) \wedge (e_{14} - 2e_{25} + e_{36})\\ &\quad + 2(e_7 + 2e_8) \wedge (e_{14} + e_{25} - 2e_{36}))\\ &= 6(e_{123} + e_{456} + e_7 \wedge (e_{14} - e_{25}) + e_8 \wedge (e_{14} - e_{36})).\end{aligned}$$

□

Let

$$w = e_{123} + e_{456} + e_7 \wedge (e_{14} - e_{25}) + e_8 \wedge (e_{14} - e_{36}).$$

By Proposition 21.8, w is fixed by PGL(3).

Let $\widetilde{T} = \mathrm{Ker}(G \to \mathrm{GL}(V))$. It is easy to see that

$$\widetilde{T} = \{(t^{-3}, tI_8) \mid t \in \mathrm{GL}(1)\} \cong \mathrm{GL}(1).$$

Let L_1 be the set of elements X as in (21.3), and L_2 the set of elements of the form $(-3t, tI_8)$. Since (21.3) is the matrix representation of the action of the Lie algebra of PGL(3),

$$L_1 \oplus L_2 \subset T(G_w)_e.$$

Proposition 21.9. *The representation (G, V) is a regular prehomogeneous vector space. Moreover, $G_w^\circ \cong \mathrm{PGL}(3) \times \widetilde{T}$.*

Proof. We first show that $T(G_w)_e = L_1 \oplus L_2$. Let $A = (a_{ij})$ be an 8×8 matrix, and $g(A) = I_8 + \epsilon A$ where $k[\epsilon]/(\epsilon^2)$ is the ring of dual numbers. Since we know $L_1 \oplus L_2 \subset T(G_w)_e$, it is enough to show that if $g(A)w = w$ and

$$a_{11} = a_{22} = a_{18} = a_{28} = a_{38} = a_{48} = a_{58} = a_{68} = 0,$$

then $A = 0$.

By $I_8 + \epsilon A$,

$$\begin{aligned}&e_1 \to a_{21}e_2 + \cdots + a_{81}e_8,\\ &e_2 \to a_{12}e_1 + a_{32}e_3 + \cdots + a_{82}e_8,\\ &e_j \to a_{1j}e_1 + \cdots a_{7j}e_8 \text{ for } j = 3, \cdots, 7,\\ &e_8 \to a_{78}e_7 + a_{88}e_8.\end{aligned}$$

So

$$
\begin{aligned}
(I_8+\epsilon A)w = {} & w + a_{33}e_{123} + (-a_{27}+a_{43})e_{124} + (-a_{17}+a_{53})e_{125} \\
& + a_{63}e_{126} + (a_{15}+a_{24}+a_{73})e_{127} + (a_{24}+a_{83})e_{128} \\
& - (a_{37}+a_{42})e_{134} - a_{52}e_{135} - a_{62}e_{136} + (a_{34}-a_{72})e_{137} \\
& + (a_{16}+a_{34}-a_{82})e_{138} + (a_{16}+a_{57})e_{145} + (-a_{15}+a_{67})e_{146} \\
& + (a_{44}+a_{77}+a_{78})e_{147} + (a_{44}+2a_{88})e_{148} + a_{14}e_{156} \\
& + (-a_{12}+a_{54})e_{157} + a_{54}e_{158} + a_{64}e_{167} + (-a_{13}+a_{64})e_{168} \\
& + (a_{74}-a_{84})e_{178} + a_{41}e_{234} + (a_{37}+a_{51})e_{235} + a_{61}e_{236} \\
& + (-a_{35}+a_{71})e_{237} + (a_{26}+a_{81})e_{238} + (a_{26}+a_{47})e_{245} \\
& - a_{25}e_{246} + (a_{21}-a_{45})e_{247} + a_{21}e_{248} + (a_{24}-a_{67})e_{256} \\
& - (a_{55}+a_{77})e_{257} - a_{87}e_{258} - a_{65}e_{267} - a_{23}e_{268} + a_{85}e_{278} \\
& + a_{36}e_{345} - a_{35}e_{346} + a_{31}e_{347} + (a_{31}-a_{46})e_{348} + a_{34}e_{356} \\
& - a_{32}e_{357} - a_{56}e_{358} - a_{78}e_{367} - (a_{33}+a_{66}+a_{88})e_{368} \\
& - a_{76}e_{378} + (a_{44}+a_{65}+a_{66})e_{456} + (-a_{42}-a_{51}+a_{76})e_{457} \\
& + (-a_{51}+a_{86})e_{458} + (-a_{61}+a_{75})e_{467} + (-a_{43}-a_{61}+a_{85})e_{468} \\
& + (-a_{71}+a_{81})e_{478} + (a_{62}+a_{74})e_{567} + (-a_{53}+a_{84})e_{568} \\
& - a_{82}e_{578} + a_{73}e_{678}.
\end{aligned}
$$

The above condition immediately implies that many of a_{ijk}'s are zero. Eliminating them from the above condition recursively, we have that $a_{ij}=0$ except for $a_{15}, a_{24}, a_{67}, a_{83}, a_{44}, a_{55}, \cdots, a_{88}$ and that

$$
\begin{cases}
a_{15}+a_{24}=0, \\
a_{15}-a_{67}=0, \\
a_{24}-a_{67}=0, \\
a_{24}+a_{83}=0,
\end{cases}
$$

$$
\begin{cases}
a_{44}+a_{66}=0, \\
a_{44}+a_{77}=0, \\
a_{44}+2a_{88}=0, \\
a_{55}+a_{77}=0, \\
a_{66}+a_{88}=0.
\end{cases}
$$

The first set of equations implies that

$$a_{15}=a_{24}=a_{67}=a_{83}=0$$

if $\operatorname{ch} k \neq 2$, and the second set of equations implies that

$$a_{44}=a_{55}=a_{66}=a_{77}=a_{88}=0$$

if $\operatorname{ch} k \neq 3$. Therefore, $T(G_w)_e = L_1 \oplus L_2$. Since $\dim T(G_w) = 9 = \dim G - \dim V$, Gw is open and G_w is smooth over k. Since $L_1 \cap L_2 = \{0\}$, $G_w \cap \widetilde{T}$ is finite and reduced. If $(t^{-3}, tI_8) \in \mathrm{PGL}(3)$, then $t^3 = t^8 = 1$. This implies that $t=1$. Therefore,

$\mathrm{PGL}(3) \times \widetilde{T} \subset G_w^\circ$. Since

$$9 = \dim(\mathrm{PGL}(3) \times \widetilde{T}) \le \dim G_w^\circ \le \dim T(G_w)_e = 9,$$

$G_w^\circ = \mathrm{PGL}(3) \times \widetilde{T}$, which is reductive. Therefore, (G, V) is a regular prehomogeneous vector space. □

Let

$$\tau = \begin{pmatrix} 0 & I_3 & 0 \\ I_3 & 0 & 0 \\ 0 & 0 & -I_2 \end{pmatrix}.$$

Proposition 21.10. *Assumption 12.1 is satisfied with* $i = 2$. *Moreover,* τ *maps to the non-trivial element of* $\mathfrak{S}_2$.

Proof. We show that G_w is generated by G_w° and τ. We may assume that $k = \bar{k}$. Let X be as in (21.3). Then $\tau X \tau = -{}^t X$. Therefore, the conjugation by τ induces an outer automorphism of PGL(3). Since the Dynkin diagram of PGL(3) is of type A_2, the automorphism group of this diagram is $\mathfrak{S}_2$. So if $g \in G_w$, multiplying τ if necessary, we may assume that the conjugation by g induces an inner automorphism of PGL(3). Note that $\widetilde{T}$ is contained in the center of G.

By multiplying an element of PGL(3) if necessary, we may assume that g commutes with elements of G_w°. By Schur's lemma, there exist $t_1, t_2 \in k^\times$ such that $g = (t_1, t_2 I_8)$. Since g fixes w, $t_1 = t_2^{-3}$. This proves that G_w is generated by G_w° and $\widetilde{T}$. □

The above proposition implies that $G_w \cong \mathrm{Aut}\,(\mathrm{PGL}(3)) \times \mathrm{GL}(1)$. Since $\mathrm{H}^1(k, G) = \mathrm{H}^1(k, \widetilde{T}) = \{1\}$, we get the following theorem.

