Cohomological invariants of reflection groups

Diplomarbeit

vorgelegt von Christian Hirsch
Betreuer: Prof. Dr. Fabien Morel

Fakultät für Mathematik, Informatik und Statistik
Ludwig-Maximilians-Universität München

Dezember 2009
Zusammenfassung

Das Ziel dieser Arbeit ist die Untersuchung der Invarianten $\text{Inv}_{k_0}^*(W,M)$, wobei $W$ eine endliche Spiegelgruppe und $M$ eine $A^1$-invariante unverzweigte Garbe ist. Das wichtigste Hilfsmittel hierzu ist das Prinzip von Serre, welches –unter der Voraussetzung $\text{char}(k_0) \nmid |W|$ – besagt, dass ein Element aus $\text{Inv}_{k_0}^*(W,M)$ bereits durch seine Restriktionen auf die Invarianten der von Spiegelungen erzeugten elementar abelschen 2-Untergruppen eindeutig bestimmt ist. Unter Zuhilfenahme dieses Ergebnisses können wir beispielsweise $\text{Inv}_{k_0}^*(W,M)$ unter den Voraussetzungen $\text{char}(k_0) \nmid |W|$ sowie $-1 \in k_0^{\times 2}$ berechnen, wobei $W$ eine beliebige Weyl-Gruppe und $M$ ein beliebiger $\mathbb{Z}$-graduierter $A^1$-Modul mit $K^M/2$-Modul Struktur ist. In diesem Fall ist $\text{Inv}_{k_0}^*(W,M)$ isomorph zu einer direkten Summe von Summanden der Form $M_{-d}(k_0)$ für gewisse $d \geq 0$. Weitere Voraussetzungen an den Grundkörper $k_0$ erlauben es uns dieses Ergebnis auf beliebige euklidische Spiegelgruppen zu verallgemeinern. Unter Verwendung eines Resultats von Totaro können wir diese Berechnungen benutzen, um $\text{Inv}_{k_0}^*(W,M)$ für einen beliebigen Zykelmodul $M$ zu bestimmen.
Erklärung
Hiermit versichere ich, dass ich diese Diplomarbeit selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe.
München, den 1. Dezember 2009
Acknowledgements

First, I would like to use the opportunity to express my gratitude to my advisor Prof. Fabien Morel. For his remarkable patience, advice, guidance, inspiration and of course for introducing me to an exciting part of mathematics. Merci beaucoup!

Next, I want to thank Dr. Stefan Gille for his support, in particular during the early phase of this thesis. His experience was a great help to single out useful ideas amongst all the background noise in my head. Furthermore, my thanks go to Prof. James Swenson for sending me his PhD thesis [Sw] on the mod 2 cohomology of finite Coxeter groups. It enhanced my understanding of reflection groups and in particular it corrected some of my naïve views on elementary abelian 2-subgroups.

I also would like to thank Daniel Harrer for proofreading some parts of this thesis and Lukas-Fabian Moser for illuminating discussions.

Last but not least, I want to thank my parents for always having supported the ways I chose and my fellow students for all those colourful and vivid memories.
Consider the following topological problem: You are given a CW-complex $X$, a topological group $G$ and a principal $G$-bundle $\xi \to X$ and you want to show that $\xi$ is not isomorphic to the trivial bundle. One possible strategy is the following: Let $k_G$ be the contravariant functor mapping a CW-complex $Y$ to the pointed set of isomorphism classes of principal $G$-bundles over $Y$ and sending a map $f : Z \to Y$ to $(\eta \mapsto f^* \eta)$. Furthermore let $h'$ be some nice cohomology theory. If we can find a natural transformation $a$ between $k_G$ and $h'$ such that $a_X(\xi) \neq a_X(X \times G)$, then certainly $\xi$ cannot be isomorphic to the trivial bundle. Since the functor $k_G$ – when considered as a functor from the homotopy category – is representable by the classifying space $BG$, we can interpret natural transformations between $k_G$ and $h'$ also in terms of elements of $h'(BG)$. These are typically called characteristic classes.

The counterpart of principal $G$-bundles in algebraic geometry are the $G$-torsors. Already in the case $X = \text{Spec}(k)$ is the spectrum of a field, the classification of $G$-torsors over $k$ may be highly non-trivial. For instance, if $G = O_n$ is the orthogonal group and $\text{char}(k) \neq 2$, this problem is equivalent to classifying all isomorphism classes of non-degenerate quadratic forms of rank $n$ over $k$.

To fix ideas, let $k_0$ be a field and let $G$ be a smooth affine algebraic group over $k_0$. Furthermore, let $T_h$ be the category of finite type, separable field extensions of $k_0$. If we use the innocent notation $H^i(k, G)$ for the pointed set of $G$-torsors over $k$, then $H^i(-, G)$ can be turned into a functor from $T_h$ to $\text{Set}$. To continue the analogy from topology, we need a substitute for the cohomology-theory $h'$. It turns out that $A^1$-invariant unramified sheaves of abelian groups are quite suitable for this job. If $M$ is such a sheaf, then we could expect from topology that it may be interesting to determine the natural transformations from $H^i(-, G)$ to $M$; this set will be denoted by $\text{Inv}^G_k(G, M)$. By an argument due to Totaro, even the interpretation of characteristic classes in terms of elements of $h'(BG)$ has an analogue in algebraic geometry.

The main goal of this diploma thesis is the computation of $\text{Inv}^G_k(W, M)$, for $W$ a finite Euclidean reflection group. If $W$ is a Weyl group, this goal is achieved in the following two cases:

1. $M$ is a $\mathbb{Z}$-graded $A^1$-module with $K^M/2$-structure, $\text{char}(k_0) \nmid |W|$ and $-1 \in k_0^{\times 2}$. See 2.8.2.

2. $M$ is a cycle module, $\text{char}(k_0) \nmid |W|$, $-1 \in k_0^{\times 2}$ and $k_0$ is perfect. See 2.8.3.

In both cases, we use $\text{Inv}^G_k(W, M) \equiv M_k(k_0) \oplus \oplus_{d_i} M_{-d_i}(k_0)(2)$, where the $d_i$ are certain non-negative integers and (2) denotes the 2-torsion part. If we consider an arbitrary finite Euclidean reflection group, then we can draw the same conclusion, if we additionally assume that $5 \in k_0^{\times 2}$ and that $k_0$ contains all $|W|$-th roots of unity. The main tool for the computations is Serre’s splitting principle [CMS Theorem 25.15] which guarantees that $\text{Inv}(W, M)$ is detected by the elementary abelian 2-subgroups generated by reflections.

The structure of this thesis is as follows: In section 1, we recall various preliminaries such as quotients in algebraic geometry, torsors and $\mathbb{Z}$-graded $A^1$-modules. Of course, for most of these notions, one can find detailed accounts in the literature. However, we hope that a certain level of self-containment will increase the understandability of the main section. 2.1 provides the formal definition and some generalities on invariants. Subsection 2.2 is devoted to the proof of of Totaro’s theorem. Arguably the most important tool for us is Serre’s splitting principle which is proven in 2.3. Subsection 2.4 is kind of a short intermezzo, where we recall some basic facts on finite Euclidean reflection groups (mostly without proofs). Based on the structure of the invariants of $(\mathbb{Z}/2)^e$ and $O_n$ – which are determined in 2.5 and 2.6 respectively – we describe the invariants of finite Euclidean reflection groups in 2.7. The order in which the various types are treated is not arbitrary. When trying to determine the structure of the invariants of a certain type, we will often need results from types that we treated beforehand. Therefore we recommend to read them in the given order. Finally in 2.8 we summarize the results and point out some open questions. Appendix A contains some easy and well-known facts from algebraic geometry for which I was unable to provide an appropriate reference. In appendices B and C we discuss how a GAP-program can be used to determine the invariants in the $E_7$ and $E_8$-case. The sourcecode of this program is to be found in appendix D.
1 Preliminaries

1.1 Notations and conventions

For a field $k$, we denote by $k_0$, a separable closure of $k$. By $\Gamma_1$ or just $\Gamma$, we denote the absolute Galois group $\text{Gal}(k_0/k)$.

From section 3 on, all our schemes are assumed to be locally Noetherian. On the one hand, this will be totally sufficient for our purposes and on the other hand it ensures that we don’t need to have second thoughts when using results from [MI] (who also assumes schemes to be locally Noetherian). By $\text{Sch}/S$ we denote the category of schemes over some base scheme $S$. For $X, Y \in \text{Sch}/S$ we will often just write $X \times Y$ instead of $X \times_\text{Spec}(S) Y$; occasionally, we will also use the notation $X_Y$ (if we want to consider $X \times Y$ as a scheme over $Y$). In particular, if $k \subseteq \ell$ is an inclusion of fields and $X$ is a $k$-scheme, we write $X_\ell$ instead of $X \times_{\text{Spec}(k)} \text{Spec}(\ell)$.

Furthermore, we borrow the notations $\mathcal{F}_{k_0}, \mathcal{S}_{k_0}, \mathcal{S}_{k_0}'$ from [Mo3]: Let $k_0$ be a field. We denote by $\mathcal{F}_{k_0}$ the category whose objects are pairs $(\ell, i)$, where $\ell$ is a field and $i : k_0 \to \ell$ is a morphism of fields, such that $(k_0) \subseteq \ell$ is a finite type separable field extension. A morphism $\phi$ from $(\ell_1, i_1)$ to $(\ell_2, i_2)$ is a morphism $\ell_1 \to \ell_2$ of fields such that $\phi \circ i_1 = i_2$. We will often use sloppy notation by not mentioning the embedding $i$ explicitly. By $\mathcal{S}_{k_0}$, we denote the category of smooth, separated, finite type $k_0$-schemes. Furthermore, we denote by $\mathcal{S}_{k_0}'$ the category of essentially smooth $k_0$-schemes. Its objects are $k$-schemes $X$ such that $X = \lim_{i \in \mathcal{I}} X_i$, where $\mathcal{I}$ is a left-filtering system, the $X_i \in \mathcal{S}_{k_0}$ and all the transition maps $X_i \to X_j$ are smooth and affine. If $F$ is a presheaf on $\mathcal{S}_{k_0}$, then we define $F(X) := \colim_{\mathcal{I}} F(X_i)$. A discrete valuation $v$ on $K \in \mathcal{F}_{k_0}$ is always assumed to be a geometric one. That is, there exists $X \in \mathcal{S}_{k_0}$, irreducible with $k(X) = K$ and a point $x \in X$ of codimension 1, such that $v$ coincides with the discrete valuation defined by $x$.

For $i, j \in \mathbb{Z}$, $i \leq j$, we define $[i; j] := \{n \in \mathbb{Z} | i \leq n \leq j\}$.

To avoid illegible double subscripts, we will sometimes write $x_{a,b}$ or $x_{a,j}$ instead of $x_{a,1}^j$.

Starting from section 1.4, a sheaf will always mean a sheaf in the Nisnevich topology on $\mathcal{S}_{k_0}$.

1.2 Group schemes

1.2.1 Generalities

Before we can talk about invariants, we need a solid understanding of group schemes, group actions and quotients. We will review some basic definitions and properties. As our applications concern predominantly constant finite group schemes, we will pay special attention to this case.

**Definition 1.2.1.** Let $S$ be a scheme. Then a group scheme over $S$ is an $S$-scheme $G$ together with $S$-morphisms $\mu : G \times_S G \to G$, $\imath : G \to G$, $e : S \to G$ such that the following familiar diagrams commute:

![Diagram](image)

We will denote by $\text{GrpSch}/S$ the category whose objects are group schemes over $S$ and whose morphisms are $S$-morphisms of $S$-schemes which respect the group structure.

For instance, we can consider every (abstract) finite group as a group scheme as follows:

**Example 1.2.2.** Let $G$ be a finite group. Define $G_{\text{sch}/S} := \coprod_{g \in G} S$. The maps (of sets) defining the group structure on the abstract group $G$ then canonically give rise to $S$-morphisms

\[
\mu : \coprod_{g \in G} S \times_S S \cong \coprod_{(g, h) \in G \times G} S \to \coprod_{g \in G} S,
\]

\[
\imath : \coprod_{g \in G} S \to \coprod_{g \in G} S.
\]

\[
e : S \to \coprod_{g \in G} S
\]
endowing $\coprod_{s\in S} S$ with the structure of a group scheme over $S$. It will be called the \textit{constant finite group scheme associated to $G$}.

From its definition, it is clear that $G_{Sch/S}$ satisfies the following adjunction property: For any $H \in \text{GrpSch}/S$ there is a natural bijection $\text{Mor}_{\text{GrpSch}/S}(G_{Sch/S}, H) \cong \text{Mor}_{\text{abstract groups}}(G(H(S)))$. Moreover, if $G$ is a constant finite group scheme and $s \in S$ is arbitrary, then we will denote by $G_{Set} = G(s)$ its underlying abstract group (this does not depend on the particular choice of the point $s$).

**Example 1.2.3.** Let $R$ be a commutative ring. Then we can define a group structure over $R$ on $G_{m,R} := \text{Spec}(R[X, X^{-1}])$ induced by the following homomorphisms:

$$\Delta: R[X, X^{-1}] \to R[X, X^{-1}] \otimes_R R[X, X^{-1}]$$

$$X \mapsto X \otimes X, \quad S: R[X, X^{-1}] \to R[X, X^{-1}]$$

$$X \mapsto X^{-1}, \quad e: R[X, X^{-1}] \to R$$

$$X \mapsto 1.$$

**Example 1.2.4.** More generally put $G_{l,n} := \text{Spec}(A)$, where $A = R[X_{1,1}, \ldots, X_{n,n}, \det((X_{i,j}))_{1 \leq i, j \leq n})$, i.e. the polynomial ring in $n^2$ variables localized at the determinant. The homomorphisms of $R$-algebras

$$\Delta: A \to A \otimes_R A$$

$$X_{i,k} \mapsto \sum_{1 \leq j \leq n} X_{i,j} \otimes X_{j,k},$$

$$S: A \to A$$

$$X_{k,t} \mapsto (-1)^{k+t} \det((X_{i,j})_{1 \leq i, j \leq n})^{-1} \cdot \det((X_{i,j})_{k\neq i, t\neq k}),$$

$$e: A \to R$$

$$X_{i,j} \mapsto \delta_{i,j}$$

then induce morphisms $\mu: G_{l,n} \times_R G_{l,n} \to G_{l,n}$, $\iota: G_{l,n} \to G_{l,n}$ and $e: \text{Spec}(R) \to G_{l,n}$ that endow $G_{l,n}$ with the structure of an $R$-group scheme. In fact, if $A$ is an $R$-algebra, then to give $\text{Spec}(A)$ the structure of an $R$-group scheme is equivalent to giving $A$ the structure of a commutative Hopf algebra over $R$.

**Example 1.2.5.** Define $O_{n} := \text{Spec}(A/I)$, where $A$ is as above and $I$ is the ideal generated by $\{\sum_{1 \leq i, k \leq n} X_{i,k}X_{k,i} - \delta_{i,k} | 1 \leq i, k \leq n\}$. The maps $\Delta$, $S$ and $e$ from above induce maps $\overline{\Delta}: A/I \to A/I \otimes_R A/I$, $\overline{S}: A/I \to A/I$ and $\overline{e}: A/I \to R$. In this way, $O_{n}$ becomes an $R$-group scheme. More precisely, it is a a closed subgroup scheme of $G_{l,n}$.

Next, we want to formalize the notion of group actions in algebraic geometry:

**Definition 1.2.6.** Let $X \in Sch/S$ and $G \in \text{GrpSch}/S$. A right action of $G$ on $X$ is an $S$-morphism $\rho: X \times_S G \to X$ such that the following diagrams commute

$$\begin{array}{c}
X \times_S G \times_S G \\
\downarrow^\rho \quad \downarrow^\id \\
X \times_S G
\end{array}$$

$$\begin{array}{c}
X \times_S G \\
\downarrow^\rho
\end{array}$$

For $T \in Sch/S$, $x \in X(T)$ and $g \in G(T)$ we will often write just $x^g$ for $\rho(T)(x, g)$.

It goes without saying that also the notion of a left action may be extended to group schemes.

**Remark 1.2.7.** If $G$ is a constant finite group scheme, then a right-action $\rho: X \times_S G \to X$ is the same as an anti-homomorphism of abstract groups $G_{set} \to \text{Aut}_S(X)$.

We will also need algebro-geometric analogues of free actions:

**Definition 1.2.8.** Let $G \in \text{GrpSch}/S$ and $X \in Sch/S$. An action $X \times_S G \to X$ is called \textit{set-theoretically free}, if for any $T \in Sch/S$ and for any $(x, g) \in X(T) \times G(T)$ the invariance $x^g = x$ implies $g = e$ (or more precisely $g = e \circ pr_s$, where $pr_s: T \to S$ is the canonical projection). The action is called \textit{scheme-theoretically free}, if the map

$$\Psi := (pr_1, \rho): X \times_S G \to X \times_S X$$

is a closed immersion.
Remark 1.2.9. The definition of set-theoretical freeness is taken from [DG] III, §2, 2.3. The definition of scheme-theoretical freeness is taken from [GIT] Def. 0.8] (where such an action is simply called free).

Lemma 1.2.10. Let $X \in \text{Sch}/S$, let $G \in \text{Sch}/S$ and let $\rho: X \times_S G \to X$ be a scheme-theoretically free right action. Then $\rho$ is set-theoretically free.

Proof. For $T \in \text{Sch}/S$ we conclude from [A.0.1] that the map $(pr_1(T), \rho(T)): X(T) \times G(T) \subset X(T) \times X(T)$ is an injection. This implies right away the condition in the definition [1.2.8].

It may be quite hard to check that an action is free directly by using the definition. Therefore, the following easy lemma will be very useful for our purposes.

Proposition 1.2.11. Let $X \in \text{Sch}/S$ be separated. Let $G \in \text{Sch}/S$ be constant finite and let $\rho: X \times_S G \to X$ be a right action. Then the following statements are equivalent:

(i) $G$ acts scheme-theoretically freely on $X$.

(ii) $G$ acts set-theoretically freely on $X$.

Hence, if $G \in \text{Sch}/S$ is a constant finite group scheme acting on a separated $X \in \text{Sch}/S$, then the two notions of freeness coincide and we will just say that the action is free.

Furthermore, if $S = \text{Spec}(k)$ is the spectrum of a field and $X$ is additionally assumed to be of finite type over $k$, then the following property is also equivalent to (i) and (ii) above:

(iii) $G_{\text{set}} \equiv G(\bar{k})$ acts freely on $X(\bar{k})$.

Proof. (i) $\Rightarrow$ (ii) is the previous lemma. Thus we move on to show (ii) $\Rightarrow$ (i). For each $g \in G_{\text{set}}$, the graph $\Gamma_g: X \to X \times_S X$, $x \mapsto (x, xg)$ is a closed immersion (since $X$ is separated). Now $(pr_1, \rho)$ can be factored as

$$X \times_S G \cong \bigsqcup_{g \in G_{\text{set}}} X \xrightarrow{\rho_g} X \times_S X.$$

By [A.0.2] it is then sufficient to show that the images of the $\Gamma_g$ are pairwise disjoint.

So suppose, we had $y \in \Gamma_g(X) \cap \Gamma_{g'}(X)$ for some $g \neq g' \in G_{\text{set}}$. Wlog, we may assume $g' = e$. Indeed $y$ is the set-theoretic image of the two morphisms

$$\text{Spec}(\kappa(y)) \to X \times_S X \xrightarrow{pr_1} X \xrightarrow{\Gamma_g} X \times_S X$$

and

$$\text{Spec}(\kappa(y)) \to X \times_S X \xrightarrow{pr_1} X \xrightarrow{\Gamma_{g'}} X \times_S X.$$

Composing with right multiplication by $(g')^{-1}$, we obtain that the two morphisms

$$\text{Spec}(\kappa(y)) \to X \times_S X \xrightarrow{pr_1} X \xrightarrow{\Gamma_{g'(g')^{-1}}} X \times_S X$$

and

$$\text{Spec}(\kappa(y)) \to X \times_S X \xrightarrow{pr_1} X \xrightarrow{\Gamma_{g}} X \times_S X$$

have the same set-theoretic image and this yields an element in $\Gamma_{g(g')^{-1}}(X) \cap \Gamma_e(X)$.

The definition of set-theoretic stability gives us a diagram of cartesian squares:

$$\begin{array}{ccc}
\text{Spec}(\kappa(y)) & \longrightarrow & X \\
\downarrow & & \downarrow \\
& \xrightarrow{\psi} & \\
\text{Spec}(\kappa(y)) & \longrightarrow & X \times_S X
\end{array}$$

Thus $\Psi^{-1}(\Gamma_e(X))$ consists only of the component $X \subset \bigsqcup_{g \in G_{\text{set}}} X \cong X \times_S G$ corresponding to the neutral element $e$ and we conclude $\Gamma_g(X) \cap \Gamma_e(X) = \emptyset$ for $g \neq e$.

Now suppose $S = \text{Spec}(k)$ and $X$ of finite type over $k$. The implication (ii) $\Rightarrow$ (iii) is trivial. So suppose now that (iii) holds and let us show (i). Just as above, it suffices to prove that for all $g \neq g' \in G_{\text{set}}$, we have $\Gamma_g(X) \cap \Gamma_{g'}(X) = \emptyset$. Suppose, we could find $g, g'$, such that $Y := \Gamma_g(X) \cap \Gamma_{g'}(X) \neq \emptyset$. Then $Y \subset X \times X$ is a closed subscheme; hence it contains a closed point $y$ of $X \times X$. Now we can again assume $g' = e$ and draw a similar commutative diagram as above (leaving out the middle column). As before, we obtain the desired contradiction.

Remark 1.2.12. In fact the equivalence (ii) $\Leftrightarrow$ (iii) holds (without the hypothesis on separatedness) for all $G$ (not necessarily constant finite) that are of finite type over $k$, if the field $k$ is of characteristic $0$. See [DG] III, §2, 2.5.
1.2.2 Quotients

In general, the notion of quotients in algebraic geometry is a rather complicated one. In this subsection, we want to recall the basic definitions and treat the relatively easy case of constant finite group schemes in detail. The notion of a torsor will be introduced in the following section. Except for minor adaptations, most of the material is taken directly from [SGA1, V.1, V.2] and [DG, III, §2].

**Definition 1.2.13** (Categorical quotient). Let S be a scheme, $G \in \text{GrpSch/S}$ and $X \in \text{Sch/S}$ be such that $X$ is endowed with a right $G$-action $\rho: X \times_S G \to X$. An $S$-scheme $Y$ together with an $S$-morphism $\pi: X \to Y$ is called *categorical quotient* of $X$ by $G$, if it induces a commutative, cocartesian square

$$
\begin{array}{ccc}
X \times_S G & \xrightarrow{\rho_1} & X \\
\downarrow \pi & & \downarrow \pi \\
X & \xrightarrow{\pi} & Y.
\end{array}
$$

In particular, $Y$ is uniquely determined up to isomorphism and we will often write $X/G$ for $Y$.

Let us first consider the affine case.

**Proposition 1.2.14.** Let $R$ be a commutative ring and $G$ be a finite (abstract) group acting on an $R$-algebra $A$ by $R$-algebra isomorphisms. The inclusion $A^G \subset A$ induces a map $p: X = \text{Spec}(A) \to Y = \text{Spec}(A^G)$. Then we have

(i) $p$ is integral, closed and surjective

(ii) Let $[X], [Y]$ denote the underlying topological spaces of $X, Y$. Then $p$ induces a homeomorphism $[X]/G \xrightarrow{\sim} [Y]$.

(iii) $p^* : O_Y \to p_* O_X$ induces an isomorphism of sheaves $O_Y \xrightarrow{\sim} (p_* O_X)^G$

(iv) $X \to Y$ is a categorical quotient

**Proof.** The first item is clear, as any $a \in A$ is a root of the monic polynomial $\prod_{g \in G}(X - g(a))$ which has coefficients in $A^G$. Now use that any integral morphism is universally closed (see [EGA II, Prop. 6.1.10]). Since $\text{Spec}(A) \to \text{Spec}(A^G)$ is dominant, we conclude that it is also surjective.

To prove the injectivity of (ii), assume we have $p_1, p_2 \in \text{Spec}(A)$ such that $p_1 \cap A^G = p_2 \cap A^G =: a$. Then $\prod_{g \in G} g(p_1) \subset p_1 \cap A^G = a \subset p_2$ and there exists $g_0 \in G$ such that $g_0(p_1) \subset p_2$. But as $g_0(p_1)$ is another prime ideal lying over $a$, we conclude that $g_0(p_1) = p_2$ (due to integrality, there are no proper inclusion of prime ideals lying over $a$ (see [Ma, Theorem 9.3])). Together with (i), we conclude that $[X]/G \to [Y]$ is bijective, continuous and closed; hence a homeomorphism.

Claim (iii) boils down to showing that for $f \in A^G$, the natural inclusion $(A^G)_f \subset (A_f)^G$ is in fact an equality. Every $x \in (A_f)^G$ can be written as $x = \frac{a}{f}$ for certain $m \geq 0, a \in A$ such that $\frac{a}{f} = g(\frac{x}{f}) = \frac{g(a)}{g(f)}$ holds for all $g \in G$. That is, we can choose some $N$ such that for all $g \in G$ the equality $f^N(a - g(a)) = 0$ holds. But this implies that $f^N a \in A^G$ and we can write $\frac{a}{f^N}$ as $\frac{a}{f^N}$ in $(A^G)_f$.

To prove the last assertion, we proceed as in [GIT, §2, Prop. 0.1]. Suppose that $\psi: X \to Z$ is a $G$-invariant morphism. Cover $Z$ by open affines $Z = \bigcup_{i \in I} V_i$. Then $\psi^{-1}(V_i)$ is $G$-invariant and open. By (ii), we can then find $U_i \subset Y$ open, such that $\psi^{-1}(U_i) = \psi^{-1}(V_i)$. Since $V_i$ is affine, constructing a map $\chi_i: U_i \to V_i$ with $\psi = \chi_i \circ p$ is the same as giving a morphism of rings $\phi_i: \Gamma(V_i, O_V) \to \Gamma(U_i, O_{U_i})$ such that $\psi^\circ(V_i) = p^\circ(U_i) \circ \phi_i$ (and then we will have $\phi_i = \chi_i^\circ(\psi(V_i))$). But since $\psi^\circ(V_i)$ is $G$-invariant, and $\Gamma(U_i, O_{U_i}) = \Gamma(\psi^{-1}(V_i), O_X)^G$ (by (iii)), such a morphism always exists (and is unique). Hence, there is a unique morphism $\chi_i: U_i \to V_i$ such that $\psi|_{\psi^{-1}(V_i)} = \chi_i \circ p|_{\psi^{-1}(V_i)}$. Furthermore, any morphism $\chi: Y \to Z$ which has the required factorization property $\psi = \chi \circ p$ must satisfy $\chi^{-1}(V_i) = p^*(\chi^{-1}(V_i)) = \psi^{-1}(V_i)) = p(\psi^{-1}(V_i)) = p(U_i) = U_i$. Thus, the above discussion shows already that there exists at most one $\chi$. To conclude the existence, it remains to check that the various $\chi_i$ coincide. So let $y \in U_i \cap U_j$, and choose an $f \in A^G$, such that $y \in D(f) \subset U_i \cap U_j$. But if we apply the uniqueness just obtained to the morphism $p^{-1}(D(f)) \ni \text{Spec}(A_f) \to Z$, we conclude that $\chi_i$ and $\chi_j$ coincide on $D(f)$. 

The next lemma shows that property (iii) of the previous proposition is quite strong:

**Proposition 1.2.15.** Let $X, Y \in \text{Sch/S}$ and let $p: X \to Y$ be an affine morphism of $S$-schemes; let $G \in \text{Sch/S}$ be constant finite. Suppose, we have an action of $G$ on $X$ such that $p$ is $G$-invariant. Suppose further that the canonical map $O_Y \to (p_* O_X)^G$ is an isomorphism. Then the assertions (i), (ii), (iv) of the previous theorem hold.
Proof. The statements (i), (ii) are local on $S$ and $Y$. Thus to prove them, we may assume $S, Y$ and hence also $X$ to be affine. If $X = \text{Spec}(A)$, then the assumption implies $Y = \text{Spec}(A^G)$. (i) and (ii) then follow from what we have proved above. To prove (iv), we may proceed exactly as above, since we did not use explicitly the fact that $X$ or $Y$ was affine; we just used (i), (ii), (iii), which are also valid in the current situation. \hfill \Box

Corollary 1.2.16. In the situation of the previous proposition, let moreover $U \subset Y$ be open. Then $U$ is a categorical quotient of $p^{-1}(U)$ by $G$.

Proof. Indeed, restricting $O_Y \cong (p_*O_X)^G$ to $U$ yields $O_U \cong (p_*O_{p^{-1}(U)})^G$. \hfill \Box

The following technical proposition shows that certain properties of $X$ carry over to the quotient.

Proposition 1.2.17. Suppose again that we are in the situation of 1.2.15. Then $X$ is affine/separated over $S$ iff $Y$ is affine/separated over $S$. Furthermore, if $X$ is of finite type over $S$, then so is $Y$ and if additionally $S$ is locally Noetherian, then the map $X \to Y$ is finite.

Proof. The proof is not that exciting; see [SGA1, V, Cor. 1.5]. \hfill \Box

Proposition 1.2.18. Let $X \in \text{Sch}/S$, let $G \in \text{GrpSch}/S$ be constant finite and let $\rho : X \times_S G \to X$ be a right action. Then $X$ can be written as a union of $G$-invariant open affine subschemes if and only if every orbit of $G$ in $X$ is contained in an open affine subscheme; we say that $G$ acts admissibly on $X$. In this case, there exists a categorical quotient $Y = X/G$. Additionally, $X \to Y$ is affine and satisfies conditions (i), (ii), (iii) of 1.2.14.

Proof. First let’s show that the two conditions are indeed equivalent. Clearly, if $X$ is a union of $G$-invariant open affine subschemes, then every orbit is contained in an open affine subscheme.

For the converse, let $x \in X$ be arbitrary and let $M := \{s^g \mid g \in G\}$ be its orbit. Choose an open affine subset $U \supseteq M$. Then $U' = \bigcap_{u \in U} U^G$ is open, $G$-invariant and contains $M$. Since $U' \subset U$ and $U$ is affine, there exists an open subset of the form $D(f), f \in \Gamma(U, O_U)$, such that $M \subset D(f) \subset U'$ (this is the prime avoidance lemma from commutative algebra in disguise: if $A$ is a ring, $I \subset A$ an ideal and $p_1, \ldots, p_r \in \text{Spec}(A) - V(I)$, then there exists $f \in I$ with $f \notin \bigcup_{i=1}^r p_i$). Since $U$ is separated, the intersection of the conjugates of $D(f)$ is again affine (and of course $G$-invariant).

Now we are ready to tackle the main assertion: Suppose $\bigcup X_i = X$ is a covering by $G$-invariant open affine subschemes. By 1.2.14 the categorical quotients $p_i : X_i \to Y_i = X_i/G$ exist, are affine and satisfy all the properties stated there. In particular, using the uniqueness of categorical quotients and 1.2.14 we see that for all $i, j$ there is a canonical isomorphism $p_i(X_i \cap X_j) \cong p_j(X_i \cap X_j)$ (note that we can use (ii) of 1.2.14 to conclude from $p_i^{-1}(p_i(X_i \cap X_j)) = X_i \cap X_j$ that $p_i(X_i \cap X_j)$ is open). After glueing the schemes $Y_i$ along the open subschemes $p_i(X_i \cap X_j)$, we obtain an $S$-scheme $Y$ and an affine morphism of $S$-schemes $p : X \to Y$. Since the induced map $O_Y \to p_*O_X^G$ is an isomorphism (this may be checked on each of the $Y_i$), we are done after applying 1.2.15. \hfill \Box

Remark 1.2.19. The condition of 1.2.18 is automatically satisfied, when $X$ is quasi-projective: Let $U \subset \mathbb{P}^n$ be open, such that $X \subset U$ is closed. Denote by $\overline{X}$ the closure of $X$ in $\mathbb{P}^n$ (endowed with the reduced induced subscheme structure). We claim that for any finite set of points $x_1, \ldots, x_k \in X = \overline{X} \cap U$ there exists a hypersurface $S \subset \mathbb{P}^n$ containing $\mathbb{P}^n - U$ but not any of the points $x_1, \ldots, x_k$.

