Lines on cubic surfaces, Witt invariants and Stiefel-Whitney classes

Eva Bayer-Fluckiger and Jean-Pierre Serre

February 2, 2023

Introduction

This paper is a contribution to the classical topic of the 27 lines of a cubic surface, and the Weyl group G of E_6.

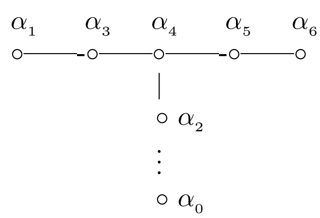
We show how the theory of "cohomological invariants" and "Witt invariants" can be used to clarify the structure of some of the quadratic forms and Stiefel-Whitney classes associated with the surface.

The first two sections recall well-known facts about several lattices associated with G. These lattices are G-stable, hence give rise to G-*quadratic forms* over any ground field k of characteristic $\neq 2$. Among these, the quadratic form of rank 7 has a geometric interpretation in terms of sheaf cohomology (Levine-Raksit [LR 18], cf. §7.3), and the rank 27 one is the trace form of the étale algebra of the 27 lines. The relations between these forms are discussed in §§3-6. The main tool of the proofs is the "splitting principle" for Witt invariants, as in [Se 03].

An appendix gives a formula for the Stiefel-Whitney classes of any linear representation of G, in terms of four basic invariants w_1, w_2, w_3, w_4. Here also, the splitting principle plays an essential role.

§1. Lattices associated with Weyl(E_6).

Let R be a root system of type E_6, with basis $\{\alpha_1, ..., \alpha_6\}$ numbered as in Bourbaki [Bo 68], §4.12:



where α_0 is the opposite of the highest root $\tilde{\alpha} = \alpha_1 + 2\alpha_2 + 2\alpha_3 + 3\alpha_4 + 2\alpha_5 + \alpha_6$. Let $\{\omega_1, ..., \omega_6\}$ be the corresponding fundamental weights. Let Q be the root lattice, which is generated by the α_i; its discriminant is 3. Its dual lattice P

is the weight lattice, with basis the ω_i. We have $Q \subset P$ and $(P : Q) = 3$; let $\mathrm{e} : P \to \mathbf{Z}/3\mathbf{Z}$ be the homomorphism with kernel Q such that $\mathrm{e}(\omega_1) = 1$. [This choice of e means that we have "oriented" the Dynkin diagram, by choosing one of its extremities.]

The scalar product on P will be denoted by $x\cdot y$; it takes values in $\frac{1}{3}\mathbf{Z}$; for instance $\omega_1\cdot\omega_1 = \frac{4}{3}$. We have $x\cdot y \in \mathbf{Z}$ if $x \in P, y \in Q$; if α is a root, we have $\alpha\cdot\alpha = 2$; we have $\alpha_i\cdot\omega_j = \delta_i^j$.

Let now L be the sublattice of $\mathbf{Z} \oplus P$ made up of the pairs (n, p) such that $n \equiv e(p) \pmod 3$. We define a scalar product q_L on L by the formula:

$$q_L(n, p; n', p') = nn'/3 - p\cdot p'.$$

Its values lie in $\mathbf{Z}$, and it is "$\mathbf{Z}$-unimodular", i.e., it gives an isomorphism of L onto its $\mathbf{Z}$-dual. Its signature over $\mathbf{R}$ is (1,6); its discriminant is 1.

[As we shall recall in §7, the lattice L is isomorphic to the Néron-Severi group of a smooth cubic surface, and the scalar product q_L corresponds to the intersection form.]

Note that Q embeds in L by $x \mapsto (0, x)$; this embedding transforms q_L into the opposite of the scalar product of Q. In particular, a root α, viewed as an element of L, is such that $q_L(\alpha, \alpha) = -2$.

The intersection of L with $\mathbf{Z}$ is generated by the element

$$h = (3, 0).$$

We have $q_L(h, h) = 3$ and $q_L(h, x) = 0$ if $x \in Q$.

The element $\omega_1' = (1, \omega_1)$ of L is such that $q_L(\omega_1', \omega_1') = -1$ and $q_L(h, \omega_1') = 1$; hence, if $\gamma = h - \omega_1'$, we have $q_L(\gamma, \gamma) = 0$.

[From the cubic surface point of view of §7, h corresponds to a plane section, and ω_1' corresponds to a line. The formula $q_L(h, h) = 3$ means that the surface has degree 3 and the formula $q_L(h, \omega_1') = 1$ means that a line and a plane intersect in one point.]

Let G be the Weyl group of R, i.e., the subgroup of $\mathrm{Aut}(Q \otimes \mathbf{R})$ generated by the reflections s_α associated with the roots $\alpha \in R$. The group G acts on P and Q. We extend its action to $\mathbf{Z} \oplus P$, and hence to L, by making it act trivially on the factor $\mathbf{Z}$; the scalar product q_L is invariant by G.

Proofs of the following theorem can be found in the standard texts on cubic surfaces (cf. [Ma 74], chap.IV, [De 80], [Do 12], chap.9).

Theorem 1.

(a) *An element α of L is a root if and only if $q_L(h, \alpha) = 0$ and $q_L(\alpha, \alpha) = -2$.*

(b) *Let Y be the set of $y \in L$ such that $q_L(h, y) = 1$ and $q_L(y, y) = -1$. This set has 27 elements, namely the pairs $(1, \omega)$ where ω belongs to the G-orbit of ω_1.*

(c) *If y, y' are two distinct elements of Y, then $q_L(y, y') = 0$ or 1.*

(d) *Let Ω be the graph with set of vertices Y, two vertices y, y' being adjacent if and only if $q_L(y, y') = 1$. The natural injection $G \to \mathrm{Aut}(\Omega)$ is bijective.*

Remark.

Since ω_1 is orthogonal to the α_i for $i \geqslant 2$, it is fixed by the group H generated by $(s_{\alpha_2}, ..., s_{\alpha_6})$, which is a Weyl group of type D_5, and has index 27 in G since $|G| = 2^7 \cdot 3^4 \cdot 5$ and $|H| = 2^7 \cdot 3 \cdot 5$. Hence $Y \simeq G/H \simeq \mathrm{Weyl}(\mathsf{E}_6)/\mathrm{Weyl}(\mathsf{D}_5)$.

§2. The 27-vertices graph Ω of Theorem 1.

2.1. *Properties of* Ω.

Every vertex belongs to 10 edges; every edge belongs to a unique triangle. Hence the number of vertices, edges, triangles, tetrahedra is: 27, 135, 45, 0.

If x and x' are two distinct and non adjacent vertices, the element $x - x'$ of L is a root: this follows from Theorem 1 (a) since $q_L(x - x', x - x') = -1 - 1 = -2$ and $q_L(h, x - x') = 0$. Every root is obtained in such a way by *six* disjoint couples (x_i, x'_i), $i = 1, ..., 6$. Every x_i is adjacent to every x'_j with $j \neq i$. The reflection defined by the root $\alpha = x_1 - x'_1 = ... = x_6 - x'_6$ permutes x_i and x'_i for every i, and fixes the other 15 vertices of Ω. The twelve vertices $x_1, ..., x_6, x'_1, ..., x'_6$ make up a *double-six*, see §2.2 below.

Let g be an element of G of order 2. Assume it is not a reflection. The number of the vertices fixed by g is then either 7 or 3. The first case occurs if and only if g is a product of two reflections.

2.2. *An explicit construction of* Ω.

Let us explain how one can describe the graph Ω in combinatorial terms, following Schläfli [Sch 58].

Let $X = \{1, 2, ..., 6\}$ and let X' be a copy of X; if $x \in X$, the corresponding point of X' is denoted by x'; let S be the set of all subsets of X with 2 elements. The graph Ω of Theorem 1 is isomorphic to the graph Ω_X whose set of vertices Y is the disjoint union $X \sqcup X' \sqcup S$, two vertices being adjacent in the following cases (and only in those):

$x \in X$ adjacent to $y' \in X' \iff x \neq y$,
$x \in X$ adjacent to $s \in S \iff x \in s$,
$x' \in X'$ adjacent to $s \in S \iff x \in s$,
$s_1 \in S$ adjacent to $s_2 \in S \iff s_1 \cap s_2 = \varnothing$.

Note that every element $\{x, y\}$ of S defines two edges: $x - y'$ and $y - x'$. There are no edges connecting vertices that are both in X, or both in X': the full subgraph of Ω with set of vertices the double-six $X \sqcup X'$ is a bipartite graph.

The group S_6 of permutations of X acts on Ω_X by *transport de structure*; an element of that group is a reflection in G if and only if it is a transposition. Let ε be the automorphism of order 2 of Ω_X which fixes the points of S and exchanges $x \in X$ with $x' \in X'$; that automorphism is also a reflection and it commutes with the action of S_6. We thus obtain an embedding of the group $\{1, \varepsilon\} \times \mathsf{S}_6$ into $\mathrm{Aut}(\Omega_X)$. From the Weyl group point of view, this corresponds to the embedding of $\mathrm{Weyl}(\mathsf{A}_1 \times \mathsf{A}_5) \simeq \{1, \varepsilon\} \times \mathsf{S}_6$ into $\mathrm{Weyl}(\mathsf{E}_6)$ defined by the inclusion $\mathsf{A}_1 \times \mathsf{A}_5 \to \mathsf{E}_6$.