Theorem 21.11. (Sato-Kimura, Igusa) *The orbit space* $G_k \backslash V_k^{\mathrm{ss}}$ *is in bijective correspondence with* k*-forms of* PGL(3).

By the above correspondence, if $x \in V_k^{\mathrm{ss}}$, $G_x^\circ / \widetilde{T}$ is isomorphic to the corresponding k-form of PGL(3). We leave this to the reader.

Exercise 21.12. Prove that there exists a relative invariant polynomial of degree 16 in the following manner. Since we may use Proposition 14.4, we assume that $k = \mathbb{Q}$ in the following.

(1) Let $D : \wedge^3 W \to \wedge^2 W \otimes W$ be the equivariant map defined in (15.1). Define

$$\phi : x \to x \wedge D(x) \wedge D(x) \in W^* \otimes W \otimes W \cong \mathrm{Hom}(W, W) \otimes W.$$

Regard ϕ as a homomorphism with entries in W. Considering the composition, regard $\phi \circ \phi \in \mathrm{Hom}(W, W) \otimes \mathrm{Sym}^2 W$. Define $\Phi(x) = \mathrm{tr}(\phi(x) \circ \phi(x)) \in \mathrm{Sym}^2 W$. Let $\Delta_1(x)$ be the discriminant of $\Phi(x)$. Express $\Phi((t,g)x), \Delta_1((t,g)x)$ in terms of $\Phi(x), \Delta_1(x)$ explicitly.

(2) Find $\Phi(w)$ and $\Delta_1(w)$ and show that $\Delta_1(x)$ is a relative invariant polynomial of degree 48.

(3) Define $j_x : W \to W^*$ similarly as in (20.17). Put $\Delta_2(x) = (x, \wedge^3(j_x)(x))$. Show that $\Delta_2(x)$ is a relative invariant polynomial of degree 128.

22. Type (25)

In this and the next sections we consider the cases (25), (26) in the Sato-Kimura classification following [33]. We assume that $\operatorname{ch} k \neq 2, 3$.

We first define the representation precisely. Let $W = \mathrm{Aff}^7$ be the standard representation of GL(7) (i.e., the space of seven dimensional column vectors), and $e_1, \cdots, e_7$ the standard coordinate vectors. We use the notation e_{ijk}, etc. as before. We consider the natural representation of GL(7) on $\wedge^3 W$. Let $\overline{G} = \mathrm{GL}(7)$ and

$$\bar{w} = e_{234} + e_{567} + e_1 \wedge (e_{25} + e_{36} + e_{47}) \in \wedge^3 W.$$

We define G_1 to be the set of $g \in \mathrm{GL}(7)$ such that $g\bar{w} = c(g)\bar{w}$ for some $c(g) \in \mathrm{GL}(1)$. Then G_1 becomes a closed subgroup of GL(7), and $c : G_1 \to \mathrm{GL}(1)$ is a character of G_1 both defined over k. Let $H = \mathrm{Ker}(c) \cap \mathrm{SL}(7)$.

In the next two sections, we consider the following two representations

(1) $G = G_1,\ V = W$,
(2) $G = G_1 \times \mathrm{GL}(2),\ V = W \otimes \mathrm{Aff}^2$.

Let $w = {}^t\begin{pmatrix}1 & 0 & \cdots & 0\end{pmatrix}$. We use the notation $d(A), u_1(a,b,c), u_2(d,e,f)$ defined in (20.10). Define

$$F = \{d(A) \mid A \in \mathrm{SL}(3)\}.$$

It is easy to see that $F \subset H_w \subset G_{1\,w}$.

Let

$$\Lambda = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix},\ \tau = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & \Lambda \\ 0 & \Lambda & 0 \end{pmatrix}.$$

Obviously $\tau^2 = 1$.

Proposition 22.1. (1) *The groups G_1, H are connected.*

(2) *The representation (G_1, W) is a regular prehomogeneous vector space. Moreover, $G_{1\,w}$ is generated by $G^\circ_{1\,w} = F$ and τ.*

Proof. Let $A(a, \cdots, f, X)$ be as in (20.7). We put

$$L_1 = \{A(a, \cdots, f, X) \mid a, \cdots, f \in k,\ \mathrm{tr}(X) = 0\},$$
$$L_2 = \{tI_7 \mid t \in k\}.$$

We have shown in section 20 that the Lie algebra of $\mathrm{Ker}(c)$ is L_1. Since

$$1 \longrightarrow \mathrm{Ker}(c) \longrightarrow G \xrightarrow{\ c\ } \mathrm{GL}(1) \longrightarrow 1$$

is exact and $\mathrm{Ker}(c)$ is smooth over k, G_1 is smooth over k also. Moreover, the Lie algebra of G_1 is $L_1 \oplus L_2$.

Let $k[\epsilon]/(\epsilon^2)$ be the ring of dual numbers again. It is easy to see that if $I_7 + \epsilon(A(a, \cdots, f, X) + tI_7)$ fixes w, then $a, \cdots, f = 0, t = 0$. Therefore, $T(G_{1\,w})_e$ coincides with the Lie algebra of F. Since $F \subset G_{1\,w}$, this shows that $F = G^\circ_{1\,w}$, which is reductive. Since $\dim T(G_{1\,w})_e = 8 = \dim G_1 - \dim W$, $G_1 w$ is open and $G_{1\,w}$ is smooth over k. It is easy to see that τ induces an outer automorphism of F. So by a similar argument as before, $G_{1\,w}$ is generated by $G^\circ_{1\,w}$ and τ.

Let

$$\Delta(x) = x_1^2 - 4(x_2x_5 + x_3x_6 + x_4x_7). \tag{22.2}$$

Proposition 20.24 and (20.25) imply that there exists a rational character $\chi : G_1 \to \mathrm{GL}(1)$ such that $\Delta(gx) = \chi(g)\Delta(x)$.

It remains to show (1). We may assume that $k = \bar{k}$ for that purpose. We put

$$X = \{x \in W \mid \Delta(x) = -1\}.$$

Since $\operatorname{ch} k \neq 2, 3$, X is irreducible and so is connected.

Consider the map $H \to X$ defined by $H \ni h \to hw$. Since $H_w = G_{1\,w} \cap H = F$ and $\dim F = 8$, $\dim Hw = 14 - 8 = 6 = \dim X$ by Theorem 3.25. This implies that Hw is dense in X and so is irreducible. Therefore, Hw is connected. Since the fibers of the map $H \to Hw$ are isomorphic to F, which is connected, H is connected.

By Proposition 20.33, the center of H is trivial. So $H \cap \{tI_7 \mid t \in \mathrm{GL}(1)\} = \{1\}$. Therefore, $H \times \{tI_7 \mid t \in \mathrm{GL}(1)\} \subset G_1$. Counting the dimension, $G_1^\circ = H \times \{tI_7 \mid t \in \mathrm{GL}(1)\}$. So any element of G_1° may be written uniquely as a product of elements of H and a scalar matrix.

Let $g \in G_1$. Then the conjugation by g induces an automorphism of $H \times \{tI_7 \mid t \in \mathrm{GL}(1)\}$ and so an automorphism of H. Since H has no outer automorphisms, by multiplying an element of H if necessary, we may assume that g commutes with elements of H. Then by Schur's lemma, g is a scalar matrix and so belongs to G_1°. This shows that G_1 is connected. □

Corollary 22.3. *We have*

(1) $G_1 = H \times \{tI_7 \mid t \in \mathrm{GL}(1)\}$,
(2) $c = (\chi')^3,\ \chi = (\chi')^2$, *and* $H = \operatorname{Ker}(\chi')$.

Proof. The statement (1) was already shown in the proof of the above proposition.