This is easy, as soon as we have found the right algebraic translation. $\mathbb{P}^n - U$ is defined by a homogeneous ideal $J \subset k[Y_0, \ldots, Y_n]$ and the points $x_i$ correspond to homogeneous prime ideals $p_i$ such that $J \notin p_i$ for all $1 \leq i \leq k$. By homogeneous prime avoidance ([1,3, Lemma 3.2]), we can choose a homogeneous $g \in J$ not contained in any $p_i$. It defines the hypersurface we were looking for.

Now $\overline{X} - S$ is affine (as a closed subscheme of the open affine subscheme $D_+(g) \subset \mathbb{P}^n$, open in $X$ (from $\mathbb{P}^n - S \subset U$, we deduce $\overline{X} - S \subset \overline{X} \cap U = X$) and contains all of the points $x_1, \ldots, x_k$ by construction.

In the case of a free action, the quotient is particularly nice.

Corollary 1.2.20. Let $G, X, \rho$ be as in 1.2.18. Assume further that $X$ is locally of finite type over $S$, that $S$ is locally Noetherian and that $G$ acts scheme-theoretically freely on $X$. Then $\Psi = (pr, \rho) : X \times_S G \cong \bigsqcup_{g \in G} X \to X \times Y$ $X$ is an isomorphism (where $Y = X/G$) and $p : X \to Y$ is faithfully flat.

Proof. We follow [DG, III, §2, 4]. As usual, we may assume $S, Y$ and thus also $X$ to be affine, $S = \text{Spec}(R), X = \text{Spec}(A), Y = \text{Spec}(B) = \text{Spec}(A^G)$. We then need to show that the map

$$\psi : A \otimes_R A \to \bigsqcup_{g \in G} A$$

$$a_1 \otimes a_2 \mapsto (g(a_1)a_2)_{g \in G}$$
is an isomorphism and that \( A \) is flat as \( B \)-module. Since \( \mathcal{V} \) is a closed immersion, \( \psi \) is surjective.

If we can prove for all \( q \in \text{Spec}(B) \) that \( \psi_q \) is bijective and that \( A_q \) is flat as \( B_q \)-module, then \( \psi \) is an isomorphism and \( A \) is a flat as \( B \)-module.

Thus, we may assume \( B = B_q \) is local, \( A = A_q \) semilocal and the maximal ideal of \( B \) lies in the radical of \( A \) (this follows, since \( X \to Y \) is finite by \[1.2.17\]). Now we need a technical lemma from \[DG, \text{III, \S2, 4.7}\] (which we state without proof).

**Lemma 1.2.21.** Let \( B \) be a local ring with infinite residue field and let \( A \) be a semi-local ring together with a homomorphism \( i: B \to A \) sending the maximal ideal of \( B \) into the radical of \( A \). Suppose further that \( M \) is a free \( A \)-module of finite rank and that \( N \subset M \) is a \( B \)-submodule generating \( M \) as \( A \)-module. Then \( N \) contains a basis of \( M \) as \( A \)-module.

Now let us return to the proof of the corollary. We first settle the case, where the residue field of \( B \) is infinite. Then we may apply the above lemma to \( M = \prod_{g \in G} A \) (endowed with the \( A \)-module structure defined by \( a \cdot (a_g)_{g \in G} = (aa_g)_{g \in G} \) and \( N = A \) with the inclusion \( N \subset M \) given by \( a \mapsto (g(a))_{g \in G} = \psi(a \otimes 1) \) (observe that \( \psi(A \otimes 1) \) generates \( M \) as \( A \)-module, since \( \psi \) is surjective). Thus we can choose \( a_1, \ldots, a_n \in A \), such that \( \psi(a_i \otimes 1) \) is an \( A \)-basis of \( \prod_{g \in G} A \). We would like to show that these \( a_1, \ldots, a_n \in A \) form a basis of \( A \) over \( B \), since this would imply that \( \psi \) sends a basis to a basis and is thus an isomorphism (and of course then \( A \) is also flat as \( B \)-module).

Consider the following diagram of \( B \)-modules (unlabeled arrows will be explained below):

\[
\begin{array}{ccc}
0 & \longrightarrow & \mathbb{Z}^n \otimes B \\
& & \downarrow \text{id} \\
0 & \longrightarrow & A \\
& & \downarrow \psi(\text{id}) \\
& & \prod_{g \in G} A \\
& & \downarrow \prod_{(g,h) \in G \times G} A \\
& & \prod_{(g,h) \in G \times G} A
\end{array}
\]

- The unlabeled horizontal arrows in the first row are given by \( e_i \otimes a \mapsto e_i \otimes (a_g)_{g \in G} \) and \( e_i \otimes a \mapsto e_i \otimes (g(a))_{g \in G} \)
- The unlabeled horizontal arrows in the second row are given by \( (a_g)_{g \in G} \mapsto (a_{g,h})_{(g,h) \in G \times G} \) and \( (a_g)_{g \in G} \mapsto (h(a_g))_{(g,h) \in G \times G} \).
- The vertical arrows are \( e_i \otimes b \mapsto a_i b, e_i \otimes a \mapsto (g(a))_{g \in G} \) and \( e_i \otimes (a_h)_{h \in G} \mapsto (h g(a))_{(g,h) \in G\times G} \).

It is a matter of patience to check that this diagram commutes and that the rows are exact. By the choice of the \( a_i \), the middle vertical map is an isomorphism and it is not hard to check that the right one is, too. Hence we conclude that the left map is an isomorphism as well.

If the residue field is not infinite, we take a look at the strict Henselization \( B^{sh} \) of \( B \). Since \( B^{sh} \) is flat over \( B \), tensoring the exact sequence

\[
0 \longrightarrow B \longrightarrow A \longrightarrow \prod_{g \in G} A
\]

by \( B^{sh} \) over \( B \) yields an exact sequence

\[
0 \longrightarrow B^{sh} \longrightarrow A \otimes_B B^{sh} \longrightarrow \prod_{g \in G} A \otimes_B B^{sh}
\]

(where the double arrows are induced by \( a \mapsto (a)_{g \in G} \) and \( a \mapsto (g(a))_{g \in G} \) respectively). After what we have just proved, we conclude that

\[
\psi^{sh}: (A \otimes_B A) \otimes_B B^{sh} \to \left( \prod_{g \in G} A \right) \otimes_B B^{sh}
\]
is an isomorphism and that \( B^{sh} \otimes_B A \) is flat as \( B^{sh} \)-module. The original theorem now follows from faithfully flat descent. \( \square \)

The corollary shows how to construct principal homogeneous sets or \( G \)-torsors for constant finite group schemes. In the next section we will recall the precise definition of this important notion.

### 1.3 Torsors

#### 1.3.1 Generalities

Let us discuss now the algebro-geometric analogue of the topological notion of a principal \( G \)-bundle. Before we start with the definitions, here is a short remark for the experts: In our approach we only consider torsors that are represented by schemes and not the a priori more general notion of sheaf torsors. Since we are
only interested in $G$-torsors, where $G$ is a smooth affine algebraic group, these two notions are quite close anyway. Indeed by [Mi] III, Theorem 4.3] in this case, any sheaf torus over a scheme is representable by a scheme. However, note that in section 22 it is important to work with scheme-torsors (as we want the quotient space to be a scheme). Let us start with a variant of the definition in [Mi] III, §4:

**Definition 1.3.1** ($G$-torsor). Let $G \in \text{GrpSch}/S$ be flat and locally of finite type over $S$. Let $X, Y \in \text{Sch}/S$ and $\pi: X \to Y$ be faithfully flat and locally of finite type. Furthermore, let $\rho: X \times_S G \to X$ be a right action. Then $X$ is called a $G$-torsor over $Y$, if $\pi$ is equivariant when $Y$ is considered to be endowed with the trivial $G$-action and if $\Psi = (pr_1, \rho): X \times_S G \to X \times_Y X$ is an isomorphism.

**Remark 1.3.2.** The definition in Milne is the one given above in the case $S = Y$. The only reason for us to differ from Milne is that we prefer to write $G$-torsor instead of $G_Y$-torsor. Indeed suppose $G \in \text{GrpSch}/S$ is flat and locally of finite type over $S$. Then $X \to Y$ is a $G$-torsor as defined above, if it is a $G_Y$-torsor in the sense of Milne.

**Remark 1.3.3.** It follows from the definition that the pull-back of a $G$-torsor $\pi: X \to Y$ along a morphism $Z \to Y$ gives rise to a $G$-torsor $X \times_Y Z \to Z$.

**Remark 1.3.4.** Let $X \in \text{Sch}/S, G \in \text{GrpSch}/S$. If $\pi: X \to S$ is a $G$-torsor with a section $s: S \to X$ of $\pi$, then the torsor is trivial, i.e. $X \cong G$ equivariantly. Indeed, one can check explicitly that

$$\phi: G = S \times_S G \xrightarrow{(s, id)} X \times_S G \xrightarrow{\rho} X$$

and

$$\psi: X = S \times_S X \xrightarrow{(s, id)} X \times_S X \xrightarrow{w^{-1}} X \times_S G \xrightarrow{pr_c} G$$

are $G$-equivariant morphisms over $S$ and inverse to one another.

We have already seen one example of $G$-torsors in [12.2a]. Here is another one:

**Example 1.3.5.** Let $k$ be a field. Let $G$ be an affine algebraic group over $k$, i.e. a group scheme of the form $G \cong \text{Spec}(A)$, where $A$ is a finite type $k$-scheme. Furthermore, let $H \subset G$ be a closed subgroup. It follows from [SGA3] VI$_{AI}$, Thm. 3.2] that the categorical quotient $G \to G/H$ exists, is faithfully flat and of finite type and that $\Psi: G \times H \to G \times_{G/H} G$ is an isomorphism. Thus $G \to G/H$ is an $H$-torsor.

**Remark 1.3.6.** Before we continue, it is convenient to recall the following descent statement. If $P$ is a property of morphisms of schemes which is stable by base change, local on the target and which descends with respect to faithfully flat and quasi-compact morphisms, then it also descends with respect to morphisms that are faithfully flat and locally of finite type; in particular, this applies to all the properties stated in [EGA IV] Prop. 2.7.1]. Indeed, suppose we are given a cartesian diagram

$$
\begin{array}{ccc}
X' & \xrightarrow{g} & X \\
\downarrow{f'} & & \downarrow{f} \\
Y' & \xrightarrow{g} & Y
\end{array}
$$

where $f'$ is $P$ and $g$ is faithfully flat and locally of finite type. Since $P$ is stable by base change and local on the target, we may assume $Y$ affine. Now recall from [EGA IV] Prop. 2.4.6] that flat morphisms which are locally of finite type are open (as all our schemes are assumed to be locally Noetherian). So, if we choose a covering of $Y'$ by open affines, we obtain a covering $\cup \mathcal{U}(U)$ of $Y$ by open subsets. Since $Y$ is affine, it is quasi-compact and we may cover it by finitely many of the $\mathcal{U}(U)$. Let $U \subset Y'$ be the union of the corresponding $\mathcal{U}_i$. Then the restriction $g_{|U}$ is faithfully flat and quasi-compact. Now we just need to apply the descent property on the cartesian diagram

$$
\begin{array}{ccc}
U & \xrightarrow{g} & Y \\
\downarrow{f^{-1}(U)} & & \downarrow{f^{-1}} \\
\mathcal{U} & \xrightarrow{g} & \mathcal{U}
\end{array}
$$

**Example 1.3.7.** Let $\pi: X \to Y$ be a $G$-torsor and let $U \subset X$ be a $G$-invariant open subscheme. We claim that $U \to \pi(U)$ is a $G$-torsor and that $\pi^{-1}(\pi(U)) = U$. First observe that $\pi(U) \subset Y$ is open, since $\pi$ is flat and locally of finite type. By pulling back the isomorphism $\Psi: X \times_S G \xrightarrow{\sim} X \times_Y X$ along $U \to X$, we obtain an isomorphism $U \times_S G \xrightarrow{\sim} U \times_Y X \cong U \times_{\pi(U)} \pi^{-1}(\pi(U))$. But since $U$ is $G$-invariant, this isomorphism factors through the open immersion $U \times_{\pi(U)} U \subset U \times_{\pi(U)} \pi^{-1}(\pi(U))$. By descent, we conclude $U \cong \pi^{-1}(\pi(U))$ and thus $U \to \pi(U)$ is a $G$-torsor.
The following proposition (taken from [Mi], III, Prop. 4.1] explains why torsors may be considered as locally trivial \( G \)-bundles.

**Proposition 1.3.8.** Let \( X \in \text{Sch}/S \). Let \( G \in \text{GrpSch}/S \) be flat and locally of finite type over \( S \). Furthermore, let \( \rho : X \times_S G \to X \) be a right action. Then the following statements are equivalent:

(i) \( X \to S \) is a \( G \)-torsor.

(ii) There exists a covering \( (U_i \to S)_{i \in I} \) in the fppf-topology such that for all \( i \) we have a \( G \)-equivariant isomorphism \( U_i \times_S G \cong U_i \times_S X \) over \( U_i \).

Proof. (i) \( \Rightarrow \) (ii) is trivial, as we may take the family \( (U_i \to S)_{i \in I} \) to consist of the single element \( X \to S \).

(ii) \( \Rightarrow \) (i): First note that \( U \cong \bigsqcup_{i \in I} U_i \to S \) is faithfully flat and locally of finite type. Putting the given isomorphisms together, we obtain a \( G_U \)-equivariant isomorphism \( G_U \cong X_U \). In particular, \( X_U \) is faithfully flat and locally of finite type over \( U \). By descent, we conclude that the same holds for \( X \to S \). Now we want to check that \((\text{id}_{X_U}, \rho_U) : X_U \times_U G_U \to X_U \times_U X_U \) is an isomorphism. After using the \( G_U \)-equivariant isomorphism \( G_U \cong X_U \), this is equivalent to the following map being an isomorphism

\[
(id_{X_U}, \mu) : G_U \times_U G_U \to G_U \times_U X_U.
\]

But clearly, an inverse is given by \((g, h) \mapsto (g, s^{-1}h)\). Thus \((id_{X_U}, \rho_U)\) is an isomorphism and by descent so is \((id_X, \rho)\).

\( \square \)

**Example 1.3.9.** Let us take a closer look at the situation \( S = \text{Spec}(k) \) is the spectrum of a field and \( G \) is a smooth affine algebraic group over \( k \). Let \( X \to \text{Spec}(k) \) be a \( G \)-torsor. From 1.3.8 and descent, we obtain that \( X \to \text{Spec}(k) \) is smooth and of finite type. Now note the following result from [EGA IV, Cor. 17.16.3]:

**Lemma 1.3.10.** Let \( X \to S \) be a smooth surjective morphism. Then there exists a scheme \( S' \) and a surjective, étale morphism \( S' \to S \) such that \( X \times_S S' \to S' \) has a section.

If we apply this lemma with \( S = \text{Spec}(k) \) and use 1.3.4 we conclude that \( G_U \cong X_U \) for some étale covering \( U \to k \). By [Mi], I, Prop. 3.2], we can write \( U \cong \bigsqcup_{\ell_i \mid k} \text{Spec}(\ell_i) \), where the \( \ell_i \supset k \) are finite, separable field extensions of \( k \). Since we have an isomorphism \( G_U \cong X_U \) over \( U \), we conclude \( G_{\text{Spec}(\ell_i)} \cong X_{\text{Spec}(\ell_i)} \).

In particular, we have a \( G_k \)-equivariant isomorphism \( G_k \cong X_k \). On the other hand, suppose \( X \) is a \( k \)-scheme with a \( G \)-action and such that we have a \( G_k \)-equivariant isomorphism \( G_k \cong X_k \). In particular \( X_k \to \text{Spec}(k) \) is smooth and of finite type; hence so is \( X \to \text{Spec}(k) \) by descent. Thus we already have \( G_k \cong X_k \) over some finite Galois extension \( k \subset L \subset k \). But \( \text{Spec}(L) \to \text{Spec}(k) \) is certainly faithfully flat and locally of finite type. By 1.3.8 \( X \to \text{Spec}(k) \) is a \( G \)-torsor.

Here is an important property of \( G \)-torsors.

**Proposition 1.3.11.** Let \( X, X' \in \text{Sch}/S \) be \( G \)-torsors over \( S \) and let \( f : X \to X' \) be a \( G \)-equivariant \( S \)-morphism. Then \( f \) is an isomorphism.

Proof. The proof is taken from [DG, III, §4.1.4]. Since \( X \to S, X' \to S \) are both faithfully flat, so is \( X \times_S X' \to S \). By descent, it suffices to show that the induced morphism \((id_{X'}, id_X, f) : X \times_S X' \times_S X \to X \times_S X' \times_S X' \) is an isomorphism. By the definition of a torsor, we have isomorphisms

\[
(id_X, \psi') : X \times_S (X' \times_S G) \cong X \times_S X' \times_S X'
\]

and

\[
(id_{X'}, \psi) : X' \times_S (X \times_S G) \cong X' \times_S X \times_S X.
\]

Furthermore, we also have an isomorphism

\[
\psi := t_{1,2} \circ (id_{X'}, \psi) \circ t_{1,2} : X \times_S X' \times_S G \cong X \times_S X' \times_S S.
\]

where \( t_{1,2} \) denotes the switching of the first two coordinates. Thus, there exists a unique \( G \)-equivariant morphism \( \alpha : X \times_S X' \times_S G \to X \times_S X' \times_S G \) making the following diagram commutative

\[
\begin{array}{ccc}
X \times_S X' \times_S G & \xrightarrow{\psi} & X \times_S X' \times_S X \\
\downarrow & & \downarrow
\end{array}
\]

\[
\begin{array}{ccc}
X \times_S X' \times_S G & \xrightarrow{(id_X, \psi')} & X \times_S X' \times_S X' \times_S G.
\end{array}
\]

It follows from the construction that \( \alpha \) is of the form \( \alpha(x, x', g) = (x, x', \beta(x, x', g)) \). As \( \alpha \) is \( G \)-equivariant, we conclude \( \beta(x, x', g') = \beta(x, x', g) \cdot g \). In particular \( \beta(x, x', g) = \beta(x, x', e) \cdot g \) and an easy computation shows that \( (x, x', g) \mapsto (x, x', \beta(x, x', e^{-1}g)) \) provides an inverse to \( \alpha \).

\( \square \)
We have already seen in [1.2.20] how quotients may give rise to torsors. Here is a result in the other direction:

**Proposition 1.3.12.** Let \( X,Y \in \text{Sch}/S \), let \( G \in \text{GrpSch}/S \) be faithfully flat and of finite type and suppose \( \pi: X \to Y \) is a \( G \)-torsor. Then \( Y \) is a categorical quotient of \( X \) by \( G \), i.e. \( Y \cong X/G \).

**Proof.** To prove \( X/G \cong Y \), we need to show that the following diagram is cocartesian:

\[
\begin{array}{ccc}
X \times_S G & \xrightarrow{\pi_1} & X \\
\downarrow \rho & & \downarrow \pi \\
X & \xrightarrow{\pi} & Y.
\end{array}
\]

Since \( \pi \) is a \( G \)-torsor, this diagram is isomorphic to

\[
\begin{array}{ccc}
X \times_Y X & \xrightarrow{\rho_1} & X \\
\downarrow \rho_2 & & \downarrow \pi \\
X & \xrightarrow{\pi} & Y.
\end{array}
\]

The property that this square should be cartesian can be rephrased by saying that for all \( Z \) the diagram

\[
\text{Hom}_Y(Y,Z \times_S Y) \to \text{Hom}_X(X,Z \times_S X) \xrightarrow{\pi_*} \text{Hom}_{X \times_S X}(X \times_Y X,Z \times_S X) \times_Y X
\]

is an equalizer. But this is true, since \( X \to Y \) is faithfully flat and quasi-compact. See [SGA1, VIII, Thm. 5.3]. \( \square \)

Now the stage is set to introduce one of the main protagonists:

**Definition 1.3.13** (Versal torsor). Let \( G \in \text{GrpSch}/k_0 \) be a smooth affine algebraic group. Let \( K \) be a field extension of \( k_0 \). A \( G \)-torsor \( P \to \text{Spec}(K) \) is said to be versal, if there exists a smooth, irreducible \( k_0 \)-scheme \( X \) with function field \( K \) and a \( G \)-torsor \( Q \to X \) satisfying the following conditions:

- If we denote the generic point of \( X \) by \( \eta \), then \( P \to \text{Spec}(K) \) is the generic fiber of \( Q \to X \), i.e. we have a cartesian diagram

\[
\begin{array}{ccc}
P & \xrightarrow{\pi} & Q \\
\downarrow & & \downarrow \\
\text{Spec}(K) & \xrightarrow{\eta} & X.
\end{array}
\]

- Let \( k/k_0 \) be a field extension with \( k \) infinite and let \( Y \to \text{Spec}(k) \) be a \( G \)-torsor. Then the set of \( k \)-rational points \( x \in X(k) \) such that the fiber \( Q_x \to \text{Spec}(k) \) is isomorphic to \( Y \to \text{Spec}(k) \) is dense in \( X \).

Before we can show the existence of versal torsors, it is convenient to know the cocycle interpretation of \( G \)-torsors. This will be recalled in the next section.

**1.3.2 \( G \)-torsors and \( H^1(k,G) \)**

The aim of this section is to introduce the non-abelian cohomology set \( H^1(k,G) \) and to show that it classifies isomorphism classes of \( G \)-torsors over \( k \). As we will see, there are situations where it is far more convenient to work with elements of \( H^1(k,G) \) rather than dealing with \( G \)-torsors directly. Much of the material covered in this section is taken from [SGA1].

First we recall some notation: \( k \) will always denote a field and \( k_s \) a separable closure of \( k \). We denote by \( \Gamma = \Gamma_k = \text{Gal}(k_s/k) \) the absolute Galois group of \( k_s/k \).

Let \( A \) be a \( \Gamma \)-group, i.e. \( A \) is a (not necessarily commutative, not necessarily finite) abstract group, on which \( \Gamma \) acts continuously by group automorphisms. Here \( A \) is endowed with the discrete topology. Another way to express this continuity is to say that for each element \( a \in A \) the stabilizer subgroup \( \{ \sigma \in \Gamma \mid \sigma(a) = a \} \) is open in \( \Gamma \).

**Example 1.3.14.** Let \( G \) be a smooth affine algebraic group over \( k \), then \( G(k_s) \) is a continuous \( \Gamma \)-module. Given \( x: \text{Spec}(k_s) \to G \) and \( a \in \Gamma \), the left action of \( \sigma \) on \( x \) is defined to be the point

\[
\text{Spec}(k_s) \xrightarrow{\sigma} \text{Spec}(k_s) \to G,
\]
i.e. \( \sigma(x) := x(\sigma') := x \circ \sigma' \). This action is continuous. Indeed \( G(k) \) consists of closed points \( x \in G \) whose residue field \( v(x) \) can be embedded into \( k_\sigma \). But since \( x \) is closed, \( k(x) \) is actually a finite extension of \( k \). After taking the normal closure of \( k(x) \subset k_\sigma \), we see that \( \text{Spec}(k) \to G \) factors as \( \text{Spec}(k_\sigma) \to \text{Spec}(L) \to G \) for some finite Galois extension \( L \supset k \). Thus \( \text{Gal}(k/L) \) acts trivially on \( x \).

In the case of \( G = \text{GL}_n \), we can give another interpretation of this action: Let \( V \cong k^n \) be an \( n \)-dimensional \( k \)-vector space and \( L/k \) be a finite Galois extension. For \( v \in \mathbb{A}^n(L), g \in \text{GL}_n(L) \) and \( \sigma \in \text{Gal}(L/k) \) we then have \( g(\sigma') \cdot v(\sigma') = (g \cdot v)(\sigma') \). That is, \( \sigma(g) \in \text{GL}_n(L) \) is the \( L \)-linear automorphism \( \sigma \circ g \circ \sigma^{-1} \) of \( L^n \) (where \( \sigma \) is the \( k \)-linear automorphism obtained by applying \( \sigma \in \text{Gal}(L/k) \) diagonally to each coordinate of \( L^n \)).

Now let \( A \) be a \( \Gamma \)-group. By \( Z^1(\Gamma, A) \), we denote the pointed set of 1-cocycles from \( \Gamma \) to \( A \). This is the set of continuous functions

\[
c : \Gamma \to A \quad \sigma \mapsto c_\sigma,
\]

such that \( \forall \sigma, \tau \in \Gamma \) we have \( c_{\sigma \tau} = c_\sigma \cdot \sigma(c_\tau) \). Before we continue, let us first think a moment about the consequences of the continuity. It implies that \( c^{-1}(e) = \text{Gal}(k/L) \) for some finite Galois extension \( L \supset k_0 \). But this means that for any \( \sigma \in \Gamma, \tau \in \text{Gal}(k/L) \) we have

\[
c_{\sigma \tau} = c_\sigma \cdot \sigma(c_\tau) = c_\sigma \cdot \sigma(e) = c_\sigma.
\]

Hence \( c : \Gamma \to A \) factors as \( \Gamma \to \text{Gal}(L/k) \overset{\pi}{\to} A \), for some cocycle \( \overline{c} : \text{Gal}(L/k) \to A \).

One can define an equivalence relation on \( Z^1(\Gamma, A) \), such that for \( a, b \in Z^1(\Gamma, A) \) we have \( a \sim b \) iff there exists \( c \in A \) satisfying \( a_\sigma = c^{-1} \cdot b_\sigma \cdot \sigma(c) \) for all \( \sigma \in \Gamma \). We say that two such cocycles are cohomologous. The set of equivalence classes \( Z^1(\Gamma, A) / \sim \) will be denoted by \( H^1(\Gamma, A) \). It is pointed by the class of the trivial cocycle. This is well-defined in the sense that taking another separable closure of \( k \) yields a cohomology set which is canonically isomorphic to the old one (see [Se2], X, §4). If \( G \) is a smooth affine algebraic group over \( k \), we define \( H^1(k, G) := H^1(k, G(k)) \), where \( G(k) \) is viewed as a discrete group. Now we want to establish a bijection between \( G \)-torsors over \( k \) and elements of \( H^1(k, G) \). Before we can do this, let us recall two important technical lemmas:

**Lemma 1.3.15.** Let \( k \) be a field and \( k \subset \ell \) be a finite Galois extension. Let \( V \) be an \( \ell \)-vector space endowed with a semi-linear \( \text{Gal}(\ell/k) \)-action. Let \( V^{\text{Gal}(\ell/k)} := \{ v \in V \mid \sigma(v) = v \text{ for all } \sigma \in \Gamma \} \). Then the canonical map

\[
v^{\text{Gal}(\ell/k)} \otimes_k \ell \to V
x \otimes \lambda \mapsto \lambda \cdot x
\]

is an isomorphism.

**Proof.** Well-known. See e.g. [Bos] 4.11, Satz 4. \( \square \)

**Corollary 1.3.16** (Hilbert 90). \( H^1(k, \text{GL}_n) = \{ e \} \).

**Proof.** Let \( c \in Z^1(\Gamma, \text{GL}_n) \). Choose a finite Galois extension \( \ell/k \) such that \( \sigma \mapsto c_\sigma \) factors through \( \text{Gal}(\ell/k) \). Let \( V = \ell^n \) and define a left-action of \( G := \text{Gal}(\ell/k) \) on \( V \) by

\[
\star : G \times V \to V
(\sigma, v) \mapsto \sigma \star v = c_\sigma \cdot v(\sigma') \cdot \sigma(v).
\]

If we consider \( v \) as an element of \( \mathbb{A}^n(\ell) \), we may also write this action as \( \sigma \star v = c_\sigma \cdot v(\sigma') \). Since \( c \) is a cocycle, we thus compute

\[
c_\sigma \cdot (c_\tau \cdot v(\tau'))(\sigma') = c_\sigma \cdot c_\tau(\sigma') \cdot v(\tau' \circ \sigma') = c_{\sigma \tau} \cdot v(\sigma \tau').
\]

This shows that \( \star \) does indeed define an action of \( G \) on \( V \). Now it follows from the previous lemma that \( V^{\text{Gal}(\ell/k)} \) has dimension \( n \); let \( \{ b_1, \ldots, b_n \} \) be a basis of this space. Now let \( g \in \text{GL}_n(\ell) \) be the map sending \( b_i \mapsto e_i \),
where $e_1, \ldots, e_n \in V$ is the standard basis. Then we have
\[
\begin{align*}
g^{-1}(\sigma(g)(b_i))) &= g^{-1}(\sigma(g(b_i))) \\
&= g^{-1}(\sigma(e_i)) \\
&= b_i \\
&= c_\sigma(b_i).
\end{align*}
\]
This proves $c_\sigma = g^{-1} \cdot \sigma(g)$.

Now let us start with a $G$-torsor $Y \to \text{Spec}(k)$ to which we want to associate a cocycle. We can choose a finite Galois extension $L \supset k$ and a $G_L$-equivariant isomorphism $\alpha: G_L \cong Y_L$. In particular, if we choose an arbitrary element $y_0 \in Y(L)$, then for any $\sigma \in \text{Gal}(L/k)$ there exists a unique $c_\sigma \in G(L)$, such that $\sigma(y_0) = y_0 \cdot c_\sigma$. The assignment $\sigma \mapsto c_\sigma$ satisfies the cocycle condition and thus induces a continuous cocycle $\Gamma \to \text{Gal}(L/k) \to G(k)$. Moreover, one can check that choosing another $y_0' \in Y(L)$ yields a cocycle which is cohomologous to $c_\sigma$.

Defining an inverse is slightly harder. So let $c \in Z(\Gamma, G(k))$ be a continuous cocycle. Since it is continuous, it factors as $\Gamma \to \text{Gal}(L/k) \to G(L)$ for some finite Galois extension $L/k$. The idea is to define the desired $G$-torsor as the quotient of $G_L$ by a certain kind of twisted action of $\text{Gal}(L/k)$. Let us turn to the technical details. Since $G$ is an affine algebraic group over $k$, we can write it as $G = \text{Spec}(A)$ for some finite type $k$-algebra $A$. We claim that there is a semi-linear left action of $\text{Gal}(L/k)$ on $A \otimes_k L$ defined by
\[
(\sigma, a) \mapsto \sigma \ast a := (1 \otimes \sigma)(\lambda^{\#}_{\text{cyc}}(a)).
\]
Here $\lambda_{\text{cyc}}: G_L \to G_L$ is the left multiplication by $c_{\text{cyc}}$ and $\lambda^{\#}_{\text{cyc}}: A \otimes L \to A \otimes L$ is the induced map on the coordinate rings. To see that it is a left action, it is sufficient to check that the induced map on schemes is a right action. So we need to verify that
\[
\begin{align*}
G \times \text{Spec}(L) &\stackrel{(\text{id}_L, \text{id}_L)}{\longrightarrow} G \times \text{Spec}(L) \\
&\stackrel{\lambda_{\text{cyc}}}{\longrightarrow} G \times \text{Spec}(L) \\
&\stackrel{(\text{id}_L, \text{id}_L)}{\longrightarrow} G \times \text{Spec}(L)
\end{align*}
\]
agree. It suffices to prove that
\[
\text{Spec}(L) \overset{\alpha'}{\longrightarrow} \text{Spec}(L) \overset{(\cdot)_{\text{cyc}}}{\longrightarrow} G \times \text{Spec}(L) \overset{\mu \times \text{id}_{\text{Spec}(L)}}{\longrightarrow} G \times \text{Spec}(L)
\]
and
\[
\text{Spec}(L) \overset{\alpha' \ast}{\longrightarrow} \text{Spec}(L) \overset{(\cdot)_{\text{cyc}}}{\longrightarrow} G \times \text{Spec}(L) \overset{\mu \times \text{id}_{\text{Spec}(L)}}{\longrightarrow} G \times \text{Spec}(L)
\]
coincide. But by the cocycle condition we have
\[
ce_{\text{cyc}}(\alpha \ast \sigma) = c_{\text{cyc}} \cdot c_{\text{cyc}}((\sigma^{-1})^-1)((\sigma^{-1})^-1)
\]

Let $A^\ast \subset A \otimes L$ be the subring of elements invariant under the $\ast$-action. The multiplication $\mu: G \times G \to G \times L$ is equivariant with respect to this action and by $[13,13]$ $A^\ast$ is a twisted form of $A$ in the sense that $A^\ast \otimes_k L \cong A \otimes L$. Thus $\text{Spec}(A^\ast) \to \text{Spec}(k)$ is indeed a $G$-torsor. This construction does not depend on the choice of a representative of the cocycle class $[c]$. Indeed, let $a \in G(L)$ and consider the cocycle $\tilde{d}$ defined by $\sigma \mapsto a^{-1} \cdot c_{\text{cyc}} \cdot \sigma(a)$. Then $\lambda_{\text{cyc}}: G_L \to G_L$ induces an isomorphism $\text{Spec}(A^\ast) \cong \text{Spec}(A^\ast)$.