§3. Involutions and cubes in $G = \mathrm{Weyl}(\mathsf{E}_6)$

3.1. *Finite Coxeter groups.*

We recall first a few definitions and results that apply to every finite Coxeter group G, and are easy to prove.

Let $g \in G$ be an *involution*, i.e. an element g such that $g^2 = 1$. The multiplicity of -1, as an eigenvalue of g in the Coxeter representation, is called the *degree* of g. An involution of degree 1 is a reflection.

A *cube* (cf. [Se 18]) of G is an abelian subgroup of G generated by reflections. It is elementary abelian of type (2,...,2). If C is a cube, the set S_C of the reflections contained in C is a basis of C (viewed as an $\mathbf{F}_2$-vector space), i.e. every element g of C can be written uniquely as $g = \prod_{s \in I} s$, where I is a subset of S_C, and we then have $\deg(g) = |I|$. If the rank of C is n, i.e. if $|S_C| = n$, then C contains a unique element of degree n, namely the product of all the $s \in S_C$; we call that element the *extremity* of C.

Every involution is the extremity of at least one cube.

From the root system point of view, a reflection corresponds to a pair of opposite roots, and a cube corresponds to a family of mutually orthogonal roots.

The following properties are valid for every Weyl group G, and they can easily be checked in the special case where G is of type E_6, see §3.2 below.

(3.1) *The involutions of G of maximal degree are G-conjugate.*

(3.2) *If G is simply-laced* [1]*, any two cubes of G with the same extremity are G-conjugate.*

(3.3) *If C is a maximal cube of G, the centralizer of C in G is equal to C.*

3.2. *The involutions of* Weyl(E_6).

From now on, we assume again that G is of type E_6, as in §1. Then:

(3.4) *The involutions have degree* $0, 1, 2, 3$ *or* 4.

(3.5) *Any two involutions of the same degree are G-conjugate.*

(3.6) *The number of involutions of degree* $0, 1, 2, 3, 4$ *is* $1, 36, 270, 540, 45$ *respectively.*

These three facts can be read off from the character table of G (see [ATLAS], pp.26-27, where our G is denoted by $G.2$). Another possible proof of (3.4) is to use the fact that every involution is contained in the centralizer of a reflection; that centralizer is a Weyl group of type $\mathsf{A}_1 \times \mathsf{A}_5$, and we only have to check that the involutions of Weyl(A_5) $\simeq \mathsf{S}_6$ have degree 0, 1, 2 or 3. The same argument proves (3.2) and (3.3), and also (3.9) below.

3.3. *The maximal cubes.*

By (3.3) and (3.4), we have

(3.7) *The maximal cubes of G have order 2^4, and they are G-conjugate.*

This implies:

[1] Recall that a Coxeter group is called *simply laced* if it is a product of Weyl groups of types $\mathsf{A}, \mathsf{D}, \mathsf{E}$; this is equivalent to asking that the product of two reflections has order 1, 2 or 3.

(3.8) *A maximal cube of* G *contains* $1, 4, 6, 4, 1$ *involutions of degrees* $0, 1, 2, 3, 4$ *respectively.*

(3.9) *The number of maximal cubes is* 135.

Examples.

a) The roots $(\alpha_2, \alpha_3, \alpha_5, \alpha_2+\alpha_3+\alpha_5+2\alpha_4)$ are mutually orthogonal. Hence they define a maximal cube. That cube is contained in the $\mathsf{D_4}$-subroot system of $\mathsf{E_6}$ with basis $(\alpha_2, \alpha_3, \alpha_4, \alpha_5)$. Another example is the cube defined by $(\alpha_1, \alpha_4, \alpha_6, \alpha_0)$.

b) In terms of the combinatorial description of §2, we may choose as maximal cube the group generated by the following four reflections: the automorphism ε and the three transpositions (12),(34),(56) in $\mathsf{S_6}$.

The normalizer of a maximal cube.

Let C be a maximal cube and let N be its normalizer in G. The group N/C acts on C, and hence permutes the four reflections of C. We thus get a homomorphism $N/C \to \mathsf{S_4}$.

(3.10) *The homomorphism* $N/C \to \mathsf{S_4}$ *is bijective.*

The injectivity follows from (3.3). The surjectivity can be proved, either by writing explicitly enough elements of N, or by counting: since the number of cubes is 135, and the order of G is 51840, the order of N is $51840/135 = 384$ and the order of N/C is $384/16 = 24$.

3.4. *Action of a maximal cube on the vertices of the graph* Ω.

Let C be a maximal cube of G. We shall later need the following information on the action of C on the set Y of Theorem 1 (the "twenty-seven lines").

Lemma 1. *The action of* C *on* Y *has three fixed points, and six orbits of order* 4; *these orbits are isomorphic to* $C/C_i,\ i = 1, ..., 6$, *where the* C_i *are the six cubes of order* 4 *contained in* C.

Proof. We use the description of Y of §2.2, as $Y = X \sqcup X' \sqcup S$, and we use for C the cube defined in Example b) of §3.3, namely the one generated by the reflections $\varepsilon, (12), (34), (56)$.

The action of C fixes the points $\{1, 2\}, \{3, 4\}, \{5, 6\}$ of S. The four points $\{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}$ of S make up an orbit isomorphic to C/C_1 where C_1 is the subgroup of C generated by ε and the transposition (56); there are two other similar orbits in S. In $X \sqcup X'$, the points $1, 1', 2, 2'$ make up an orbit isomorphic to C/C_4, where C_4 is generated by the transpositions (34) and (56); there are two other similar orbits.

§4. The G-quadratic forms q_6, q_7, q_{27} and the C-quadratic form q_4.

4.1. Let G be a group. A G*-bilinear form* over a commutative ring A is a bilinear form q over an A-module E, together with an A-linear action of G on E that fixes q.

In the above case, where $G = \mathrm{Weyl}(\mathsf{E_6})$, we have three such examples, with $A = \mathbf{Z}$, which are of rank 6, 7 and 27.

(i) The bilinear form $\alpha\cdot\beta$ on Q, cf. §1.

(ii) The bilinear form q_L on L.

(iii) The bilinear form q_Y on $\mathbf{Z}^Y$, given by $q_Y(e_y, e_{y'}) = \delta_y^{y'}$, where $(e_y)_{y\in Y}$ is the natural basis of $\mathbf{Z}^Y$.

In each case, the action of G is the obvious one, and the form is symmetric.

4.2. In what follows, k is a field of characteristic $\neq 2$. This will allow us to identify quadratic forms and symmetric bilinear forms, hence to write $q(x)$ instead of $q(x,x)$.

The base change $\mathbf{Z} \to k$ transforms the three G-bilinear forms above into G-quadratic forms over k. We denote them by q_6, q_7, q_{27}, but, for convenience, we divide by 2 the first one. In other words, we put

(4.1) $q_6(\alpha,\beta) = \frac{1}{2}\alpha.\beta$,

so that $q_6(\alpha,\alpha) = 1$ for every $\alpha \in R$.

The forms q_7 and q_{27} are non-degenerate. The same is true of q_6 provided $\mathrm{char}(k) \neq 3$.

With standard notation, we have an isomorphism of G-quadratic forms:

(4.2) $q_7 = \langle 3\rangle + \langle -2\rangle q_6$ *if* $\mathrm{char}(k) \neq 3$,

with G acting trivially on the rank 1 form $\langle 3\rangle$: this follows from the definition of q_L in §1.

There is no such simple formula for the G-form q_{27}, since the underlying linear representation of G is not a linear combination of exterior powers of the standard degree 6 representation.

4.3. *The C-quadratic form q_4.*

Let C be the maximal cube introduced in §3 from the combinatorial point of view. It contains four reflections $s_1, ..., s_4$, namely ε and the transpositions (12), (34) and (56). Let $\beta_1, ..., \beta_4$ be the roots (well-defined up to signs) corresponding to $s_1, ..., s_4$. Let V be the k-vector subspace of $Q \otimes k$ generated by the β_i, and let q_4 denote the restriction of q_6 to V; we have $q_4(\beta_i, \beta_j) = \delta_i^j$. The group C acts in a natural way on V; hence *q_4 is a C-quadratic form of rank* 4. The space V splits under the action of C into four 1-dimensional subspaces, orthogonal to each other. This gives a splitting of q_4 as

(4.3) $q_4 = r_1 + \cdots + r_4$,

where r_i is the C-quadratic form of rank 1 generated by β_i, on which s_i acts by -1 and the other s_j act trivially.

4.4. *Relations between the G-quadratic forms q_6, q_7, q_{27} and the C-quadratic form q_4.*

Any G-quadratic form q defines, by restriction of the action of the group, a C-quadratic form, which we denote by $q|C$. This applies in particular to q_6, q_7, q_{27}. The C-quadratic forms so obtained can all be expressed in terms of q_4. Namely

Theorem 2. *We have the following isomorphisms of C-quadratic forms*

(4.4) $q_6|C \;=\; q_4 + \langle 2,6\rangle \quad$ *if* $\operatorname{char}(k) \neq 3$,

(4.5) $q_7|C \;=\; \langle -2\rangle q_4 + \langle -1,-1,1\rangle$,

(4.6) $q_{27}|C = \lambda^2 q_4 + 3q_4 + 9$.