Since H has no non-trivial characters and

$$c(tI_7) = t^3 = \chi'(tI_7)^3,\ \chi(tI_7) = t^2 = \chi'(tI_7)^2,$$

$c = (\chi')^3,\ \chi = (\chi')^2$ by (1).

Since H has no non-trivial characters, $H \subset \operatorname{Ker}(\chi')$ is obvious.

Suppose $g = g'(tI_7) \in \operatorname{Ker}(\chi')$ where $g' \in H$. Then $\chi'(g) = \chi'(tI_7) = t = 1$. Therefore, $g \in H$. □

For the rest of this section, we put $G = G_1$ and $V = W$.

Since $\langle \tau \rangle \cong \mathfrak{S}_2 \subset G_w$, there is a map

$$\mathfrak{Ex}_2 = \mathrm{H}^1(k, \mathfrak{S}_2) \to \mathrm{H}^1(k, G_w).$$

Lemma 22.4. *The map* $\mathfrak{Ex}_2 \to \mathrm{H}^1(k, G)$ *is trivial.*

Proof. The field k as the degree one extension of k corresponds to the trivial class of $\mathrm{H}^1(k, \mathfrak{S}_2)$ and the lemma is trivial for this case. Let $t^2 + a_1t + a_2 \in k[t]$ be an irreducible quadratic polynomial with roots $\alpha = (\alpha_1, \alpha_2)$. Let σ be the non-trivial element of $\mathrm{Gal}(k(\alpha)/k)$. We put

$$g_\alpha = \begin{pmatrix} -a_1 & -2\alpha_1 & 0 & 0 & -2\alpha_2 & 0 & 0 \\ a_2 & -\alpha_1^2 & 0 & 0 & -\alpha_2^2 & 0 & 0 \\ 0 & 0 & \alpha_1 & \alpha_2 & 0 & \alpha_2 & -\alpha_1 \\ 0 & 0 & -1 & -1 & 0 & -1 & 1 \\ 1 & -1 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & \alpha_2 & \alpha_2 & 0 & \alpha_1 & -\alpha_1 \\ 0 & 0 & a_2 & \alpha_2^2 & 0 & a_2 & -\alpha_1^2 \end{pmatrix}. \tag{22.5}$$

Lemma 22.6. *We have $g_\alpha \in G_{1\,k(\alpha)}$.*

Proof. Let $\alpha_1 = \beta + \gamma,\ \alpha_2 = \beta - \gamma$. Straightforward computations show that

$$g_\alpha = (2\gamma I_7) d(A_1) u_1(\beta, 0, 0) d(A_2) d(A_3) u_1(1/2, 0, 0) u_2(-1, 0, 0),$$

where

$$A_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -\beta \\ 0 & 0 & 1 \end{pmatrix},$$

$$A_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -\frac{1}{2} \\ 0 & 0 & 1 \end{pmatrix},$$

$$A_3 = \begin{pmatrix} 2 & 0 & 0 \\ 0 & \frac{1}{2} & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

This shows that $g_\alpha \in G_{1\,k(\alpha)}$. □

By the form of g_α, it is obvious that

$$g^\sigma = g_\alpha \tau.$$

Therefore, the cohomology class in $\mathrm{H}^1(k, \mathfrak{S}_2)$ which corresponds to the field $k(\alpha)$ maps to the trivial class $(g_\alpha^{-1} g_\alpha^\sigma)$ in $\mathrm{H}^1(k(\alpha)/k, G)$. □

Definition 22.7. We define $w_\alpha = g_\alpha w = {}^t\begin{pmatrix} -a_1 & a_2 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$.

Since $\sigma \to g_\alpha^{-1} g_\alpha^\sigma$ may be identified with the natural isomorphism $\mathrm{Gal}(k(\alpha)/k) \to \mathfrak{S}_2$, $w_\alpha \in V_k^{\mathrm{ss}}$ corresponds to the field $k(\alpha)$. Since $\Delta(w_\alpha) = a_1^2 - 4a_2 = (\alpha_1 - \alpha_2)^2$, we get the following proposition.

Proposition 22.8. *We have $k(\alpha) = k(\Delta(w_\alpha)^{\frac{1}{2}})$.*

Let R be any k-algebra. We define $R(\alpha) = R \otimes k(\alpha)$. The non-trivial element $\sigma \in \mathrm{Gal}(k(\alpha)/k)$ acts on $R(\alpha)$ by $(r \otimes x)^\sigma = r \otimes (x^\sigma)$. For $A \in \mathrm{SL}(3)_{R(\alpha)}$, we define $A^\sigma, {}^*A = {}^tA^\sigma$ entry-wise. Let

$$\mathrm{SU}_\alpha(2,1)_R = \{A \in \mathrm{SL}(3)_{R(\alpha)} \mid A\Lambda{}^*A = \Lambda\}.$$

We define $\mathrm{SU}_\alpha(2,1)$ to be the group over k such that the set of R-valued points is $\mathrm{SU}_\alpha(2,1)_R$ for any k-algebra R.

Let $d(A)$ be as in (20.10).

Proposition 22.9. *We have $G^\circ_{w_\alpha} = g_\alpha \{d(A) \mid A \in \mathrm{SU}_\alpha(2,1)\}\, g_\alpha^{-1} \cong \mathrm{SU}_\alpha(2,1)$.*

Proof. Let R be any k-algebra. Consider $R(\alpha)$ as above with the action of σ. Regarding $G_{w_\alpha} \subset \mathrm{GL}(7)$, we consider the entry-wise action of σ for elements in $G^\circ_{w_\alpha\, R(\alpha)}$ also. Then

$$G^\circ_{w_\alpha\, R} = \{g \in G^\circ_{w_\alpha\, R(\alpha)} \mid g^\sigma = g\}.$$

Over $R(\alpha)$, we can express elements of $G^\circ_{w_\alpha\, R(\alpha)}$ as $g_\alpha d(A) g_\alpha^{-1}$ where $A \in \mathrm{SL}(3)_{R(\alpha)}$. This element is in $G^\circ_{w_\alpha\, R}$ if and only if

$$\begin{aligned} g_\alpha d(A) g_\alpha^{-1} &= g_\alpha^\sigma d(A^\sigma)(g_\alpha^\sigma)^{-1} \\ &= g_\alpha \tau d(A^\sigma) \tau g_\alpha^{-1} \\ &= g_\alpha d(\Lambda^* A^{-1} \Lambda) g_\alpha^{-1}. \end{aligned}$$

This condition is satisfied if and only if $A \in \mathrm{SU}_\alpha(2,1)_R$. Therefore, the proposition follows from Theorem 13.32. □

Let $F_1 = \mathrm{SU}_\alpha(2,1)$ and $F_2 = \mathrm{R}_{k(\alpha)/k}(\mathrm{SL}(3))$. For $g \in \mathrm{SL}(3)_{k(\alpha)}$, we denote the entry-wise action of σ by g^σ. We define ${}^*g = {}^t g^\sigma$. For $g \in F_{ik(\alpha)}$ $(i = 1,2)$, let $\phi_{F_i}(\sigma)(g)$ be the action of σ induced from the k-structure of F_i.

We use the notation $i_k, i_{k(\alpha)}$ for the natural imbeddings $F_{1\,k} \to F_{2\,k}, F_{1\,k(\alpha)} \to F_{2\,k(\alpha)}$. We denote the natural inclusion map $F_{i\,k} \to F_{i\,k(\alpha)}$ by $j_{i\,k(\alpha)}$ for $i = 1,2$. Obviously, the following diagram is commutative.

$$\begin{array}{ccc} F_{1\,k} & \xrightarrow{j_{1\,k(\alpha)}} & F_{1\,k(\alpha)} \\ {\scriptstyle i_k}\downarrow & & \downarrow{\scriptstyle i_{k(\alpha)}} \\ F_{2\,k} & \xrightarrow{j_{2\,k(\alpha)}} & F_{2\,k(\alpha)} \end{array}$$

We may identify $F_{1\,k(\alpha)} \cong \mathrm{SL}(3)_{k(\alpha)}$, $F_{2\,k(\alpha)} \cong \mathrm{SL}(3)_{k(\alpha)} \times \mathrm{SL}(3)_{k(\alpha)}$. With this identification,

$$\begin{aligned} &i_{k(\alpha)}(g) = (g, \Lambda {}^t g^{-1} \Lambda),\ j_{1k(\alpha)}(g) = g,\ j_{2k(\alpha)}(g) = (g, g^\sigma), i_k(g) = g, \\ &\phi_{F_1}(\sigma)(g) = \Lambda^* g^{-1} \Lambda,\ \phi_{F_2}(\sigma)(g_1, g_2) = (g_2^\sigma, g_1^\sigma). \end{aligned}$$

For $i = 1,2$, we may consider $g \to g^\sigma$ as a k-automorphism of the k-group F_i and denote it by $\psi_{F_i}(\sigma)$. Note that $\psi_{F_2}(\sigma)(g_1, g_2) = (g_2, g_1)$ for $(g_1, g_2) \in F_{2\,k(\alpha)}$.