Now we have constructed two maps: one which takes a $G$-torsor over $k$ and returns an element of $H^1(k, G)$; and one which goes the other way. It remains to show that these two are in fact inverse. So first let $c \in H^1(\Gamma, G)$ be a cocycle and let $\text{Spec}(A^\ast)$ be the $G$-torsor constructed above. Let $x_0 \in \text{Spec}(A^\ast)(L)$ be the image of the neutral element $e \in G(L)$ under the morphism $G_L \to \text{Spec}(A^\ast)_L$ and let $(g, s) \in (G \times L)(L)$ be arbitrary. Then $(g, s)$ and $(c_{\text{cyc}}((\sigma')^{-1} \circ s) \cdot g, (\sigma')^{-1} \circ s)$ have the same image in $(\text{Spec}(A^\ast))(L)$. If we apply this with $s = \sigma'$ and $g = e$, we obtain $\sigma = c_{\text{cyc}}$.

On the other hand, let $X \to \text{Spec}(k)$ be any $G$-torsor over $k$ and choose an arbitrary $x_0 \in X(L)$. Let $\sigma \mapsto c_{\text{cyc}}$ be the cocycle defined by this point. We have a map $\beta: G_L \to X_L, g \mapsto x_0 \cdot g$. Let us show that this map is equivariant with respect to the right action of $\text{Gal}(L/k)$. Here the left hand side carries the $\ast$-action, while $\sigma \in \text{Gal}(L/k)$ acts on $X_L$ by $(x, s) \mapsto (x, \sigma^{-1} \circ s)$. As soon as this is proven, we obtain a $G$-equivariant map.
Spec(A') → X. Since both schemes are G-torsors, this is automatically an isomorphism. So let σ ∈ Gal(L/k), T ∈ Sch/k, g ∈ G(T), ℓ ∈ L(T); define ℓ' := σ* ◦ ℓ. Then we have
\[(x_{0}(ℓ') \cdot c_{σ^{-1}}(ℓ') \cdot g, ℓ') = (x_{0}(ℓ) \cdot c_{σ}(ℓ) \cdot c_{σ^{-1}}(ℓ') \cdot g, ℓ') \]
\[= (x_{0}(ℓ) \cdot c_{σ}(ℓ) \cdot g, ℓ'), \]
We conclude:

**Theorem 1.3.17.** Let G be smooth, affine algebraic group over k. Then the above constructions induce a bijection
\[\text{Tors}(k, G) \leftrightarrow H^1(k, G).\]

**Remark 1.3.18.** Of course, this theorem is just a very special case of [MüIII, III, Corollary 4.7]. However, taking into account the general style of our approach and the kind of examples we will meet later, I considered it preferable to give a more pedestrian proof in the spirit of [SeI, III, Prop. 1.3].

**Example 1.3.19.** The construction is functorial in the following sense: Let K ⊆ k be a field extension and X → Spec(k) be a G-torsor; then X_K is a G-torsor over K. Using the explicit construction above, the map X → X_K can be described in terms of cocycles as follows:

Let K/K be a separable closure; let k be the separable closure of k in K (which is then a separable closure of k). Put Γ_k := Gal(k/K) and Γ_K := Gal(K/k). Clearly, each automorphism σ ∈ Γ_K restricts to an element of Γ_k; this gives a group homomorphism ρ: Γ_K → Γ_k. For each continuous cocycle c: Γ_k → G(k) the composite \(\tilde{c}: \Gamma_K \xrightarrow{\rho} \Gamma_k \xrightarrow{c} G(k) \rightarrow G(K)\) is again a continuous cocycle.

Now let X → Spec(k) be a G-torsor and choose an element \(x_0: \text{Spec}(k) \rightarrow X\), let \(t_k: K \subseteq K_s, s_k: k_s \subseteq k_s\) be the inclusions and consider the \(K_s\)-rational point \(x'_0 := (x_0(t^*_k), t^*_k) \in X_K(K_s)\). Let \(c \in Z^1(\Gamma_K, G)\) be the cocycle defined by the point \(x_0\). For σ ∈ Γ_K, we have
\[\sigma((x_0(t_k^*), t_k^*)) = (x_0(t_k^* \circ \sigma^*, t_k^* \circ \sigma^*)) \]
\[= (x_0(\rho(\sigma^*) \circ t^*_k), t^*_k) \]
\[= (x_0(t^*_k) \cdot c_{\rho(\sigma)}(t^*_k), t^*_k) \]
Thus the cocycle associated to \(x'_0 \in X_K(K_s)\) is just \(\tilde{c} \in Z^1(\Gamma_K, G)\). Sometimes we will also write \(\text{res}_k^X(c)\) for \(\tilde{c}\).

One example, where it is often more convenient to work with cocycles instead of torsors is the following:

**Example 1.3.20.** Let G, G' be smooth affine algebraic groups over k and let \(f: G' \rightarrow G\) be a map of algebraic groups. Furthermore, let \(c \in Z^1(\Gamma, G')\) be a continuous cocycle of G. Furthermore this assignment maps cohomologous cycles to cohomologous cycles. Thus it induces a map of pointed sets \(f^*: H^1(k, G') \rightarrow H^1(k, G)\). In particular, if \(G' \subseteq G\) is a closed subgroup, we will call this the induction map and denote it by \(\text{ind}_{G'}^{G}\). Furthermore, we have:

**Lemma 1.3.21.** Let G be a smooth affine algebraic group over k and let \(g \in G(k)\) be a k-rational point. Let \(t_g: G \rightarrow G\) be the conjugation by g (i.e. \(t_g(h) = g \cdot h \cdot g^{-1}\)). Then \(t_g\) induces the identity on \(H^1(k, G)\)

**Proof.** Let \(c \in Z^1(\Gamma, G)\) be a cocycle; then \(t_g^*(c)\) is the cocycle
\[d: \Gamma \rightarrow G(k)\]
\[\sigma \mapsto g \cdot c_\sigma \cdot g^{-1} = g \cdot c_\sigma \cdot (\sigma^{-1}).\]
Thus c and d are cohomologous. \(\square\)

Before we do some concrete computations, let us note the following useful technical lemma:

**Lemma 1.3.22.** Let \(A \subseteq B\) be \(\Gamma\)-groups, then we have a "long" exact sequence
\[1 \rightarrow A^\Gamma \rightarrow B^\Gamma \rightarrow (B/A)^\Gamma \xrightarrow{\delta} H^1(k, A) \rightarrow H^1(k, B).\]

**Proof.** The connecting morphism \(\delta\) is constructed as follows. Let \(b \in B\) represent a class \(\bar{B} \in (B/A)^\Gamma\). Then for each \(\sigma \in \Gamma\) there exists a unique \(a_\sigma \in A\) such that \(\sigma(b) = b \cdot a_\sigma\). It is not hard to check that this gives rise to a cocycle \(\sigma \mapsto a_\sigma\) whose class in \(H^1(k, A)\) is independent of the choice of a representative \(b\) for \(\bar{B}\). For the rest of the proof see [SeI, VII, Annexe, Prop. 1]. \(\square\)
Example 1.3.23. We have already observed that $H^1(k, Gl_n) = \{ \ast \}$. We can also compute $H^1(k, \mu_\ell)$ explicitly: Let $\ell$ be a prime and $\text{char}(k) \neq \ell$. By considering the “long” exact cohomology sequence associated to the short exact sequence

$$1 \rightarrow \mu_\ell \rightarrow k^\times \xrightarrow{\cdot \ell} k^\times \rightarrow 1,$$

and by using Hilbert 90, we obtain $H^1(k, \mu_\ell) \cong k^\times/(k^\times)^\ell$. Furthermore note the following lemma which follows immediately from the definition of first cohomology sets:

Lemma 1.3.24. Let $G, H$ be smooth affine algebraic groups over $k$. Then we have a canonical isomorphism of pointed sets $H^1(k, G \times H) \xrightarrow{\sim} H^1(k, G) \times H^1(k, H)$.

Assume $\text{char}(k) \neq 2$. Then $\mu_2$ is isomorphic to the constant finite group scheme $\mathbb{Z}/2$. Using the computation and the lemma above, we obtain $H^1(k, (\mathbb{Z}/2)^n) \cong (k^\times/k^\times)^n$.

Using the results of this section, we can now prove the existence of versal torsors for smooth affine algebraic groups (the proofs are taken from [GMS, Chapter 5]).

Example 1.3.25. Let $G$ be a smooth affine algebraic group over $k_0$ and choose some closed embedding $G \subset Gl_N$ (such an embedding always exists; see e.g. [BG, Prop. 1.10]). Now consider the torsor $Q := Gl_N \rightarrow X := Gl_N/G$. Let $P \rightarrow \text{Spec}(k(X))$ be the generic fiber of $\pi : Q \rightarrow X$ and let $k/k_0$ be a field extension. By taking the fiber, every $k$-rational point $x : \text{Spec}(k) \rightarrow X$ defines a $G$-torsor $Q_x \rightarrow \text{Spec}(k)$. It follows from the long exact sequence [3.22] that the cohomology classes of torsors obtained in this way form exactly the kernel of the map $H^1(k, G) \rightarrow H^1(k, Gl_N)$. But by Hilbert 90 this means, that every $G$-torsor $T \rightarrow \text{Spec}(k)$ is obtained in this way. In other words, if we start with a field extension $k/k_0$ and a $G$-torsor $T \rightarrow \text{Spec}(k)$, then we can find a $k$-rational point $x \in X(k)$, such that $T = Q_x$.

To show that $Q$ is a versal torsor, we only need to prove that if $k$ is infinite, then the set of such $k$-rational points is in fact dense in $X$. So let $x \in X(k)$ be one of these. First suppose $k = k_0$ and consider the map

$$\rho_x : Gl_N \rightarrow X$$

$$g \mapsto g \cdot x.$$

We claim that

Lemma 1.3.26. $\rho_x$ is surjective.

Proof. $\rho_x$ is obtained after base change along $\text{Spec}(k) \rightarrow X$ of the map

$$Gl_N \times X \rightarrow X \times X$$

$$(g, \overline{x}) \mapsto (g \cdot \overline{x}, \overline{x}).$$

On the other hand, pulling back the map just defined along $\pi : Q \rightarrow X$, we conclude by descent that it suffices to prove surjectivity of

$$Gl_N \times Q \rightarrow X \times Q$$

$$(g, q) \mapsto (\pi(g \cdot q), q).$$

This is clear, as both maps occurring in the composite $Gl_N \times Q \xrightarrow{\rho_x} X \times Q \xrightarrow{\pi, \text{id}_Q} X \times Q$ are surjective. \qed

Now let’s continue the proof of the existence of versal torsors. Let $U \subset X$ be any non-empty open subscheme. Then $\rho_x^{-1}(U) \subset Gl_N$ is a non-empty open subscheme. Since $k$ is infinite, $Gl_N(k) \subset Gl_N$ is dense. Hence there exists $g \in Gl_N(k) \cap \rho_x^{-1}(U)$, i.e. $g \cdot x \in U$. Now we only need to observe that for $g \in Gl_n(k)$, multiplication by $g$ induces an isomorphism of $G$-torsors $Q_x \cong Q_g x$.

In the general case, we have a cartesian square

$$\begin{array}{ccc}
Q_k & \longrightarrow & Q \\
\downarrow & & \downarrow \\
X_k & \longrightarrow & X.
\end{array}$$

Any non-empty, open subscheme $U \subset X$ induces a non-empty, open subscheme $U_k \subset X_k$. Thus we conclude by the special case treated above.

This ensures the existence of versal torsors. However, there is another construction which is often nicer to work with.
Example 1.3.27. Let \( G \) be a smooth affine algebraic group over \( k_0 \) and choose some closed embedding \( G \subset \text{GL}_N \). Put \( V := \mathbb{A}^N_{k_0} \). Assume that there exists a non-empty, open, \( G \)-invariant subscheme \( V' \subset V \) such that the categorical quotient \( X := V'/G \) exists and \( V' \rightarrow X \) is a \( G \)-torsor. We claim that the generic fiber \( P \rightarrow \text{Spec}(k(X)) \) of \( V' \rightarrow X \) is a versal torsor.

Let \( k \succ k_0 \) be infinite and \( T \rightarrow \text{Spec}(k) \) be a \( G \)-torsor. We first assume \( k = k_0 \) and let \( 0 \neq v \in V'(k) \) be any \( k \)-rational point (which exists, since \( k \) is infinite). Now

\[
\text{GL}_N \cong k \times_k \text{GL}_N \xrightarrow{(v,0)} V \times_k \text{GL}_N \xrightarrow{\phi} V
\]

is a \( G \)-equivariant dominant morphism. Indeed, \( \text{GL}_N(k) \) acts transitively on \( V(k) - \{0\} \) and each non-empty, open subscheme of \( V \) contains a \( k \)-rational point. Let \( U \subset \text{GL}_N \) be the preimage of \( V' \subset V \) under this morphism. Then \( U \subset \text{GL}_N \) is a non-empty, open, \( G \)-invariant subscheme and we have a dominant, equivariant morphism \( \tilde{\phi} : U \rightarrow V' \). By \[1.3.5\] and \[1.3.7\] the quotient \( U \rightarrow U/G \) exists and is a \( G \)-torsor. Furthermore, \( \tilde{\phi} \) induces a map \( \phi : U/G \rightarrow X \).

If \( W \subset X \) is open and non-empty, then so is \( \tilde{\phi}^{-1}(W) \subset U/G \). By the previous example, there exists a \( k \)-rational point \( y \in \phi^{-1}(W)(k) \) such that \( \pi_{\tilde{U} \rightarrow U/G}(y) \rightarrow \text{Spec}(k) \) is isomorphic to the given torsor \( T \rightarrow \text{Spec}(k) \).

That is, we have a commutative diagram of cartesian squares

\[
\begin{array}{ccc}
T & \longrightarrow & U \\
\downarrow & & \downarrow \\
\text{Spec}(k) & \longrightarrow & U/G \\
\end{array}
\]

Thus \( V' \rightarrow X \) is indeed versal. As in the previous example, we obtain the general case by substituting in the above arguments \( V \) by \( V_{\ell} \), \( V' \) by \( V'_{\ell} \) etc. and observing that all the arguments given there also hold after changing the base field.

Remark 1.3.28. Let \( G \) be an affine algebraic group over \( k_0 \) acting set-theoretically freely on a finite type \( k \)-scheme \( X \). Then there exists a dense, open, \( G \)-invariant subscheme \( U \subset X \) such that the categorical quotient \( U/G \) exists and \( U \rightarrow U/G \) is a \( G \)-torsor. This follows from \[SGA3, \text{V, Thm. 8.1}\] or its specialization to our situation as stated in \[BF, \text{Prop. 4.7}\].

In particular, we may use the above example in the case of constant finite group schemes:

Corollary 1.3.29. Let \( V \) be a finite dimensional \( k_0 \)-vector space and let \( G \) be a constant finite group scheme. Choose a faithful representation of \( G \) on a finite-dimensional \( k_0 \)-vector space \( V \). Then \( \text{Spec}(k(V)) \rightarrow \text{Spec}(k(V)^G) \) is a versal \( G \)-torsor.

Proof. The injection \( G \subset \text{GL}_n(k_0) \) of abstract groups induces a closed immersion \( \varphi : G \rightarrow \text{GL}_n \). For each \( g \in G \), we can consider the linear subspace \( \{ x \in V(k) \mid \varphi(g)(x) = x \} \). This defines a hyperplane \( Z_x \subset V \) (observe that the \( \varphi(g) \) are defined over \( k_0 \)). Now \( U := V - \cup_{g \in G} Z_g \subset V \) is non-empty, open and \( G \)-invariant. By construction the action of \( G \) on \( U \) is free on the closed points. By \[1.2.11\] it is then scheme-theoretically free. Now the claim follows from the previous example and \[1.2.20\].

\[ \square \]

Example 1.3.30. Suppose \( \text{char}(k_0) \neq 2 \). We have a faithful representation of \( \mathbb{Z}/2 \) on \( \mathbb{A}^1 \), where the action of the non-trivial element in \( \mathbb{Z}/2 \) is given by the linear automorphism

\[
\mathbb{A}^1 \rightarrow \mathbb{A}^1 \\
x \mapsto -x.
\]

This induces a faithful representation of \( G := (\mathbb{Z}/2)^n \) on \( \mathbb{A}^n \). The action of \( G \) is free on the \( G \)-invariant open subscheme \( (G_0)^n \subset \mathbb{A}^n \). Thus \( (G_0)^n \rightarrow (G_0)^n/G \) is a \( G \)-torsor and taking the fiber over the generic point, we obtain that \( \text{Spec}(k_0(t_1, \ldots, t_n)) \rightarrow \text{Spec}(k_0(t_1^2, \ldots, t_n^2)) \) is a versal \( G \)-torsor.

1.3.3 \( H^1 \) and twisted forms

In the previous section, we saw that classifying all \( G \)-torsors over \( k \) is equivalent to understanding \( H^1(k, G) \). Now we want to recall another characterization of certain cohomology sets in terms of twisted forms. Our presentation is modeled after the standard sources \[Se1, \text{III, \S1}\] and \[Se2, \text{X, \S2}\].

We are interested in pairs \( (V, x) \), where \( V \) is a finite-dimensional \( k \)-vector space and \( x \in V^\otimes \otimes (V')^\otimes \cong \text{Hom}_k(V^\otimes, V'^\otimes) \). Two such pairs \( (V, x), (V', x') \) are called \( k \)-isomorphic, if there exists an isomorphism \( f : V \rightarrow V' \), such that \( f(x) := f^\otimes \otimes ((f)^{-1})^\otimes(x) = x' \).
For \( K/k \) a field extension, we can create a new pair \((V_k, x_k)\) out of \((V, x)\) by defining \( V_K := V \otimes_k K \) and \( x_K := x \otimes 1 \in V^\text{op} \otimes (V^\text{op})^\text{op} \otimes K \). As soon as we have fixed some \((V, x)\), we denote by \( E(K/k) \) the set of \( K \)-forms of \((V, x)\) up to \( k \)-isomorphism. That is, \( E(K/k) = \{(V', x') | (V'_K, x'_K) \cong (V_K, x_K)\}/\sim \) where \((V', x') \sim (V'', x'')\), iff they are \( k \)-isomorphic.

Now we want to study the connection between \( K \)-forms and \( H^1 \). So let \( K = k \) be a separable closure of \( k \). Denote by \( A(K) \) the set of \( K \)-automorphisms of \((V_k, x_k)\) and put \( \Gamma := \text{Gal}(K/k) \). We have a continuous left action of \( \Gamma \) on \( A(K) \) defined by \( \sigma(f) := \sigma \circ f \circ \sigma^{-1} \) and we can form \( H^1(\Gamma, A(K)) \). Now let \((V', x') \in E(K/k)\) and let \( f : V_K \rightarrow V'_K \) be a \( K \)-isomorphism; then \( c_\sigma := f^{-1} \circ \sigma(f) \) satisfies the cocycle condition and thus defines a class \([c] \in H^1(\Gamma, A(K))\). It can be checked that this yields a well-defined map \( \theta : E(K/k) \rightarrow H^1(\Gamma, A(K)) \).

Now we have the following important theorem:

**Theorem 1.3.31.** \( \theta \) is an isomorphism.

**Proof.** We start by checking injectivity. So let \((V'_1, x'_1), (V'_2, x'_2)\) be two \( K \)-forms inducing the same class in \( H^1(\Gamma, A(K)) \) and let \( f_i : V_K \rightarrow V'_K \) be \( K \)-isomorphisms for \( i = 1, 2 \). Then there exists \( g \in A(K) \) such that \( f_i^{-1} \sigma(f_i) = (f_2g)^{-1} \sigma(f_2g) \) for all \( \sigma \in \Gamma \). But this means that the isomorphism \( f_2g f_1^{-1} \) is in fact already defined over \( k \). Now we need to show surjectivity.

Let \( c \in Z^1(\Gamma, A(K)) \) be a 1-cocycle. Since we have \( A(K) \subseteq \text{GL}(V_k) \), we conclude from \[1.3.15\] the existence of \( f \in \text{GL}(V_k) \) with the property \( c_\sigma = f^{-1} \circ \sigma(f) \) for all \( \sigma \in \Gamma \). Put \( x' := f(x) \). Then we claim that \( x' \) is already defined over \( k \). Indeed, we have

\[
\sigma(x') = \sigma(f(x)) = \sigma(f)(\sigma(x)) = \sigma(f)(x) = f \circ c_\sigma(x) = f(x).
\]

Thus \((V', x') \in E(K/k)\) and its image under \( \theta \) is just the cocycle \( c \in Z^1(\Gamma, A(K)) \).

Now let us mention two examples that will be treated in greater detail in the following sections.

**Example 1.3.32.** Let us consider the case, where \( p = 1, q = 2 \); i.e. we consider a finite dimensional \( k \)-vector space \( A \) and a bilinear mapping \( \mu : A \otimes A \rightarrow A \). For instance, if \( A \) is a finite-dimensional \( k \)-algebra, then we may take \( \mu \) to be the multiplication. For \( k/k \) an arbitrary field extension, the \( K \)-forms of \( A \) are precisely the finite-dimensional \( k \)-algebras \( B \), such that \( B \otimes_k K \cong A \otimes_k K \) (as \( k \)-algebras). Indeed, if \( \mu_k : B_K \otimes_k B_K \rightarrow B_K \) satisfies the algebra axioms, then so does \( \mu : B \otimes B \rightarrow B \). In particular, consider the case \( A = k \times k \times \ldots \times k \cong k^n \). A \( k \)-form of \( A \) is called \( \text{étale} k \)-algebra. Clearly, \( A(k) \cong S_n \) and we conclude from the theorem that \( H^1(k, S_n) \) classifies \( \text{étale} k \)-algebras.

**Example 1.3.33.** Suppose \( \text{char}(k) \neq 2 \). Now consider the case, where \( p = 0, q = 2 \); i.e. we consider a finite dimensional \( k \)-vector space \( V \) and a bilinear form \( b : V \otimes V \rightarrow k \). For instance, if \( V = k^n \), we may define \( b \) by \( b(x, y) = \sum_i x_i y_i \). The \( K \)-forms of \( (k^n, b) \) are then the spaces \((V', b')\) that become isometric to \((V, b)\) over \( K \). In particular, if \( k = k_s \) is a separable closure of \( k \), then all quadratic forms of rank \( n \) are isomorphic over \( k_s \). Thus \( E(k_s/k) \) classifies the quadratic forms of rank \( n \) over \( k \). Furthermore, we have \( A(k_s) \cong O_n(k_s) \) and conclude that \( H^1(k, O_n) \) classifies quadratic forms of rank \( n \) over \( k \).

### 1.3.4 \( G \)-torsors and \( \text{étale}/\text{Galois} \) algebras

Now we want to obtain a better understanding of \( S_n \)-torsors and of \( G \)-torsors, where \( G \) is a constant finite group scheme. We will see that the first kind is described by \( \text{étale} \) algebras, while the second one is described by \( \text{Galois} \) algebras. We have met the notion of \( \text{étale} \) algebras already in the previous section. Let us recall the precise definition:

**Definition 1.3.34.** A finite dimensional \( k \)-algebra \( L \) is called \( \text{étale} \), if \( L \otimes_k k_s \cong k_s^\text{dim}L = k_s \times k_s \times \ldots \times k_s \).

One can characterize \( \text{étale} \) algebras as follows:

**Lemma 1.3.35.** Let \( L \) be a finite-dimensional \( k \)-algebra. Then the following statements are equivalent:

(i) \( L \) is an \( \text{étale} \) \( k \)-algebra

(ii) \( |\text{Hom}_n(L, k)| = \text{dim}L \)
(iii) $L \cong K_1 \times \cdots \times K_r$, with $K_i/k$ finite separable field extension

Proof. See e.g. [BouI] V, p. 29-34

Let $G$ be a finite abstract group. We want to define the notion of a $G$-Galois algebra, which is a generalization of a Galois field extension with Galois group $G$. Let us first recall the definition from [KMRT], 18.15.

Definition 1.3.36. Let $L$ be an étale $k$-algebra and $G$ be a finite group. If we are given a left action of $G$ on $L$ by $k$-automorphisms, then we call $L$ a $G$-algebra. If in addition $|G| = \dim_k L$ and the induced right action of $G$ on $\text{Hom}_k(L, k_s)$ (given by $\xi^* \colon \xi \circ \alpha$) is transitive, then $L$ is called $G$-Galois algebra.

Our interest in Galois algebras stems from the following proposition:

Proposition 1.3.37. There is a $1-1$ correspondence between $G$-Galois algebras $L/k$ and $G$-torsors with base $\text{Spec}(k)$.

Proof. Let $L$ be a $G$-Galois algebra. We want to provide a $G_k$-equivariant isomorphism $G_k \xrightarrow{\sim} \text{Spec}(L)_k$. Since $L$ is an étale algebra of dimension $|G|$, $\text{Spec}(L)_k$ is a disjoint union of $|G|$ copies of $\text{Spec}(k_s)$. Let $x_0$ be one of these points. We claim that

$$\phi \colon G_k \cong \bigsqcup_{\sigma \in G} \text{Spec}(k_s) \rightarrow \text{Spec}(L)_k$$

is an isomorphism, where $\phi$ is defined on the $\sigma$-th copy via $\sigma \circ x_0$. Indeed, both sides of the map are sums of $|G|$ disjoint copies of $\text{Spec}(k_s)$. For each $\sigma \in G$, the map $\phi$ sends the point $\text{Spec}(k_s)$ of $G_k$, corresponding to the element $\sigma$ isomorphically to one of the points of $\text{Spec}(L)_k$. But since the action of $G$ on $\text{Hom}_k(L, k_s)$ was assumed to be simply transitive, this shows that $\phi$ is in fact an isomorphism.

Conversely, suppose $X$ is a $G$-torsor over $k$. Since $G_k$ is finite over $k_s$, we conclude by descent that $X$ is finite over $k$; thus $X = \text{Spec}(L)$ for some finite-dimensional $k$-algebra $L$. Since $\text{Spec}(L)$ is a $k_s$-form of $|G|$ distinct points, it is an étale algebra of dimension $|G|$. Specializing the isomorphism $\Psi \colon X \times G \rightarrow X \times X$ to $k_s$-points, we see that $G$ acts simply transitively on $\text{Hom}_k(L, k_s)$.

It is clear that these two construction are inverse.

Let us now consider a particular situation that we will meet later:

Example 1.3.38. Let $k$ be a field, let $K/k$ be an arbitrary field extension and let $K_s/K$ be a separable closure. Furthermore, let $E \subset K$ be such that $E/k$ is a finite Galois extension with primitive element $\alpha \in K_s$; we will denote by $f$ its minimal polynomial over $k$. Let $a = \alpha_1, \alpha_2, \ldots, \alpha_n \in E$ be the roots of $f$ and let $G := \text{Gal}(E/k)$ be the Galois group of the extension $E/k$. Then $\text{Spec}(E) \rightarrow \text{Spec}(k)$ is a $G$-torsor and we can consider its class $[E/k] \in H^1(k, G)$. We claim that there exists an injection $\phi \colon \text{Gal}(K(\alpha)/K) \rightarrow \text{Gal}(E/k)$ and that $[E \otimes_k K]$ lies in the image of $\phi$. Let $a = \text{ind}_{\text{Gal}(K(\alpha)/K)}^{\text{Gal}(E/k)} H^1(K, \text{Gal}(K(\alpha)/K)) \rightarrow H^1(K, \text{Gal}(E/k))$. First let us construct $\phi$. Let $\sigma \in \text{Gal}(K(\alpha)/K)$; since $E/k$ is Galois, $\sigma$ induces an element in $\text{Gal}(E/k)$. Then we define $\phi(\sigma)$ to be this element. It is clear that $\phi \colon \text{Gal}(K(\alpha)/K) \rightarrow \text{Gal}(E/k)$ is a group homomorphism. Furthermore, we have

$$\phi(\sigma) = \text{id}_E \iff \sigma(\alpha) = \alpha \iff \sigma = \text{id}_{K(\alpha)}.$$

Thus $\phi$ is injective.

The class $[E/k] \in H^1(k, G)$ is represented by the canonical projection $c \colon \Gamma_k \rightarrow \Gamma_k/\text{Gal}(k_s/E) \cong \text{Gal}(E/k) \cong G$. By base change, we obtain a $G$-torsor $E \otimes_k K$ over $K$. We have seen before that its cocycle class is determined by $c \colon \Gamma_K \rightarrow \Gamma_K \rightarrow \text{Gal}(E/k)$. Now we conclude from the commutative diagram

$$\begin{array}{ccc}
\Gamma_K & \longrightarrow & \text{Gal}(K(\alpha)/K) \\
\downarrow & & \phi \downarrow \\
\Gamma_k & \longrightarrow & \text{Gal}(E/k)
\end{array}$$

that $[E \otimes_k K] = [\overline{\alpha}] = \text{ind}_{\text{Gal}(E/k)}^{\text{Gal}(K(\alpha)/K)} [K(\alpha)/K]$.
1.3.5 \( O_n \)-torsors

In this section we assume \( \text{char}(k) \neq 2 \). We want to review again in greater detail the connection between quadratic forms over \( k \) and the elements of \( H^1(k, O_n) \). Furthermore, we will give concrete examples for such conversions. These will be used in later chapters.