[Here, $\langle 2,6\rangle$ denotes the quadratic form $\langle 2\rangle + \langle 6\rangle$ with trivial action of C. Similarly, $3q_4$ means $\langle 1,1,1\rangle \otimes q_4 = q_4 + q_4 + q_4$ and 9 means the direct sum of nine copies of $\langle 1\rangle$ with trivial action of C. As for $\lambda^2 q_4$, it is the second exterior power of q_4, with the natural action of C, cf. [Se 03], §27.1.]

Proof of (4.4). This is a simple computation in the root lattice Q. With Bourbaki's notation ([Bo 68], §4.12), we may choose for the β_i of §4.3 the roots $\varepsilon_1+\varepsilon_2$, $\varepsilon_1-\varepsilon_2$, $\varepsilon_3+\varepsilon_4$, $\varepsilon_3-\varepsilon_4$. They are orthogonal to $\gamma = \varepsilon_5$ and $\delta = \varepsilon_8 - \varepsilon_6 - \varepsilon_7$. Moreover, γ and δ are orthogonal to each other, $\frac{1}{2}\gamma.\gamma = \frac{1}{2}$, and $\frac{1}{2}\delta.\delta = \frac{3}{2}$. Hence the orthogonal complement V' of V in $Q \otimes k$ is quadratically isomorphic to $\langle \frac{1}{2}, \frac{3}{2}\rangle = \langle 2,6\rangle$, and the action of C on V' is trivial.

Proof of (4.5). Let V'' be the orthogonal complement of V in $L \otimes k$. The restriction q_3 of q_L to V'' is a rank 3 quadratic form. We have $q_7|C = q_4|C + q_3$. The action of C on q_3 is trivial: indeed, the reflections which generate C fix every element orthogonal to the corresponding roots, hence fix V''. Since the discriminants of q_7 and q_4 are equal to 1, the same is true of q_3. By Lemma 1, C fixes three points of Y. Let y be one of them, and let $x = h - y$. Both x and y belong to V''. Since $q_7(h,h) = 3, q_7(h,y) = 1$ and $q_7(y,y) = -1$, we have $q_L(x,x) = 0$; moreover, x is nonzero since $q_7(x,h) = 2$. Hence q_3 is isotropic; it contains the 2-dimensional quadratic form $\langle -1,1\rangle$. Since its discriminant is 1, we have $q_3 = \langle -1,-1,1\rangle$, as claimed.

Proof of (4.6). Lemma 1 gives a decomposition of $q_{27}|C$ as the orthogonal sum of $\langle 1,1,1\rangle$ with trivial action, and six C-quadratic forms q'_i associated with the permutation sets C/C_i, where the C_i are the six cubes of order 4 contained in C. Consider for instance the case where C_i is generated by s_1, s_2, as in §4.3. In that case, one finds that $q'_i = 1 + r_3 + r_4 + r_3 r_4$, where the r_i are the C-quadratic forms of rank 1 occurring in (4.3). The other q'_i correspond similarly to the pairs $\{1,3\}, \{1,4\}, \{2,3\}, \{2,4\}, \{3,4\}$. Adding up gives

$$q_{27}|C = 3 + 6 + 3\ \Sigma_{n=1}^{4}\ r_n + \Sigma_{1 \leqslant m < n \leqslant 4}\ r_m r_n.$$

By (4.3), we have $\Sigma_{n=1}^{n=4}\ r_n = q_4$ and $\Sigma_{1 \leqslant m < n \leqslant 4}\ r_m r_n = \lambda^2 q_4$. We thus obtain (4.6).

Remark. One may also prove (4.4) by combining (4.5) and (4.2).

§5. Twists.

5.1. We keep the assumption that the characteristic of k is $\neq 2$. Let k_s be a separable closure of k. Let $\Gamma_k = \operatorname{Gal}(k_s/k)$ be the "absolute Galois group" of k. If $\varphi : \Gamma_k \to G$ is a continuous homomorphism, we may view φ as a 1-cocycle of Γ_k with values in the orthogonal group $\mathrm{O}_q(k_s)$, and use it to *twist* q, cf. [Se 64], chap.III, §1.2. We thus get a quadratic form q_φ over k.

[Let us recall an explicit construction of q_φ.

Let V be the k-vector space on which q is defined and G acts. On $V_s = k_s \otimes V$ there is a natural k_s-linear action of G (denoted by gx if $g \in G$ and $x \in V_s$) and also a natural semi-linear action of Γ_k (denoted by γx if $\gamma \in \Gamma_k$ and $x \in V_s$). These two actions commute. Hence they can be combined to define another semi-linear action of Γ_k on V_s, namely $\gamma \bullet x = \gamma(\varphi(\gamma)x)$.

Let V_φ be the set of $x \in V_s$ such that $\gamma \bullet x = x$ for every $\gamma \in \Gamma_k$. It is a k-vector subspace of V_s, and the natural map $k_s \otimes V_\varphi \to V_s$ is an isomorphism, i.e. V_s is a "k-form" of V, cf. [Bo 81], §10, prop.7. The form q extends to a k_s-quadratic form q_s of V_s, which is G-invariant and Γ_k-equivariant: $q_s(\gamma x) = \gamma q_s(x)$ for every $\gamma \in \Gamma_k$ and every $x \in V_s$.

If $x \in V_\varphi$, then, for every $\gamma \in \Gamma_k$, we have $x = \gamma(\varphi(\gamma)x)$, hence:

$$q_s(x) = \gamma(q_s(\varphi(\gamma)x)) = \gamma(q_s(x)),$$

which shows that $q_s(x)$ belongs to k. Hence the restriction of q_s to V_φ is a k-valued quadratic form on V_φ: it is the quadratic form q_φ we wanted to describe.

Remark. Let $x \in V$ be fixed under the action of $\varphi(\Gamma_k)$. Then x belongs to V_φ and $q_\varphi(x) = q(x)$. In particular:

(Iso) *If V contains a non-zero isotropic vector fixed under $\varphi(\Gamma_k)$, then q_φ is isotropic.*]

5.2. This construction applies in particular to the G-forms q_6, q_7, q_{27} above; we thus obtain the quadratic forms $q_{6,\varphi}, q_{7,\varphi}$ and $q_{27,\varphi}$. The forms $q_{7,\varphi}$ and $q_{27,\varphi}$ are non-degenerate. The form $q_{6,\varphi}$ is non-degenerate if $\mathrm{char}(k) \neq 3$.

Theorem 3. *The form $q_{7,\varphi}$ is isotropic.*

Proof. Assume first that Γ_k fixes a point y of Y. Then it also fixes $x = h - y$, and we have $q_7(x) = q_7(h) - 2q_7(h, y) + q_7(y) = 3 - 2 - 1 = 0$. By (Iso) above this shows that $q_{7,\varphi}$ is isotropic.

In the general case, since the set Y has odd order, the same is true of one of the orbits of Γ_k, i.e., there exists $y \in Y$ which is fixed by an open subgroup of Γ_k of odd index. That subgroup is of the form $\Gamma_{k'}$ with k'/k of odd degree. Hence $q_{7,\varphi}$ becomes isotropic after the base change $k \to k'$. By a well-known theorem of Springer ([Sp 52]), this implies that $q_{7,\varphi}$ is isotropic over k.

Corollary 1. *There exists a unique quadratic form $q_{5,\varphi}$ over k, of rank 5, such that*

(5.1) $q_{7,\varphi} = \langle -2\rangle q_{5,\varphi} + \langle 1, -1\rangle$.

(The factor $\langle -2\rangle$ is included in order to have formula (5.2) below.)

Corollary 2. *If* $\mathrm{char}(k) \neq 3$, *we have*:

(5.2) $q_{6,\varphi} = q_{5,\varphi} + \langle 6\rangle$.

(5.3) $q_{7,\varphi} = \langle -2\rangle q_{6,\varphi} + \langle 3\rangle$.

Formula (5.3) follows from (4.2). By combining it with (5.1), we get

(5.4) $\langle -2\rangle q_{6,\varphi} + \langle 3\rangle = \langle -2\rangle q_{5,\varphi} + \langle 3, -3\rangle$, *since* $\langle 1, -1\rangle = \langle 3, -3\rangle$,

hence $\langle -2\rangle q_{6,\varphi} = \langle -2\rangle q_{5,\varphi} + \langle -3\rangle$, which is equivalent to (5.2).

Remark. When $\mathrm{char}(k) \neq 3$, the quadratic form $q_{5,\varphi}$ is **not** the twist of a G-quadratic form of rank 5, if only because G has no non-trivial linear representation of degree 5.

5.3. *The quadratic form $q_{27,\varphi}$.*

This form may be viewed as a *trace form.* Indeed, the group Γ_k acts on Y via φ, and this defines an étale algebra of rank 27 over k whose trace form is $q_{27,\varphi}$, cf. e.g., [BS 94], §1.