Let U be the k-vector space of 3×3 Hermitian matrices (with respect to the extension $k(\alpha)/k$). Then F_2 acts on U by $H \to g H {}^t\psi_{F_2}(\sigma)(g)$. We may identify $U_{k(\alpha)} \cong \mathrm{M}(3,3)_{k(\alpha)}$ and the action of $(g_1, g_2) \in F_{2\,k(\alpha)}$ is $H \to g_1 H {}^t g_2$. The determinant $\det H$ is a function on U defined over k. We define $X = \{H \in U \mid \det H = -1\}$.

Since $\mathrm{Gal}(k(\alpha)/k) \cong \mathfrak{S}_2$, any element of $\mathrm{H}^1(k(\alpha)/k, F_1)$ is determined by a single element $h \in F_{1\,k(\alpha)} \cong \mathrm{SL}(3)_{k(\alpha)}$ satisfying the cocycle condition $h\phi_{F_1}(\sigma)(h) = h\Lambda^* h^{-1} \Lambda = 1$. So we express such a cohomology class by (h). Note that the cocycle condition for (h) is equivalent to $h\Lambda$ or $h^{-1}\Lambda$ being Hermitian.

Proposition 22.10. (1) *We have* $G_k \backslash X_k \cong \mathrm{H}^1(k, F_1)$.

(2) *Any element of* $\mathrm{H}^1(k, F_1)$ *is represented by an element of* $\mathrm{H}^1(k(\alpha)/k, F_1)$.

(3) *If* $(h) \in \mathrm{H}^1(k(\alpha)/k, F_1)$, *the corresponding Hermitian form is* $h^{-1}\Lambda$.

Proof. For $H \in X_k$, we can find an element $g \in F_{2\,k^{\mathrm{sep}}}$ which maps Λ to H. Then $c_H = (g^{-1}g^{\eta})_{\eta \in \mathrm{Gal}(k^{\mathrm{sep}}/k)}$ defines a cohomology class in $\mathrm{H}^1(k, F_1)$. Note that $\mathrm{H}^1(k, F_2) = \{1\}$. So by the argument of Theorem 11.3, the map $G_k \backslash X_k \ni H \to c_H \in \mathrm{H}^1(k, F_1)$ is bijective. This proves (1).

For $H \in X_k$, put $g_1 = H\Lambda^{-1}$. Then $\det g_1 = 1$. So if we choose $g = (g_1, 1)$, $g \in F_{2\,k(\alpha)}$ and it maps Λ to H. This means that c_H is represented by the element $\{g^{-1}g^{\sigma}\} \in \mathrm{H}^1(k(\alpha)/k, F_1)$. This proves (2). Also if we express $c_H = (h)$,

$$\begin{aligned} i_{k(\alpha)}(h) &= (g_1, 1)^{-1}\phi_{F_2}(\sigma)(g_1, 1) \\ &= (g_1^{-1}, g_1^{\sigma}) \\ &= (g_1, \Lambda g_1 \Lambda) \text{ since } H \text{ is Hermitian} \\ &= i_{k(\alpha)}(g_1^{-1}). \end{aligned}$$

Therefore, $H = g_1\Lambda = h^{-1}\Lambda$. This proves (3). □

Lemma 22.11. *For any $x \in V_k^{\mathrm{ss}}$, there exists $g \in G_k \cap \mathrm{SL}(7)_k$ such that gx is in the form $\begin{pmatrix} 0 & 1 & 0 & 0 & x_5 & 0 & 0 \end{pmatrix}$.*

Proof. Let $x = {}^t\begin{pmatrix} x_1 & \cdots & x_7 \end{pmatrix}$ and $\Delta(x) \neq 0$. Suppose $(x_2, \cdots, x_7) \neq 0$. Then $(x_2, x_3, x_4) \neq 0$ or $(x_5, x_6, x_7) \neq 0$. Multiplying τ if necessary, we may assume that $(x_2, x_3, x_4) \neq 0$. Multiplying an element of $\mathrm{SL}(3)$, we may assume that $(x_2, x_3, x_4) = (1, 0, 0)$. Then $u_2(-\frac{x_1}{2}, 0, 0)x$ is of the form ${}^t\begin{pmatrix} 0 & 1 & \cdots \end{pmatrix}$. Multiplying an element of $\mathrm{SL}(3)$, we may assume that $x_3 = x_4 = 0$. Since $\Delta(x) \neq 0$, $x_5 \neq 0$. Multiplying an element of $\mathrm{SL}(3)$ again, we may assume $x_6 = x_7 = 0$.

Suppose $x_2 = \cdots = x_7 = 0$. Then the second entry of $u_1(1, 0, 0)x$ is non-zero and it reduces to the previous case. □

Let $\alpha_V : G_k \backslash V_k^{\mathrm{ss}} \to \mathfrak{Ex}_i$ be the map defined after Definition 12.6.

Theorem 22.12. *The map $\alpha_V : G_k \backslash V_k^{\mathrm{ss}} \to \mathfrak{E}_2$ is bijective. If $x \in V_k^{\mathrm{ss}}$ corresponds to $k(\alpha)$ ($\alpha \notin k, \alpha^2 \in k$), $G_x^{\circ} \cong \mathrm{SU}_{\alpha}(2,1)$. Moreover, for any $x \in V_k^{\mathrm{ss}}$, the corresponding field is $k(\Delta(x)^{\frac{1}{2}})$.*

Proof. By the above lemma, any orbit in $G_k \backslash V_k^{\mathrm{ss}}$ is represented by a point of the form $\begin{pmatrix} 0 & 1 & 0 & 0 & x_5 & 0 & 0 \end{pmatrix}$, where $x_5 \in k^{\times}$. It is easy to see that this element belongs to the orbit $G_k w_{\alpha}$ for some α such that $\alpha^2 \in k$. This implies that the orbits of w_{α}'s which we constructed exhaust all the orbits in $G_k \backslash V_k^{\mathrm{ss}}$. Therefore, α_V is bijective.

Finally, the character χ is a square of the character χ'. So if $x = gw_{\alpha}$ and $g \in G_k$, the field corresponding to x is $k(\alpha)$ and $\Delta(x) = \chi'(g)^2\Delta(w_{\alpha})$. This proves $k(\Delta(x)^{\frac{1}{2}}) = k(\Delta(w_{\alpha})^{\frac{1}{2}}) = k(\alpha)$. □

This theorem itself was easy to verify and we didn't have to consider Galois cohomology. However, this has the following important interpretation in terms of Galois cohomology, which we need to deal with more interesting type (26).

Corollary 22.13. *The map $\mathrm{H}^1(k, \mathrm{SU}_{\alpha}(2,1)) \to \mathrm{H}^1(k, G)$ is injective.*

23. Type (26)

In this section we consider the cases (26) in the Sato-Kimura classification. We still assume that $\operatorname{ch} k \neq 2,3$.