So let us start with a cocycle \( c \in \mathbb{Z}(\Gamma, \text{O}_n) \); our goal is to define a quadratic form \( q \) of rank \( n \) over \( k \), whose associated cocycle is \( c \). Let us recall how to do this. First put \( V := k^n \) and define an action of \( \Gamma \) on \( V_{ks} := V \otimes_k k_s \) by \( \sigma \ast v = c_{\sigma}(\sigma(v)) \). Let \( V^{sT} := \{ v \in V_{ks} \mid \sigma \ast v = v \text{ for all } \sigma \in \Gamma \} \). Then choose elements \( v_1, \ldots, v_n \in V_{ks} \) which form a basis of the \( k \)-vector space \( V^{sT} \) (this vector space has dimension \( n \) by \[ \text{1.3.15} \]). Now let \( \varepsilon_1, \ldots, \varepsilon_n \) be the canonical basis of \( V = k^n \) and let \( \mathbb{I}_n \) be the quadratic form defined by \((1, \ldots, 1)\) in this basis. Let \( f \in \text{GL}_n(k) \) be the map sending \( v_1, \ldots, v_n \) to \( \varepsilon_1, \ldots, \varepsilon_n \) and let \( q_f \) be the quadratic form obtained from \( \mathbb{I}_n \) by pulling back along \( f^{-1} \). Let \( b := b_{\varepsilon_1} \) be the bilinear form associated to the quadratic form \( \mathbb{I}_n \). The new quadratic form is determined by \( b_{\varepsilon_1}(\varepsilon_1, \varepsilon_i) = b(v_i, v_i) \). Now we have

\[
\sigma(b(v_i, v_j)) = b(\sigma(v_i), \sigma(v_j)) = b(c^{-1}_\sigma(v_i), c^{-1}_\sigma(v_j)) = b(v_i, v_j).
\]

Thus \( q_f \) is indeed defined over the base field \( k \). Furthermore we compute

\[
f^{-1} \circ \sigma(f(v_i)) = f^{-1}(\sigma(v_i)) = f^{-1}(\varepsilon_i) = v_i.
\]

Using \( \sigma(v_i) = c^{-1}_\varepsilon(v_i) \), we conclude that the cocycle associated to \( f \) is \( c \).

**Example 1.3.39.** Consider the homomorphism of algebraic groups over \( k \)

\[
(\mathbb{Z}/2)^2 \rightarrow \text{O}_2
\]

\[
e_1 \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad e_2 \mapsto \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}.
\]

Let \( (\alpha, \beta) \in (k^\times/k^\times 2)^2 \) be a \((\mathbb{Z}/2)^2\)-torsor over \( k \). Then a basis of \( V^{sT} \) is given by \( v_1 = (\sqrt{\alpha} - \sqrt{\alpha})^T, \ v_2 = (\sqrt{\beta}, \sqrt{\beta})^T \). We obtain that the induced bilinear form is defined by the matrix

\[
\begin{pmatrix}
2\alpha & 0 \\
0 & 2\beta
\end{pmatrix}.
\]

**Example 1.3.40.** Consider

\[
\mathbb{Z}/2 \rightarrow \text{O}_2
\]

\[
e_1 \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.
\]

Let \( \alpha \in k^\times/k^\times 2 \) be a \( \mathbb{Z}/2 \)-torsor. Applying the above example with \( \beta = 1 \), we see that this quadratic form is defined by

\[
\begin{pmatrix}
2\alpha^2 & 0 \\
0 & 2
\end{pmatrix}.
\]

**Example 1.3.41.** Consider

\[
(\mathbb{Z}/2)^2 \rightarrow \text{O}_2
\]

\[
e_1 \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad e_2 \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.
\]

Let \( (\alpha, \beta) \in (k^\times/k^\times 2)^2 \) be a \((\mathbb{Z}/2)^2\)-torsor over \( k \). Then a basis of \( V^{sT} \) is given by \( v_1 = (1, 1)^T, \ v_2 = (\sqrt{\alpha}, -\sqrt{\alpha})^T \). The induced bilinear form is defined by

\[
\begin{pmatrix}
2 & 0 \\
0 & 2\alpha \beta
\end{pmatrix}.
\]
Another easy and useful lemma is the following

**Lemma 1.3.42.** Let \( c : \Gamma \to O_m(k) \), \( d : \Gamma \to O_n(k) \) be two cocycles and let \( q_c, q_d \) be the associated quadratic forms. Then the quadratic form defined by \( c \times d : \Gamma \to O_m(k) \times O_n(k) \to O_{m+n}(k) \) is \( q_c \oplus q_d \).

**Proof.** Let \( v_1, \ldots, v_n \in k^n \), \( w_{n+1}, \ldots, w_{m+n} \in k^m \) be a basis which is invariant under the \(*\)-action defined by \( c \) respectively \( d \). Then certainly \( v_1, \ldots, v_n, w_{n+1}, \ldots, w_{m+n} \in k^{n+m} \) is a basis which is invariant under the \(*\)-action defined with respect to the cocycle \( c \times d \) (where we embed the \( v \)'s using the first \( n \) and the \( w \)'s using the last \( m \) coordinates). Let \( b \) be the bilinear form on \( k^{n+m} \) defined by \( b(x, y) = \sum_i x_i y_i \). Then we have \( b(v_i, v_j) = b_i(e_i, e_j) \), \( b(w_i, w_j) = b_j(e_i, e_j) \) and \( b(w_i, v_j) = 0 \). Thus we conclude \( q_{c \times d} \cong q_c \oplus q_d \). \( \square \)

We need yet another computation. Since it is slightly more complicated than the ones we met above, we first need to introduce some notation.

For any \( 0 \leq k \leq 2^n - 1 \) let \( k = b_{n-1}2^{n-1} + \ldots + b_0 \) be its binary representation. For \( S \subseteq \{0; n-1\} \) let \( f_S \) be the function switching the bits at all positions in \( S \). That is:

\[
\begin{align*}
f_S : [0; 2^n - 1] & \to [0; 2^n - 1] \\
b_{n-1}2^{n-1} + \ldots + b_0 & \mapsto \sum_{i \in S} b_i 2^i + \sum_{i \notin S} (1-b_i) 2^i.
\end{align*}
\]

**Lemma 1.3.43.** Let \( k \) be a field, \( \text{char}(k) \neq 2 \). Let \( (e_0, \ldots, e_{n-1}) \in (k^2/k^2)^n \) be a \((\mathbb{Z}/2)^n\)-torsor over \( k \). Then

\[
\phi : (\mathbb{Z}/2)^n \to S_{2^n}
\]

\[
\sum_{s \in S} e_s \mapsto f_S
\]

is a group homomorphism and the quadratic form induced by the composite \( \Gamma_k \to (\mathbb{Z}/2)^n \to S_{2^n} \to O_{2^n}(k) \) is the generalised \( n \)-fold Pfister form \( (2^n) \otimes \langle \langle -e_0 \rangle \rangle \otimes \langle \langle -e_1 \rangle \rangle \otimes \ldots \otimes \langle \langle -e_{n-1} \rangle \rangle \).

**Proof.** To prove that \( \phi \) is a group homomorphism, we only have to check \( \phi(e_i)\phi(e_j) = \phi(e_j)\phi(e_i) \) (and \( \phi(e_i)\phi(e_i) = id \), but this is clear). But this translates to the observation that it doesn’t matter, if we change first the \( i \)-th bit and then the \( j \)-th bit or the other way round.

For \( 0 \leq p \leq 2^n - 1 \), write \( p = \sum_{i=0}^{n-1} b_i 2^i \). Then define \( v_p \in k(\sqrt{e_0}, \ldots, \sqrt{e_{n-1}})^{2^n} \) to have the components

\[
(v_p)_\ell = (-1)^{\sum_{s \in S} e_s b_s} \prod_{j=0}^{n-1} \sqrt{e_j}
\]

where \( 0 \leq \ell \leq 2^n - 1 \) and the \( c_s \in \{0, 1\} \) are determined by \( \ell = c_{n-1}2^{n-1} + \ldots + c_0 \). We claim that the \( v_p \) form a basis of \( V^{\perp} \). First we need to check \( v_p \in V^{\perp} \). Since in our situation, the cocycle has values in an elementary abelian 2-group, this means we need to prove \( c_s(v_p) = \sigma(v_p) \). Let \( \sigma \in \Gamma \) be arbitrary; then we can write \( e_s = \sum_{s \in S} e_s \) for some \( S \subseteq \{0;n-1\} \). Let \( 0 \leq \ell \leq 2^n - 1 \) be arbitrary and write \( \ell = \sum_{s=0}^{n-1} \epsilon_m 2^m \) for some \( \epsilon_m \in \{0, 1\} \). Then we have

\[
\sigma \left( (v_p)_\ell \right) = \sigma \left( (-1)^{\sum_{s \in \ell} e_s b_s} \prod_{j=0}^{n-1} \sqrt{e_j} \right)
\]

\[
= (-1)^{\sum_{s \in \ell} e_s b_s + \sum_{s \in \ell} (1-c_s)b_s} \prod_{j=0}^{n-1} \sqrt{e_j}
\]

which is exactly \( (v_p)_\ell \sigma(e) \). Thus, all the \( v_p \) are invariant under the \(*\)-action. We do not know yet, whether they form a basis, but this will follow automatically, as soon as we have evaluated \( b(v_p, v_q) \) (here \( b \) is the bilinear form given by \( b(x, y) = \sum_i x_i y_i \)). On the one hand, we have

\[
b(v_p, v_q) = \sum_{0 \leq s \leq 2^n - 1} (v_p)_s (v_q)_s
\]

\[
= 2^n \prod_{j=0}^{n-1} e_j.
\]
On the other hand, we claim that \( b(v_p, v_q) = 0 \), if \( p \neq q \). As soon as this is achieved, the theorem is proven.

So we want to show \( \sum_{0 \leq r < 2^n} (v_p)_{(r)} (v_q)_r = 0 \). Writing \( p = \sum_i b_i 2^i, \ q = \sum_i c_i 2^i \), this is equivalent to
\[
\sum_{0 \leq r < 2^n} d_i (b_i + r) = 0.
\]

By assumption, there is at least one \( b_i \) such that \( b_i \neq c_i \). We can partition \([0; 2^n - 1]\) into \([0; 2^{n-1}] = U_0 \cup U_1 \)
where \( U_i = \{ u = \sum_i d_i 2^i \mid u \in [0; 2^{n-1}] \}, \ d_i = i \) for \( i = 0, 1 \). Then \( f_{U_1} \) induces a bijection \( U_0 \to U_1 \). Now we have

\[
\sum_{0 \leq r < 2^n} (-1)^{j} d_i (b_i + r) = \sum_{u \in M} \left( (-1)^{j} \sum_{h} d_i (b_i + r) + (-1)^{j} \sum_{h} d_i (b_i + r)_{*1} \right) = 0.
\]

\[ \square \]

Remark 1.3.44. This lemma is more useful and more broadly applicable, than it may seem at first. Suppose we are given a left action of \((\mathbb{Z}/2^n)\) on \([0; 2^n - 1] \); this induces a map \( \psi : (\mathbb{Z}/2^n) \to S_{2^n} \). We claim that if the action is simply transitive, then \( \psi \) is conjugate to the map \( \phi \) above. To show this, put \( G := (\mathbb{Z}/2^n) \) and define \( x \in S_{2^n} \), such that \( \psi(g)(0) = \alpha(\phi(g)(0)) \) for all \( g \in G \); this is well-defined, since both actions are simply transitive. Now for all \( g, h \in G \), we have

\[
\psi(g)(\alpha(\phi(h)(0))) = \psi(gh)(0) = \alpha(\phi(g)(\phi(h)(0))).
\]

As \( h \) traverses \( G \), \( \phi(h)(0) \) traverses \([0; 2^n - 1] \). Thus, for all \( g \in G \) we have \( \psi(g) = \alpha \circ \phi(g) \circ \alpha^{-1} \).

1.4 \textit{Z}-graded \( \mathbb{A}^1 \)-modules

So far we have described \( G \)-torsors in some detail. To study certain invariants associated to them, we still need to define suitable coefficients, i.e. target spaces for these invariants. In [GMS] mainly Galois cohomology and Witt rings are used as coefficients. This is unnecessarily restrictive, as most of the results also hold for \( \mathbb{Z} \)-graded \( \mathbb{A}^1 \)-modules or more generally \( \mathbb{A}^1 \)-invariant unramified sheaves of abelian groups. Examples of \( \mathbb{Z} \)-graded \( \mathbb{A}^1 \)-modules include Rost’s cycle modules and (Milnor-)Witt K-theory. In fact, for us the main motivation to use \( \mathbb{Z} \)-graded \( \mathbb{A}^1 \)-modules instead of cycle modules was to stress that in the construction of concrete invariants, we do not need transfers.

Starting from this section, a sheaf will always mean a sheaf in the Nisnevich topology on \( \text{Sm}_{\mathbb{Z}} \). \( \mathbb{Z} \)-graded \( \mathbb{A}^1 \)-modules are introduced in [Mo3] and this article is the source of the current section. Let us first talk about unramified sheaves, since they are quite easy to define:

Definition 1.4.1 (Unramified Sheaf). Let \( S \) be a sheaf of sets in the Nisnevich topology on \( \text{Sm}_{\mathbb{Z}} \). \( S \) is called unramified, if it satisfies the following two axioms:

1. For any irreducible \( X \in \text{Sm}_{\mathbb{Z}} \) and any non-empty, open \( U \subset X \), the canonical map \( S(X) \to S(U) \) is injective.
2. For any irreducible \( X \in \text{Sm}_{\mathbb{Z}} \), the inclusion \( S(X) \subset \cap_{\mathbb{Z}} S(M_{\mathbb{Z}}) \) is an equality.

Furthermore recall the notion of \( \mathbb{A}^1 \)-invariance and strong \( \mathbb{A}^1 \)-invariance

Definition 1.4.2. Let \( C \) be a category and let \( S : (\text{Sm}_{\mathbb{Z}})^{op} \to C \) be a presheaf. Then \( S \) is called \( \mathbb{A}^1 \)-invariant if for all \( X \in \text{Sm}_{\mathbb{Z}} \) the map \( S(p) : S(X) \to S(X \times \mathbb{A}^1) \) induced by the projection \( p : X \times \mathbb{A}^1 \to X \) is an isomorphism.

Definition 1.4.3. Let \( M \) be a sheaf of groups in the Nisnevich topology on \( \text{Sm}_{\mathbb{Z}} \). \( M \) is called strongly \( \mathbb{A}^1 \)-invariant, if for \( i = 0, 1 \) the maps

\[
H^i_{\text{Nis}}(X, M) \to H^i_{\text{Nis}}(X \times \mathbb{A}^1, M)
\]

induced by the projection \( X \times \mathbb{A}^1 \to X \) are isomorphisms for all \( X \in \text{Sm}_{\mathbb{Z}} \).

Now let us define \( \mathbb{Z} \)-graded \( \mathbb{A}^1 \)-modules. These are functors \( M_\ast : \mathcal{F}_{\mathbb{Z}} \to \mathbb{A}^b \), (i.e. functors with values in families of abelian groups indexed by \( \mathbb{Z} \)) that have some extra data and satisfy a certain set of axioms. Before we can give the precise definition, there is a certain general requirement/convention which needs to be stated first: We will always assume that there exists a perfect subfield \( k_0 \subset k \) and a functor \( M' : \mathcal{F}_{\mathbb{Z}} \to \mathbb{A}^b \), such that \( k_0 \) is of finite type over \( k_0 \) and such that \( M_\ast = M'_\mathbb{Z} \). That is, for any \( k \in \mathcal{F}_{\mathbb{Z}} \) we have \( M_\ast(k) = M'_\mathbb{Z}(k) \). If \( k_0 \subset k \) is any finite type field extension, we define \( M_\ast(k) = M'_\mathbb{Z}(k) \). If we say that \( M'_\mathbb{Z} \) is endowed with some structure, we actually mean that \( M'_\mathbb{Z} \) is endowed with this kind of structure (over \( k_0 \)). If \( M \) is supposed to satisfy a certain axiom, we actually mean that \( M'_\mathbb{Z} \) satisfies this axiom.
Definition 1.4.4. A functor $M_\cdot: \mathcal{F}_{k_n} \to \mathcal{A}b.$ is called $\mathbb{Z}$-graded $\mathbb{A}^1$-module, if it is endowed with extra structures as described in (D4) and satisfies the axioms (B0)-(B5) and (HA) stated below.

(D4)(i) For all $k \in \mathcal{F}_{k_n}$, the abelian group $M_n(k)$ has a $\mathbb{Z}[k^\times/k^\times]$-module structure denoted by $(u, \alpha) \mapsto (u)\alpha \in M_n(k)$, where $\alpha \in M_n(k)$ and $u \in k^\times/k^\times$. Furthermore, this structure is required to be functorial in $\mathcal{F}_{k_n}$.

(D4)(ii) For all $k \in \mathcal{F}_{k_n}$, we have a map
\[
k^\times \times M_{n-1}(k) \to M_n(k)
\]
\[(u, \alpha) \mapsto [u]\alpha\]
which is additive in the second argument. Again this is required to be functorial in $\mathcal{F}_{k_n}$.

(D4)(iii) For all $k \in \mathcal{F}_{k_n}$, all discrete valuations $v$ of $k$ and all uniformizers $\pi \in k^\times$ of $v$, we have graded epimorphism of degree $-1$
\[
\partial_v^n: M_r(k) \to M_{r-1}(\kappa(v)).
\]
We require functoriality in the following sense: Let $k, \ell \in \mathcal{F}_{k_n}$ and $k \subset \ell$ be a field extension. Let $v$ be a discrete valuation on $\ell$, such that $v$ restricts to a discrete valuation $w$ on $k$ and such that $v/w$ has ramification index $1$. Finally let $\pi$ be a uniformizer of $w$. Then the following diagram commutes
\[
\begin{array}{ccc}
M_r(k) & \xrightarrow{\partial_v^n} & M_{r-1}(\kappa(w)) \\
\downarrow & & \downarrow \\
M_r(\ell) & \xrightarrow{\partial_v^n} & M_{r-1}(\kappa(v)).
\end{array}
\]

Remark 1.4.5. To those readers who wonder about the way the axioms are enumerated: Data (D1)-(D3) and axioms (A1)-(A6) are introduced in [Mo3] to describe unramified $\mathcal{F}_{k_n}$-sets (with some extra properties). It is shown in [Mo3, Theorem 2.46] that any $\mathbb{Z}$-graded $\mathbb{A}^1$-module is in particular an unramified $\mathcal{F}_{k_n}$-set satisfying the axioms (A1)-(A6). We will discuss some of those properties later. For a complete definition, we refer to [Mo3] 2.1, 2.2.

Now, let us state axioms (B0)-(B5)

(B0) For all $k \in \mathcal{F}_{k_n}$, all $u, v \in k^\times$ and all $\alpha \in M_n(k)$ we have $[uv]\alpha = [u][v][\alpha]$ and $[u][v][\alpha] = (-1)[v][u][\alpha]$.

(B1) Let $A$ be an integral domain which is smooth over $k_0$; let $k$ be its field of fractions. Then for all $\alpha \in M_n(k)$ there is a finite subset $S \subseteq \text{Spec}(A)^{(1)}$ such that for all $x \in \text{Spec}(A)^{(1)} \setminus S$ and all uniformizers $\pi$ of $x$, we have $\partial_v^n(\alpha) = 0$.

(B2) For all $k \in \mathcal{F}_{k_n}$, all discrete valuations $v$ of $k$, all uniformizers $\pi$ of $v$, all units $u \in O_v^\times$ and all $\alpha \in M_n(k)$ we have $\partial_v^n(u\alpha) = [\overline{\pi}]\partial_v^n(\alpha) \in M_n(\kappa(v))$ and $\partial_v^n(u\alpha) = [\overline{\pi}]\partial_v^n(\alpha) \in M_n-1(\kappa(v))$.

(B3) Let $k, \ell \in \mathcal{F}_{k_n}$ and let $k \subset \ell$ be a field extension. Let $v$ be a discrete valuation on $\ell$ which restricts to a discrete valuation $w$ on $k$. Let $e$ be the ramification index of $v/w$. Let $\pi \in O_v$ be a uniformizer for $v$ and $\rho \in O_w$ be a uniformizer for $w$; thus we can write $\rho = u \cdot \pi^e$ for some unit $u \in O_v^\times$. Furthermore let $\alpha \in M_n(k)$. Then we have $\partial_v^n(\alpha|_v) = e_{\overline{\pi}}(\partial_w^n(\alpha)|_{\kappa(v)} \in M_{n-1}(\kappa(v))$, where for any positive integer $n$, we put $n_e := \sum_{i=1}^{\infty}((-1)^{i-1})^e$.

(HA)(i) Let $k \in \mathcal{F}_{k_n}$. Then we have a short exact sequence
\[
0 \to M_r(k) \to M_r(k(T)) \xrightarrow{\partial_T^n} \bigoplus_{P \in \text{Spec}(\mathcal{A})^{(n)}} M_{r-1}(k(T)/P) \to 0.
\]
Observe that the second map is well-defined by (B1).

(HA)(ii) Let $k \in \mathcal{F}_{k_n}, \alpha \in M_n(k)$. Then we have $\partial_T^n([T]\alpha|_{k(T)}) = \alpha$.

To state axiom (B4), we need some preliminary discussion. Let $k \in \mathcal{F}_{k_n}$, let $v$ be a discrete valuation on $k$ and $\pi \in O_v$ a uniformizer. Denote by $v[T]$ the discrete valuation on $k(T)$ determined by the divisor $G_{mk[v]} \subseteq G_{mk}$. Then $\pi$ is also a uniformizer for $v[T]$. Suppose $M_\cdot$ is a functor with data (D4) and which satisfies axioms (B0)-(B3), (HA). Now consider the following diagram, whose lines are exact by (HA) and
where the $\partial_{\pi}^{P}$ are defined to be the unique maps making the whole diagram commutative (observe that the left square commutes by (D4)(iii))

$$
\begin{array}{ccccccccc}
0 & \rightarrow & M_{1}(k) & \rightarrow & M_{1}(k(T)) & \rightarrow & \bigoplus_{v \in \mathcal{O}} M_{-1}(k(T)/P) & \rightarrow & 0 \\
& & \downarrow \partial_{\pi}^{P} & & \downarrow \partial_{\pi}^{P} & & \downarrow \partial_{\pi}^{P} & & \\
0 & \rightarrow & M_{-1}(\kappa(v)) & \rightarrow & M_{-1}(\kappa(v)(T)) & \rightarrow & \bigoplus_{Q \in \mathcal{O}} M_{-2}(\kappa(v)[T]/Q) & \rightarrow & 0.
\end{array}
$$

Then axiom (B4) can be expressed as follows:

(B4)(i) If the closed point $Q \in \mathbb{A}^{1}_{k(\kappa)} \subset \mathbb{A}^{1}_{k}$ does not lie in the divisor $D_{P} \subset \mathbb{A}^{1}_{k}$ with generic point $P \in \mathbb{A}^{1}_{k} \subset \mathbb{A}^{1}_{k}$, then $\partial_{\pi}^{P}$ is zero.

(B4)(ii) If $P \in \mathcal{O}_{k}[T]$, is primitive and $Q$ is in the divisor $D_{P}$ and if $\mathcal{O}_{D_{P},Q}$ is a discrete valuation ring with uniformizer $\pi$, then we have

$$
\partial_{\pi}^{P} = -\left(\frac{-P^{'}}{Q^{'}}\right) \partial_{\pi}^{Q} : M_{1}(k[T]/P) \rightarrow M_{-1}(\kappa(v)(T)/Q),
$$

where $P', Q'$ are the derivatives of $P, Q$.

To state axiom (B5), there is again a little bit of preparatory work to be done. Let $M$, be a functor satisfying all the previous axioms. Let $k \in \mathcal{F}_{k}$ and let $\nu$ be a discrete valuation on $k$. Then define $M_{\nu} : \mathcal{O}_{\nu} : M_{1}(k) \rightarrow M_{-1}(\nu(\kappa(\nu)))$. In fact, this does not depend on the choice of $\nu$ (this follows from (B3) in the case $k = \ell$). For $X \in \mathcal{M}_{k}$ irreducible put $M_{\nu}(X) := \cap_{v \in \nu(k)} M_{\nu}(\mathcal{O}_{\nu,k})$. Define $H_{1}(X; M_{\nu}) := M_{\nu}(k(X))/M_{\nu}(\mathcal{O}_{\nu,k})$. Now let $X \in \mathcal{M}_{k}$ be irreducible, local (i.e. the Spec of a local ring) and 2-dimensional. Let $z \in X$ be its closed point and let $k$ be its function field. From the definitions and from (B1) it follows that we have a canonical exact sequence

$$
0 \rightarrow M_{1}(X) \rightarrow M_{1}(k) \rightarrow \bigoplus_{y \in X^{(1)}} H_{1}^{1}(X, M_{\nu}).
$$

Now let $y_{0} \in X^{(1)}$ be such that $\overline{y_{0}}$ is smooth over $k_{0}$ and consider the morphism

$$
M_{1}(k)/M_{1}(X) \rightarrow \bigoplus_{y \in X^{(1)}, y \neq y_{0}} H_{1}^{1}(X, M_{\nu}). \quad (1.4.1)
$$

From the exact sequence above, we see that the kernel of this map injects into $H_{1}^{1}(X, M_{\nu})$. Furthermore, observe that the map $\partial_{\pi}$ induces an isomorphism $H_{1}^{1}(X, M_{\nu}) \cong M_{-1}(\kappa(y_{0}))$. With these preliminaries, the formulation of axiom (B5) (which is only required to hold for $M_{\nu(k)}(\kappa)$) is quite short:

(B5) The kernel of (1.4.1) is equal to $M_{-1}(\mathcal{O}_{\nu,k}) \subset M_{-1}(\kappa(y_{0}))$.

This is the complete set of axioms. Here are some examples of such modules:

Example 1.4.6. By [Mo3] Remark 2.50] any cycle module in the sense of Rost defines a $\mathbb{Z}$-graded $\mathbb{A}^{1}$-module. In particular (mod n) Milnor $K$-theory and Galois cohomology are $\mathbb{Z}$-graded $\mathbb{A}^{1}$-modules.

Example 1.4.7. Let char$(k_{0}) \neq 2$. Let $k \in \mathcal{F}_{k}$ and let $W_{\mathbb{R}}(k)$ be the Witt-Grothendieck ring of $k$. As an abelian group, this is the Grothendieck ring of the monoid of isomorphism classes of non-singular quadratic forms over $k$. The multiplication on $W_{\mathbb{R}}(k)$ is induced by the tensor product. The Witt ring $W(k)$ is the quotient of $W_{\mathbb{R}}(k)$ by the ideal generated by the hyperbolic plane, i.e. the quadratic form which diagonalizes to $(1, -1)$. There is a well defined map $rk : W(k) \rightarrow \mathbb{Z}/2$ which is determined by sending a non-degenerate quadratic form to the parity of its rank. Let $I(k) \subset W(k)$ be the kernel of this map and let $I^{d}(k) \subset W(k)$ be the $d$-th power of the ideal $I(k)$. It can be shown that $I^{d}(k)$ is additively generated by the $n$-fold Pfister forms $\langle a_{1}, \ldots, a_{n} \rangle := \langle 1, -a_{1} \rangle \otimes \cdots \otimes \langle 1, -a_{n} \rangle$, where $a_{i} \in k^{2}$ (see [Lam] 10, Prop 1.2). Then $I^{d}(k)$ (and thus also $I^{n}(k)$) is a $\mathbb{Z}$-graded $\mathbb{A}^{1}$-module (where $I^{d}(k) = W(k)$ for $d \leq 0$). See e.g. [Mo3] Example 3.34.

By [Mo3] Theorem 2.46, any such functor $M$, induces an unramified sheaf of abelian groups satisfying (A1)-(A6). Let $k \in \mathcal{F}_{k}$, $v$ be a discrete valuation on $k$ and $\pi$ a uniformizer for $v$; then the specialization map (which is part of the structure of an $\mathcal{F}_{k}$-unramified sheaf of sets) is defined by

$$
s_{v} : M_{1}(\mathcal{O}_{k}) \rightarrow M_{1}(\kappa(v))
$$

$$
\alpha \mapsto \partial_{\pi}^{v}([\pi] \alpha).
$$

21
(One can show that this is in fact independent of the choice of the uniformizer \( \pi \)). In particular, \( M \) has the following properties

- \( M \) defines an \( \mathbb{A}^1 \)-invariant sheaf of abelian groups: For any \( X \in Sm_k \) the map \( \pi^* : M(X) \to M(X \times \mathbb{A}^1) \) induced by the projection is an isomorphism.

(A1) Let \( k \subset \ell \) be a separable field extension in \( \mathcal{F}_{k_0} \). Let \( v \) be a discrete valuation on \( \ell \) which restricts to a discrete valuation \( w \) on \( k \) such that \( v/w \) has ramification index 1. Then the map \( M(k) \to M(\ell) \) induces a morphism \( M(O_w) \to M(O_v) \) and the following diagram is commutative:

\[
\begin{array}{ccc}
M(O_w) & \longrightarrow & M(O_v) \\
\downarrow \kappa & & \downarrow \kappa \\
M(k) & \longrightarrow & M(\ell).
\end{array}
\]

Moreover, if the induced map \( \kappa(w) \to \kappa(v) \) is an isomorphism, then the square is cartesian.

(A3)(i) Let \( k \subset \ell \) be a separable field extension in \( \mathcal{F}_{k_0} \). Let \( v \) be a discrete valuation on \( \ell \) which restricts to a discrete valuation \( w \) on \( k \). Suppose that the ramification index of \( v/w \) is 1. If furthermore both \( \kappa(v) \) and \( \kappa(w) \) are separable over \( k_0 \), then we have a commutative diagram

\[
\begin{array}{ccc}
M(O_w) & \longrightarrow & M(O_v) \\
\downarrow \kappa_w & & \downarrow \kappa_v \\
M(\kappa(w)) & \longrightarrow & M(\kappa(v)).
\end{array}
\]

(A3)(ii) Let \( k \subset \ell \) be a field extension in \( \mathcal{F}_{k_0} \). Let \( v \) be a discrete valuation on \( \ell \) which is trivial on \( k \). Then the image of \( M(k) \to M(\ell) \) is contained in \( M(O_v) \).

(A3)(iii) If moreover \( \kappa(v) \) is separable over \( k \), then the composition \( M(k) \to M(O_v) \to M(\kappa(v)) \) is in fact equal to the map induced by the inclusion \( k \subset \kappa(v) \).

Remark 1.4.8. Due to our convention at the beginning of this section, the separability of \( \kappa(v)/k_0 \) and \( \kappa(w)/k_0 \) can be ignored when working with \( \mathbb{Z} \)-graded \( \mathbb{A}^1 \)-modules.

Let us compute an easy example which we will meet again later:

Example 1.4.9. Let \( R \) be a smooth, connected, finite type \( k_0 \)-algebra and \( r_1, \ldots, r_n \in R \) pairwise distinct; put \( P_i := T - r_i \in R[T] \). Then we have isomorphisms

\[
M_*(D(P_1 \cdots P_n)) \cong M_*(R) \oplus \bigoplus_{k=1}^n M_{*-1}(R) \cong M_*(R) \oplus \bigoplus_{k=1}^n M_{*-1}(R).
\]

Proof. Observe that we have an exact sequence

\[
0 \to M_*(R[T]) \to M_*(D(P_1 \cdots P_n)) \xrightarrow{\partial_*^{D(P_n)}} \bigoplus_{k=1}^n M_{*-1}(R),
\]

where we use (B4)(ii), to see that the image of \( \partial_*^{D(P_n)} : M_*(D(P_1 \cdots P_n)) \to M_{*-1}(\text{Quot}(R)) \) is contained in \( M_{*-1}(R) \).