It can be expressed in terms of $q_{5,\varphi}$, namely:

Theorem 4. *We have*

(5.5) $q_{27,\varphi} = \lambda^2 q_{5,\varphi} \ + \ \langle 1,2\rangle q_{5,\varphi} \ + 6 + \langle 2\rangle.$

The proof will be given in §6, using the method of [Se 03] (extended in [Se 18] to all Weyl groups): checking first the case where $\varphi : \Gamma_k \to G$ takes values in a maximal cube, and then showing that this special case implies the general one.

Remark.

Here also, formula (5.5) can be rewritten in terms of $q_{6,\varphi}$ and $q_{7,\varphi}$. One finds

(5.6) $q_{27,\varphi} = \lambda^2 q_{6,\varphi} \ + \ \langle 3\rangle q_{6,\varphi} \ + \ 6,$ if $\mathrm{char}(k) \neq 3.$

and

(5.7) $q_{27,\varphi} = \lambda^2 q_{7,\varphi} \ + \ (\langle -1\rangle - \langle 2\rangle) q_{7,\varphi} \ + \ 7 - \langle -2\rangle.$

§6. Proof of Theorem 4.

6.1. *Proof of Theorem 4 when φ maps Γ_k into the cube C.*

In that case, we may use φ to twist the C-quadratic form q_4 of §4.3, and we obtain a quadratic form $q_{4,\varphi}$. Formulas (4.5) and (4.6) imply

(6.1) $q_{7,\varphi} = \langle -2\rangle q_{4,\varphi} + \langle -1,-1,1\rangle.$

and

(6.2) $q_{27,\varphi} = \lambda^2 q_{4,\varphi} + 3q_{4,\varphi} + 9.$

Since $3 = \langle 1,1,1\rangle = \langle 1,2,2\rangle$, we may rewrite (6.2) as

(6.3) $q_{27,\varphi} = \lambda^2 q_{4,\varphi} + \langle 1,2,2\rangle q_{4,\varphi} + 9,$

By (5.1), we have

(6.4) $q_{7,\varphi} = \langle -2\rangle q_{5,\varphi} + \langle 1,-1\rangle.$

Comparing (6.1) and (6.4) gives

(6.5) $q_{5,\varphi} = q_{4,\varphi} + \langle 2\rangle,$

hence

(6.6) $\lambda^2 q_{5,\varphi} = \lambda^2 q_{4,\varphi} + \langle 2\rangle q_{4,\varphi}.$

Using (6.4) and (6.5) we may rewrite (6.3) as

(6.7)
$$\begin{aligned} q_{27,\varphi} &= \lambda^2 q_{5,\varphi} - \langle 2\rangle q_{4,\varphi} + \langle 1,2,2\rangle q_{4,\varphi} + 9 \\ &= \lambda^2 q_{5,\varphi} + \langle 1,2\rangle q_{4,\varphi} + 9 \end{aligned}$$

$$= \lambda^2 q_{5,\varphi} + \langle 1,2\rangle(q_{5,\varphi} - \langle 2\rangle) + 9$$
$$= \lambda^2 q_{5,\varphi} + \langle 1,2\rangle q_{5,\varphi} + 9 - \langle 1,2\rangle$$
$$= \lambda^2 q_{5,\varphi} + \langle 1,2\rangle q_{5,\varphi} + 6 + \langle 2\rangle,$$

which is (5.5).

6.2. *The Witt-Grothendieck invariants defined by* $q_4, q_5, q_6, q_7, q_{27}$.

(In what follows, we use freely the definitions and the elementary properties of the "invariants" of a finite group given in the first sections of [Se 03].)

The cohomology set $H^1(k, G)$ of all G-torsors over k may be identified with the conjugation classes of continuous homomorphisms $\varphi : \Gamma_k \to G$, cf. e.g. [BS 94], §1. Since the Galois twists defined by conjugate homomorphisms are isomorphic, we may interpret the maps $\varphi \mapsto q_{5,\varphi}, q_{7,\varphi}, q_{27,\varphi}$ as maps of $H^1(k, G)$ into the Witt-Grothendieck ring $WGr(k)$ of k; let us denote them by $a_{5,k}, a_{7,k}, a_{27,k}$. This construction applies to all the field extensions K of k, and we thus obtain three Witt-Grothendieck invariants a_5, a_7, a_{27} of G, i.e. three elements of the group $\mathrm{Inv}_k(G, WGr)$, cf. [Se 03], §27.1. We also get an invariant a_4 by $a_4 = a_5 - \langle 2\rangle$; note that this invariant is not in general *effective*: its values cannot always be represented by quadratic forms of degree 4 (but they can be if φ takes values in C). Moreover, when $\mathrm{char}(k) \neq 3$, we have the invariant $a_6 = a_7 - \langle 6\rangle$.

In what follows, we mainly use a_4.

For every subgroup H of G, there is a natural restriction map

$$\mathrm{Inv}_k(G, WGr) \to \mathrm{Inv}_k(H, WGr),$$

cf. [Se 03], §13.

6.3. *The splitting principle.*

A basic fact about such invariants is:

Theorem 5. *Let $\mathcal{G}$ be a Weyl group, and let $a \in \mathrm{Inv}_k(\mathcal{G}, WGr)$. Assume that the restriction of a to every cube of $\mathcal{G}$ is* 0. *Then $a = 0$.*

This is proved in [Se 03], §29, when $\mathcal{G}$ is a symmetric group (for Witt invariants - the case of the Witt-Grothendieck invariants follows). The proof for an arbitrary Weyl group is similar; it has not been published yet, but we hope it will soon be.

In the Appendix, we shall need the analogue of Theorem 5 for the case of the group $\mathrm{Inv}_k(\mathcal{G})$ of the *cohomological invariants* mod 2 of $\mathcal{G}$ (i.e. the group $\mathrm{Inv}_k(\mathcal{G}, \mathbf{Z}/2\mathbf{Z})$ of [Se 03], §4.1):

Theorem 6. *Let a be an element of* $\mathrm{Inv}_k(\mathcal{G})$. *If the restriction of a to every cube of $\mathcal{G}$ is* 0, *then $a = 0$.*

A proof can be found in [GH 19], under the assumption that $\mathrm{char}(k)$ does not divide $|\mathcal{G}|$; that assumption (which, for Weyl(E_6), would eliminate characteristics 3 and 5) is not necessary, as one sees by the method sketched in [Se 18].

6.4. *End of the proof of Theorem 4.*

We apply Theorem 5 with $\mathcal{G} = G$, and with $a \in \mathrm{Inv}_k(G, WGr)$ defined by

(6.8) $a = a_{27} - \lambda^2 a_5 - \langle 1,2\rangle a_5 - 6 - \langle 2\rangle$.

By §6.1, the restriction of a to C is 0. Since every cube C' of G is conjugate to a subgroup of C, the restriction of a to C' is 0. By Theorem 4, this implies $a = 0$; hence (5.5).

Remarks.

1. The same method can be used to describe the structure of $\mathrm{Inv}_k(G, WGr)$. The result is simpler to state for the Witt invariant ring $\mathrm{Inv}_k(G, W)$: this ring is a free $W(k)$-module with basis the five elements $\lambda^i a_4, i = 0, ..., 4$ (or, equivalently, the $\lambda^i a_5$ or the $\lambda^i a_7, i = 0, ..., 4$).

2. Let T be a finite G-set, and let $\varphi : \Gamma_k \to G$, be as above; we thus have an action of Γ_k on T, hence an étale k-algebra $E_{T,\varphi}$. (For the dictionary "finite Γ_k -set $\Longleftrightarrow$ étale k-algebras", see [Bo 68], chap.V, §10.10 and [KMRT 98], §18.A.)

Let $q_{T,\varphi}$ be its trace form. It follows from Remark 1 above that we have

$$(6.9)\quad q_{T,\varphi} = t_0 + t_1 q_{4,\varphi} + t_2\lambda^2 q_{4,\varphi} + t_3\lambda^3 q_{4,\varphi} + t_4\lambda^4 q_{4,\varphi},$$

where the t_i are quadratic forms of type either $\langle 1, ..., 1, 1\rangle$ or $\langle 1, ..., 1, 2\rangle$. (Note that $\langle 2, 2\rangle = \langle 1, 1\rangle$, so that there is no point in having more $\langle 2\rangle$'s.) All what is needed is the decomposition of T with respect to the action of C; the orbits of order 2 or 8 are the ones which introduce a factor $\langle 2\rangle$.

A typical example is when T is the set of the 45 triangles of Ω (they correspond to the tritangent planes in the cubic surface interpretation of §7). One finds that C has one fixed point, six orbits of order 2 and four orbits of order 8. By looking at the structure of these orbits, one gets:

(6.10) $q_{T,\varphi} = 11 + \langle 1,1,2\rangle q_{4,\varphi} + \langle 1,1,2\rangle\lambda^2 q_{4,\varphi} + \langle 2\rangle\lambda^3 q_{4,\varphi}$.

This formula becomes slightly simpler when expressed in terms of $q_{5,\varphi}$:

(6.11) $q_{T,\varphi} = 9 + \langle 2\rangle + q_{5,\varphi} + \langle 1,2\rangle\lambda^2 q_{5,\varphi} + \langle 2\rangle\lambda^3 q_{5,\varphi}$.

§7. The cubic surfaces and their 27 lines.