Let G_1 be as in the previous section. Let $G_2 = \mathrm{GL}(2)$, $G = G_1 \times G_2$, and $V = W \otimes \mathrm{Aff}^2$. We regard this space as the set of linear forms $x = M(v)$ in two variables $v = (v_1, v_2)$ with entries in W. Let $W_1 = v_1 W$ be the subspace of forms $x = M(v)$ such that $M(0, v_2) = 0$. We define $W_2 = v_2 W$ similarly. Then $W = W_1 \oplus W_2$.

We define an action of $g = (g_1, g_2) \in G$ on $x = M(v)$ by $gx = g_1 M(vg_2)$. This defines a representation of G on V. Let $\{e_1, \cdots, e_7\}$ be the standard basis of W. Considering $V = v_1 W \oplus v_2 W$, let $e_{i,j} = v_i e_j$ for $i = 1,2, j = 1, \cdots, 7$. Then $\{e_{i,j} \mid i = 1,2, j = 1, \cdots, 7\}$ is a basis of V. Let $x = (x_{i,j})$ be the coordinate of $x \in V$ with respect to this basis. We may also use the notation $x = (x_1, x_2)$ where $x_i = {}^t\begin{pmatrix} x_{i,1} & \cdots & x_{i,7} \end{pmatrix}$ for $i = 1, 2$.

Let $\widetilde{T} = \operatorname{Ker}(G \to \mathrm{GL}(V))$. Then

$$\widetilde{T} = \{(t^{-1} I_7, t I_2) \mid t \in \mathrm{GL}(1)\} \cong \mathrm{GL}(1),$$

and $\widetilde{T}$ is contained in the center of G.

Consider the element

$$w = v_1 \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} + v_2 \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}.$$

Let Δ be as in (22.2). For $x = (x_1, x_2) \in V$, we define

$$F_x(v) = \Delta(v_1 x_1 + v_2 x_2).$$

This is a binary quadratic form. It is easy to see that if $g = (g_1, g_2) \in G$,

$$F_{gx}(v) = \chi(g_1) F_x(v g_2).$$

Therefore, the discriminant of $F_x(v)$ is a relative invariant polynomial. Note that $F_w(v) = -4 v_1 v_2$.

Definition 23.1. For $A \in \mathrm{GL}(2)$, we define $d(A) = (d_1(A), d_2(A))$ where

$$d_1(A) = \begin{pmatrix} 1 & & & & \\ & (\det A)^{-1} & & 0 & \\ & & A & & \\ & 0 & & \det A & \\ & & & & {}^t A^{-1} \end{pmatrix}, \quad d_2(A) = \begin{pmatrix} \det A & 0 \\ 0 & (\det A)^{-1} \end{pmatrix}.$$

By the imbedding $A \to \begin{pmatrix} (\det A)^{-1} & 0 \\ 0 & A \end{pmatrix}$, $\mathrm{GL}(2)$ becomes a closed subgroup of $\mathrm{SL}(3) \subset G_1$. So $\mathrm{GL}(2)$ is a closed subgroup of G by the imbedding $A \to d(A)$. It is easy to see that elements of the form $d(A)$ fix w. Since $\mathrm{GL}(2)$ is connected, $\mathrm{GL}(2)$ is a closed subgroup of G_w°. We leave the following proposition to the reader

Proposition 23.2. *We have* $\dim T(G_w)_e = 5$.

It is easy to see that $\mathrm{GL}(2) \cap \widetilde{T} = \{1\}$. Therefore, $G^\circ = \mathrm{GL}(2) \times \widetilde{T}$. In particular $\mathrm{GL}(2) \times \widetilde{T}$ is a normal subgroup of G_w.

We define $\tau = (\tau_1, \tau_2)$ where

$$\Lambda = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \ \tau_1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & \Lambda \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & \Lambda & 0 & 0 \end{pmatrix}, \ \tau_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Proposition 23.3. *The representation* (G, V) *is a regular prehomogeneous vector space. Moreover,* G_w *is generated by* $G^\circ = \mathrm{GL}(2) \times \widetilde{T}$ *and* τ.

Proof. As before, we may assume that k is algebraically closed. Suppose that U is an irreducible representation of $\mathrm{GL}(2)$. Then there exist two integers k, l such that the highest weight of elements of the form $\begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix}$ is t^k and $t_2 I_2$ acts by t_2^l. Note that $k \geq 0$. Since U is determined by k, l, we say U is of type (k, l).

Let

$$U_{i,0} = \langle e_{i,1} \rangle, \ U_{i,1} = \langle e_{i,2} \rangle, \ U_{i,2} = \langle e_{i,3}, e_{i,4} \rangle,$$
$$U_{i,3} = \langle e_{i,5} \rangle, \ U_{i,4} = \langle e_{i,6}, e_{i,7} \rangle$$

for $i = 1, 2$.

Suppose $g = (g_1, g_2) \in G_w$. Then $F_w(v g_2)$ is a scalar multiple of $F_w(v)$. Multiplying τ if necessary, we may assume that $\begin{pmatrix} 1 & 0 \end{pmatrix} g_2$, $\begin{pmatrix} 0 & 1 \end{pmatrix} g_2$ are scalar multiples of $\begin{pmatrix} 1 & 0 \end{pmatrix}$, $\begin{pmatrix} 0 & 1 \end{pmatrix}$ respectively. This implies g_2 is a diagonal element and commutes with $d_2(A)$ for any $A \in \mathrm{GL}(2)$.

Since g normalizes $\mathrm{GL}(2) \times \widetilde{T}$, the conjugation by g maps the center of $\mathrm{GL}(2) \times \widetilde{T}$ to itself. Since $\widetilde{T}$ is contained in the center of G, the conjugation by g_1 induces either the identity map or the inverse on the center of $\mathrm{GL}(2) \subset G_1$ (imbedded by d_1) modulo $\widetilde{T}$. Since g_2 commutes with $d_1(A)$ for any $A \in \mathrm{GL}(2)$, g_1 must induce the identity map on the center of $\mathrm{GL}(2) \subset G_1$ modulo $\widetilde{T}$. Therefore, g commutes with the center of $\mathrm{GL}(2) \subset G$ modulo $\widetilde{T}$.

Since g_2 is diagonal, $g(W_1) = W_1, \ g(W_2) = W_2$. Note that $\widetilde{T}$ acts trvially on V. So by the above consideration, g does not change the weights with respect to tI_2 of elements in W_1. The types of $U_{1,j}$ for $j = 0, \cdots, 4$ are

$$(0,2), (0,0), (1,3), (0,4), (1,1).$$

Therefore, g_1 must be of the form

$$g_1 = \begin{pmatrix} a & & & & \\ & b & & 0 & \\ & & A & & \\ & 0 & & b^{-1} & \\ & & & & {}^t A^{-1} \end{pmatrix},$$

where $a, b \in \mathrm{GL}(1), \ A \in \mathrm{GL}(2)$.

Multiplying $d(bA^{-1})$ and an element of $\widetilde{T}$, we may assume that $b=1,\ A=I_2$. It is easy to see that if

$$g=\left(\begin{pmatrix} a & 0\\ 0 & I_6\end{pmatrix},\begin{pmatrix} b & 0\\ 0 & c\end{pmatrix}\right)\in G$$

fixes w, then $a=b=c=1$.

Since $5=\dim T(G_w)_e=\dim G-\dim V$, this proves the proposition. □

By the above proposition, we have a split exact sequence

$$1\to \mathrm{GL}(2)\times\mathrm{GL}(1)\to G_w\to\mathfrak{S}_2\to 1$$

where τ maps to the non-trivial element of $\mathfrak{S}_2$. As before, we may regard $\mathfrak{Ex}_2\cong \mathrm{H}^1(k,\mathfrak{S}_2)$ as a subset of $\mathrm{H}^1(k,G_w)$. So there is a natural map $\mathfrak{E}_2\to\mathrm{H}^1(k,G)$.

Let $k(\alpha)/k$ be a quadratic extension such that $\alpha\notin k$ and $\alpha^2\in k$. Let $g_{\alpha,1}$ be the matrix defined in (22.5) as g_α. Let

$$g_{\alpha,2}=\begin{pmatrix}1 & 1\\ \alpha & -\alpha\end{pmatrix},\ g_\alpha=(g_{\alpha,1},g_{\alpha,2})\in G_{k(\alpha)}$$

Definition 23.4. We define $w_\alpha=g_\alpha w$.