It follows from (B2), (A3)(ii) and (A3)(iii) that we can construct a section of the last map. Namely, it is given by

\[
\bigoplus_{k=1}^n M_{*-1}(R) \to M_*(D(P_1 \cdots P_n))
\]

\[
(y_i)_{1 \leq i \leq n} \mapsto \sum_{i=1}^n [P_i] \cdot y_i.
\]

Thus we have

\[
M_*(D(P_1 \cdots P_n)) \cong M_*(R[T]) \oplus \bigoplus_{k=1}^n M_{*-1}(R) \cong M_*(R[T]) \oplus \bigoplus_{k=1}^n M_{*-1}(R).
\]

Now homotopy invariance proves the claim. \( \square \)
Definitions

1.4.12 Remark

Let \( K \) be functorial with respect to \( \pi \). For instance \( [M_1, D \ \text{Déf. 3.1}] \):

Example 1.4.10. Let \( p: E \to B \) be a vector bundle. Then for every \( A^1 \)-invariant sheaf of sets \( S \) the induced map \( p^*: S(B) \to S(E) \) is an isomorphism. To prove this, let \( s: B \to E \) be the zero section. It suffices to show that \( s \circ p \) is \( A^1 \)-homotopic to \( id_E \). If the vector bundle is trivial, we can define a homotopy

\[
H: A^1 \times (B \times A^n) \to (B \times A^n)
\]

\[
(t, (b, v)) \mapsto (b, t \cdot v),
\]

such that \( H \circ i_0 = s \circ p \) and \( H \circ i_1 = id_E \). In the general case, we cover \( B \) by open subschemes \( \cup_i U_i = B \), such that \( p^{-1}(U_i) \equiv U_i \times A^n \) and such that the transition maps are linear. Then we may define homotopies as above on each \( p^{-1}(U_i) \) and the linearity of the transition maps ensures that these glue to give the required homotopy \( A^1 \times E \to E \).

For the computations of invariants of finite reflection groups it is convenient to further specialize the coefficients as follows:

Definition 1.4.11. Let \( M_n \) be a \( \mathbb{Z} \)-graded \( A^1 \)-module. By abuse of terminology, we say that \( M_n \) has a \( K^M/2 \)-module structure, if the following holds:

- For all \( k \in \mathcal{F}_b \), all \( u \in k^\times/k^{\times 2} \) and all \( \alpha \in M_n(k) \) we have \( \langle u \rangle \alpha = \alpha \).
- The map \( [-] : \mathbb{Z}[k^\times] \times M_{n-1}(k) \to M_n(k) \) induces a \( K^M(k)/2 \)-module structure on \( M_n(k) \) in the usual sense.

For instance all 2-torsion cycle modules satisfy the above definition.

Remark 1.4.12. In the same spirit, we can make the following definition (where \( K^W \) denotes Witt \( K \)-theory; see for instance [Mo] Déf. 3.1]):

Definition 1.4.13. Let \( M_n \) be a \( \mathbb{Z} \)-graded \( A^1 \)-module. Again by abuse of terminology, we say that \( M_n \) has a \( K^W \)-module structure, if \( M_n \) is a \( K^W \)-module in the usual sense (i.e. each \( M_n(k) \) is a \( K^W(k) \)-module and this is functorial with respect to \( \mathcal{F}_b \)) satisfying the following properties:

- For \( u \in k^\times/k^{\times 2} \) define the element \( (u) := 1 - \eta[u] \in K^W_0(k) \). Let \( m \in M_n(k) \). On the one hand, we can form \( (u) \cdot m \) using the \( K^W \)-module structure; on the other hand, we can consider the element \( (u) \cdot m \) obtained from the \( \mathbb{Z} \)-graded \( A^1 \)-module structure. Then we require that these two elements coincide.
- For \( u \in k^\times \) we can form the element \( [u] = -[u] \in K^W_1(k) \). Let \( m \in M_n(k) \). On the one hand, we can form \( [u] \cdot m \) using the \( K^W \)-module structure; on the other hand we can consider the element \( [u] \cdot m \) obtained from the \( \mathbb{Z} \)-graded \( A^1 \)-module structure. Again we require that these two elements coincide.
2 Invariants

2.1 Invariants

After the recollections on G-torsors and on \( \mathbb{Z} \)-graded \( \mathbb{A} \)-modules in the first chapter, we can now introduce the definition of invariants. Let us first begin with the most general version:

**Definition 2.1.1.** Let \( F: \mathcal{F}_{k_0} \to \text{Set} \) and \( E: \mathcal{F}_{k_0} \to \mathcal{A} \) be functors. Any natural transformation between \( F \) and \( E \) will be called an invariant of \( F \) with values in \( E \) (where we consider \( E \) as having values in \( \text{Set} \)). The set (\( \mathcal{F}_{k_0} \) is essentially small!) of such natural transformations will be denoted by \( \text{Inv}_{k_0}(F, E) \) (or just \( \text{Inv}(F, E) \) in sloppy notation). In concrete terms, to give an invariant \( a \) is the same as to give for each \( k \in \mathcal{F}_{k_0} \) a map of sets \( a_k: F(k) \to E(k) \) such that for every field extension \( k \subset \ell \) in \( \mathcal{F}_{k_0} \) we have a commutative diagram

\[
\begin{array}{ccc}
F(k) & \xrightarrow{a_k} & E(k) \\
\uparrow & & \uparrow \\
F(\ell) & \xrightarrow{a_\ell} & E(\ell).
\end{array}
\]

If \( E \) is a functor that takes values in \( \mathcal{A} \), (i.e. families of abelian groups indexed by \( \mathbb{Z} \)), then we obtain a family \( \{ \text{Inv}_{k_0}(F, E_n) \}_{n \in \mathbb{Z}} \). We will also write \( \text{Inv}_{k_0}^*(F, E) \) for \( \text{Inv}_{k_0}(F, E) \).

**Caution 2.1.2.** We want to stress that by \( \text{Inv}_{k_0}(F, E) \) we really do not mean \( \text{Inv}_{k_0}(F, \bigoplus_{n \in \mathbb{Z}} E_n) \) but the family \( \{ \text{Inv}_{k_0}(F, E_n) \}_{n \in \mathbb{Z}} \). Occasionally, we take sums of elements of different degrees. We then always want these elements to live in \( \text{Inv}_{k_0}^*(F, E) \) determined by \( \text{Inv}_{k_0}(F, E) \) := \( \bigoplus_{n \in \mathbb{Z}} \text{Inv}_{k_0}(F, E_n) \). In particular, we want this convention to be true, when \( E_n = M \) is a \( \mathbb{Z} \)-graded \( \mathbb{A} \)-module.

**Example 2.1.3.** The category \( \mathcal{F}_{k_0} \) has the initial object \( k_0 \). Thus, if we choose \( e \in E(k_0) \), we obtain a constant invariant \( e \) which is defined by taking \( e_k: F(k) \to E(k) \) to be the unique map sending the entire source to the element \( E(\text{incl}_{k_0,ck_0})(e) \). Suppose that the functor \( F \) comes with a base-point \( * \in F(k_0) \). Then we denote by \( \text{Inv}_{k_0}^\text{norm}(F, E) \) the subset of those \( a \in \text{Inv}(F, E) \) such that \( a_{k_0}(*) = 0 \). The inclusion of the constant invariants \( E(k_0) \subset \text{Inv}(F, E) \) then induces a splitting \( \text{Inv}(F, E) \cong E(k_0) \oplus \text{Inv}_{k_0}^\text{norm}(F, E) \).

In order to be able to derive interesting result, let us consider more concrete situations. For the rest of this subsection, we will assume \( G \) to be a smooth affine algebraic group over \( k_0 \).

**Example 2.1.4.** Let \( M \) be an unramified sheaf of abelian groups. Now we may consider the functor

\[
\mathbb{H}^1(-, G): \mathcal{F}_{k_0} \to \text{Set} \\
\qquad k \mapsto \mathbb{H}^1(k, G).
\]

We write \( \text{Inv}_{k_0}(G, M) \) for \( \text{Inv}_{k_0}(\mathbb{H}^1(-, G), M) \).

A morphism \( f: G \to H \) of smooth affine algebraic groups over \( k_0 \) induces for each \( k \in \mathcal{F}_{k_0} \) a map \( f_k: \mathbb{H}^1(k, G) \to \mathbb{H}^1(k, H) \). To be more precise, we should call this map \( (f_k)_k \), but in fact the \( (f_k)_k \) form a natural transformation of functors from \( \mathcal{F}_{k_0} \) to \( \text{Set} \) and therefore we will primarily use the shorter notation. For \( a \in \text{Inv}_{k_0}(H, M) \) we can define a new invariant \( f^*(a) \in \text{Inv}_{k_0}(G, M) \) by \( (f^*(a))_k := a_k \circ (f_k)_k \). If \( G \subset H \) is a closed immersion of smooth affine algebraic groups, then we call \( (\text{incl}_{G,H})^!(a) = a \circ \text{ind}_{G,H}^! \) the restriction of \( a \) to \( G \) and denote it by \( \text{res}_{H/G}^!(a) \).

1.3.21 yields the following:

**Proposition 2.1.5.** Let \( g \in G(k_0) \) be a \( k_0 \)-rational point. Let \( t_g: G \to G \) be the conjugation by \( g \) (i.e. \( t_g(h) = g \cdot h \cdot g^{-1} \)). Then \( t_g^! \) induces the identity on \( \text{Inv}_{k_0}(G, M) \).

**Example 2.1.6.** Let \( \text{char}(k) \neq 2 \). Another interesting example (which for \( n \geq 4 \) is not of the type \( \mathbb{H}^1(-; G) \)) is the functor \( F: k \mapsto F^*(k) \), where \( F^*(k) \) is the \( n \)-th power of the fundamental ideal \( I(k) \subset W(k) \). It follows from the Milnor conjecture that one can define an element \( e_n \in \text{Inv}^n(F^*, K_n^M/2) \) determined by

\[
e_n: F^*(k) \to K_n^M(k)/2 \\
\langle\langle a_1\rangle\rangle \otimes \cdots \otimes \langle\langle a_n\rangle\rangle \mapsto \prod_{i=1}^n \langle a_i\rangle.
\]

This is proven in [OVV, Theorem 4.1].
In the previous sections, we have learned how to construct versal torsors; however, the purpose of this notion remained a mystery. Now we want to prove that cohomological invariants are in fact determined by their value at a versal torsor. That is, if \( T \) is a versal \( G \)-torsor over a field \( k \) and \( M \) is an unramified sheaf of abelian groups, then the map \( \text{Inv}_{k}(G, M) \to M(k) \) given by evaluation at \( T \) is injective. We will prove this in \( \text{2.1.11} \). Most of the material covered in the rest of this section is a reformulation of [GMS, §11, §12] using unramified sheaves of abelian groups instead of Galois cohomology as coefficients. The formulation of the crucial [GMS, Proposition 11.1] is slightly inappropriate when using these coefficients. I want to thank Prof. Morel for explaining to me, how to adapt it.

**Theorem 2.1.7.** Let \( M \) be an unramified sheaf of abelian groups and let \( a \in \text{Inv}_{k}(G, M) \). Let \( K \) be a discrete valuation on \( K \). Suppose that the residue field \( k(v) \) is separable over \( k \). Then the image of the following composition lies in fact in \( M(O_{c}): \)

\[
H^{1}(O_{c}, G) \to H^{1}(K, G) \xrightarrow{a_{k}} M(K).
\]

Furthermore, the image of any torsor \( T \in H^{1}(O_{c}, G) \) under the composition

\[
H^{1}(O_{c}, G) \xrightarrow{a_{\kappa}(\text{incl}_{O_{c} \to K})} M(O_{c}) \xrightarrow{\delta_{v}} M(k(v))
\]

is \( a_{\kappa(v)}(T_{k(v)}) \).

**Remark 2.1.8.** We should say a word on \( H^{1}(X, G) \), if \( X \) is not necessarily the spectrum of a field. For our purposes, it will be sufficient to define this as the set of isomorphism classes of \( G \)-torsors over \( X \). In [Mi, III, Corollary 4.7, Theorem 4.3] it is shown that this set is in fact isomorphic to the first non-abelian Čech-cohomology set with coefficients in \( G \) with respect to the fppf-topology.

**Proof.** Let \( T \in H^{1}(O_{c}, G) \) be arbitrary and assume first that \( k_{0} \subset k(v) \) is finite separable and that \( k(v) \) is \( O_{c} \)-liftable with respect to \( T \). By this, we mean that there exists a map \( i : \kappa(v) \to O_{c} \) such that \( u \mapsto O_{c} \xrightarrow{\text{incl}_{O_{c} \to K}} k(v) \) is the identity and such that the induced map \( H^{1}(O_{c}, G) \xrightarrow{p} H^{1}(k(v), G) \xrightarrow{\delta_{v}} H^{1}(O_{c}, G) \) is the identity on \( T \). Now consider the following diagram

\[
\begin{array}{ccc}
H^{1}(O_{c}, G) & \xrightarrow{\text{incl}_{O_{c} \to K}} & H^{1}(K, G) \\
\downarrow p & & \downarrow (\text{incl}_{O_{c} \to K},) \\
H^{1}(k(v), G) & \xrightarrow{a_{\kappa(v)}} & M(k(v)).
\end{array}
\]

The square is commutative, since \( a \) is an invariant. The triangle may not be commutative, but certainly the images of the torsor \( T \) are compatible by assumption. Now we can conclude from \( k(v) \subset O_{c} \) that \( v \) is trivial on \( k(v) \). Thus the image of \( M(k(v)) \to M(K) \) lies in \( M(O_{c}) \) by (A3)(ii).

For the second assertion, we can use the commutative diagram

\[
\begin{array}{ccc}
H^{1}(O_{c}, G) & \xrightarrow{a_{\kappa}(\text{incl}_{O_{c} \to K})} & M(O_{c}) \\
\downarrow i & & \downarrow \delta_{v} \\
H^{1}(k(v), G) & \xrightarrow{a_{\kappa(v)}} & M(k(v)).
\end{array}
\]

Observe that the first map in the upper row is well-defined by what we have just proved. Again the middle square commutes, because \( a \) is an invariant and the right triangle commutes by (A3)(ii). The second claim now follows from our assumption \( \iota_{v}(T_{k(v)}) = T \).

Now let us drop the assumption that \( k(v) \) is \( O_{c} \)-liftable (but still assume that \( k_{0} \subset k(v) \) is finite). Let \( O_{c}^{\dagger} \) be the Henselization of \( O_{c} \). Since \( O_{c}^{\dagger} \) is Henselian and \( k_{0} \subset k(v) \) is finite and separable, we can find \( i : k(v) \to O_{c}^{\dagger} \) such that \( k(v) \xrightarrow{i} O_{c}^{\dagger} \xrightarrow{p} k(v) \) is the identity. Furthermore, we conclude from [SGA3, Exp. XXIV, Prop. 8.1.(iii)] that the induced map \( p : H^{1}(O_{c}^{\dagger}, G) \to H^{1}(k(v), G) \) is an isomorphism. Since \( H^{1}(k(v), G) \xrightarrow{\delta_{v}} H^{1}(O_{c}^{\dagger}, G) \) is the identity, we conclude that \( H^{1}(O_{c}^{\dagger}, G) \xrightarrow{\delta_{v}} H^{1}(k(v), G) \xrightarrow{\delta_{v}} H^{1}(O_{c}^{\dagger}, G) \) is also just the identity. By convention, the valuation \( v \) is a geometric one, i.e., we can find \( X \in Sm_{k} \) and \( x \in X^{(1)} \) such that \( O_{c} \equiv O_{X,x} \). Then \( \text{Spec}(O_{c}) \) can be written as the inverse limit over a left filtering system of smooth irreducible Nisnevich neighbourhoods of \( x \) such that all the transition maps are affine. Observe that by the definition of the Nisnevich topology, the transition maps are all etale. By the results of [EGA IV, §8] we can find \( Y \in Sm_{k}, y \in Y^{(1)} \) and a map \( f : Y \to X \) with \( f(y) = x \) such that \( Y \) is a Nisnevich neighbourhood of \( x \) with
the property that \( \kappa(v) \equiv \kappa(y) \equiv \kappa(x) \) is \( \mathcal{O}_x \)-liftable with respect to \( T' := T \times_{\text{Spec}(O_x)} \text{Spec}(O_{y'}) \). More precisely, the reasoning is as follows: As \( \kappa(v) \) is a finite field extension of \( k_0 \), the embedding \( \kappa(v) \to \mathcal{O}_x \) factors already as \( \kappa(v) \to O_{X}(\overline{Y}) \to \mathcal{O}_x \) for some smooth affine irreducible Nisnevich neighbourhood \( \overline{Y} \) of \( x \). Denote by \( T'' \) the pull-back of \( T \times_{\text{Spec}(O_x)} \overline{Y} \to \overline{Y} \) along the morphism \( \overline{Y} \to \text{Spec}(k(v)) \) \( \overline{Y} \). Then the canonical map from the pull-back of \( T \to \text{Spec}(O_x) \) along \( \text{Spec}(\mathcal{O}_x) \to \text{Spec}(k(v)) \to \text{Spec}(O_{y'}) \) to \( T \times_{\text{Spec}(O_x)} \text{Spec}(\mathcal{O}_x) \) is the projective limit of \( T'' \times_{\overline{Y}} Z \to \text{Spec}(\mathcal{O}_x) \times_{\overline{Y}} Z \), where \( Z \) is an element of the left-filtering system of smooth affine irreducible Nisnevich neighborhoods of \( x \) that factor through \( \overline{Y} \); we observed above that this projective limit is an isomorphism. Thus, by [EGA IV] Cor. 8.8.25, there exists a Nisnevich neighbourhood \( Y \) of \( x \) with the desired properties. Now let \( L \) be the quotient field of \( \mathcal{O}_{y'} \). Then we have a commutative diagram

\[
\begin{array}{ccc}
H^1(\mathcal{O}_{y}, G) & \to^a & M(\kappa) \\
\downarrow & & \downarrow \\
H^1(\mathcal{O}_{Y,y'}, G) & \to^{a_i} & M(L).
\end{array}
\]

If we apply the previous discussion to \( T' \), we see that the image of \( T \in H^1(\mathcal{O}_{y'}, G) \) under the above diagram is contained in \( M(\mathcal{O}_{Y,y'}) \subset M(L) \). Now observe that \( K \subset L \) is separable, that \( \mathcal{O}_{y'} \subset \mathcal{O}_{Y,y'} \) has ramification index 1 and that \( \kappa(v) \equiv \kappa(y) \). Thus we may apply (A1) and conclude that the image of \( T \) under the upper line is contained in \( M(\mathcal{O}_{y'}) \). For the second assertion, we use the diagram

\[
\begin{array}{ccc}
H^1(\mathcal{O}_{y'}, G) & \to^{a_k(v)(\dim \mathcal{O}_{y'})} & M(\mathcal{O}_{X,x}) \\
\downarrow & & \downarrow \\
H^1(\mathcal{O}_{Y,y'}, G) & \to^{a_i(v)(\dim \mathcal{O}_{Y,y'})} & M(\mathcal{O}_{Y,y}).
\end{array}
\]

where the last square commutes by (A3)(i).

Finally, let us do the general case. Let \( n \) be the transcendence degree of the field extension \( k_0 \subset \kappa(v) \) and choose \( t_1, \ldots, t_n \in \mathcal{O}_x^* \) whose images in \( \kappa(v) \) form a separating transcendence basis of \( \kappa(v)/k_0 \). Then we have \( k_0(t_1, \ldots, t_n) \subset \mathcal{O}_x \) and the hypotheses of the theorem are still valid, if we replace \( k_0 \) by \( k_0(t_1, \ldots, t_n) \). \( \square \)

**Remark 2.1.9.** In the proof, it was crucial to know that the projection \( \mathcal{O}_x^* \to \kappa(v) \) induces an isomorphism

\[H^1(\mathcal{O}_x^*, G) \to H^1(\kappa(v), G).\]

Presheaves with this property are also called rigid.

**Proposition 2.1.10.** Let \( X \in \text{Sm}_{k_0} \) be irreducible and let \( T \) be a G-torsor over \( X \). Let \( \eta \in X \) be the generic point and let \( x \in X \) be a point whose residue field \( \kappa(x) \) is separable over \( k_0 \). Let \( M \) be an unramified sheaf of abelian groups. Furthermore, let \( a \in \text{Inv}_{k_0}(G, M) \). Then \( a_{(\kappa(x))}(T_x) = 0 \) implies \( a_{(\kappa)}(T_{x_1}) = 0 \).

**Proof.** We prove the theorem by induction on the codimension of \( [x] \). If the codimension is 0, then the claim is trivial. If the codimension is 1, we conclude from (2.1.7) that \( 0 = s_{(\kappa(x))}(T_{(\kappa(x))}) = a_{(\kappa)}(T_{(\kappa(x))}) \).

So now let \( x \in X \) be of arbitrary codimension. Put \( A = \mathcal{O}_{X,x} \) and let \( m = m_x \) be the maximal ideal of \( A \). Write \( m = (t_1, \ldots, t_n) \), where \( n = \dim(A) \) and the \( t_i \) form a regular system of parameters. After replacing \( X \) by some open neighbourhood of \( x \), we can assume that there exist closed irreducible subschemes \( X_i \subset X \) with generic points \( x_i \), such that \( \mathcal{O}_{X_i,x} \equiv A/\langle t_1, \ldots, t_i \rangle \) (in particular \( X_0 = [x] \)). Since the \( t_i \) form a regular sequence and since \( \kappa(x)/k \) is separable, the point \( x \) is a smooth point of each \( X_i \). But now the smooth locus is open; thus after further shrinking the open neighbourhood around \( x \), we may assume that all the \( X_i \) are in fact smooth and of codimension 1. Now we can argue as follows. By the codimension 1 case, we conclude that \( a_{(\kappa(x))}(T_{(\kappa(x))}) = 0 \) (observe that \( \kappa(x_1)/k \) is separable, since \( X_1 \) is smooth). Applying induction to \( x \in X_1 \), this yields \( a_{(\kappa(x_1))}(T_{(\kappa(x_1))}) = 0 \). \( \square \)

**Theorem 2.1.11.** Let \( M \) be an unramified sheaf of abelian groups. Let \( P \in H^1(K, G) \) be a versal torsor and \( a, b \in \text{Inv}_{k_0}(G, M) \) be such that \( a(P) = b(P) \). Then \( a = b \).

**Proof.** Clearly, we may assume \( b = 0 \). In other words, we want to show that \( a(P) = 0 \) implies \( a(T) = 0 \) for all \( k \in \mathcal{T}_{k_0} \) and all \( T \in H^1(K, G) \). Suppose first that \( k \) is infinite. Let \( \pi : Q \to X \) be as in the definition of a versal torsor. Then there exists \( x \in X(k) \) such that \( T = Q_x \). We have \( Q_{\eta} = P \) and \( a_{k}(P) = 0 \). Thus we may apply the previous proposition and conclude \( a_{k}(Q_x) = 0 \).

It remains to consider the case, where \( k \) is finite. By base change, \( T \) defines a torsor \( T_i \in H^1(k(t), G) \). From what we have just shown, we conclude \( a_{k(t)}(T_i) = 0 \). Let \( v \) be the discrete valuation on \( k(t) \) defined by \( t \). From
and we obtain \( M(k) \to M(k[t]) \rightarrow M(k) \) is the identity. In particular, \( M(k) \to M(k(t)) \) is injective and we obtain \( \overline{a}_t(T) = 0 \). \( \square \)

In the following, we will often need to assume that a sheaf satisfies a convention similar to the one expressed at the beginning of [1.4]. To be more precise:

**Definition 2.1.12** (Convention (C)). Let \( M \) be a sheaf in the Nisnevich topology on \( Sm_{k_0} \). We say that \( M \) satisfies convention (C) if the following holds: There exists a perfect base field \( k_0 \) such that \( k_0 \) is a finite type field extension of \( k \) and such that \( M \) is induced by a Nisnevich sheaf \( M' \) on \( Sm_{k_0} \) (i.e. \( M'(X) = M(X) \) for all \( X \in Sm_{k_0} \)). If \( X \) is a scheme over \( k_0 \) such that \( X \in Sm_{k_0} \) we will write \( M(X) \) where we actually mean \( M'(X) \).

This being said, we have:

**Corollary 2.1.13.** Let \( M \) be a unramified sheaf of abelian groups satisfying convention (C). Let \( Y \in X \to T \to Y \) be a \( G \)-torsor over \( Y \). Let \( \eta = \text{Spec}(k) \) be the generic point of \( Y \). Let \( a \in \text{Inv}^r(G, M) \). Then \( a_X(T) \in M(Y) \).

Proof. If we consider \( Y \) as an element of \( Sm_{k_0} \), then for all points \( y \in Y \) the field extension \( \overline{k_0} \subset \kappa(y) \) is separable. We then conclude by applying [2.1.7] and recalling the definition \( M(Y) = \bigcap_{y \in Y} M(O_{Y,y}) \). \( \square \)

We end this section with a useful technical proposition concerning the invariants of a product \( G \times H \), where \( G, H \) are smooth linear algebraic groups. But first, it is convenient to introduce an abuse of terminology:

**Definition 2.1.14** (Free \( M \)-module). Let \( R \) be a commutative ring and \( M \subset N \) be \( R \)-modules. Let \( I \) be a finite index set and let \( \{ r_i \} \subset I \) if the map

\[
\bigoplus_{i \in I} M \to N
\]

\[
(m_i) \mapsto \sum_{i \in I} r_i m_i
\]

is an isomorphism.

If \( R = R_0 \), is graded and \( M = M_0 \subset N = N_0 \) are graded \( R_0 \)-modules, then we say \( N_0 \) is a free \( M_0 \)-module, provided the following holds: There exists a finite index set \( I \) and homogeneous elements \( \{ r_i \} \subset I \), such that

\[
\bigoplus_{i \in I} M_{-|r_i|} \to N_0
\]

\[
(m_i) \mapsto \sum_{i \in I} r_i m_i
\]

is an isomorphism.

**Example 2.1.15.** We will meet this notion quite frequently in the following context: \( R = \text{Inv}^r(G, K^W) \) or \( R = \text{Inv}^r(G, K^M/2); M = M_0(k_0) \), where \( M_0 \) is a \( \mathbb{Z} \)-graded \( A^1 \)-module with \( K^W \) (resp. \( K^M/2 \))-module structure and \( N = \text{Inv}^r(G, M) \).

Here is the proposition:

**Proposition 2.1.16.** Let \( G, H \) be smooth affine algebraic groups and let \( M_0 \) be a \( \mathbb{Z} \)-graded \( A^1 \)-module with \( K^M/2 \)-module structure. Furthermore, suppose that there exist homogeneous elements \( \{ g_i \} \subset \text{Inv}^r(G, K^M/2) \) such that for every \( k \in F_{k_0} \), \( \text{Inv}^r_k(M_0, G) \) is a free \( M_0(k) \)-module with basis \( \{ g_i \} \) (or rather the restriction of the \( g_i \) to \( \text{Inv}^r_k(G, K^M/2) \)). Then the map

\[
\text{Inv}^r_k(G, K^M/2) \otimes_{K^M(k_0)/2} \text{Inv}^r_k(H, M) \to \text{Inv}^r_k(G \times H, M)
\]

\[
\times \otimes y \mapsto x \cdot y
\]

is an isomorphism.

Proof. First let us show injectivity. Let \( a = \sum g_i \otimes h_i \) be an arbitrary element such that for all \( k \in F_{k_0} \), all \( x \in H^1(k, G) \) and all \( y \in H^1(k, H) \) we have \( a(x, y) = 0 \); we want to show that all the \( h_i \) are 0. So let \( k \in F_{k_0} \) and \( y \in H^1(k, H) \) be arbitrary. Then by assumption, for all \( \ell \in F_k \) and all \( x \in H^1(\ell, G) \) we have \( \sum g_i \in \text{incl}_{k \cdot \ell}(h_i(y)) = 0 \). This means that the invariant \( \bar{a} \in \text{Inv}^r_k(G, M) \) defined by

\[
\bar{a}(x) := \sum_i g_i \cdot \text{incl}_{k \cdot \ell}(h_i(y))
\]

is an isomorphism.
is 0. By our hypothesis on the $g_i$, we conclude that all the $h_i(y)$ are 0.

Now let’s turn to surjectivity. Let $a \in \text{Inv}_{k_0}^c (G \times H, M)$ be an arbitrary invariant. Let $k \in T_{k_0}$ and $y \in H^1(k, H)$ be arbitrary. Then we can define an invariant $a_y \in \text{Inv}_{k_0}^c (G, M)$ as follows. For $\ell \in T_k$ and $x \in H^1(\ell, G)$ put $a_{x,y}(x) = a(x, y)$. By assumption, we can find unique $m_{i,y} \in M_{i,k_0}$ such that $a_y = \sum \alpha_i g_i : m_{i,y}$. Uniqueness then implies that the maps $y \mapsto m_{i,y}$ define elements $h_i \in \text{Inv}_{k_0}^c (H, M)$. But now $\sum \alpha_i g_i \otimes h_i$ maps to $a$. □

### 2.2 Totaro’s theorem

Let $G$ be a smooth affine algebraic group over a field $k$. It follows from [2.1.13 and 2.1.11] that the evaluation at a versal torsor $P \to \text{Spec}(k)$ induces an injection $\text{Inv}(G, M) \to M(X)$ (with $X$ as in the definition of versal torsor). Totaro proved in [GMS, Appendix C] that in some favorable cases this evaluation map is in fact an isomorphism. Before we can state and prove his theorem, there are some chores to be done. Let us first introduce a linguistic convenience: For $X$ a finite type $k$-scheme endowed with a $G$-action, we say that $X/G \text{ exists as } G$-torsor, if there is a finite type $k$-scheme $Y$ such that $X \to Y$ is a $G$-torsor (by [1.3.12] this implies that the categorical quotient $X/G$ exists and $Y \equiv X/G$).

**Lemma 2.2.1.** Let $G$ be a smooth affine algebraic group over a field $k$. Let $E \to \text{Spec}(k)$ be a $G$-torsor and $\rho: A_k^n \times_k G \to A_k^n$ be a linear action. Then $(E \times_k A_k^n)/G \text{ exists as } G$-torsor.

**Sketch of proof.** First observe that $E \times_k A_k^n \to E$ is affine. To define a candidate for $(E \times_k A_k^n)/G$, we first recall from descent theory (e.g. [Mi, I, Theorem 2.23]) what we need to do in order to define a scheme $Z$ together with an affine morphism $\pi: Z \to E/G$. To give such data is equivalent to defining a scheme $Z'$ and an affine morphism $\alpha: Z' \to E$ plus an isomorphism $\phi: Z' \times_k (E \times E/G) \to (E \times E/G) \times E$ (isomorphism over $E \times E/G$) satisfying a certain cocycle condition. Since $E \to E/G$ is a $G$-torsor, we have a $G$-equivariant isomorphism $E \times_k G \equiv E \times E/G$. Thus to define the isomorphism $\phi$, we only need to find a morphism $\tilde{\rho}$ making the following diagram commutative and cartesian:

$$
\begin{array}{ccc}
Z' & \xrightarrow{\alpha} & Z' \\
\downarrow \alpha & & \downarrow \alpha \\
E \times_k G & \xrightarrow{\tilde{\rho}} & E.
\end{array}
$$

Now, if $\tilde{\rho}$ is an action of $G$ on $Z'$ making the above diagram commutative, then this diagram will automatically be cartesian. Furthermore one can also check that the relations imposed by a group action imply that the cocycle condition holds.

Of course we apply the above discussion to the case, where $Z' = E \times_k A_k^n$ and $\tilde{\rho}: E \times_k A_k^n \times_k G \to E \times_k A_k^n$ is the diagonal action. From descent theory, we then obtain a cartesian square:

$$
\begin{array}{ccc}
E \times_k A_k^n & \longrightarrow & Z \\
\downarrow pr_1 & & \downarrow \\
E & \longrightarrow & E/G.
\end{array}
$$

In particular, $E \times_k A_k^n \to Z$ is faithfully flat and of finite type. Furthermore, $(E \times_k A_k^n) \times_k G \to (E \times_k A_k^n) \times_Z (E \times_k G)$ is obtained from $E \times_k G \to E \times E/G$ by pulling back along $Z \to E/G$. Hence it is an isomorphism and $E \times_k A_k^n \to Z$ is a $G$-torsor. □

**Lemma 2.2.2.** Let $G$ be a smooth affine algebraic group over $k$. Let $E \to \text{Spec}(k)$ be a $G$-torsor over $\text{Spec}(k)$ and let $\rho: A_k^n \times_k G \to A_k^n$ be a linear action. Then $(E \times_k A_k^n)/G \to \text{Spec}(k)$ is a vector bundle.