7.1. In this subsection, we drop our assumptions on the ground field k, i.e., we allow $\mathrm{char}(k) = 2$.

Let $V \subset \mathbf{P}_3$ be a smooth cubic surface over k. It is well known that, over a suitable field extension of k, it contains 27 lines, cf. [Ha 77], chap.5.4, [Do 12], chap.9 and [Ma 74], chap.IV. These lines are rational over k_s, cf. [Co 88], Theorem 1 and [KW 17], Corollary 53. Let L_V be the Néron-Severi group of V over k_s, equipped with the symmetric $\mathbf{Z}$-bilinear form "intersection product". It is a lattice of rank 7, and it contains the following elements

(a) The class h_V of the hyperplane sections of V; we have $h_V \cdot h_V = 3$.

(b) The set Y_V of the classes of the 27 lines; if $y \in Y_V$, we have $y\cdot y = -1$ and $h_V \cdot y = 1$; if $y' \in Y_V$ is distinct from y, we have $y \cdot y' = 0$ if the corresponding lines are disjoint, and $y \cdot y' = 1$ if they meet.

It is well known that the triple $T_V = (L_V, h_V$, intersection product) is isomorphic to the triple $T = (L, h, q_L)$ of §1; see the above references. More precisely, let Θ_V denote the set of isomorphisms $\theta : T_V \to T$. We have a left action of $G = \mathrm{Weyl}(\mathsf{E}_6) = \mathrm{Aut}(\mathsf{T})$ on Θ_V, by $g\theta = g \circ \theta$; that action is free, and transitive. On the other hand, we have a right action of Γ_k on Θ_V, by $\theta\gamma = \theta \circ \gamma$, for $\gamma \in \Gamma_k$. These two actions commute. We may view such a situation in the following equivalent ways (cf. [BS 94], §1.3):

(7.1) The action of Γ_k on Θ_V defines an étale algebra E_V, on which G acts, and one hence gets a *G-Galois algebra over k*.

(7.2) The k-finite étale scheme Spec E_V is a G-torsor over k, whose set of k_s-points is Θ_V.

(7.3) If we choose a point θ of Θ_V, for every $\gamma \in \Gamma_k$ there is a unique element $\varphi(\gamma)$ of G such that $\varphi(\gamma)\theta = \theta\gamma$, and the map $\gamma \mapsto \varphi(\gamma)$ is a continuous homomorphism $\varphi : \Gamma_k \to G$. Changing the choice of θ replaces φ by a conjugate.

Each of these points of view shows that *we have associated with V a G-torsor over k*, i.e. an element e_V of $H^1(k, G)$.

7.2. Assume again that $\mathrm{char}(k) \neq 2$. As in §5, we may define the virtual quadratic form $q_{4,\varphi}$ and the quadratic forms $q_{5,\varphi}, q_{7,\varphi}, q_{27,\varphi}$; if $\mathrm{char}(k) \neq 3$, we also have $q_{6,\varphi}$. Since these forms depend only on V, we may denote them by $q_{4,V}, q_{5,V}, q_{7,V}, q_{27,V}$ and $q_{6,V}$. By (5.5), (5.5) and (5.6), we have

Theorem 7.

(7.4) $\quad q_{27,V} = \lambda^2 q_{5,V} \ + \ \langle 1,2\rangle q_{5,V} \ + \ 6 + \langle 2\rangle.$

(7.5) $\quad q_{27,V} = \lambda^2 q_{6,V} \ + \ \langle 3\rangle q_{6,V} \ + \ 6,$ *if* $\mathrm{char}(k) \neq 3.$

(7.6) $\quad q_{27,V} = \lambda^2 q_{7,V} \ + \ (\langle -1\rangle - \langle 2\rangle) q_{7,V} \ + \ 7 - \ \langle -2\rangle.$

7.3. *Interpretations of $q_{7,V}$ and $q_{27,V}$.*

(a) *The case of $q_{7,V}$.*

Let V_s be the k_s-variety deduced from V by the base change $k \to k_s$. The Néron-Severi group L_V is equal to the divisor class group $H^1(V_s, \mathcal{O}^\times_{V_s})$. The map $f \mapsto df/f$ gives a homomorphism $\mathcal{O}^\times_{V_s} \to \Omega^1_{V_s}$; we thus get a homomorphism $L_V \to H^1(V_s, \Omega^1_{V_s})$, hence also $k_s \otimes_{\mathbf{Z}} L_V \to H^1(V_s, \Omega^1_{V_s})$. Since V_s is a smooth rational surface, this map is an isomorphism [2]. Moreover, it transforms the intersection form on $k_s \otimes_{\mathbf{Z}} L_V$ into the cup-product:

$$H^1(V_s, \Omega^1_{V_s}) \otimes H^1(V_s, \Omega^1_{V_s}) \to H^2(V_s, \Omega^2_{V_s}) \simeq k_s.$$

By descent, this gives an interpretation of $q_{7,V}$ as the quadratic space $H^1(V, \Omega^1_V)$ endowed with its natural cup-product form. (This is almost the same as the Euler characteristic $\chi(V/k)$ in the sense of Levine and Raskit, cf. [LR 18], theorem 3.1; the only difference is that they incorporate the 1 dimensional quadratic spaces $H^0(V, \Omega^0_V) \simeq k$ and $H^2(V, \Omega^2_V) \simeq k$ in the definition of $\chi(V/k)$.)

[2] This may be proved by showing that, if it is true for V, it is also true for its blow up at any point. One needs to know that the dimension of $H^1(V_s, \Omega^1_{V_s})$ goes up by one, cf. [Ha 77], Chap.V, Exerc.5.3.

(b) *The case of* $q_{27,V}$.

That quadratic form is the trace form of the étale algebra A_{27} defined by the Γ_k-set Y_V of the 27 lines. One may also view A_{27} as the subalgebra of the G-Galois algebra E_V of (7.1.1) which is fixed by the subgroup $H \simeq \mathrm{Weyl}(\mathsf{D}_5)$ defined at the end of §1.

7.4. *Questions.*

It would be interesting to be able to compute the quadratic form $q_{7,V}$ (and hence also $q_{27,V}$) directly from the knowledge of a cubic equation F defining V; this is probably possible (with computer help) from the interpretation of $q_{7,V}$ given in §7.3(a).

A related question is whether the invariants $w_1, ..., w_4$ of the Appendix satisfy any other identities than those listed at the end of §A.3. The difficulty is that not every $\varphi : \Gamma_k \to \mathsf{E}_6$ comes from a cubic surface.

Appendix - Stiefel-Whitney classes

The aim of this Appendix is to show how to compute the Stiefel-Whitney classes of the linear representations of G, and also those of the quadratic forms $q_{7,\varphi}, q_{27,\varphi}, ...$ of §5. For instance (cf. §A.4, example 2), we have:

$$w_{\rho_{27}} = \ (1 + ew_1 + w_2)(1 + e^3 w_1 + w_4)(1 + e^6 w_2 + e^4 w_4),$$

where $e = (-1)$ is the class of -1 in $H^1(k)$, and $w_1, ..., w_4$ are the basic cohomological invariants of G, cf. Theorem 8.

We start with recalling some basic definitions (cf. [Ka 84] and [GKT 89]).

A.1. *Stiefel-Whitney classes of real linear representations of G : the group cohomology point of view.*

Here G is any finite group; we denote by $H(G)$ its cohomology with coefficients in $\mathbf{F}_2$.

Let $\rho : G \to \mathrm{GL}_n(\mathbf{R})$ be a real linear representation of G of dimension n. Let BG and $B\mathrm{GL}_n(\mathbf{R})$ be the classifying spaces of G and $\mathrm{GL}_n(\mathbf{R})$ in the sense of algebraic topology (cf. [Bo 55], §8) - they are well-defined up to homotopy equivalence. The homomorphism ρ induces a map: $BG \to B\mathrm{GL}_n(\mathbf{R})$, hence also a map $\rho^* : H(B\mathrm{GL}_n(\mathbf{R})) \to H(BG)$, where the letter H means cohomology mod 2. Since $\mathrm{O}_n(\mathbf{R})$ is a maximal compact subgroup of $\mathrm{GL}_n(\mathbf{R})$, we may identify $H(B\mathrm{GL}_n(\mathbf{R}))$ with $H(B\mathrm{O}_n(\mathbf{R}))$ which is known to be a polynomial algebra $\mathbf{F}_2[w_1, ..., w_n]$ in the *Stiefel-Whitney classes* $w_1, ..., w_n$, of degrees $1, ..., n$, cf. [Bo 55], §9. Let $w_i(\rho) \in H^i(G)$ be the images of the w_i by ρ^*; we put $w_i(\rho) = 1$ if $i = 0$ and $w_i(\rho) = 0$ for $i > n$. The *total Stiefel-Whitney class of* ρ is

$$w(\rho) = \sum_{n \geqslant 0} w_i(\rho).$$

These classes only depend on the equivalence class of ρ, i.e. of the character χ_ρ of ρ. They enjoy the same properties as the standard Stiefel-Whitney classes. For instance:

(A1) $w(\rho_1 \oplus \rho_2) = w(\rho_1) \cdot w(\rho_2)$.