Let $\sigma\in\mathrm{Gal}(k(\alpha)/k)$ be the non-trivial element as before. Since g_α satisfies the condition $g_\alpha^\sigma=g_\alpha\tau$, we get the following proposition.

Proposition 23.5. *The map $\mathfrak{E}_2\to\mathrm{H}^1(k,G)$ is trivial, $w_\alpha\in V_k^{\mathrm{ss}}$, and w_α corresponds to the field $k(\alpha)$.*

Since the roots of the polynomial $F_{w_\alpha}(v)$ are $\pm\alpha$, we get the following corollary.

Corollary 23.6. *The field $k(\alpha)$ is generated by roots of the polynomial $F_{w_\alpha}(v)$.*

For $A\in\mathrm{GL}(2)_{k(\alpha)}$, we define ${}^*A$ as in §2.

Definition 23.7. We define $\mathrm{U}_\alpha(1,1)=\{A\in\mathrm{GL}(2)_{k(\alpha)}\mid A\Lambda{}^*A=\Lambda\}$.

We consider $\mathrm{U}_\alpha(1,1)$ as an algebraic group over k.

The proof of the following proposition is similar to that of Proposition (22.9) and is left to the reader.

Proposition 23.8. *We have $G_{w_\alpha}^\circ=\{g_\alpha d(A)g_\alpha^{-1}\mid A\in\mathrm{U}_\alpha(1,1)\}\times\widetilde{T}\cong\mathrm{U}_\alpha(1,1)\times\widetilde{T}$.*

We consider the fiber structure of $\alpha_V: G_k\backslash V_k^{\mathrm{ss}}\to\mathfrak{Ex}_2$. Since $\mathrm{H}^1(k,\mathrm{GL}(2)\times\mathrm{GL}(1))=\{1\}$, $\alpha_V^{-1}(k)=G_kw$.

Let $k(\alpha)/k$ be a quadratic extension such that $\alpha^2\in k$, and $\sigma\in\mathrm{Gal}(k(\alpha)/k)$ the non-trivial element. To determine the fiber over $k(\alpha)$, we have to consider the map $\mathrm{H}^1(k,G_{w_\alpha}^\circ)\to\mathrm{H}^1(k,G)$.

Note that $g_\alpha\tau g_\alpha^{-1}\in G_{w_\alpha,k}$. Therefore, $(G_{w_\alpha}/G_{w_\alpha}^\circ)_k\cong\mathfrak{S}_2$. Now Theorem 12.10 implies that

$$\alpha_V^{-1}(k(\alpha))\cong\mathfrak{S}_2\backslash\mathrm{Ker}(\mathrm{H}^1(k,\mathrm{U}_\alpha(1,1))\to\mathrm{H}^1(k,G)).$$

Let Y_k be the set of non-degenerate 2×2 Hermitian matrices. As in Proposition (22.10), $\mathrm{H}^1(k,\mathrm{U}_\alpha(1,1))$ is represented by elements of $\mathrm{H}^1(k(\alpha)/k,\mathrm{U}_\alpha(1,1))$. We express elements of $\mathrm{H}^1(k(\alpha)/k,\mathrm{U}_\alpha(1,1))$ as (h) where $h\in\mathrm{U}_\alpha(1,1)_{k(\alpha)}\cong\mathrm{GL}(2)_{k(\alpha)}$.

Then $(h) \to h^{-1}\Lambda$ induces a bijection $\mathrm{H}^1(k, \mathrm{U}_\alpha(1,1)) \cong \mathrm{GL}(2)_{k(\alpha)}\backslash Y_k$. Moreover, the map $\mathrm{H}^1(k, \mathrm{SU}_\alpha(2,1)) \to \mathrm{H}^1(k, \mathrm{U}_\alpha(1,1))$ is identified with

$$Y_k \ni H \to \begin{pmatrix} -(\det H)^{-1} & 0 \\ 0 & H \end{pmatrix} \in X_k.$$

Lemma 23.9. *Suppose H is a 2×2 Hermitian matrix and the matrices*

$$\begin{pmatrix} -(\det H)^{-1} & 0 \\ 0 & H \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & \Lambda \end{pmatrix}$$

are $\mathrm{SL}(3)_{k(\alpha)}$-equivalent. Then there exists $s \in k^\times$ such that H is $\mathrm{GL}(2)_{k(\alpha)}$-equivalent to

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

Proof. Note by an analogue of the Gram–Schmidt process, we can diagonalize H. So we may assume

$$H = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$$

where $a, b \in k^\times$. Let $\mathrm{N}_{k(\alpha)/k}$ be the norm of $k(\alpha)/k$. By assumption, there exists a non-zero vector $x = {}^t\begin{pmatrix} x_1 & x_2 & x_3 \end{pmatrix}$ such that

$$-\frac{1}{ab}\mathrm{N}_{k(\alpha)/k}(x_1) + a\mathrm{N}_{k(\alpha)/k}(x_2) + b\mathrm{N}_{k(\alpha)/k}(x_3) = 0.$$

Suppose $x_1 = 0$. Let $z = \frac{x_3}{x_2}$. Then $-\frac{b}{a} = \mathrm{N}_{k(\alpha)/k}(z)$. So

$$\begin{pmatrix} z & 0 \\ 0 & 1 \end{pmatrix} H^* \begin{pmatrix} z & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} -b & 0 \\ 0 & b \end{pmatrix}.$$

Let

$$A = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}^{-1} \begin{pmatrix} b^{-1} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}.$$

Then

$$A \begin{pmatrix} -b & 0 \\ 0 & b \end{pmatrix} A = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Suppose $x_1 \neq 0$. Let

$$z_1 = \frac{bx_3}{x_1}, \; z_2 = \frac{ax_2}{x_1}, \; A = \begin{pmatrix} bz_2^\sigma & -az_1^\sigma \\ z_1 & z_2 \end{pmatrix}.$$

Since $a\mathrm{N}_{k(\alpha)/k}(z_1) + b\mathrm{N}_{k(\alpha)/k}(z_2) = 1$, $\det A = 1$. It is easy to see

$$AH^*A = \begin{pmatrix} ab & 0 \\ 0 & 1 \end{pmatrix}.$$

□

Suppose $(h) \in \mathrm{H}^1(k, \mathrm{U}_\alpha(1,1))$ maps to the trivial element of $\mathrm{H}^1(k, G)$. Let H be the corresponding 2×2 Hermitian matrix. By Corollary 22.13, the Hermitian matrices

$$\begin{pmatrix} -(\det H)^{-1} & 0 \\ 0 & H \end{pmatrix}, \ \begin{pmatrix} 1 & 0 \\ 0 & \Lambda \end{pmatrix}$$

are $\mathrm{SL}(3)_{k(\alpha)}$-equivalent. Therefore, by Lemma 23.9, H is equivalent to a matrix of the form

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

Conversely, we show that elements of the above form correspond to orbits in V_k^{ss}. For $s \in k^\times$, let

$$H(s) = \begin{pmatrix} -s & 0 \\ 0 & 1 \end{pmatrix}, \ \overline{H}(s) = \begin{pmatrix} s^{-1} & 0 & 0 \\ 0 & -s & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

We put

$$h(s) = \begin{pmatrix} -s^{-1} & 0 \\ 0 & -1 \end{pmatrix}, \ \overline{h}(s) = \begin{pmatrix} s0 & 0 & \\ 0 & -s^{-1} & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

Then $(h(s)) \in \mathrm{H}^1(k, \mathrm{U}_\alpha(2,1))$ and $(\overline{h}(s)) \in \mathrm{H}^1(k, \mathrm{SU}_\alpha(2,1))$ correspond to $H(s)$ and $\overline{H}(s)$ respectively. We define

$$w(s) = v_1 \begin{pmatrix} 0 \\ 0 \\ \frac{1+s}{2} \\ \frac{1-s}{2} \\ 0 \\ 0 \\ 0 \end{pmatrix} + v_2 \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ \frac{1+s}{2} \\ -\frac{1-s}{2} \end{pmatrix}.$$

Definition 23.10. We define $w_\alpha(s) = g_\alpha w(s)$.