**Sketch of proof.** It follows from an elaborate version of Hilbert’s Theorem 90 that any rank $n$ vector bundle in the fppf-topology is also a vector bundle in the Zariski topology (see e.g. [Mi, III, Prop. 4.9]; strangely enough it is stated only for line bundles, although the proof also works perfectly well in the general case). Furthermore we have an isomorphism $\phi: E \times_k A_k^n \xrightarrow{\sim} ((E \times_k A_k^n)/G) \times_E G$ over $E$. Thus we only need to check that the transition map is linear; this means the following: $pr_1^*(\phi), pr_2^*(\phi)$ yield two isomorphisms of schemes over $E \times E/G$; we want to show that

$$
pr_1^*(\phi)^{-1} \circ pr_2^*(\phi): A_k^n \times_k (E \times E/G) \to (E \times E/G) \times_k A_k^n
$$

is linear over the base $E \times E/G$. The base is isomorphic to $E \times_k G$ and it can be checked that the resulting map

$$
pr_1^*(\phi)^{-1} \circ pr_2^*(\phi): A_k^n \times_k (E \times_k G) \to (E \times_k G) \times_k A_k^n
$$

is given by $(v, x, g) \mapsto (x, g, v \cdot \rho(g)^{-1})$. Since the action $\rho$ was assumed to be linear, this proves the claim. □
Now we can prove Totaro’s geometric description of \( \mathrm{Inv}_k(G, M) \):

**Theorem 2.2.3.** Let \( M \) be an unramified \( A^1 \)-invariant sheaf of abelian groups over \( k_0 \) satisfying convention (C). Let \( G \) be a smooth affine algebraic group over \( k_0 \), let \( V \equiv A^n \) be a finite dimensional \( k_0 \)-vector space and let \( p : V \times G \to V \) be a linear action of \( G \) on \( V \). Furthermore, let \( U \subset V \) be an open, \( G \)-invariant subscheme such that \( \mathrm{codim}_V(V - U) \geq 2 \) and such that \( U/G \) exists as \( G \)-torsor. Then there is an isomorphism

\[
\mathrm{Inv}_k(G, M) \xrightarrow{\sim} M(U/G) \subset M(k(U/G))
\]

defined by the evaluation of an invariant at the versal torsor \( U \to \mathrm{Spec}(k(U/G)) \).

**Proof.** For the sake of brevity, in this proof, we will use the following notation: Suppose the affine algebraic group \( G \) acts on \( X \) and on \( Y \); then it acts diagonally on \( X \times Y \) and we will denote by \( X \times^G Y \) the categorical quotient \( (X \times Y)/G \) (provided it exists).

Put \( K := k(U/G) \) and let \( a \in \mathrm{Inv}(G, M) \). Then the claim \( a_k(U_k) \in M(U(G)) \) is just [2.1.13] and the evaluation map \( \mathrm{Inv}_k(G, M) \to M(K) \) is injective by [2.1.11]. It remains to show surjectivity.

Let \( x \in M(U(G)) \) be arbitrary. Our aim is to construct an invariant \( a^x \) such that \( a^x_k(U_k) = x \). So let \( k \in FR \) and let \( E \to \mathrm{Spec}(k) \) be an arbitrary \( G \)-torsor. Recall that \( U_k \to (U/G)_k \) is a \( G \)-torsor; in particular \( U_k/G_k \equiv (U/G)_k \).

Furthermore, by [2.2.1] and [1.3.7] \( E \times^{G_k} U_k \) exists as \( G_k \)-torsor. The morphisms \( E \times^{G_k} U_k \to U_k/G_k \to U/G \) induce maps \( M(U(G)) \to M(U_k/G_k) \to M(E \times^{G_k} U_k) \). Since the codimension of the complement of \( E \times^{G_k} U_k \) in \( E \times^{G_k} V_k \) is bigger than 1 (A.0.7 is applicable, since \( E \times^{G_k} V_k \) is a vector bundle over \( \mathrm{Spec}(k) \), hence irreducible), both schemes have the same codimension 1 points and we obtain \( M(E \times^{G_k} U_k) \to M(E \times^{G_k} V_k) \).

By the previous lemma, \( E \times^{G_k} V_k \) is a vector bundle over \( E/G_k \). Thus we conclude from [1.4.10] that \( M(k) \to M(E \times^{G_k} V_k) \) is an isomorphism, where \( p : E \times^{G_k} V_k \to E/G_k \) is the projection. Then we define \( a^x_k(E) \) to be the image of \( x \) under the composition

\[
M(U(G)) \xrightarrow{p^*} M(U_k/G_k) \xrightarrow{a^x_k} M(E \times^{G_k} U_k) \xrightarrow{\sim} M(E \times^{G_k} V_k) \xrightarrow{p^*} M(k).
\]

The \( F_{k_0} \)-functoriality of this construction is assured by the presheaf structure of \( M \). It remains to show that \( a^x_k(U_k) = x \).

Observe that we have the following commutative diagram

\[
\begin{array}{ccc}
M(U(G)) & \xrightarrow{p^*} & M(U \times^{G_k} U) \xrightarrow{p^*} M(U(G)) \\
\downarrow & & \downarrow \\
M(U_k/G_k) & \xrightarrow{\sim} & M(U_k \times^{G_k} U_k) \xrightarrow{\sim} M(U_k/G_k) \\
\downarrow & & \downarrow \\
M(U \times^{G_k} U_k) & \xrightarrow{\sim} & M(U \times^{G_k} U_k)
\end{array}
\]

We conclude from this diagram and from the construction of \( a^x_k(U_k) \) that it suffices to show that the two projections \( p_{1,2} : U \times^{G_k} U \to U/G \) induce the same maps \( p^*_{1,2} : M(U(G)) \to M(U \times^{G_k} U) \).

We have a morphism

\[
\bar{\phi} : A^1 \times U \times U \to V \\
(t, x, y) \mapsto tx + (1 - t)y.
\]

In order to have [A.0.6] at our disposal, it is important to show that

**Lemma 2.2.4.** \( \bar{\phi} \) is flat.

**Proof.** It suffices to show that the morphism

\[
\psi : A^1 \times V \times V \to V \\
(t, x, y) \mapsto tx + (1 - t)y
\]

is flat. The restriction of \( \psi \) to \( (A^1 - \{0\}) \times V \times V \) factors as

\[
(A^1 - \{0\}) \times V \times V \xrightarrow{\psi_0} (A^1 - \{0\}) \times V \xrightarrow{\psi_1} V,
\]

where \( \psi_0 : (A^1 - \{0\}) \times V \to (A^1 - \{0\}) \) and \( \psi_1 : V \to V \) are both flat.
where $\psi(t, u, v) := (t, v, tu + (1 - t)v)$ We conclude that the restriction of $\psi$ to $(A^1 - \{0\}) \times V \times V \to V$ is flat, as it can be written as the composition of an isomorphism and the flat projection $(A^1 - \{0\}) \times V \times V \to V$. Similarly one also shows that the restriction of $\psi$ to $(A^1 - \{1\}) \times V \times V \to V$ is flat.

Let $W := \phi^{-1}(U)$. We can define a $G$-action on $A^1 \times U \times U$ by letting $G$ act trivially on $A^1$ and diagonally on $U \times U$. Since $\phi$ is equivariant with respect to this action (the action of $G$ on $V$ being linear) and since $U$ is $G$-invariant, this induces an action of $G$ on $W$. By (2.2) and (3.7) $W/G$ exists as $G$-torsor. Furthermore, $\tilde{\phi}$ induces a morphism $\phi: W/G \to U/G$. Since the complement of $W \subset A^1 \times U \times U$ is of codimension $> 1$ by (4.5), so is the complement of $W/G \subset A^1 \times U \times U$ (by (4.7). In particular we have $M(W/G) \cong M(A^1 \times (U \times U))$.

The inclusions of the closed points 0 or 1 in $A^1$ induce maps $h_0: U \times G \to W$ and composing these two maps with the open immersion $W/G \to A^1 \times (U \times U)$, we obtain $h_0: U \times G \to A^1 \times (U \times U)$. Thus, it is sufficient to show $\tilde{j}_0 = j_1$. But from homotopy invariance, we know $\tilde{j}_0 = j_1$. Since $M(A^1 \times (U \times U)) \to M(W/G)$ is an isomorphism, this proves the theorem.

Remark 2.2.5. There is yet another way to express Totaro’s theorem. Let us recall first some notation from [Deg]. Let us denote by $N^G$ the category of sheaves with transfers (in the Nisnevich topology on $Sm_{S}$) and let us write $HN^G$ for the full subcategory of homotopy invariant sheaves with transfers. It is proven in [Deg] 3.1.7 that the forgetful functor $HN^G \to N^G$ has a left adjoint $h_0$. Let us furthermore recall the notion of geometric classifying space from [MV] section 4.2. We will give a variant of the construction discussed there (more precisely, we consider a certain admissible gadget). Let $G$ be a smooth affine algebraic group over $k_0$ and let $i: G \to G_0$ be an embedding as a closed subgroup. Let $U \in A^n$ be an open $G$-invariant subscheme such that $U \times G$ exists as $G$-torsor (where the action of $G$ on $A^n$ is defined by $i$). Now let us define inductively open $G$-invariant subschemes $U_m \subset A^{mn}$. We start with $U_1 := U$ and put $U_{m+1} := (U \times A^n) \cup (A^{mn} \times U)$. Then the closed immersions $A^{mn} \subset A^{mn+1}$, $\nu \to (\nu, 0)$ induce closed immersions $U_{m+1} \to U_m$. Furthermore, we claim that if we let act $G$ diagonally on $A^{mn}$, then the quotient $V_m := U_m/G$ exists as $G$-torsor; we prove this by induction on $m$. The case $m = 1$ is true by assumption. For $m \geq 1$, we know by induction and (2.2) that the quotients of both $U_m \times A^n$ and $A^{mn} \times U$ by the diagonal action exist as $G$-torsors. Glueing these quotients along the open subscheme $U_m \times ^G U$ we obtain a scheme $V_{m+1}$ such that $V_{m+1} \to V_{m+1}$ is a $G$-torsor; in particular $V_m \cong U_{m+1}/G$ (to see that $U_{m+1} \to V_{m+1}$ is a $G$-torsor, one may choose fpf-covers of $U_m \times A^n$ and $A^{mn} \times U$ as in (3.8) to obtain a suitable fpf-cover of $V_{m+1}$). We then define the sheaf $B_{gm}(G, i) := colim_{V_m}$, where the colimit is taken in the category of sheaves in the Nisnevich topology over $Sm_{S}$. Note that the codimension of the complement of $U_m$ in $A^{mn}$ is at least $m$. Thus, for each $m \geq 2$ we have isomorphisms

$$Inv(G, M) \cong M(V_m) \cong Hom_{HN^G}([Z_0[V_m]], M) \cong Hom_{HN^G}(h_0([Z_0[V_m]], M)).$$

(2.2.1)

Now let’s check that these isomorphisms are compatible, if $m$ varies. The second and the third isomorphisms are certainly functorial with respect to the closed immersion $s: V_m \to V_{m+1}$. For the first isomorphism, let $a \in Inv(G, M)$ be arbitrary and let $\eta_{m_1}, \eta_{m_2}$ be the generic points of $V_m, V_{m+1}$. We claim that for all $a \in Inv(G, M)$ we have $s^*(a((U_{m_1})_{\eta_{m_1}} \to \eta_{m_1}))) = a((U_m)_{\eta_{m}} \to \eta_{m})$. First note that $s$ factors as

$$s: V_m \to U_m \times A^n \to V_{m+1},$$

where $t$ is the closed immersion induced by the zero section $U_m \to U_m \times A^n$ and $j$ is an open immersion. Clearly, we have $(U_{m+1})_{\eta_{m+1}} = (U_m \times A^n)_{\eta_{m}}$ and $j^*: M(V_{m+1}) \to M(U_m \times A^n)$ is just an inclusion. Thus it suffices to check $t^*(a((U_m \times A^n)_{\eta_{m}} \to \eta_{m+1}))) = a((U_m)_{\eta_{m}} \to \eta_{m})$. Furthermore, $U_m \times ^G A^n$ is a vector bundle over $U_m/G$ and we conclude that $t^*$ is the inverse of the isomorphism $p'$ induced by the projection $p: U_m \times ^G A^n \to U_m/G$. But since $a$ is an invariant, we have $p'(a((U_m)_{\eta_{m}} \to \eta_{m+1}))) = a((U_m \times A^n)_{\eta_{m}} \to \eta_{m+1})$.

By abuse of notation, we let write $h_0(V_m) = h_0([Z_0[V_m]])$ and $h_0(B_{gm}(G, i)) = h_0([Z_0[B_{gm}(G, i)]])$. Using fancy language, we can say that the functor $M \mapsto Inv(G, M)$ is represented by any of the objects $h_0(V_m), m \geq 2$ and $h_0(B_{gm}(G, i))$ (considered as a functor from the category $HN^G$ to $Set$). The Yoneda lemma then gives us canonical isomorphisms $h_0(V_m) \cong h_0(B_{gm}(G, i));$ moreover, we conclude that there is no harm in suppressing the concrete embedding $i$ in the notation.

It is sometimes convenient to consider reduced versions. Choosing a rational point $x \in U_1$ gives rise to a basepoint in all the $U_m, V_m$ and in $B_{gm}(G, i)$. The inclusion of this rational point induces splittings $h_0(V_m) \cong \mathbb{Z} \oplus h_0(V_m)$ and $h_0(B_{gm}(G)) \cong \mathbb{Z} \oplus h_0(B_{gm}(G))$. Moreover it is not hard to check that the isomorphism $Inv(G, M) \cong Hom_{HN^G}([Z_0[B_{gm}(G)]], M)$ maps the constant invariants onto $Hom_{HN^G}(\mathbb{Z}, M) \subset Hom_{HN^G}(\mathbb{Z} \oplus h_0(B_{gm}(G)), M)$. Thus we obtain an isomorphism $Inv_{norm}(G, M) \cong Hom_{HN^G}(h_0(B_{gm}(G)), M).$
2.3 Serre’s Splitting principle

Next, we want to prove Serre’s splitting principle for finite reflection groups which tells us that the invariants of such groups are detected by the invariants of its elementary abelian 2-subgroups generated by reflections. This is proved in [CMS, Theorem 24.9] for the case of $S_3$, and it is observed in [CMS, Theorem 25.15] that it can be generalized to reflection groups. As usual, we first do some recollections. Let $V$ be a finite dimensional $k_0$-vector space. An automorphism $s: V \to V$ is called pseudo-reflection, if $\ker(s-1)$ is a hyperplane in $V$. A finite group $W$ together with an embedding $W \subset \text{GL}(V)$ is called pseudo-reflection group, if it is generated by pseudo-reflections (when considered as a subgroup of $\text{GL}(V)$).

Moreover, suppose that $V$ is endowed with a non-degenerate symmetric bilinear form $(\cdot, \cdot): V \times V \to V$. An automorphism $s: V \to V$ is called orthogonal reflection, if it is a pseudo-reflection and an element of $O(V)$. A finite group $W$ together with an embedding $W \subset O(V)$ is called orthogonal reflection group, if it is generated by orthogonal reflections (when considered as a subgroup of $O(V)$).

Remark 2.3.1. Any orthogonal reflection $s$ has order 2 and the orthogonal complement of $\ker(s-1)$ is an anisotropic subspace. Indeed, by assumption $\ker(s-1)$ is $n-1$-dimensional; hence $s$ has exactly one other eigenvalue $\lambda \in k_0$ and the eigenspace $\ker(s-\lambda)$ is 1-dimensional. For $v_1 \in \ker(s-\lambda)$ and $v_1 \in \ker(s-1)$ we have $(v_1, v_1) = (s(v_1), s(v_1)) = \lambda(v_1, v_1)$. Thus $\ker(s-1) \subset \ker(s-\lambda)^\perp$ and since $(\cdot, \cdot)$ is non-degenerate, we have in fact equality. From $\ker((s-1) \cap \ker(s-\lambda) = \{0\}$, we conclude that $\ker(s-\lambda)$ is an anisotropic subspace.

Now we obtain from $(v_1, v_1) = (s(v_1), s(v_1)) = \lambda^2(v_1, v_1)$ that $\lambda = -1$ and $s^2 = id$. As a corollary, we see that $s$ can be computed using the usual formula

$$v \mapsto v - 2 \frac{(v, v)}{(v_1, v_1)} v_1.$$

Conversely, if we take instead of $v_1$ any anisotropic vector $v' \in V$, then the above formula defines an orthogonal reflection $s_{v'} \in O(V)$.

For a finite dimensional $k_0$-vector space $V$ let $S(V)$ be the symmetric algebra over $V$ and let $V^\vee$ be the dual of $V$. From the theory of pseudo-reflection groups, we will need the following two key theorems:

Theorem 2.3.2. Let $V$ be a finite-dimensional $k_0$-vector space and let $W \subset \text{GL}(V)$ be a pseudo-reflection group such that $\text{char}(k_0) \nmid |W|$. Then $S(V)^W$ is a polynomial algebra over $k_0$, where $S(V)$ is the symmetric algebra of $V$.

Proof. [Bou2, V, Thm. 4] □

Theorem 2.3.3. Let $V$ be a finite-dimensional $k_0$-vector space and let $W \subset \text{GL}(V)$ be a pseudo-reflection group. Suppose that $S(V)^W$ is a polynomial algebra over $k_0$. Then for any $\phi \in V^\vee$ the stabilizer group $W_\phi := \{w \in W \mid w^\vee(\phi) = \phi\} \subset W$ is a subgroup generated by pseudo-reflections.

Proof. [Bou2, Exercices, §5 no. 8] □

Let us note the following corollary

Corollary 2.3.4. Let $V$ be a finite-dimensional $k_0$-vector space endowed with a non-degenerate symmetric bilinear form $(\cdot, \cdot)$ and let $W \subset O(V)$ be an orthogonal reflection group. Suppose that $S(V)^W$ is a polynomial algebra over $k_0$. Then for any $v \in V$ the stabilizer $W_v := \{w \in W \mid w(v) = v\} \subset W$ is a subgroup generated by orthogonal reflections.

Proof. Put $\phi := (v, \cdot)$. Clearly we have $w^\vee(\phi) = (w^{-1}v, \cdot)$ and from non-degeneracy, we conclude that $w^\vee(\phi) = \phi \iff w(v) = v$. Now apply the theorem. □

We will need another lemma:

Lemma 2.3.5. Let $V$ be a finite dimensional $k_0$-vector space endowed with a non-degenerate symmetric bilinear form $(\cdot, \cdot)$ and let $W \subset O(V)$ be an orthogonal reflection group. Let $v \in V$ be anisotropic such that $s_v \in W$ and put $\phi_v := (v, \cdot) \in S(V^\vee)$. Then the stabilizer of the (prime) ideal $(\phi_v) \subset S(V^\vee)$ under the action of $W$ is given by $(s_v) \times W_v \equiv (s_v, W_v) \subset W$.

Proof. Let us start by proving that $s_v$ and any $w \in W_v$ commute. Since $w \in O(V)$ stabilizes $(v)$ it also stabilizes $(v)^\perp = \ker(s_v - 1)$. Thus for any $v_1 \in \ker(s_v - 1)$, we have $s_v(w(v_1)) = w(v_1) = w(s_v(v_1))$. Together with $s_v(w(v)) = s_v(v) = -v = w(s_v(v))$ this shows that $s_v$ and $W_v$ commute.

Clearly, $W_v$ and $s_v$ both stabilize the ideal $(\phi_v) \subset S(V^\vee)$. On the other hand, suppose $w \in W$ stabilizes this ideal; then we have $w^\vee(\phi_v) = \lambda \cdot \phi_v$ for some $\lambda \in k_0^\times$. Thus $w^{-1}(\lambda) = \lambda \cdot v$. But since $v$ is anisotropic and $w \in O(V)$, we conclude $\lambda = \pm 1$. If $\lambda = 1$, then $w \in W_v$ and if $\lambda = -1$, then $w \cdot s_v \in W_v$. □

Definition 2.3.6. Let $W \subset \text{GL}(V)$ be an orthogonal reflection group. A set $\Phi = \{v_1, \ldots, v_l\} \subset V$ of anisotropic vectors is called root system, if it has the following properties:
(i) $\Phi$ is invariant under $W$ (as a set; not elementwise).
(ii) $(k_0 \cdot v_1) \cap \Phi = \{v_0, -v_0\}$.
(iii) The set $\{s_{\epsilon_1}, \ldots, s_{\epsilon_m}\} \subset W$ is precisely the set of orthogonal reflections in $W$.

Remark 2.3.7. Any orthogonal reflection group has a root system. Indeed, start first with any $v_1 \in V$, such that $s_{\epsilon_1} \in W$. Let $(v_1, \ldots, v_m)$ be the orbit of $v_1$ under $W$. If every reflection in $W$ is of the form $s_{\epsilon_i}$ for some $1 \leq i \leq m$, we are done. Otherwise choose some $s_{v_i(v_1+1)} \in W$ which is not covered yet. Now iterate.

For the proof of Serre’s principle, we need to recall some results from elementary number theory.

Definition 2.3.8. Let $K$ be a field and $v$ a discrete valuation on $v$ and let $\widetilde{K}$ be the completion of $K$ with respect to $v$. Then we denote by $K^h_v \subset \widetilde{K}$ the separable (algebraic) closure of $K$ inside $\widetilde{K}$ and call it the Henselization of $K$ with respect to $v$.

Remark 2.3.9. It follows from the discussion at the beginning of [NK, II, §6] that $K^h_v \cap O_v$ is indeed a Henselian ring. A rigorous proof can be found in [EP, Cor. 4.1.5]

Now let us prove a lemma which tells us that $K^h_v$ is in fact something quite familiar:

Lemma 2.3.10. We use the same notation as in the definition 2.3.8 above. Denote by $O_v^h$ the Henselization of $O_v$ (i.e. the one defined via the universal property, see [Mi, I, Discussion prior to Lemma 4.8]). Then $K^h_v$ is isomorphic to the quotient field of $O_v^h$.

Proof. By [Mi, I, Exercise 4.9], $A := O_v^h$ can be taken to be the intersection of all local Henselian $R \subset O_v$ with the property that the maximal ideal of $R$ lies in the maximal ideal of $O_v$. Put $B := K^h_v \cap O_v$ and let $\bar{K}$ be the quotient field of $A$. By the remark above, $B$ is Henselian and we conclude $A \subset B$, thus $\bar{K} \subset K^h_v$.

To prove the reverse inclusion, let $b \in K^h_v$ be arbitrary. As $b$ is separable over $K$, we conclude that $\bar{K}(b)/\bar{K}$ is a separable field extension. Since $\bar{K}$ is Henselian, it follows from [NK, II, Satz 6.8] that $[\bar{K}(b) : \bar{K}] = e_f$, where $e$ is the ramification index and $f$ the residue class degree. Let $w$ be the restriction of $v$ to $\bar{K}(b)$. Then $\kappa(v) \subset \kappa(w) \subset \kappa(\bar{K}) = \kappa(v)$ implies $f = 1$. Furthermore, if $r \in w$, then we claim that the inclusion $\pi_{O_w} \subset (\pi_{O_v}) \cap O_w$ is an equality. Indeed given $x \in O_v$ such that $r \cdot x \in O_w$, we conclude right away that $x \in \bar{K}(b) \cap O_v = O_w$ and thus $e = 1$. But this implies $[\bar{K}(b) : \bar{K}] = 1$; in other words $b \in \bar{K}$.

Lemma 2.3.11. Let $K, v, K_v, K^h_v$ be as in the previous definition. Let $\widetilde{K}_v$ be a separable closure of $K_v$. Let $E/K$ be a finite Galois extension and let $w$ be a discrete valuation on $E$ extending $v$. We consider $E$ as a subfield of $\widetilde{K}_v$. It is well-known from number theory that there exists an element $\alpha \in E$ such that $E = K(\alpha)$ and such that $\widetilde{K}_v(\alpha)$ is the completion of $E$ with respect to the valuation $w$ (see e.g. [NK, II, Satz 8.2]). Then $[\sigma \in \text{Gal}(E/K) \mid \sigma(w) = w] \cong \text{Gal}(\widetilde{K}_v(\alpha)/K_v) \cong \text{Gal}(K^h_v(\alpha)/K_v)$

Proof. The first isomorphism is well-known (see [Sel, II, §3, Cor.4]), so it suffices to show the second one. First observe that $K^h_v(\alpha)/K_v$ is a Galois extension, since $K(\alpha)/K$ is. If $f$ is the minimal polynomial of $\alpha$ over $K_v$, we claim that $f$ is also the minimal polynomial of $\alpha$ over $\widetilde{K}_v$. Indeed let $f = g \cdot h$ be a non-trivial factorization in $\widetilde{K}_v[X]$ such that $g, h$ are monic. As $f$ is separable, all of its roots are separable over $K$ and therefore so are the coefficients of $g, h$. We conclude $g, h \in K_v[X]$, contradicting the choice of $f$. Thus $[\text{Gal}(\widetilde{K}_v(\alpha)/K_v)] = [\text{Gal}(K^h_v(\alpha)/K_v)]$ and the injection $\text{Gal}(\widetilde{K}_v(\alpha)/K_v) \to \text{Gal}(K^h_v(\alpha)/K_v)$ is in fact an isomorphism.

Before we prove Serre’s splitting principle, let us fix some notation. Let $W \subset O(V)$ be an orthogonal reflection group. Put $E := \text{Quot}(S(V^*))$ and $K := E^W$. Let $\Phi \subset V$ be any root system of $V$ and define the open subscheme $U := \text{Spec}(\pi_{w_0}(\Phi)) \subset \text{Spec}(S(V^*)) = V$. We claim that $W$ acts freely on $U$. By [1.2.11] it suffices to check this on closed points. So suppose we had $z \neq w \in W$ and a closed point $z \in U(K_0)$ such that $w(z) = z$. From [2.3.3] we conclude that $W_z$ is generated by orthogonal reflections. In particular, since this group is non-trivial, we know that it contains at least one reflection $s_{z_i}$ for some $v \in \Phi$. Thus we have $s_z(z) = z$, or equivalently $\phi_z(z) = 0$. But this contradicts $z \in U$. Now it’s about time to prove Serre’s principle for finite reflection groups:

Theorem 2.3.12 (Serre’s splitting principle). Let $V$ be a finite dimensional $k_0$-vector space endowed with a non-degenerate bilinear form $(\cdot, \cdot)$. Let $W \subset O(V)$ be an orthogonal reflection group, such that $\text{char}(k_0) \nmid |W|$. Let $M$ be an unramified $\mathcal{A}^1$-invariant sheaf of abelian groups satisfying convention (C) (see [2.1.12]). Furthermore, suppose that $a \in \text{Inv}_0(W, M)$ satisfies $\text{res}_V(a) = 0$ for all elementary abelian 2-subgroups $P \subset W$ which are generated by reflections. Then $a = 0$. 

32
Proof. In the course of this proof it will be better to denote elementary abelian 2-subgroups by the letter $H$ instead of $P$ (which will be needed for codimension 1 points). We prove the theorem by induction on $|W|$; our induction hypothesis is that the theorem holds for all infinite fields $k_0$, all $V$ over such $k_0$, etc. and all $|W|$, such that $|W| \leq n$. In other words, in the proof we want to have the freedom to use the induction hypothesis for any base field. The case $|W| = 1$ is clear.

Let us first prove a special case, namely if there exists an anisotropic $v \in V$ such that $W = \langle s_v \rangle \times W_v$. For every $k \in \mathcal{F}_v$, and every $\beta \in H^1(k, \mathbb{Z}/2) = k^2/k^{2\mathbb{Z}}$ we can then define an invariant $\alpha^\beta_v \in \text{Inv}_v(W_v, M)$ by
\[
\alpha^\beta_v : H^1(\ell, W_v) \to M(\ell, x) \mapsto a_\ell(\beta, x),
\]
where $\ell \in \mathcal{F}_v$. If $H \subset W_v$ is an elementary abelian 2-subgroup generated by reflections and $x \in H^1(\ell, H)$, we have
\[
\alpha^\beta_v(\text{ind}^W_{H}(x)) = a_\ell(\beta, \text{ind}^W_{H}(x)) = a_\ell(\text{ind}^W_{(\alpha, x)}(\beta, x)) = 0.
\]
Thus we can apply induction to conclude $\alpha^\beta_v = 0$ for all $k \in \mathcal{F}_v$, all $\beta \in H^1(k, \mathbb{Z}/2)$ and all $\ell \in \mathcal{F}_v$. But this means $a_v = 0$.

Now we tackle the general case. Using the notation introduced above, we know that $\text{Spec}(E) \to \text{Spec}(k)$ is $H^1(K, W)$ is a versal torsor. According to 2.1.11, it suffices to prove $a_\ell(E) = 0$. Let us first show $a_\ell(E) \in \text{Inv}(\text{Spec}(k) \to \text{Inv}(\text{Spec}(k), \mathbb{P}(\mathbb{O}))$ for all $\ell \in \text{Spec}(\mathbb{S}^\vee W))$.

We start with the case $P \not\subseteq U/W$. Then the $W$-torsor $\text{Spec}(E) \to \text{Spec}(k)$ is obtained by pulling back the $W$-torsor $U \to U/W$ along $\text{Spec}(k) \to \text{Spec}(\mathbb{O}) \to U/W$. But by 2.1.17, the image of the composite
\[
H^1(U/W, W) \to H^1(\mathbb{O}_P, W) \to H^1(\text{Spec}(k), W) \to M(K)
\]
is contained in $M(\mathbb{O}_P)$.

Now suppose $P \not\subseteq U/W$. Applying 2.3.2 we conclude that $S(V^\vee W) \cong S(V^\vee W)$ is a polynomial algebra. In particular, it is factorial. Thus we can find $f \in S(V^\vee W)$ such that $\ell$ generates the prime ideal of height 1 corresponding to $P \subseteq \text{Spec}(S(V^\vee W))$. Let $\Phi$ be the root system of $W$ chosen above. Since $P \not\subseteq U/W$, we have $f \not\in \prod_{\varphi_P \in \Phi} \mathbb{P}(\mathbb{O}_P)$ and we can find $\varphi_1 \in \Phi$, such that $f = \varphi \cdot \prod_{\varphi_P \in \Phi} \mathbb{P}(\mathbb{O}_P)$. Let $t$ be the discrete valuation $\mathbb{K}$ defined by the prime element $f$. Fix an element $v \in \mathbb{K}_t$. Let $u$ be the extension of $t$ to $E$ corresponding to the prime element $\varphi_v \in S(\mathbb{V})$. Let $\mathbb{K}$ be the completion of $K$ with respect to $t$, let $\mathbb{K} \subset \mathbb{K}$ be the Henselization of $\mathbb{K}$ with respect to $t$. By number theory, we can find an $a \in \mathbb{K}$ and a discrete valuation $\varphi$ on $\mathbb{K}$ such that $E \cong K(a)$ and such that $a \not\in \mathbb{K}$. By 2.3.11 we know that $K^\beta(a)/K^\beta$ is a Galois field extension with Galois group $W_{\varphi}^\text{dec} = [w \in W \mid w^\varphi(\varphi_v)] = (\varphi_v)$. Observe that by 2.3.3 we know that $W_{\varphi}^\text{dec} = \langle \varphi_v \rangle \times W_v$, where $W_v \subset W$ is the stabilizer of $v \in V$. Furthermore, we can assume $W \not\cong W^\text{dec}$ (otherwise we are in the special case considered above).