Suppose $n = 1$, in which case $\rho(G)$ is contained in $\{\pm 1\}$, i.e. ρ may be identified with an element $[\rho]$ of $H^1(G) = \mathrm{Hom}(G, \mathbf{Z}/2\mathbf{Z})$. We then have:

(A2) $w(\rho) = 1 + [\rho]$.

Note that (A1) and (A2) give a way to compute $w(\rho)$ for every ρ when G is an elementary abelian 2-group (for instance a cube), since ρ is then a direct sum of one-dimensional representations.

In dimension < 4, we have:

(A3) $w_1(\rho) = [\det(\rho)]$,

(A4) $w_2(\rho)$ is the obstruction to lifting ρ to $\widetilde{\mathrm{GL}_n(\mathbf{R})}$, where $\widetilde{\mathrm{GL}_n(\mathbf{R})}$ is the central extension of $\mathrm{GL}_n(\mathbf{R})$ by $\{\pm 1\}$ characterized by the fact that a reflection (resp. a product of two commuting distinct reflections) of $\mathrm{GL}_n(\mathbf{R})$ lifts to an element of order 2 (resp. of order 4) of $\widetilde{\mathrm{GL}_n(\mathbf{R})}$.

(A5) $w_3(\rho) = w_1(\rho) \cdot w_2(\rho) \ + \ \mathrm{Sq}^1 w_2(\rho)$,

where Sq^1 is the first Steenrod square operator (i.e. the Bockstein map).

Remark. The definitions above use topology. The reader will find in [GKT 89] a purely algebraic definition of the $w_i(\rho)$, based on functoriality, and properties (A1), (A2), (A4).

A.2. *Galois Stiefel-Whitney classes.*

We keep the notation above.

Let us first recall a general construction. Let k be a field of characteristic $\neq 2$, and let $t \in H^1(k, G)$ be a G-torsor over k. Let $\varphi_t : \Gamma_k \to G$ be a homomorphism corresponding to t.

Let z be an element of $H(G)$. With $t \in H^1(k, G)$ we associate $z_t = \varphi_t^*(z) \in H(k)$. This defines a map $H^1(k, G) \to H(k)$, and, when this construction is applied to all the extensions of k, it gives a *cohomological invariant* of G mod 2, i.e. an element of $\mathrm{Inv}_k(G, \mathbf{Z}/2\mathbf{Z})$, cf. [Se 03], §, Chap.VI. The map

$$H(G) \to \mathrm{Inv}_k(G, \mathbf{Z}/2\mathbf{Z})$$

so defined is one of the main methods for constructing cohomological invariants.

If we apply this to the cohomology class $w_i(\rho) \in H^i(G)$, we obtain an element of $\mathrm{Inv}_k^i(G, \mathbf{Z}/2\mathbf{Z})$, which we write $w_{i,\rho}$; one may call it the *i-th Galois Stiefel-Whitney invariant.* The total invariant is:

(A6) $w_\rho = \sum_{i \geqslant 0} w_{i,\rho}$.

Example. When $G = \mathsf{S}_n$ and ρ is the standard representation of degree n of G, the $w_{i,\rho}$ are the same as the $w_i^{\mathrm{g}al}$ of [Se 03], §25.1.

Remark. The algebraic properties of the $w_{i,\rho}$ are somewhat simpler than those of the $w_i(\rho)$. For instance, property (A5) becomes:

(A5)′ $w_{3,\rho} = w_{1,\rho} w_{2,\rho}$,

since Sq^1 vanishes on $H^2(k)$. More generally, one has ([Ka 84], Corollary to Theorem 4):

(A6)′ $w_\rho = (1 + w_{1,\rho})(1 + w_{2,\rho})(1 + w_{4,\rho})(1 + w_{8,\rho}) \cdots$

A.3. *The case* $G = \mathrm{Weyl}(\mathsf{E}_6)$. *Preliminaries.*

From now on, we assume that $G = \mathrm{Weyl}(\mathsf{E}_6)$. Let ρ_6 be the natural 6-dimensional representation of G, and let $w_i = w_{i,\rho_6} \in \mathrm{Inv}_k^i(G, \mathbf{Z}/2\mathbf{Z})$ be its Stiefel-Whitney invariants. We have:

(A7) $w_i = 0$ *for* $i > 4$.

Proof. Let C be a maximal cube of G. The restriction $\rho_6|C$ of ρ_6 to C is the direct sum of the standard representation ρ_4 of C with a trivial 2-dimensional representation. By (A1), we have

(A8) $w_i(\rho_6|C) = w_i(\rho_4)$ *for every* i,

hence $w_i(\rho_6|C) = 0$ for $i > 4$. This shows that the restrictions to C of the $w_i, i > 4$, are 0. By Theorem 6, this implies (A7).

Theorem 8. *The classes* $\{w_0, w_1, w_2, w_3, w_4\}$ *make up a basis of the* $H(k)$-*module* $\mathrm{Inv}_k(G, \mathbf{Z}/2\mathbf{Z})$.

Proof. Let S be the set of the four reflections belonging to C. By [Se 03], §16.4, the $H(k)$-algebra $\mathrm{Inv}_k(C, \mathbf{Z}/2\mathbf{Z})$ has a natural basis a_I indexed by the subsets I of S. The normalizer N of C acts on C and hence on $\mathrm{Inv}_k(C, \mathbf{Z}/2\mathbf{Z})$; it follows from (3.10) that it acts transitively on the a_I with the same $|I|$. Let us denote by $\mathrm{Inv}_k(C, \mathbf{Z}/2\mathbf{Z})^{\mathrm{sym}}$ the subalgebra of $\mathrm{Inv}_k(C, \mathbf{Z}/2\mathbf{Z})$ made up of the elements which are fixed under that action. If $0 \leqslant i \leqslant 4$, let $a_i = \sum_{|I|=i} a_I$. The a_i make up an $H(k)$-basis of $\mathrm{Inv}_k(C, \mathbf{Z}/2\mathbf{Z})^{\mathrm{sym}}$. On the other hand, we have:

(A9) $a_i = w_i|C$.

The restriction map $\mathrm{Inv}_k(G, \mathbf{Z}/2\mathbf{Z}) \to \mathrm{Inv}_k(C, \mathbf{Z}/2\mathbf{Z})$ takes its values in $\mathrm{Inv}_k(C, \mathbf{Z}/2\mathbf{Z})^{\mathrm{sym}}$. It is injective by Theorem 6, and it is surjective by (A9). Hence it is an isomorphism; this proves Theorem 8.

Remark. The proof above is essentially the same as the one used in [Se 03], §25.5 to determine $\mathrm{Inv}_k(\mathsf{S}_n)$.

Multiplication formulas for the w_i. Before giving these formulas, one more notation is necessary:

If α is an element of $k^\times$, we denote by $(\alpha)_k$, or simply (α), the corresponding element of $H^1(k) = k^\times/k^{\times 2}$. The case $\alpha = -1$ will be especially useful; we write $(-1)_k$ as e_k, or simply e. We have $x^2 = xe$ for every $x \in H^1(k)$, or equivalently $x(-x) = 0$. More generally, it follows from Milnor's conjecture (now a theorem) that $x^2 = xe^d$ for every $x \in H^d(k)$.

With this notation, we have:

$w_i^2 = w_i e^i \ (i \geqslant 0), w_1 w_2 = w_3, w_1 w_3 = w_3 e, w_1 w_4 = 0, w_2 w_4 = 0, w_3 w_4 = 0.$

A.4. *Statement of the theorem.*

Let ρ be a real representation of G. Our aim is to give an explicit formula for the total Stiefel-Whitney class w_ρ in terms of the character χ_ρ of ρ. Since w_ρ depends only on the restriction of ρ to C, it will be enough to know the values of χ_ρ on the five classes of involutions of G. For $i = 0, ..., 4$, let g_i be an involution of degree i, and let m_i be the multiplicity of -1 as an eigenvalue of $\rho(g_i)$. We have $m_0 = 0$ and:

(A10) $m_i = \frac{1}{2}(\chi_\rho(g_0) - \chi_\rho(g_i))$.

Example 1. If $\rho = \rho_6$, then $m_i = i$ for every i.

Example 2. If ρ is the permutation representation ρ_{27} of degree 27 given by the action of G on the set Y, the m_i are equal to 0, 6, 10, 12, 12. This follows from Lemma 1 of §3.4.

Example 3. For the representation ρ_{45} of degree 45 given by the action of G on the set of triangles, the m_i are equal to 0, 15, 20, 19, 16. This follows from the decomposition of ρ_{45} in irreducible factors: $1 + \rho_{20} + \rho_{24}$, given in [ATLAS 85], p.26, combined with the values of the characters of ρ_{20} and ρ_{24} given on the next page.

Theorem 9. $w_\rho = 1 + w_1 p_1(e) + w_2 p_2(e) + w_3 p_3(e) + w_4 p_4(e)$,
where the polynomials $p_i(x) \in \mathbf{F}_2[x]$ *are characterized by the equations*:

(A11) $x \cdot p_1(x) = 1 + (1+x)^{m_1}$,
(A12) $x^2 p_2(x) = 1 + (1+x)^{m_2}$,
(A13) $x^3 p_3(x) = 1 + x \cdot p_1(x) + x^2 p_2(x) + (1+x)^{m_3}$,
(A14) $x^4 p_4(x) = 1 + (1+x)^{m_4}$.