Lemma 23.11. *The class $(h(s)) \in \mathrm{H}^1(k, \mathrm{U}_\alpha(1,1))$ maps to the trivial element in $\mathrm{H}^1(k, G)$ and corresponds to the orbit of $w_\alpha(s)$.*

Proof. Let

$$\begin{aligned} A(s) &= \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} \frac{1}{2} & -\frac{1}{2} & 0 \\ \frac{1}{2} & \frac{1}{2} & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} -s^{-1} & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\ &\quad \times \begin{pmatrix} 1 & 1 & 0 \\ -1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} -s & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 0 & 1 \\ \frac{1+s}{2} & \frac{1-s^{-1}}{2} & 0 \\ \frac{1-s}{2} & \frac{-1-s^{-1}}{2} & 0 \end{pmatrix}. \end{aligned}$$

Then

$$A(s)\overline{H}(s)^{*}A(s) = \begin{pmatrix} 1 & 0 \\ 0 & \Lambda \end{pmatrix}.$$

Note that ${}^{*}A(s) = {}^{t}A(s)$. Also

$${}^{*}A(s)^{-1} = \begin{pmatrix} 0 & 0 & 1 \\ \frac{1+s^{-1}}{2} & \frac{1-s}{2} & 0 \\ \frac{1-s^{-1}}{2} & \frac{-1-s}{2} & 0 \end{pmatrix}.$$

Let

$$B_1(s) = \begin{pmatrix} 1 & 0 \\ 0 & \Lambda \end{pmatrix} {}^{*}A(s)^{-1} \begin{pmatrix} 1 & 0 \\ 0 & \Lambda \end{pmatrix},\ B_2(s) = \begin{pmatrix} s & 0 \\ 0 & 1 \end{pmatrix},$$

$$B(s) = \left(\begin{pmatrix} 1 & 0 & 0 \\ 0 & B_1(s) & 0 \\ 0 & 0 & {}^{*}B_1(s)^{-1} \end{pmatrix}, B_2(s) \right).$$

Then

$$\begin{aligned} B_1(s)^{-1} \begin{pmatrix} 1 & 0 \\ 0 & \Lambda \end{pmatrix} {}^{*}B_1(s)^{-1} \begin{pmatrix} 1 & 0 \\ 0 & \Lambda \end{pmatrix} &= \begin{pmatrix} 1 & 0 \\ 0 & \Lambda \end{pmatrix} {}^{*}A(s) \begin{pmatrix} 1 & 0 \\ 0 & \Lambda \end{pmatrix} A(s) \\ &= \begin{pmatrix} 1 & 0 \\ 0 & \Lambda \end{pmatrix} \overline{H}(s)^{-1} = \overline{h}(s), \\ B_2(s)^{-1}\tau_2 B_2(s)\tau_2 &= \begin{pmatrix} s^{-1} & 0 \\ 0 & s \end{pmatrix}. \end{aligned}$$

So,

$$B(s)^{-1}\tau B(s)^{\sigma}\tau = B(s)^{-1}\tau B(s)\tau = d(h(s)).$$

Therefore, $(h(s))$ maps to the trivial element and it corresponds to the orbit of

$$g_\alpha B(s) g_\alpha^{-1} w_\alpha = g_\alpha B(s) w.$$

Since

$$B_1(s) = \begin{pmatrix} 0 & 0 & -1 \\ \frac{1+s^{-1}}{2} & \frac{1-s}{2} & 0 \\ -\frac{1-s^{-1}}{2} & \frac{1+s}{2} & 0 \end{pmatrix},\ {}^{*}B_1(s)^{-1} = \begin{pmatrix} 0 & 0 & -1 \\ \frac{1+s}{2} & \frac{1-s^{-1}}{2} & 0 \\ -\frac{1-s}{2} & \frac{1+s^{-1}}{2} & 0 \end{pmatrix},$$

it is easy to see that $B(s)w = w(s)$. This proves the proposition. □

Now we are ready to determine the fiber structure of α_V

Theorem 23.12. (1) $\alpha_V^{-1}(k(\alpha)) \cong \mathfrak{S}_2 \backslash k^{\times} / \mathrm{N}_{k(\alpha)/k}(k(\alpha)^{\times})$.

(2) *If $s \in k^{\times}$, the corresponding orbit is $G_k w_\alpha(s)$, and the non-trivial element of $\mathfrak{S}_2$ acts by $w_\alpha(s) \to w_\alpha(s^{-1})$.*

(3) *If $x \in \alpha_V^{-1}(k(\alpha))$, $k(\alpha)$ is generated by roots of $F_x(v)$.*

Proof. We may regard the norm

$$\mathrm{N}_{k(\alpha)/k} : \mathrm{R}_{k(\alpha)/k} \to \mathrm{GL}(1)_k$$

as a k-homomorphism between k-groups. Let $T_\alpha = \mathrm{Ker}(\mathrm{N}_{k(\alpha)/k})$. We may regard T_α as the unitary group of dimension one. So as in the case of $\mathrm{SU}_\alpha(2,1), \mathrm{U}_\alpha(1,1)$,

$\mathrm{H}^1(k, T_\alpha)$ is represented by elements of $\mathrm{H}^1(k(\alpha)/k, T_\alpha)$. We may identify $T_{\alpha\, k(\alpha)} \cong k(\alpha)^\times$, and so we express cohomology classes as (s) where $s \in k(\alpha)^\times$. Since the action of σ induced from the k-structure of T_α is $x \to (x^\sigma)^{-1}$, the cocycle condition is equivalent to $s \in k^\times$ and $s_1, s_2 \in k^\times$ are equivalent if and only if $s_1 s_2^{-1} \in \mathrm{N}_{k(\alpha)/k}(k(\alpha)^\times)$. Therefore, $\mathrm{H}^1(k, T_\alpha) \cong k^\times/\mathrm{N}_{k(\alpha)/k}(k(\alpha)^\times)$. Moreover, the map $\mathrm{H}^1(k, \mathrm{U}_\alpha(1,1)) \to \mathrm{H}^1(k, T_\alpha)$ induced by the determinant may be identified with $(h) \to (\det h)$ for $h \in \mathrm{GL}(2)_{k(\alpha)} \cong \mathrm{U}_\alpha(1,1)_{k(\alpha)}$.

It is easy to see that if $s_1, s_2 \in k^\times$ and $s_1 s_2^{-1} \in \mathrm{N}_{k(\alpha)/k}(k(\alpha)^\times)$, then $H(s_1), H(s_2)$ are $\mathrm{GL}(2)_{k(\alpha)}$-equivalent. This implies that $(h(s_1)) = (h(s_2))$ in $\mathrm{H}^1(k, \mathrm{U}_\alpha(1,1))$. So the map

$$f : k^\times/\mathrm{N}_{k(\alpha)/k}(k(\alpha)^\times) \ni s \to (h(s)) \in \mathrm{Ker}(\mathrm{H}^1(k, \mathrm{U}_\alpha(1,1)) \to \mathrm{H}^1(k, G))$$

is well defined. By Lemmas 23.9, 23.11, f is surjective. Since the composition of f and

$$\mathrm{H}^1(k, \mathrm{U}_\alpha(1,1)) \to \mathrm{H}^1(k, T_\alpha) \cong k^\times/\mathrm{N}_{k(\alpha)/k}(k(\alpha)^\times)$$

is $s \to s^{-1}$, f is bijective.

Since $\tau d(h(s))\tau = d(h(s^{-1}))$, $\mathfrak{S}_2$ acts on

$$\mathrm{Ker}(\mathrm{H}^1(k, \mathrm{U}_\alpha(1,1)) \to \mathrm{H}^1(k, G)) \cong k^\times/\mathrm{N}_{k(\alpha)/k}(k(\alpha)^\times)$$

by $s \to s^{-1}$. This proves (1), (2).