By 1.3.38 we know that $[E \otimes_K K^\beta] \cong H^1(K^\beta, W)$ is in the image of the induction map $\text{ind}^W_{W_u^\varphi} : H^1(K^\beta, W_{\varphi}^\text{dec}) \to H^1(K^\beta, W)$; more precisely, we have $[E \otimes_K K^\beta] = \text{ind}^W_{W_u^\varphi}([K^\beta(a)])$. Now recall that $\text{Spec}(\mathbb{O}_P)$ is the limit of a left-filtered system of smooth, irreducible Nisnevich neighborhoods of $P \subseteq U/W$ such that the transition maps are affine. $\text{Spec}(\mathbb{K})$ is the limit of the respective spectra of function fields. Thus we can find a smooth, affine, irreducible Nisnevich neighborhood $Y \to U/W$ with function field $L := k(Y)$, such that the canonical injection $W_{\varphi}^\text{dec} \cong \text{Gal}(K^\beta(a)/K^\beta) \to \text{Gal}(L(a)/L)$ is an isomorphism. In particular, we have $[E \otimes_K K^\beta] = \text{ind}^W_{W_u^\varphi}([L(a)])$. Since $Y \to U/W$ is a Nisnevich neighborhood, we can find a point $Q \in Y$ over $P$ such that $\mathcal{O}_{Y/Q}/\mathcal{O}_{U/W}$ is unramified and both local rings have residue field $k(f)$. Now consider the following diagram:
\[
\begin{array}{ccc}
H^1(K, W) & \xrightarrow{a_v} & M(K) \\
\downarrow & & \downarrow \\
H^1(L, W) & \xrightarrow{a} & M(L).
\end{array}
\]
If we can prove $a_\ell(E \otimes_K L) = 0$, then we conclude that the image of $[E] \in H^1(K, W)$ under the above diagram lies in $M(\mathcal{O}_{Y/Q}) \subset M(L)$. Furthermore, observe that $K \subseteq L$ is separable, that $\mathcal{O}_{Y/Q}/\mathcal{O}_{U/W}$ is of ramification index 1 and that $\ell(f) = \ell(Q)$. Then we may use (1.1) to prove that $a_\ell(E) \in M(\mathcal{O}_P)$.

To show $a_\ell(E \otimes_K L) = 0$, define $a' := \text{res}^W_{W_u^\varphi}(a) \in \text{Inv}(W_{u^\varphi}^\text{dec}, M)$. The restriction of $a'$ to an elementary abelian 2-subgroup generated by reflections vanishes, since $a$ has this property. Thus we conclude $a' = 0$ by induction. In particular, $0 = a'\ell(L(a)) = a\ell(E \otimes_K L)$. This concludes the proof of $a_\ell(E) \in M(\text{Spec}(S(V^\vee W)))$. 

33
By \( \text{Spec}(S(V^\vee)^W) \cong \mathbb{A}_n^r \); from \( \mathbb{A}^1 \)-invariance, we thus conclude \( a(E) \in M(S(V^\vee)^W) \cong M(\mathbb{A}_n^r) \cong M(k_0). \) Therefore, \( a \) is constant (since it agrees with a constant invariant on a versal torsor). But we know that the restriction of \( a \) to elementary abelian 2-subgroups generated by reflections vanishes. Thus \( a = 0. \)

\[ \square \]

Let \( W \subset O(V) \) be an orthogonal reflection group. Then we denote by \( \Omega(W) \) the set of conjugacy classes of maximal elementary abelian 2-subgroups of \( W \) generated by reflections (maximality with respect to inclusion). We may reformulate the theorem in a more convenient language:

**Corollary 2.3.13.** Let \( W \subset O(V) \) be an orthogonal reflection group. Let \( M \) be an unramified \( \mathbb{A}^1 \)-invariant sheaf of abelian groups satisfying convention (C). Then \( \text{Inv}_W \) of maximal elementary abelian 2-subgroups of \( W \) is just multiplication in \( G \) is just multiplication in \( G \). So let \( \mathcal{W} \) be an arbitrary subgroup of this type. Then we can find \( 1 \leq i \leq r \) and \( w \in W \), such that \( \mathcal{W} \preceq \mathcal{W} \preceq \mathcal{W} \) is trivial on the image of the restriction map \( \text{res}_W^P \).

**Proof.** First observe that by \( \text{2.1.5} \) the conjugation action of \( \Omega(W) \) on \( \text{Inv}_W(P,M) \) is trivial and that the conjugation action of the normalizer \( N_W(P) \) is trivial on the image of the restriction map \( \text{res}_W^P \).

Now let \( a \in \text{Inv}_W(W,M) \) be in the kernel of \( \text{res}_W^P \); we want to show that \( a = 0 \). By Serre’s principle it suffices to show that the restriction of \( a \) to an elementary abelian 2-subgroups generated by reflections is 0. So let \( P \) be an arbitrary subgroup of this type. Then we can find \( 1 \leq i \leq r \) and \( w \in W \), such that \( w^{-1}Pw \subset P_i \). Now the corollary follows from

\[
\text{res}_W^P(a) = \text{res}_W^P(a) \text{res}_W^P(a^{-1}) = \text{res}_W^P(a^{-1}) (\text{res}_W^P(a^{-1})) = 0.
\]

where \( \iota_w: W \rightarrow W \) and \( \iota_w^{-1}: W \rightarrow W \) are the conjugations by \( w \) respectively \( w^{-1} \).

\[ \square \]

**Remark 2.3.14.** In fact, if \( |Q(W)| > 1 \) then this is a somewhat generous inclusion; we do not take into account the relations between different subgroups. In a more refined version, we would replace the right hand side by a limit indexed by the Quillen category. Here are some details:

Let \( W \) be a finite orthogonal reflection group. Let us denote by \( Q(W) \) the modified Quillen category of \( W \), which is defined as follows: Its objects are the elementary abelian 2-subgroups \( W \) generated by reflections. The set of morphisms \( \text{Mor}(P_1, P_2) \) consists of those elements \( g \in G \), such that \( g^{-1}P_1g \subset P_2 \) and the composition is just multiplication in \( G \).

Furthermore, we have a functor \( \text{Inv}: Q(W)^{op} \rightarrow \text{Ab} \) sending \( P \) to \( \text{Inv}(P,M) \) and \( g \in \text{Mor}(P_1, P_2) \) to

\[
\text{Inv}(P_2,M) \xrightarrow{\text{inv}} \text{Inv}(g^{-1}P_1g,M) \xrightarrow{\iota_g^{-1}} \text{Inv}(P_1,M).
\]

The previous proposition tells us that we have an injection

\[
\text{Inv}(W,M) \rightarrow \lim_{P \in Q(W)} \text{Inv}(P,M).
\]

The reason for calling \( Q(W) \) the modified Quillen category is that in group cohomology one defines the Quillen category just as we did, except for taking as objects all elementary abelian 2-subgroups (and not only the ones generated by reflections). In group cohomology, we then have a theorem stating that a cohomology class in \( H^1(S_n, \mathbb{Z}/2) \) is 0, if its restrictions to all elementary abelian 2-subgroups vanish. Although the distinction between elementary abelian 2-subgroups generated by reflections and all elementary abelian 2-subgroups might seem innocuous at first, the opposite is the case. For instance in the case of \( S_4 \), the map from the invariants to the inverse limit over the unmodified Quillen category will not be surjective. See \( \text{2.7.5} \).
2.4 Generality on finite Euclidean reflection groups

Now let us turn to Euclidean reflection groups. This means we specialize to the situation, where the base field is $\mathbb{R}$ and $V$ is endowed with a positive definite inner product $(\cdot, \cdot)$ (however at the end of this subsection we see that these groups may also be defined over more general fields). The main source for this chapter is \textcite{Hu}. First let us make some comments on root systems:

**Definition 2.4.1 (Root System).** Let $V$ be a finite-dimensional Euclidean vector space. A finite subset $\Phi \subset V$ is called root system, if it has the following two properties:

(i) For all $a \in \Phi$ we have $Ra \cap \Phi = \{a, -a\}$.

(ii) For all $a \in \Phi$ we have $s_a(\Phi) = \Phi$.

It is easy to see that the subgroup generated by reflections at elements of $\Phi$ defines a Euclidean reflection group $W(\Phi)$. One can show (e.g. \textcite[Prop. 1.14]{Hu}) that $\Phi$ is a root system associated to $W(\Phi)$ in the sense of 2.3.6, i.e. all reflections of $W(\Phi)$ are of the form $s_v$, with $v \in \Phi$.

As our base field is ordered, we have the notion of a simple system $\Delta \subset \Phi$:

**Definition 2.4.2 (Simple System).** Let $\Phi \subset V$ be a root system. A subset $\Delta \subset \Phi$ is called simple system, if $\Delta$ is a basis of $\text{span}(\Phi)$ with the following special property: Since $\Delta$ is a basis of $\text{span}(\Phi)$, we know that any $v \in \Phi$ can be written uniquely as a linear combination of elements from $\Delta$; then we require that in this sum either all coefficients are positive or all of them are negative.

It is shown in \textcite[Theorem 1.3]{Hu} that simple systems exist for every root system. The following theorem describes an important property of simple systems:

**Theorem 2.4.3.** Let $\Phi \subset V$ be a root system and $\Delta \subset \Phi$ be any simple system. Then $W(\Phi)$ is generated by simple reflections, i.e. by reflections at elements of $\Delta$.

**Proof.** \textcite[Proposition 1.5]{Hu}. \hfill $\Box$

Moreover, we will also need that any two simple systems in $\Phi$ are conjugate by an element of $W$ (this is proven in \textcite[Theorem 1.4]{Hu}).

For each $\alpha, \beta \in \Delta$ let $m(\alpha, \beta)$ be the smallest positive integer such that $(s_\alpha s_\beta)^m(\alpha, \beta) = 1$. Using these numbers, we may define the Coxeter graph on the vertices $\Delta$ by drawing an edge between $\alpha$ and $\beta$, if $m(\alpha, \beta) > 2$. Furthermore, we assign the weight $m(\alpha, \beta)$ to this edge. Since all simple systems are conjugated, this does not depend on the choice of $\Delta \subset \Phi$. Furthermore –as an abstract group– $W$ is determined by the Coxeter graph of $\Phi$; indeed it is generated by reflections at elements of $\Delta$ and all the relations between the generators can be derived from relations of the form $(s_\alpha s_\beta)^m(\alpha, \beta) = 1$. See for instance \textcite[Theorem 1.9]{Hu}.

A root system $\Phi$ is called irreducible, if it can not be written as $\Phi = \Phi_1 \cup \Phi_2$ for certain non-empty root systems $\Phi_1, \Phi_2$. Since we have $W(\Phi) = \bigwedge \Phi$, a good understanding of the reflection groups associated to irreducible root system, will yield many results for general reflection groups. It is possible to give a complete classification of all (finite) irreducible root systems; and we will make use of it! Unfortunately, in the literature, there is no coherent choice of a simple system or of a numbering of the vertices of a Coxeter graph. We will follow the conventions chosen by \textcite{Hu}, who in turn uses the notation of \textcite[VI]{Bou2}. For convenience, we repeat the list (except for $C_n$ which we ignored, since it generates the same reflection group as $B_n$); all unlabeled edges have weight 3:

(i) $A_n = \{\pm(e_i - e_j) | 1 \leq i < j \leq n + 1\}$

![Diagram of A_n](image)

(ii) $B_n = \{\pm e_i \pm e_j | 1 \leq i < j \leq n\} \cup \{\pm e_i | 1 \leq i \leq n\}$

![Diagram of B_n](image)

(iii) $D_n = \{\pm e_i \pm e_j | 1 \leq i < j \leq n\}$

![Diagram of D_n](image)
(iv) $E_6 = \{ \pm e_i \pm e_j \mid 1 \leq i < j \leq 5 \} \cup \{ \pm \frac{1}{2} (e_8 - e_7 - \sum_{i=1}^{5} \pm e_i) \mid \text{the number of } \cdot \text{ signs in the sum } \sum \text{ is even} \}$

where

$v_1 = \frac{1}{2}(e_1 - e_2 - e_3 - e_4 - e_5 - e_6 + e_7) \\
v_2 = e_1 + e_2 \\
v_i = e_{i-1} - e_{i-2} (3 \leq i \leq 6)$

(v) $E_7 = \{ \pm e_i \pm e_j \mid 1 \leq i < j \leq 6 \} \cup \{ \pm (e_7 - e_6) \} \cup \{ \pm \frac{1}{2} (e_8 - e_7 + \sum_{i=1}^{6} \pm e_i) \mid \text{the number of } \cdot \text{ signs in the sum } \sum \text{ is odd} \}$

where

$v_1 = \frac{1}{2}(e_1 - e_2 - e_3 - e_4 - e_5 - e_6 - e_7 + e_8) \\
v_2 = e_1 + e_2 \\
v_i = e_{i-1} - e_{i-2} (3 \leq i \leq 7)$

(vi) $E_8 = \{ \pm e_i \pm e_j \mid 1 \leq i < j \leq 8 \} \cup \{ \pm \frac{1}{2} (e_8 - \sum_{i=1}^{8} \pm e_i) \mid \text{the number of } \cdot \text{ signs is even} \}$

where

$v_1 = \frac{1}{2}(e_1 - e_2 - e_3 - e_4 - e_5 - e_6 - e_7 + e_8) \\
v_2 = e_1 + e_2 \\
v_i = e_{i-1} - e_{i-2} (3 \leq i \leq 8)$

(vii) $F_4 = \{ \pm e_i \pm e_j \mid 1 \leq i < j \leq 4 \} \cup \{ \pm e_i \mid 1 \leq i \leq 4 \} \cup \{ \pm \frac{1}{2} (\pm e_1 \pm e_2 \pm e_3 \pm e_4) \}$

(viii) $G_2 = \{ \pm (2e_i - e_j) \mid \{ i, j, k \} = \{ 1, 2, 3 \} \} \cup \{ \pm (e_i - e_j) \mid 1 \leq i < j \leq 3 \}$
(ix) Let \( a := \cos(\pi/5) = \frac{1}{4} \cdot (1 + \sqrt{5}) \) and \( b := \cos(2\pi/5) = \frac{1}{4} \cdot (-1 + \sqrt{5}) \). Then define
\[
H_3 = \{ \pm e_i | 1 \leq i \leq 3 \} \cup \{ \text{all even permutations of } (\pm a, \pm b, \pm b) = \pm ae_1 \pm \frac{1}{2}e_2 \pm be_3 \}
\]
where
\[
\begin{align*}
v_1 &= ae_1 - \frac{b}{\sqrt{2}}e_2 + be_3 \\
v_2 &= -ae_1 + \frac{b}{\sqrt{2}}e_2 + be_3 \\
v_3 &= \frac{1}{2}e_1 + be_2 - ae_3
\end{align*}
\]

(x) Let \( a := \cos(\pi/5) = \frac{1}{4} \cdot (1 + \sqrt{5}) \) and \( b := \cos(2\pi/5) = \frac{1}{4} \cdot (-1 + \sqrt{5}) \). Then define
\[
H_4 = \{ \pm e_i | 1 \leq i \leq 4 \} \cup \{ \frac{1}{2}(\pm e_1 \pm e_2 \pm e_3 \pm e_4) \} \cup \{ \text{all even permutations of } (\pm a, \pm \frac{1}{2}b, \pm b, 0) = \pm ae_1 \pm \frac{1}{2}e_2 \pm be_3 + 0 \cdot e_4 \}
\]
where
\[
\begin{align*}
v_1 &= ae_1 - \frac{b}{\sqrt{2}}e_2 + be_3 \\
v_2 &= -ae_1 + \frac{b}{\sqrt{2}}e_2 + be_3 \\
v_3 &= \frac{1}{2}e_1 + be_2 - ae_3 \\
v_4 &= -\frac{1}{2}e_1 - ae_2 + be_4
\end{align*}
\]

(xi) \( I_2(m) = \{(\cos(k\pi/m), \sin(k\pi/m)) | 0 \leq k \leq 2m - 1 \} \)

Now observe that we have the following lemma

**Lemma 2.4.4.** Let \( \Phi \) be one of the irreducible root systems above, excluding those of type \( I_2(2n) \). Then all roots of equal length lie in a single conjugacy class under the action of \( W(\Phi) \).

**Proof.** [Hu] 2.9 and end of 2.13]

**Lemma 2.4.5.** Let \( \Phi \) be one of the irreducible root systems \( A_n, D_n, E_6, E_7, E_8, H_3, H_4 \) or \( I_2(2n + 1) \) (i.e. \( \Phi \neq I_2(2n) \) and all roots are of the same length). Let \( S = \{s_1, \ldots, s_n\}, T = \{t_1, \ldots, t_m\} \) be two maximal sets of pairwise orthogonal elements of \( \Phi \). Then \( S \) and \( T \) are conjugate.

**Proof.** Certainly, \( S, T \) can not be empty. Hence by the previous lemma, we may assume \( s_1 = t_1 \). Now put \( \Psi := \langle s_1 \rangle \cap \Phi \) then \( \Psi \) is a root system. Decompose \( \Psi \) into its irreducible components \( \Psi = \Psi_1 \perp \ldots \perp \Psi_r \). Observe that each \( \Psi_j \) is isometric to one of the root systems required by the lemma. For each \( i \) the elements of \( \Psi_j \cap S \) and of \( \Psi_j \cap T \) both form a maximal set of pairwise orthogonal roots of \( \Psi_j \) (if \( \Psi_j \cap S \) was not a maximal set of pairwise orthogonal vectors, we could enlarge \( S \) by an element of \( \Psi_j \) contradicting the maximality of \( S \)). Now apply induction. \( \Box \)

For the construction of a certain \( W(F_4) \)-invariant later, the following lemma is useful:

**Lemma 2.4.6.** Consider the simple system \( S = \{e_1 - e_2, e_2 - e_3, e_3 - e_4, e_3 + e_4\} \subset D_4 \). If \( g \in W(D_4) \) stabilizes \( S \), then \( g = id \).

**Proof.** Looking at the Coxeter diagram, we see that \( g \) must fix \( e_2 - e_3 \). By 2.3.4 we conclude \( g \in W((e_2 - e_3) \cap D_4) = \langle s_2, s_3 \rangle \times \langle s_{e_1 - e_4} \rangle \times \langle s_{e_1 + e_4} \rangle \). We can even say \( g \in \langle s_{e_1 - e_4} \rangle \times \langle s_{e_1 + e_4} \rangle \). Otherwise it would map \( \{e_1 - e_2, e_2 - e_3, e_3 - e_4, e_3 + e_4\} \) to a set containing two vectors with non-zero \( e_2 \) component; but we assumed that \( g \) stabilizes \( \{e_1 - e_2, e_2 - e_3, e_3 - e_4, e_3 + e_4\} \). Repeating this argument using \( e_1 \) instead of \( e_2 \), we can furthermore restrict \( g \) to being an element of \( \langle s_{e_1 - e_4} \cdot s_{e_1 + e_4} \rangle \). Now looking at the image of \( e_1 - e_2 \), we conclude that \( g = e \) is the neutral element \( \Box \)
Remark 2.4.7. Now let us discuss, in what cases the Euclidean reflection groups defined above can be realized as orthogonal reflection groups over other fields than \( \mathbb{R} \). So let \( W \subset \text{GL}_n(\mathbb{R}) \) be a finite Euclidean reflection group and let \( k_0 \) be a field of \( \text{char}(k_0) \neq 2 \). Let \( \Phi \subset \mathbb{R}^n \) be a root system of \( W \). Now suppose that there exists a subring \( A \subset \mathbb{R} \) and a map \( f: A \rightarrow k_0 \) with the following properties

- \( \Phi \subset A^n \)
- For all \( v \in \Phi, (v, v)^{-1} \in A \)
- \( f^n \) restricted to the set \( \Phi \) is injective (where \( f^n: A^n \rightarrow k_0^n \) is the map induced by \( f \))

If such \( A \) and \( f \) exist, then

Lemma 2.4.8. \( W \) can be realized as orthogonal reflection group over \( k_0 \).

Proof. Let \( v \in \Phi \). We know that \( s_v \in O_n(\mathbb{R}) \) is given by the formula \( s_v(x) = x - 2 \frac{(x, v)}{(v, v)} v \). By assumption, we have \( (v, v)^{-1} \in A \). We conclude \( s_v \in \text{GL}_n(A) \) and thus \( W \subset \text{GL}_n(A) \). Applying \( f \), we obtain a representation \( W \rightarrow \text{GL}_n(k_0) \) and we want to show that this map is injective. So suppose \( w \in W \) is mapped to the identity in \( \text{GL}_n(k_0) \). In particular, it is the identity on \( f^n(\Phi) \). But since \( f^n \) is injective on \( \Phi \), we conclude that the image of \( w \) in \( \text{GL}_n(A) \subset \text{GL}_n(\mathbb{R}) \) acts trivially on \( \Phi \). But \( w \) acts also trivially on \( \Phi^+ \) and we have \( \Phi + \Phi^+ = \mathbb{R}^n \). This shows that \( w \) must be the neutral element. \( \square \)

Let us provide some examples

- If \( W \) is a Weyl group (i.e. the reflection group associated to a disjoint union of root systems of the form \( A_n, B_n, D_n, E_6, E_7, E_8, F_4 \) or \( G_2 \)), then \( W \) may be defined as orthogonal reflection group over any field \( k_0 \) of \( \text{char}(k_0) \neq 2 \). In fact, we may take \( A = \mathbb{Z}/[1/2] \) and let \( f: A \rightarrow k_0 \) be the canonical map.
- \( H_3, H_4 \) can be defined over any field such that \( \text{char}(k_0) \neq 2, 3, 5 \) and such that \( 5 \) is a square in \( k_0 \). Indeed take \( A = \mathbb{Z}/[1/2, \sqrt{5}] \) and let \( f: A \rightarrow k_0 \) be the map taking \( \sqrt{5} \in \mathbb{R} \) to a square root of \( 5 \) in \( k_0 \).
- Consider \( I_2(n) \). Suppose that \( \text{char}(k_0) \nmid 2n \) and that \( k_0 \) contains a primitive \( 2n \)-th root of unity \( \zeta \) and a primitive \( 4 \)-th root of unity \( i \). Take

\[
A = \mathbb{Z}[(\cos(0 \cdot \pi/n), \sin(0 \cdot \pi/n), \ldots, \cos((2n - 1)\pi/n), \sin((2n - 1)\pi/n)]
= \mathbb{Z}[\cos(\pi/n), \sin(\pi/n)].
\]

Take \( f \) to be the map defined by \( \cos(\pi/n) \mapsto \frac{\zeta + \zeta^{-1}}{2}, \sin(\pi/n) \mapsto \frac{\zeta - \zeta^{-1}}{2i} \). Furthermore note that if \( n \) is odd, \( k_0 \) contains a primitive \( 2n \)-th root of unity iff it contains a primitive \( n \)-th root of unity.

- Now consider \( I_2(n) \), where \( n \) is even and \( n \geq 4 \). Then the action of \( W(I_2(n)) \) on the root system \( I_2(n) \) has the two orbits

\[
\Delta_1 := \{(\cos(2k\pi/n), \sin(2k\pi/n)) \mid 0 \leq k \leq n - 1 \}
\text{and}
\Delta_2 := \{(\cos((2k + 1)\pi/n), \sin((2k + 1)\pi/n)) \mid 0 \leq k \leq n - 1 \}.
\]

Thus, if we replace \( \Delta_2 \) by \( \Delta_2 := \{(2\cos(\pi/n) \cdot \cos(2k + 1)\pi/n), 2\cos(\pi/n) \cdot \sin((2k + 1)\pi/n)) \mid 0 \leq k \leq n - 1 \} \), we obtain another root system \( I_2(n) \subset \Delta_2 \). Of course we have \( W(I_2(n)) \cong W(I_2(n)) \). Moreover, it can be checked that we have

\[
2\cos(\pi/n) \cos((2k + 1)\pi/n) = \cos(2k\pi/n) + \cos((2k + 2)\pi/n),
2\cos(\pi/n) \sin((2k + 1)\pi/n) = \sin((2k + 2)\pi/n) + \sin(2k\pi/n).
\]

Now suppose \( \text{char}(k_0) \nmid n \) and that \( k_0 \) contains a primitive \( n \)-th root of unity \( \zeta \) and a primitive \( 4 \)-th root of unity \( i \) (i.e. \( -1 \in k_0^{\times 2} \)). The above computation shows that we may take

\[
A = \mathbb{Z}[(2\cos(\pi/n))^{-2}, \cos(2\pi/n), \sin(2\pi/n)]
\]

and \( f \) to be the map defined by

\[
\cos(2\pi/n) \mapsto \frac{\zeta + \zeta^{-1}}{2}, \quad (2\cos(\pi/n))^{-2} \mapsto \zeta + \zeta^{-1} + 2, \quad \sin(2\pi/n) \mapsto \frac{\zeta - \zeta^{-1}}{2i}.
\]
Now let $W(\Phi) \subset GL_n(k_0)$ be an orthogonal reflection group induced by a finite Euclidean reflection group as described in the previous lines. Let $s \in W(\Phi)$ be any element which is an orthogonal reflection in $GL_n(k_0)$. In particular $s^2 = id$ and the characteristic polynomial of the image of $s$ in $GL_n(\mathbb{A}) \subset GL_n(\mathbb{R})$ is of the form $(X + 1)^k(X - 1)^{n-k}$ (recall the inclusion $W \subset GL_n(\mathbb{A})$ from the proof of the above lemma). Thus the characteristic polynomial of $s$ in $GL_n(k_0)$ is also given by $(X + 1)^k(X - 1)^{n-k}$. Since the image of $s$ in $GL_n(k_0)$ is a reflection, we conclude $k = 1$. Since the image of $s$ in $GL_n(\mathbb{R})$ lies in $O_n(\mathbb{R})$, we deduce that this image must be an orthogonal reflection, too. We may use the same kind of arguments to show conversely, that if $s \in W$ is an orthogonal reflection in $GL_n(\mathbb{R})$, then so is its image in $GL_n(k_0)$.

This discussion tells us the following: If we want to derive certain properties of $W(\Phi) \subset O_n(k_0)$ as an orthogonal reflection group (such as the structure of its maximal elementary abelian 2-subgroups generated by reflections), we may instead consider the real embedding $W(\Phi) \subset O_n(\mathbb{R})$ and establish the desired properties there.

### 2.5 Invariants of $(\mathbb{Z}/2)^n$

From now on, we will give examples of how to use the tools obtained in the previous sections in order to do concrete computations. In this section, we assume that $M_n$ is a $\mathbb{Z}$-graded $A^1$-module with $K^W$-module structure (see §4.13). Furthermore, we assume $\text{char}(k_0) \neq 2$ and put $G := (\mathbb{Z}/2)^n$.

For every $I \subset \{1; n\}$ we can define an element $x_I \in \text{Inv}^{\mathbb{Z}I}(\mathbb{Z}/2)^I, K^W)$ by

$$x_I : H^1(k, (\mathbb{Z}/2)^I) = (k^2/k^{x^2})^I \to K^W_I(k)$$

$$\quad (\alpha_1, \ldots, \alpha_n) \mapsto \prod_{i \in I} [\alpha_i].$$

These invariants are well-defined, since $\{a \beta^2 = \{a\}$. Then we have the following proposition:

**Proposition 2.5.1.** The invariants $\{x_I\}_{I \subset \{1; n\}}$ form an $M_n(k_0)$-basis of $\text{Inv}^G(M,M)$

**Proof.** By §3.3 the generic fiber of $\text{Spec}(k_0[T_1^{-1}; T_1^{-1}, \ldots, T_n^{-1}, \ldots, T_n^{-1}]) \to \text{Spec}(k_0[T_1^2, T_1^{-2}, \ldots, T_n^2, T_n^{-2}])$ is a versal $G$-torsor. Put $E := k_0[T_1, \ldots, T_n]$ and $K := k_0[T_1^2, \ldots, T_n^2]$. By 2.1.11 and 2.1.13, it is then sufficient to show that the $x_I(E)$ form an $M_n(k_0)$-basis of $M_n(\text{Spec}(k_0[T_1^2, T_1^{-2}, \ldots, T_n^2, T_n^{-2}]))$. This claim follows from the lemma below, which in turn can be proven by a repeated application of §4.12.

**Lemma 2.5.2.** $M_n(\text{Spec}(k_0[T_1^2, T_1^{-2}, \ldots, T_n^2, T_n^{-2}])) \cong \bigoplus_{I \subset \{1; n\}} (\prod_{i \in I} [T_i^2])M_n[\mathbb{Z}I](k_0)$.

\[ \square \]

**Remark 2.5.3.** Let us continue the story of §2.2.4 and try to determine $h_0(B_{gm}(\mathbb{Z}/2))$. Let $k_0$ be perfect and $\text{char}(k_0) \neq 2$. Observe that $G \cong \mathbb{Z}/2$ acts linearly on $A^2$ by changing the sign of both coordinates. This action is free on the $G$-invariant open subscheme $U := A^2 - \{0\}$ (moreover note that the complement is of codimension 2); thus the quotient $X := U/(\mathbb{Z}/2)$ exists and $U \to X$ is a $\mathbb{Z}/2$-torsor. It is proven in [Voe, Lemma 6.3] that $X$ is isomorphic to $O(-2) - s(P^1)$, where $s : P^1 \to O(-2)$ denotes the zero-section (we use the sign convention, where $O(-2)$ is a line bundle without non-trivial global sections). Let $M_n$ be a cycle module and consider the following part of the localization sequence for cycle modules:

$$0 \to A^0(O(-2), M) \xrightarrow{i} A^0(X, M) \xrightarrow{d} A^0(P^1, M)_{-1} \xrightarrow{j} A^1(O(-2), M)$$.

Since $p : O(-2) \to P^1$ is a vector bundle, $p' : A^1(P^1, M) \to A^1(O(-2), M)$, is an isomorphism. Thus we can rewrite the short exact sequence above as

$$0 \to A^0(P^1, M) \xrightarrow{(pr)} A^0(X, M) \xrightarrow{d} A^0(P^1, M)_{-1} \xrightarrow{(pr)^{-1}} A^1(P^1, M)$$.

Using the projection formula (which in the context of cycle modules is proven for instance in [Dég, Prop. 4.2.47]), we can now compute for all $a \in A^0(P^1, M)$:

$$(pr)^{-1}(s(a)) = (pr)^{-1}(s([P^1] \cup a))$$

$$= (pr)^{-1} \circ s([P^1] \cup a \circ p'(a))$$

$$= ((pr)^{-1} \circ s([P^1]) \cup a.$$
classes of line bundles by defining \(c(L) \equiv (p')^{-1} \cdot s_*(\{X\}) \in A^1(X, K^{M}_1) = CH^1(X)\). Indeed this definition coincides with the usual one, as defined – for instance – in [Fu, Section 2.5]: To prove this, by [Fu, Example 2.5.4] it suffices to check the projection formula, the additivity property and for any effective Cartier divisor the relation \(e(O(D)) = [D] \in CH^1(X)\). These are proven in [EK], Prop. 53.3(1)], [EK] Prop. 57.26] and [EK] Lemma 57.24] respectively. In particular, we have \(e(O(-2)) = 2 \cdot e(O(-1))\) and our exact sequence above becomes

\[
0 \to A^0(\mathbb{P}^1, M) \xrightarrow{(p|p')} A^0(\mathbb{P}^1, M) \xrightarrow{2e(O(-1))} A^1(\mathbb{P}^1, M).
\]

From the projective bundle theorem (as proven e.g. in [Dég2, Lemme 3.11]) one can now conclude that the map

\[
A^0(\mathbb{P}^1, M), - \mapsto A^0(\mathbb{P}^1, M),
\]

is injective and \(A^0(\text{Spec}(k_0), M), - \mapsto A^0(\mathbb{P}^1, M),\) is an isomorphism. Thus we finally obtain the exact sequence

\[
0 \to A^0(\text{Spec}(k_0), M) \to A^0(X, M) \xrightarrow{(\varphi | \varphi |)} A^0(\text{Spec}(k_0), M), - \mapsto (2) \to 0,
\]

where for any module \(P\) we write \(P(2) : = \{x \in P \mid 2 \cdot x = 0\}\) for its 2-torsion part. Furthermore, the injection in the above sequence is split, since \(X\) contains a rational point. This proves \(A^0(X, M), - \equiv \oplus A(\text{Spec}(k_0), M), - (2)\) for any cycle module \(M\).