The proof will be given in §A.6.

Remark. A priori it is not obvious that the elements p_i of $\mathbf{F}_2[x, x^{-1}]$ defined by the equations (A12), (A13) and (A14) are polynomials. It will be a consequence of the proof. It can also be deduced from the following congruence properties of the m_i:

(A15) $m_2 \equiv 0 \pmod 2$; $m_3 \equiv m_1 + m_2 \pmod 4$; $m_4 \equiv 2m_2 \pmod 8$.

[Proof of (A15). For $d = 2, 3, 4$, let C_d be a cube of G of order 2^d. By a well-known property of characters of finite groups, the sum $S_d = \sum_{g \in C_d} \chi_\rho(g)$ is divisible by $|C_d| = 2^d$. We have $S_d = \sum_{i=0}^d \binom{d}{i} z_i$, where $z_i = \chi_\rho(g_i)$.
This shows that $\sum_{i=0}^d \binom{d}{i} z_i \equiv 0 \pmod{2^d}$. By (A10) we have $z_i = z_0 - 2m_i$. Hence $\sum_{i=1}^d \binom{d}{i} m_i \equiv 0 \pmod{2^{d-1}}$.
For $d = 2$, this gives $2m_1 + m_2 \equiv 0 \pmod 2$, i.e., $m_2 \equiv 0 \pmod 2$.
For $d = 3$, we get $3m_1 + 3m_2 + m_3 \equiv 0 \pmod 4$, i.e., $m_3 \equiv m_1 + m_2 \pmod 4$.
For $d = 4$, we get $4m_1 + 6m_2 + 4m_3 + m_4 \equiv 0 \pmod 8$, i.e., $8m_1 + 10m_2 + m_4 \equiv 0 \pmod 8$, hence $m_4 \equiv 2m_2 \pmod 8$, since $m_2 \equiv 0 \pmod 2$.]

Corollary. *If* -1 *is a square in* k*, then*:

(A16) $w_\rho = (1 + m_1 w_1)(1 + \frac{m_2}{2} w_2)(1 + \frac{m_4}{4} w_4)$.

Proof. Since $e = 0$, the $p_i(e)$ are reduced to their constant term. Hence:

(A16)′ $w_\rho = 1 + m_1 w_1 + \binom{m_2}{2} w_2 + (\binom{m_1}{3} + \binom{m_2}{3} + \binom{m_3}{3}) w_3 + \binom{m_4}{4} w_4$.

By (A6)′, this gives $w_\rho = (1 + m_1 w_1)(1 + \binom{m_2}{2} w_2)(1 + \binom{m_4}{4} w_4)$. The congruences of (A15) imply that $\binom{m_2}{2} \equiv \frac{m_2}{2} \pmod 2$ and $\binom{m_4}{4} \equiv \frac{m_4}{4} \pmod 2$. Hence (A16).

Example 1. If $\rho = \rho_6$, one has $p_i(x) = 1$ for $i = 1, 2, 3, 4$, and Theorem 9 gives the basic equation $w_{\rho_6} = 1 + w_1 + w_2 + w_3 + w_4$.

Example 2. If $\rho = \rho_{27}$, one finds:

$p_1(x) = x + x^3 + x^5$,
$p_2(x) = 1 + x^6 + x^8$,
$p_3(x) = x^3 + x^7 + x^9$,
$p_4(x) = 1 + x^4 + x^8$.

Hence $w_{i,\rho_{27}} = 0$ when i is odd or $i > 12$, and:

$w_{2,\rho_{27}} = ew_1 + w_2$, $\quad w_{4,\rho_{27}} = e^3 w_1 + w_4$,
$w_{6,\rho_{27}} = e^5 w_1 + e^3 w_3$, $\quad w_{8,\rho_{27}} = e^6 w_2 + e^4 w_4$,
$w_{10,\rho_{27}} = e^8 w_2 + e^7 w_3$, $\quad w_{12,\rho_{27}} = e^9 w_3 + e^8 w_4$.

In the style of (A6)′, this may also be written as:

$w_{\rho_{27}} = (1 + ew_1 + w_2)(1 + e^3 w_1 + w_4)(1 + e^6 w_2 + e^4 w_4)$.

Example 3. If $\rho = \rho_{45}$, one finds:

$p_1(x) = \frac{x^{15}-1}{x-1} = 1 + x + ... + x^{14}$,
$p_2(x) = x^2 + x^{14} + x^{18}$,
$p_3(x) = \frac{x^{18}-x^{14}+x^{13}-x^2}{x-1} = (x^2 + ... + x^{12}) + (x^{14} + ... + x^{17})$,
$p_4(x) = x^{12}$.

In particular, $w_{20,\rho_{45}} = e^{18} w_2 + e^{17} w_3$ and $w_{i,\rho_{45}} = 0$ when $i > 20$.

A.5. *A preliminary construction : the modified cohomology ring $H(C)'$.*

Let ρ be a real linear representation of C. Its Stiefel-Whitney classes $w_i(\rho)$ belong to $H(C) \simeq \mathbf{F}_2[x_1, ..., x_4]$, cf. §A.1. We are going to define them now in the following ring $H(C)'$: we introduce a new variable y of degree 1, and we define $H(C)'$ as the quotient of $H(C)[y] = \mathbf{F}_2[x_1, ..., x_4, y]$ by the ideal generated by the elements $x_i^2 + x_i y$, $i = 1, ..., 4$. Note that, in $H(C)'$, the square z^2 of an element of degree $d > 0$ is given by:

(A17) $z^2 = zy^d$.

(Proof by induction on d, using the fact that $x_i^2 = x_i y$.)

A down-to-earth description of $H(C)'$ is as follows. For every $I \subset \{1, 2, 3, 4\}$, denote by x^I the monomial $\prod_{i \in I} x_i$. Then:

(A18) $H(C)'$ *is a free* $\mathbf{F}_2[y]$*-module with basis the* x^I*, and multiplication table* $x^I x^J = x^{I\cup J} y^{|I\cap J|}$.

An interesting feature of $H(C)'$ is that it is *universal* for families of four elements in $H^1(k)$, where k is any field of characteristic $\neq 2$. More precisely:

Lemma 2. *For every family* $z_1, ..., z_4$ *of elements of* $H^1(k)$ *there exists one and only one homomorphism* $\theta : H(C)' \to H(k)$ *such that* $\theta(x_i) = z_i$ *and* $\theta(y) = e$.

This follows from the formula $x^2 = xe$ for every $x \in H^1(k)$, cf. §A.3.

The symmetric group S_4 acts on $H(C)'$. Its invariants make up a free $\mathbf{F}_2[y]$-module $H(C)'^{\mathrm{sym}}$ with basis the elementary symmetric functions $s_0, ..., s_4$ of the x_i:

$s_0 = 1,$
$s_1 = x_1 + x_2 + x_3 + x_4,$
$s_2 = x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4,$
$s_3 = x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4,$
$s_4 = x_1x_2x_3x_4.$

The s_i are the images in $H(C)'$ of the $w_i|C$ of §A.3, cf. (A9).

Remark. The natural map $H(C) \to \mathrm{Inv}_k(C)$ of §A.2 can be extended to $H(C)'$ by requiring that y is mapped to e_k. In the special case $k = \mathbf{R}$, where $H(k) = \mathbf{F}_2[e]$, one finds that $H(C)' \to \mathrm{Inv}_{\mathbf{R}}(C)$ *is an isomorphism, and* $H(C)'^{\mathrm{sym}} \simeq \mathrm{Inv}_{\mathbf{R}}(G)$.

A.6. *Proof of Theorem* 9.

Let ρ be a real linear representation of C whose character is S_4-invariant, and let $m_1, ..., m_4$ be the corresponding integers, as defined in §A.4.

Let $w(\rho) \in H(C)$ be the total Stiefel-Whitney class of ρ, cf. §A.1. Let $w(\rho)'$ be the image of $w(\rho)$ in $H(C)'$. Since $w(\rho)'$ is S_4-invariant, we may write it in a unique way as

(A19) $\quad w(\rho)' = 1 + \sum_{i=1}^{4} s_i p_i(y),$ *with* $\; p_i \in \mathbf{F}_2[y],$

where the s_i are the elementary symmetric functions of the x_i, as above.

Theorem 10. *The polynomials* p_1, p_2, p_3, p_4 *have the properties* (A11), (A12), (A13), (A14) *of Theorem 9.*

Proof. Let C_1 be a group of order 2, with generator g. Its cohomology algebra $H(C_1)$ is a polynomial algebra $\mathbf{F}_2[x]$. We may enlarge $H(C_1)$ in $H(C_1)'$ as in the previous section, by adding the indeterminate y, and dividing by the relation $x^2 = xy$. The algebra so obtained is free of rank 2 over $\mathbf{F}_2[y]$ with basis $\{1, x\}$. Note that the subalgebra of $H(C_1)'$ generated by x is isomorphic to $\mathbf{F}_2[y]$; moreover, if p is a polynomial in one variable, with coefficients in $\mathbf{F}_2$, we have

(A20) $\; x^n p(x) = x^n p(y)$ *for every* $\; n > 0.$

For $i = 1, ..., 4$, let $f_i : C_1 \to C$ be a homomorphism such that $g_i = f_i(g)$ is an element of C of degree i, and let $\rho_i = \rho \circ f_i$. The Stiefel-Whitney class $w(\rho_i)'$ is:

(A21) $w(\rho_i)' = (1 + x)^{m_i}$;

this follows from the identities (A1) and (A2) of §A.1.