By straightforward computations,

$$F_{w(s)}(v) = -s v_1 v_2.$$

So the roots of $F_{w_\alpha(s)}(v)$ are $\pm\alpha$. It is easy to see that if $g \in G_k$, the roots of $F_{g w_\alpha(s)}(v)$ and $F_{w_\alpha(s)}(v)$ generate the same field. This proves (3). $\square$

Finally we determine $G^\circ_{w_\alpha(s)}$.

Definition 23.13. We define $\mathrm{U}_\alpha(H(s)) = \{A \in \mathrm{GL}(2)_{k(\alpha)} \mid A H(s)^* A = \Lambda\}$.

We regard $\mathrm{U}_\alpha(H(s))$ as a group over k.

Proposition 23.14. *We have* $G^\circ_{w_\alpha(s)} \cong \mathrm{U}_\alpha(H(s)) \times \widetilde{T}$.

Proof. Let R be any k-algebra. We define $R(\alpha)$ and the action of σ on $R(\alpha)$ as in Proposition 22.9.

Any element in $G^\circ_{w_\alpha(s)\, R(\alpha)}$ can be expressed as a product of an element of $\widetilde{T}_R$ and

$$g_\alpha B(s) d(g) (g_\alpha B(s))^{-1},$$

where $g \in \mathrm{GL}(2)_{R(\alpha)}$.

Since $g_\alpha^\sigma = g_\alpha \tau$,

$$\begin{aligned}
(g_\alpha B(s) d(g) (g_\alpha B(s))^{-1})^\sigma &= g_\alpha^\sigma B(s) d(g^\sigma) (g_\alpha^\sigma B(s))^{-1} \\
&= g_\alpha \tau B(s) d(g) B(s)^{-1} \tau g_\alpha^{-1} \\
&= g_\alpha B(s) B(s)^{-1} \tau B(s) d(g) B(s)^{-1} \tau B(s) (g_\alpha B(s))^{-1}.
\end{aligned}$$

By straightforward computations using (23.15),

$$B(s)^{-1}\tau B(s) = \left(\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & \overline{H}(s)^{-1} \\ 0 & \overline{H}(s) & 0 \end{pmatrix}, \begin{pmatrix} 0 & -s^{-1} \\ -s & 0 \end{pmatrix} \right).$$

So,

$$B(s)^{-1}\tau B(s) d(g^{\sigma}) B(s)^{-1}\tau B(s) = d(H(s)^{-1*} g^{-1} H(s)). \tag{23.15}$$

This implies that

$$(g_{\alpha}B(s)d(g)(g_{\alpha}B(s))^{-1})^{\sigma} = g_{\alpha}B(s)d(H(s)^{-1*}g^{-1}H(s)))(g_{\alpha}B(s))^{-1}.$$

Therefore, this element belongs to $G^{\circ}_{w_{\alpha}(s)\,R}$ if and only if $g = H(s)^{-1*}g^{-1}H(s)$. This condition is equivalent to $g \in \mathrm{U}_{\alpha}(H(s))_R$. This proves the proposition again by Theorem 13.32. □

Exercise 23.16. Prove Proposition 23.2

References

[1] Altman, A., and S. Kleiman. *Introduction to Grothendieck duality*, volume 146 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, Heidelberg, New York, 1970.

[2] Borel, A. *Linear algebraic groups*. Springer-Verlag, Berlin, Heidelberg, New York, 2nd edition, 1991.

[3] Brioschi, F. Sulla risoluzione delle equazioni del quinto grado. In *Opere mathematiche*, volume I, pages 335–341. Ulrico Hoepi, Milano, 1904.

[4] De Contini, C., G. Lusztig, and C. Procesi. Homology of the zero set of a nilpotent vector field on a flag manifold. *J. Amer. Math. Soc.*, 1:15–34, 1988.

[5] Haboush, W.J. Reductive groups are geometrically reductive. *Ann. Math.*, 102:67–83, 1975.

[6] Hartshorne, R. *Algebraic geometry*, volume 52 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, Heidelberg, New York, 1977.

[7] Harvey, F.R. *Spinors and calibrations*. Academic Press, New York, San Francisco, London, 1990.

[8] Helgason, S. *Differential geometry, Lie groups, and symmetric spaces*. Academic Press, New York, San Francisco, London, 1978.

[9] Humphreys, J.E. *Linear algebraic groups*, volume 21 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, Heidelberg, New York, 1975.

[10] Igusa, J. On a certain class of prehomogeneous vector spaces. *J. of Pure and Applied Algebra*, 47:265–282, 1987.

[11] Kable, A.C., and A. Yukie. Prehomogeneous vector spaces and field extensions II. *Invent. Math.*, 130:315–344, 1997.

[12] Klein, F. *Lectures on the icosahedron and the solution of equations of the fifth degree*. Dover, New York, 1956.

[13] Kneser, M. *Lectures on Galois cohomology of classical groups*. Tata Lecture Note, Bombay, 1969.

[14] Lang, S. Algebraic groups over finite fields. *Amer. J. Math.*, 78:555–563, 1956.

[15] Lang, S. *Algebra*. Addison-Wesley, Reading, 3rd edition, 1993.

[16] Matsumura, H. *Commutative algebra*. Mathematics Lecture Note Series. Benjamin, Reading, 2nd edition, 1980.

[17] Mizuno, K. The conjugate classes of chevalley groups of type E_6. *J. Fac. Sci. Univ. Tokyo, Sect IA*, 24, 1977.

[18] Mizuno, K. The conjugate classes of unipotent elements of the chevalley groups E_7 and E_8. *Tokyo J. Math.*, 3, 1980.

[19] Mumford, D. *Lectures on curves on an algebraic surface*, volume 59 of *Annales of Mathematical Studies*. Princeton University Press, Princeton, New Jersey, 1966.

[20] Mumford, D. *The red book of varieties and schemes*, volume 1358 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, Heidelberg, New York, 1988.

[21] Mumford, D., J. Fogarty, and F. Kirwan. *Geometric invariant theory*. Springer-Verlag, Berlin, Heidelberg, New York, 3rd edition, 1994.

[22] Ochiai, H. Quotients of some prehomogeneous vector spaces. To appear in J. of Algebra.

[23] Sato, M., and T. Kimura. A classification of irreducible prehomogeneous vector spaces and their relative invariants. *Nagoya Math. J.*, 65:1–155, 1977.

[24] Serre, J.P. Extensions icosaédrique. In *Oeuvres*, volume III, pages 550–554. Springer-Verlag, Berlin, Heiderberg, New York, 1986.

[25] Springer, T.A. *Linear algebraic groups*. Birkhäuser, Boston, 2nd edition, 1998.

[26] Suzuki, M. *Group theory*, volume I. Springer-Verlag, Berlin, Heiderberg, New York, 1982.

[27] Van der Waerden, B. *History of algebra*. Springer-Verlag, Berlin, Heidelberg, New York, 1985.

[28] Waterloo Maple Software. *Maple V*. Waterloo Maple Inc., Waterloo, Ontario, 1994.

[29] Weil, A. *Adeles and algebraic groups*. Birkhäuser, Boston, 1982.

[30] Witte, D, A. Yukie, and R. Zierau. Prehomogeneous vector spaces and ergodic theory II. 352:1687–1708, 2000.

[31] Wright, D.J., and A. Yukie. Prehomogeneous vector spaces and field extensions. *Invent. Math.*, 110:283–314, 1992.

[32] Yukie, A. Prehomogeneous vector spaces and ergodic theory I. *Duke Math. J.*, 90:123–148, 1997.

[33] Yukie, A. Prehomogeneous vector spaces and field extensions III. *J. Number Theory*, 67:115–137, 1997.

[34] Yukie, A. Prehomogeneous vector spaces and ergodic theory III. *J. Number Theory*, 70:160–183, 1998.

Mathematical Institute, Tohoku University, Sendai Miyagi, 980–8578 Japan

E-mail address: `yukie@math.tohoku.ac.jp`, `http://www.math.tohoku.ac.jp/~yukie`