Let us now consider separately the four cases $i = 1, ..., 4$.

The case $i = 1$. The map $f_1 : C_1 \to C$ defines $f_1^* : H^1(C)' \to H^1(C_1)'$. The fact that $g_1 = f_1(g)$ is an involution of degree 1 is equivalent to saying that f_1^* maps one of the x_i on x and maps the other ones on 0. This implies that the images of $s_1, ..., s_4$ by f_1^* are respectively $x, 0, 0, 0$. Hence the image of $w(\rho)'$ by f_1^* is $1 + xp_1(y)$. Since that image is $w(\rho_1)'$, we obtain, by (A21):

$1 + xp_1(y) = (1 + x)^{m_1}$,

and by using (A20), we may rewrite this as:

(A22) $xp_1(x) = 1 + (1 + x)^{m_1}$, which is the same as (A11).

The case $i = 2$. The homomorphism f_2^* maps two of the x_i to x and the other ones to 0. Hence the images of $s_1, ..., s_4$ are $0, x^2, 0, 0$, and we have:

(A23) $x^2 p_2(x) = 1 + (1 + x)^{m_2}$, which is (A12).

The case $i = 3$. Here the images of $s_1, ..., s_4$ are $x, x^2, x^3, 0$, hence:

(A24) $xp_1(x) + x^2 p_2(x) + x^3 p_3(x) = 1 + (1 + x)^{m_3}$, which is (A13).

The case $i = 4$. Here the images of $s_1, ..., s_4$ are $0, 0, 0, x^4$, hence:

(A25) $x^4 p_4(x) = 1 + (1 + x)^{m_4}$, which is (A14).

This concludes the proof of Theorem 10.

Remark. The above proof is a kind of *interpolation.* It is similar to determining a polynomial through its values at special points. Here the Stiefel-Whitney class behaves as a fourth degree polynomial with constant term 1, and we used its values at the four types of subgroups of order 2.

End of the proof of Theorem 9.

The natural homomorphism $H(C) \to \mathrm{Inv}_k(C, \mathbf{Z}/2\mathbf{Z})$ can be factored through the homomorphism $H(C)' \to \mathrm{Inv}_k(C, \mathbf{Z}/2\mathbf{Z})$ mapping the element y of $H(C)'$ to $e_k = (-1)$. The images of the s_i are the w_i. By applying that homomorphism to $w(\rho)'$, and using Theorem 10, we obtain the formulas of Theorem 9 for the restrictions to C of $w_\rho, w_1, w_2, w_3, w_4$. By the splitting principle of Theorem 6, this implies Theorem 9.

Remark. The above proof only uses the following properties of G:

- It is a Weyl group in which the maximal cubes have rank 4 and are conjugate to each other.
- The involutions of G of the same degree are G-conjugate.

This shows that *Theorem 9 remains true* (*with the same polynomials* p_i) *when* G *is replaced by the symmetric groups* S_8 *or* S_9. It also remains true for every

S_n, the integer 4 being then replaced by $[n/2]$; one just needs to extend the list of the p_i beyond $i = 4$.

A.7. *The Stiefel-Whitney classes of the trace forms* $q_{T,\varphi}$.

Let T be a finite G-set and let $\varphi : \Gamma_k \to G$ be a continuous homomorphism. These data define an étale algebra; let $q_{T,\varphi}$ be its trace form, as in Remark 2 of §6.4. Let $w_i q_{T,\varphi}$ be the Stiefel-Whitney classes of $q_{T,\varphi}$ in the sense of Delzant and Milnor (see e.g. [Se 03], §17). By a theorem of B. Kahn (cf. [Ka 84] and [Se 03], §25.7), these classes are almost the same as those of the linear representation $\rho_T : G \to \mathsf{S}_n \to \mathrm{GL}_n(\mathbf{R})$, where $n = |T|$, and $G \to \mathsf{S}_n$ is the homomorphism giving the action of G on T. More precisely:

$$\text{(A26)} \quad w_i q_{T,\varphi} = \begin{cases} w_{i,\rho_T} & \text{if } i \text{ is odd} \\ w_{i,\rho_T} + (2) w_{i-1,\rho_T} & \text{if } i \text{ is even.} \end{cases}$$

One may then apply Theorem 9 to w_{ρ_T}; the integers m_i have the following interpretation: if g_i is an involution of degree i of G, m_i is the number of orbits of order 2 of $\{1, g_i\}$ in its action on T.

The case of the G-set Y with 27 elements is especially simple. We have

(A27) $wq_{Y,\varphi} = w_{\rho_{27}}$,

since all the $w_{i,\rho_{27}}$ are 0 when i is odd.

The case where T is the set of the 45 triangles is almost the same. We have

(A28) $wq_{T,\varphi} = w_{\rho_{45}} + (2)w_1$.

This follows from the fact that the product $(2)e \in H^2(k)$ is 0 since 2 is a sum of two squares. Hence all the terms of $w_{\rho_{45}}$ that are divisible by e disappear after multiplication by (2); the only one that does not is w_1.

Bibliography

[ATLAS] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker & R.A. Wilson, *Atlas of Finite Groups*, Clarendon Press, Oxford, 1985; second corrected edition, 2003.

[Bo 55] A. Borel, *Topology of Lie groups and characteristic classes*, Bull. A.M.S. 61 (1955), 397-432 (= Coll. Papers, vol. I, no 33).

[Bo 68] N. Bourbaki, *Groupes et algèbres de Lie, Chap. VI, Systèmes de racines*, Hermann, Paris, 1968; English translation, Springer-Verlag, 2002.

[Bo 81] —— , *Algèbre, Chap. V, Corps commutatifs*, Masson, Paris, 1981; English translation, Springer-Verlag, 1990.

[BS 94] E. Bayer-Fluckiger & J-P. Serre, *Torsions quadratiques et bases normales autoduales*, Amer. J. Math. 116 (1994), 1-63 (= J-P. Serre, Coll. Papers, vol. IV, no 163).

[Co 88] C.M. Coombes, *Every rational surface is separably split*, Comm. Math. Helv. 63 (1988), 305-311.

[De 80] M. Demazure, *Surfaces de Del Pezzo II-V*, L.N.M. 777 (1980), 23-69.

[Do 12] I.V. Dolgachev, *Classical Algebraic Geometry : a modern view*, Cambridge Univ. Press, 2012.

[GH 19] S. Gille & C. Hirsch, *On the splitting principle for cohomological invariants of reflection groups*, arXiv:1908.08146.

[GKT 89] J. Gunarwardena, B. Kahn & C. Thomas, *Stiefel-Whitney classes of real representations of finite groups*, J. Algebra 126 (1989), 327-347.

[Ha 77] R. Hartshorne, *Algebraic Geometry*, Springer-Verlag, 1977.

[Ka 84] B. Kahn, *Classes de Stiefel-Whitney de formes quadratiques et de représentations galoisiennes réelles*, Invent. math. 78 (1984), 223-256.

[KMRT 98] M.-A. Knus, A. Merkurjev, M. Rost & J-P. Tignol, *The Book of Involutions*, AMS Coll. Publ. 44, 1998.

[KW 17] J.L. Kass & K. Wickelgren, *An arithmetic count of the lines of a smooth cubic surface*, preprint (2017), arXiv:1708.01175.

[LR 18] M. Levine & A. Raksit, *Motivic Gauss-Bonnet formulas*, arXiv:1808.08385 [math.AG]; to appear in Algebra and Number Theory.

[Ma 74] Y. Manin, *Cubic Forms, Algebra, Geometry, Arithmetic*, North-Holland, 1974; second edit., 1986.

[Sch 58] L. Schläfli, *An attempt to determine the twenty-seven lines upon a surface of the third order, and to divide such surfaces into species in reference to the reality of the lines upon the surface*, Quart. J. Pure Appl. Math. 2 (1858), 110-120.

[Se 64] J-P. Serre, *Cohomologie galoisienne*, LN 5, Springer-Verlag, 1964; fifth revised edit., 1994; English translation, Springer-Verlag, 1997.

[Se 03] —— , *Cohomological invariants, Witt invariants and trace forms*, notes by Skip Garibaldi, ULECT 28, 1-100, AMS (2003).

[Se 18] —— , *Cohomological invariants* mod 2 *of Weyl groups*, Oberwolfach reports 21 (2018), 1284-1286; arXiv:1805.07172.

[Sp 52] T.A. Springer, *Sur les formes quadratiques d'indice zéro*, C.R.A.S. 234 (1952), 1517-1519.

Eva Bayer-Fluckiger
EPFL-FSB-MATH
Station 8
1015 Lausanne, Switzerland
eva.bayer@epfl.ch

Jean-Pierre Serre
Collège de France
3 rue d'Ulm
75005 Paris, France
jpserre691@gmail.com