It follows from [Dég1, Thm. 6.3.12] that for every \(F \in HN^\tau\) there exists a cycle module \(M\), such that \(A^0(\cdot; M) \equiv F(\cdot)\). Now we compute:

\[
F(X) \equiv M_0(\text{Spec}(k_0)) \oplus M_{-1}(\text{Spec}(k_0))(2)
\]

\[
\equiv F(\text{Spec}(k_0)) \oplus \text{Hom}_{HN^\tau}(F^M, F)(2)
\]

\[
\equiv F(\text{Spec}(k_0)) \oplus \text{Hom}_{HN^\tau}(F^M, F)
\]

\[
\equiv \text{Hom}_{HN^\tau}(\mathbb{Z} \oplus F^M / 2, F),
\]

where \(F^M = A^0(\cdot; F)\). Here the first isomorphism is [Dég1, Thm. 4.3.9] (i.e. the fact that \(A^0(\cdot; M)\), is a homotopy module) and the second one is [Dég1, Prop. 6.3.20].

The isomorphism \(F(X) \equiv \text{Hom}_{HN^\tau}(\mathbb{Z} \oplus F^M / 2, F)\) is functorial in \(F\) and so we obtain from the Yoneda lemma:

**Proposition 2.5.4.** \(h_0(B_{gm}(\mathbb{Z}/2)) \equiv h_0(X) \equiv \mathbb{Z} \oplus \mathbb{K}_1^M / 2\).

More generally, we have

**Corollary 2.5.5.**

\(h_0(B_{gm}(\mathbb{Z}/2)^n)) \equiv h_0(X^n) \equiv \mathbb{Z} \oplus \mathbb{K}_1^M / 2\)

and

\(\tilde{h}_0(B_{gm}(\mathbb{Z}/2)^n)) \equiv \tilde{h}_0(X^n) \equiv \mathbb{Z} \oplus \mathbb{K}_1^M / 2\).

**Proof.** We have isomorphisms

\[
h_0(X^n) \equiv h_0((h_0(X)^{\otimes n}) \equiv h_0((\mathbb{Z} \oplus \mathbb{K}_1^M / 2)^{\otimes n})
\]

\[
\equiv \mathbb{Z} \oplus \mathbb{K}_1^M / 2.
\]

Here the first isomorphism follows from [Dég1, Lemme 3.1.10], the second one from the previous proposition and the third one from \(S_1^* = h_0(G_m^{\otimes n}) = \mathbb{K}_1^M\) (again see [Dég1, Prop. 6.3.20]) and the right exactness of the tensor product. To deduce the reduced version one only needs to check that after choosing a rational point \(x \in X(k_0)\) (in the second isomorphism), the \(\mathbb{Z}\)-summand in the last line corresponds under the isomorphisms to the rational point \((x, \ldots, x) \in X^n(k_0)\). 

\(\square\)
2.6 Invariants of $O_n$

Most of the invariants that we will meet later come from invariants of quadratic forms. Therefore, it is convenient to recall the structure of Inv$(O_n, M)$ from [CMS §17] and from [Mo2 Section 5]. Of course, we assume char$(k_0) \neq 2$.

First observe that we have a map $(\mathbb{Z}/2)^n \to O_n$ of algebraic groups over $k_0$ defined by embedding $(\mathbb{Z}/2)^n$ as diagonal matrices. Furthermore, using the embedding $S_n \subset O_n$ defined by permutation matrices, $S_n$ normalizes $(\mathbb{Z}/2)^n$.

**Proposition 2.6.1.** Let $M$ be a strongly $\mathbb{A}^1$-invariant sheaf of abelian groups satisfying convention (C). Then the restriction map induces an isomorphism Inv$(O_n, M) \xrightarrow{\sim} \text{Inv}((\mathbb{Z}/2)^n, M)^{S_n}$.

**Proof.** There are several things to show. Let us begin by proving that the restriction map is injective. The map $H^1(k, (\mathbb{Z}/2)^n) \to H^1(k, O_n)$ is induced by sending a $(\mathbb{Z}/2)^n$-torsor $(a_1, \ldots, a_n) \in (k^\times/k^\times)^n$ to the quadratic form $\langle a_1, \ldots, a_n \rangle$. Since any non-degenerate quadratic form can be diagonalized, this is surjective for any $k \in F_{K_0}$. Consequently, the restriction map Inv$(O_n, M) \to \text{Inv}((\mathbb{Z}/2)^n, M)$ must be injective. Its image is contained in Inv$((\mathbb{Z}/2)^n, M)^{S_n}$, because conjugation by permutation matrices normalizes $(\mathbb{Z}/2)^n$. Now let us show that the image is precisely Inv$((\mathbb{Z}/2)^n, M)^{S_n}$.

So let $a \in \text{Inv}((\mathbb{Z}/2)^n, M)^{S_n}$ be arbitrary. We would like to define $\tilde{a} \in \text{Inv}((\mathbb{Z}/2)^n, M)^{S_n}$ by mapping $q \in H^1(k, O_n)$ to $a(a_1, \ldots, a_n)$, where $(a_1, \ldots, a_n)$ is a diagonalization of $q$. We need to prove that if $(\beta_1, \ldots, \beta_n)$ is another diagonalization, then $a(a_1, \ldots, a_n) = a(\beta_1, \ldots, \beta_n)$.

In general, recall that $(a_1, \ldots, a_n)$ and $(\beta_1, \ldots, \beta_n)$ are called simply chain equivalent if there exist indices $i, j$, such that $a_k = \beta_i$ for $k \neq i, j$ and such that $(a_i, a_j) \equiv (\beta_i, \beta_j)$. It is proven for instance in [Lam] Theorem 5.2 that any two isomorphic quadratic forms are in fact connected by a chain of simple chain equivalences. Thus it suffices to consider the case $n = 2$.

Suppose first that we have $a_k(1, x) = a_k(x, 1) = 0$ for all $k \in F_{K_0}$ and all $x \in k^\times/k^\times$. Let $K = k_0(t_1, t_2)$ be the field of rational functions in two variables. By [Matsumura] we know that the evaluation of $a_k$ at the versal $\mathbb{Z}/2 \times \mathbb{Z}/2$-torsor $(t_1, t_2) \in (k^\times/k^\times)^2$ lies in $M(G_m \wedge G_m) \subset M(K)$. Moreover, since $a_k(t_1, 1) = a_k(1, t_2) = 0$ this induces in fact a map $\tilde{a} : G_m \wedge G_m \to M$ (observe that for $X$ smooth and irreducible we have $M(X) \subset M(k(X))$, as $M$ is unramified). By [Mo2 Theorem 3.37] $a$ factors as $a \circ G_m \wedge G_m \to M$.

Here $K^{MW}$ are the unramified Milnor-Witt $K$-theory sheaves (see [Mo2 Section 3.2]) and $a_2$ is a map of sheaves of abelian groups whose section over fields is given by $(a_1, a_2) \mapsto [a_1][a_2]$. Then we compute for $a, b, (a + b) \in k^\times$:

$$a_k(a + b, a b(a + b)) = a_k([a + b][a + b][a + b]) = a_k([a + b][a + b]) = a_k(a + b, -a b) = a_k(a + b, -\frac{b}{a}) = a_k(a + b, \frac{-b}{a}) = \tilde{a}_k([a][\frac{-b}{a}]) = \tilde{a}_k([a, b]) = a_k(a, b).$$

Now we can conclude as in the usual proof of the presentation of the Grothendieck-Witt ring (see e.g. [Lam] proof of thm. 4.1): Since $(a_1, a_2) \equiv (\beta_1, \beta_2)$, we can find $x, y \in k, c \in k^\times$ such that $\beta_1 = a_1 x^2 + a_2 y^2$ and $a_1 a_2 = \beta_1 \beta_2 c^2$. Suppose first that $x = 0$ or $y = 0$; we will only consider the first case. Then we have

$$a_k(\beta_1, \beta_2) = a_k(a_2 y^2, a_1 a_2/(\beta_1 c^2)) = a_k(a_2, a_1) = a_k(a_1, a_2).$$

If both $x \neq 0$ and $y \neq 0$, we have

$$a_k(a_1, a_2) = a_k(a_1 x^2, a_2 y^2) = a_k(a_1 x^2 + a_2 y^2, a_1 a_2(x y)^2(a_1 x^2 + a_2 y^2)) = a_k(\beta_1, \beta_2) = a_k(\beta_1, \beta_2).$$
Thus $a_\ell$ is indeed independent of the choice of a diagonalization.

Now let us consider the general case, where we do not require $a_\ell(1, x) = 0$ any more. It suffices to prove that the invariant $b \in \text{Inv}(\mathcal{Z}/2^2, M)^G$ defined by $b(x, y) = a_\ell(x, 1) + a_\ell(y, 1)$ extends to an invariant of quadratic forms. Indeed, then we know that $a_\ell(1, 1), b_\ell$ and $a_\ell(x, y) = a_\ell(x, 1) - a_\ell(1, 1) + a_\ell(1, 1)$ all extend to invariants of quadratic forms (the last one by the case treated above); thus also $a_\ell$ extends to an invariant of quadratic forms.

First observe that the invariant $c_\ell: x \mapsto c_\ell(x) := a_\ell(x, 1)$ induces a morphism $c: G_m/2 \to M$. By [Mo3] Theorem 2.46] this factors as $G_m/2 \to K^W\to M$, where the first map is induced on fields by $x \mapsto \langle x \rangle$. Thus, we have 

\[ b_\ell(x + y, \alpha \beta (x + y)) = a_\ell(x + y, 1) + a_\ell(\alpha \beta (x + y), 1) = \overline{c}(x + y) + \overline{c}(\alpha \beta (x + y)) = \overline{c}(x) + \overline{c}(y) + (\alpha \beta (x + y)) = b_\ell(x, y) \]

and we conclude as before. \qed

**Example 2.6.2.** Let us consider the case $M = K^W$ is Witt $K$-theory. Before we start, it is convenient prove an easy technical lemma:

**Lemma 2.6.3.** Let $R$ be a commutative ring, $I$ a finite index set, $M$ an $R$-module and $G$ a finite group acting on $I$. The operation of $G$ on $I$ induces an operation of $G$ on the $R$-module $N := \oplus_{i \in I} M$ by permutation of coordinates. Let $I = I_1 \cup I_2 \cup \cdots \cup I_k$ be its orbit decomposition. Then we have $N^G = \oplus_{i=1}^k N_{I_i}$ where for $1 \leq i \leq k$, we put 

\[ N_{I_i} := \left\{ \sum_{i \in I_i} t_i(m) \mid m \in M \right\} \cong M \]

(Here $t_i: M \to N$ denotes the inclusion using the $i$-th coordinate).

**Proof.** It is clear that the sum of the $N_i$ is direct (i.e. $(\sum_{i \in I_i} N_i) \cap N_j = \{0\}$) and that $\sigma_{i=1}^k N_i \subset N^G$. So it remains to show that the $N_i$ generate $N^G$. To prove this, note that any $x \in N$ can be written uniquely as $x = \sum_{i \in I_i} t_i(m_i)$ for certain $m_i \in M$. We will prove by induction on the number of non-zero $m_i$ that any $x \in N^G$ lies in the module generated by the $N_i$. If all of them are zero, then we have won. Wlog, we may suppose $I = [1; \lvert I \rvert]$ and $m_i \neq 0$. Now let $g \in G$ be arbitrary. Comparing the $g(1)$-th entry of $x$ and of $g \cdot x$, we obtain $m_{g(1)} = m_i$. But since $g$ was arbitrary, this means that we can split of a sum $\sum_{i \in I_i} t_i(m_i) = \sum_{i \in I_i} t_i(m_i) \in N_{I_i}$ from $x$ (if we denote by $I_1$ the orbit containing 1). Now we may apply induction to $x - \sum_{i \in I_i} t_i(m_i)$. \qed

The following corollary is immediate:

**Corollary 2.6.4.** Let $R$ be a commutative, graded ring, $I^{(1)}, \ldots, I^{(r)}$ be finite index sets, $M_\ell$ be a graded $R$-module and $G$ a finite group acting on each of the $I^{(1)}$. The operation of $G$ on $I^{(1)}$ induces an operation of $G$ on the graded $R$-module $N_\ell := \oplus_{i=1}^{I^{(1)}} M_{\ell-d_i}$, where the $d_i$ are certain non-negative integers. Let $I^{(r)} = I^{(1)} \cup I^{(2)} \cup \cdots \cup I^{(r)}$ be the orbit decomposition. Then we have $N^G = \oplus_{i=1}^{I^{(1)}} \oplus_{j=1}^{I^{(2)}} N_{\ell_{ij}}$, where for $1 \leq \ell \leq r, 1 \leq i \leq n_{\ell}$ we put 

\[ (N_{\ell_{ij}})_\ell := \left\{ \sum_{i \in I^{(1)}} t_i(m) \mid m \in M_{\ell-d_i} \right\} \cong M_{\ell-d_i}. \]

Now let us return to the computation of $\text{Inv}^\ast(O_n, K^W)$. We want to define the total Stiefel-Whitney class $w \in \text{Inv}^{\text{jet}}(O_n, K^W)$. We want to define the total Stiefel-Whitney class $w \in \text{Inv}^{\text{jet}}(O_n, K^W)$. We want to define the total Stiefel-Whitney class $w \in \text{Inv}^{\text{jet}}(O_n, K^W)$. We want to define the total Stiefel-Whitney class $w \in \text{Inv}^{\text{jet}}(O_n, K^W)$. We want to define the total Stiefel-Whitney class $w \in \text{Inv}^{\text{jet}}(O_n, K^W)$. We want to define the total Stiefel-Whitney class $w \in \text{Inv}^{\text{jet}}(O_n, K^W)$. We want to define the total Stiefel-Whitney class $w \in \text{Inv}^{\text{jet}}(O_n, K^W)$. We want to define the total Stiefel-Whitney class $w \in \text{Inv}^{\text{jet}}(O_n, K^W)$. We want to define the total Stiefel-Whitney class $w \in \text{Inv}^{\text{jet}}(O_n, K^W)$. We want to define the total Stiefel-Whitney class $w \in \text{Inv}^{\text{jet}}(O_n, K^W)$. We want to define the total Stiefel-Whitney class $w \in \text{Inv}^{\text{jet}}(O_n, K^W)$. We want to define the total Stiefel-Whitney class $w \in \text{Inv}^{\text{jet}}(O_n, K^W)$. We want to define the total Stiefel-Whitney class $w \in \text{Inv}^{\text{jet}}(O_n, K^W)$. We want to define the total Stiefel-Whitney class $w \in \text{Inv}^{\text{jet}}(O_n, K^W)$. We want to define the total Stiefel-Whitney class $w \in \text{Inv}^{\text{jet}}(O_n, K^W)$. We want to define the total Stiefel-Whitney class $w \in \text{Inv}^{\text{jet}}(O_n, K^W)$. We want to define the total Stiefel-Whitney class $w \in \text{Inv}^{\text{jet}}(O_n, K^W)$. We want to define the total Stiefel-Whitney class $w \in \text{Inv}^{\text{jet}}(O_n, K^W)$. We want to define the total Stiefel-Whitney class $w \in \text{Inv}^{\text{jet}}(O_n, K^W)$. We want to define the total Stiefel-Whitney class $w \in \text{Inv}^{\text{jet}}(O_n, K^W)$. We want to define the total Stiefel-Whitney class $w \in \text{Inv}^{\text{jet}}(O_n, K^W)$. We want to define the total Stiefel-Whitney class $w \in \text{Inv}^{\text{jet}}(O_n, K^W)$. We want to define the total Stiefel-Whitney class $w \in \text{Inv}^{\text{jet}}(O_n, K^W)$. We want to define the total Stiefel-Whitney class $w \in \text{Inv}^{\text{jet}}(O_n, K^W)$. We want to define the total Stiefel-Whitney class $w \in \text{Inv}^{\text{jet}}(O_n, K^W)$. We want to define the total Stiefel-Whitney class $w \in \text{Inv}^{\text{jet}}(O_n, K^W). We want to define the total Stiefel-Whitney class $w \in \text{Inv}^{\text{jet}}(O_n, K^W)$.
following two relations:

\[ \{a + b\}(a + b)ab = \{a\}b, \]
\[ \{a + b\} + \{(a + b)ab\} = \{a\} + \{b\}. \]

Due to

\[ \{a + b\} + \{(a + b)ab\} - \{a\} - \{b\} = \{ab\} + \eta[\{a + b\}(a + b)ab] - (\{ab\} + \eta[\{a\}b]), \]

it suffices to check the first relation. We compute

\[ \{a + b\}(a + b)ab = \{a + b\}\{-ab\} \]
\[ = \{a\}\{-b/a\} + \{1 + b/a\}\{-b/a\} - \eta[\{a\}1 + b/a\] \[-b/a\] \]
\[ = \{a\}\{-b/a\} \]
\[ = \{a\}\{b\}. \]

Thus the Stiefel-Whitney classes are indeed well-defined. Observe that we have \( w(q \oplus q') = w(q) \cdot w(q') \). Now let \( M \) be a \( \mathbb{Z} \)-graded \( A^1 \)-module with \( KW \)-structure. We saw in the previous section that \( Inv^i((\mathbb{Z}/2)^\ast, M) \) is a free \( M(\mathbb{Z}_0) \)-module with basis \( \{x_i\}_{i \in [1, n]} \). We conclude that \( Inv^i(O_n, M) \equiv Inv^i((\mathbb{Z}/2)^\ast, M) \) is a free \( M(\mathbb{Z}_0) \)-module with basis \( \{w_\delta j, 0 \leq \delta \leq n\} \). In particular, if \( M = K^M/2 \), we obtain that \( Inv^i(O_n, K^M/2) \) is a free \( K^M/2 \)-module on the Stiefel-Whitney classes \( \{w_\delta j\}_{0 \leq \delta \leq n} \).

**Example 2.6.5.** The determinant defines a group homomorphism \( det: O_n \to \{ \pm 1 \} \equiv \mathbb{Z}/2 \). Furthermore, recall that there is an invariant \( x_11 \in Inv^i((\mathbb{Z}/2)^\ast, K^M/2) \). I claim that we have \( w_1 = det(x_11) \in Inv^i(O_n, K^M) \):

Let \( q \equiv (\alpha_1, \ldots, \alpha_n) \) be a non-singular quadratic form over \( k \in \mathcal{F}_{\mathbb{Z}_0} \). Then it’s easy to check that the image of \( q \) under \( det.: H^i(k, O_n) \to H^i(k, \mathbb{Z}/2) \) is the \( \mathbb{Z}/2 \)-torsor \( \alpha_1\alpha_2 \cdots \alpha_n \in \mathbb{Z}^2/k^x \). But in \( K^M(k)/2 \) we have \( w_1((\alpha_1, \ldots, \alpha_n)) = \{\alpha_1\} + \{\alpha_2\} + \ldots + \{\alpha_n\} \equiv \{\alpha_1 \cdot \cdots \cdot \alpha_n\} \).

**Example 2.6.6.** Later, we will meet some examples where it is easier to do the computations with a slight variant of the Stiefel-Whitney classes. Therefore, let us introduce modified Stiefel-Whitney classes \( \overline{w}_i \) in \( Inv^i(O_n, K^M/2) \). If \( n \) is even, we simply put \( \overline{w}_i(q) := w_i(2) \otimes q \). If \( n \) is odd, we define inductively \( \overline{w}_0 = 1 \) and \( \overline{w}_{i+1}(q) = w_{i+1}(2) \otimes q - \{2\} \overline{w}_i(q) \). Then clearly we have

\[ \overline{w}_d(2\alpha_1, \ldots, 2\alpha_n) = \sum_{k \in [1, n]} \prod_{i \in d} \{\alpha_i\}, \]

if \( n \) is even and it is easy to check that

\[ \overline{w}_d(2\alpha_1, \ldots, 2\alpha_{n-1}, 1) = \sum_{k \in [1, n-1]} \prod_{i \in d} \{\alpha_i\} \]

holds, if \( n \) is odd.

In the case of \( K^M/2 \)-coefficients, there is an easy formula for the product \( w_r \cdot w_s \) (see [GMS, Remark 17.4]). Write \( r = \sum r_i 2^i, s = \sum s_i 2^i \) for some \( R, S \subset \{0, 1, 2, \ldots\} \) and put \( m := \sum r_i s_i 2^i \). Then we have

\[ w_r \cdot w_s = (-1)^m \cdot w_{r+s-m}. \]  

(2.6.1)

As we want to have a similar formula for a variant of the Stiefel-Whitney classes later, let us recall the proof.

**Proof.** Let \( k \in \mathcal{F}_{\mathbb{Z}_0} \) and let \( q = (\alpha_1, \ldots, \alpha_n) \) be a nondegenerate quadratic form (where \( \alpha_i \in k^x \)). By elementary combinatorics and the relation \( |\alpha|\alpha = (-1)^n|\alpha| \), we compute

\[ w_r(q) \cdot w_s(q) = \left( \prod_{k \in [1, n]} \{\alpha_k\} \right) \left( \prod_{k \in [1, n]} \{\alpha_k\} \right) \]
\[ = \sum_{k \geq 0} \binom{r + s - k}{r + s - 2k} \binom{r + s - 2k}{r - k} (-1)^k w_{r+s-k}. \]

So we only need to prove the following lemma:
Lemma 2.6.7. \((r + s - k)(r + s - 2k)\) is divisible by 2, if \(k \neq m\).

Proof. Suppose first that \((r + s - k)(r + s - 2k)\) is odd. Write \(r - k = \sum_{i \in A} 2i\), \(s - k = \sum_{i \in B} 2i\) for certain \(A, B \subset \mathbb{N}\). Now recall Lucas’s theorem which says that a binomial coefficient \(\binom{n}{m}\) is odd if and only if the following holds: Whenever the binary expansion of \(n\) contains a summand \(2^j\), then the binary expansion of \(x\) also contains the summand \(2^j\). In our situation, we know that \((r + s - k)\) is odd. Using Lucas’s theorem, we conclude that \(A \cap B = \emptyset\). Thus \(r + s - 2k = \sum_{i \in A \cup B} 2i\). Let’s do the same for \((r + s - 2k)\): First write \(r = \sum_{i \in C} 2i\) for some \(C \subset \mathbb{N}\). From Lucas’s theorem, we conclude that \(C \cap (A \cup B) = \emptyset\). Thus we have \(r = \sum_{i \in C \cup B} 2i\) and \(s = \sum_{i \in B \cup C} 2i\). Now we can conclude \(R = A \cup C, S = B \cup C\) and \(R \cap S = C\); in particular, \(k = m\). Conversely, if \(k = m\) then the above arguments and Lucas’s theorem imply that \((r + s - k)(r + s - 2k)\) is odd. \(\square\)

2.7 Invariants of finite Euclidean reflection groups

Now let us determine, case by case, the invariants of finite Euclidean reflection groups associated to irreducible root systems. This part is very computational and Stembridge’s Maple package [St] turned out to be extremely helpful to compute the action of reflection groups on the respective vector spaces (in particular in complicated cases like \(E_6, E_7, E_8\) or \(H_3, H_4\)).

Remark 2.7.1. Before we descend into depths of computation, let us make an important remark concerning the coefficients we use. In the computations that follow, we use mainly \(\mathbb{Z}\)-graded \(A^1\)-modules with \(k^M/2\)-structure. However, as Prof. Morel explained to me, they are valid for all cycle modules in the following sense:

Let \(k_0\) be perfect, let \(W\) be a finite Euclidean reflection group and let \(\Omega = \{[P_1], \ldots, [P_l]\}\) (Recall that we denote by \(\Omega\) the set of conjugacy classes of maximal elementary abelian 2-subgroups generated by reflections). Translating Serre’s splitting principle via the Totaro isomorphism, we obtain for each \(F \in HN^{tr}\) an injection

\[
\text{Hom}_{HN^F}(\widetilde{h}_0(B_{gm}(W)), F) \to \varnothing_{i=1}^l \text{Hom}_{HN^F}(\widetilde{h}_0(B_{gm}(P_i)), F)
\]

which is functorial in \(F\). By a Yoneda argument, we thus obtain an epimorphism

\[
\varnothing_{i=1}^l \widetilde{h}_0(B_{gm}(P_i)) \to \widetilde{h}_0(B_{gm}(W)).
\]

Using the computations of remark 2.5.3 we conclude that \(\widetilde{h}_0(B_{gm}(W))\) is 2-torsion.

Now let \(M\) be an arbitrary 2-torsion cycle module. In the following sections, we will then explicitly compute isomorphisms of the form \(\text{Int}^F(W, M) \cong \varnothing_{\alpha}(M_{n \cdot \alpha}(k_0))\) for certain non-negative integers \(d\), and these isomorphisms are functorial in \(M\). This holds, if the base field is “nice” enough; for Weyl groups, \(-1 \in k_0^2\) and \(\text{char}(k_0) \nmid |W|\) are certainly sufficient; in general we furthermore have to assume \(5 \in k_0^2\) and that \(k_0\) contains all \(|W|\)-th roots of unity. Since \(M\) is 2-torsion, we have

\[
\text{Hom}_{HN^F}(k_M^M/2, A^0(\cdot; M)) \cong \text{Hom}_{HN^F}(k_M^M, A^0(\cdot; M))
\cong (A^0(\cdot; M))_{\varnothing - d}(k_0)
\cong M_{\varnothing - d}(k_0).
\]

Here the second isomorphism uses \(k_M^M \cong S_{\varnothing - d}^o\) and that \(A^0(\cdot; M)\) is a homotopy module (these statements are proven in [Deg1, Prop. 6.3.20] and [Deg1, Thm. 4.3.9]). Thus \(\text{Hom}_{HN^F}(\widetilde{h}_0(B_{gm}(W)), A^0(\cdot; M)) \cong \text{Hom}_{HN^F}(\varnothing_{\alpha}(k_M^M/2, A^0(\cdot; M))\). By the construction of [Deg1, Thm. 6.3.12], for any 2-torsion \(F \in HN^{tr}\) there exists a 2-torsion cycle module \(M\) with \(F = A^0(\cdot; M)\). As \(\widetilde{h}_0(B_{gm}(W))\) is 2-torsion, we can apply to the above isomorphism the Yoneda lemma in the category of 2-torsion homotopy invariant Nisnevich sheaves with transfers to conclude \(\widetilde{h}_0(B_{gm}(W)) \cong \varnothing_{\alpha}(k_M^M/2).\) In particular, the following computation holds for any cycle module \(M\):

\[
\text{Int}^\text{norm}(W, M) \cong \text{Hom}_{HN^F}(\widetilde{h}_0(B_{gm}(W)), M)
\cong \text{Hom}_{HN^F}(\varnothing_{\alpha}(k_M^M/2, M)
\cong \varnothing_{\alpha}M_{\varnothing - d}(2).
\]
2.7.1 \( A_n \)

The mod 2 invariants for the symmetric group \( S_n = W(A_{n-1}) \) have been explicitly computed in [CMS §25]. Nevertheless, we will repeat the argument here for the sake of completeness. In this section, \( M \) is assumed to be a strongly \( A^1 \)-invariant sheaf of abelian groups satisfying convention (C). To apply 2.3.12 directly, we would have to require that \( char(k_0) \uparrow [S_n] \). However, this assumption was only needed, to assure that \( S(V)^W \) is a polynomial algebra. But for \( W = S_n \) this is true regardless of the characteristic. Thus, just as in [CMS §25], we will only assume \( char(k_0) \not\equiv 2 \). First put \( m := \lceil n/2 \rceil \) and \( a_i = c_{2i-1} - c_{2i} \) for \( 1 \leq i \leq m \). Observe that by 2.4.5 \( \text{IQ}(W(A_{n-1})) \equiv 1 \). Its single element can be written as \( [P] \), where \( P := P(a_1, \ldots, a_m) \). Let \( \varphi : S_n \to S_n \) be the map induced by sending a transposition \( (i, j) \) to \( (2i - 1, 2j - 1) \cdot (2i, 2j) \); then \( N := \varphi(S_n) \subset S_n \subset O_n \) normalizes \( P \). Thus the image of the restriction \( \text{res}^P_{S_n} \) lies in \( \text{Inv}(P, M)^N \). More precisely, we have

**Proposition 2.7.2.** The restriction map \( \text{res}^P_{S_n} \) induces an isomorphism \( \text{Inv}(S_n, M) \cong \text{Inv}(P, M)^N \).

**Proof.** The map is injective by 2.3.12. It suffices to show surjectivity. During this proof, we will say that \( a \in \text{Inv}(P, M)^N \) is of order at most \( d \) if there exists \( b \in \text{Inv}((\mathbb{Z}/2)^d, M)^S \) such that for all \( k \in \mathcal{T}_{S_0} \) and all \( (a_1, \ldots, a_m) \in H^1(k, P) \) we have

\[
\alpha_k(a_1, \ldots, a_m) = \sum_{l \in [1, [m]]} b(a_l),
\]

where \( b(a_{l}) = b(a_{i_1}, \ldots, a_{i_d}) \) if \( I = \{i_1, \ldots, i_d \} \). Obviously every \( a \in \text{Inv}(P, M)^N \) is of order at most \( m \). Our plan is to use induction on the order to prove that for any \( a \in \text{Inv}(P, M)^N \) there exists \( c \in \text{Inv}(O_n, M) \equiv \text{Inv}((\mathbb{Z}/2)^m, M)^S \) such that \( \text{res}^P_{O_n}(c) = a \). If \( a \) is of order at most \( 0 \), then it is constant and we may choose \( c = a \). So suppose now that \( a \) is of order at most \( d > 0 \) and that the claim is true for all invariants of order at most \( d' \), where \( d' < d \). Furthermore, we will first consider the case, where \( n \) is even (since it is slightly less technical than the case \( n \) odd). Let \( b \in \text{Inv}((\mathbb{Z}/2)^d, M)^S \) be as in the definition of the order. Then define \( \tilde{c} \in \text{Inv}((\mathbb{Z}/2)^m, M)^S \) by

\[
(k^x/k^2)^n \to M(k)
\]

\[
(p_1, \ldots, p_m) \to \sum_{l \in [1, [m]]} b(p_l),
\]

where \( b(p_l) = b(p_{i_1}, \ldots, p_{i_d}) \) if \( I = \{i_1, \ldots, i_d \} \). Via the map \( H^1(k, P) \to H^1(k, S_n) \to H^1(k, O_n) \) the torsor \( (a_1, \ldots, a_m) \) is sent to the quadratic form \( (2, 2a_1, \ldots, 2a_m) \) (see 1.3.40). Thus we have

\[
\text{res}^P_{O_n}(\tilde{c})(a_1, \ldots, a_m) = \sum_{l \in [1, [m]]} b(a_l) + \sum_{l \in [1, [m]]} \sum_{[l] = [k]} b(a_l, 1, \ldots, 1),
\]

and \( a - \text{res}^P_{O_n}(\tilde{c}) \in \text{Inv}(P, M)^N \) is a sum of invariants of order \( < d \). By induction we can then write \( a - \text{res}^P_{O_n}(\tilde{c}) = \text{res}^P_{O_n}(c_1) \) for some \( c_1 \in \text{Inv}(O_n, M) \equiv \text{Inv}((\mathbb{Z}/2)^m, M)^S \). We should not forget the case, where \( n \) is odd. Then \( (a_1, \ldots, a_m) \in H^1(k, O_n) \) is sent to the quadratic form \( (2, 2a_1, \ldots, 2a_m, 1) \) under the map \( H^1(k, P) \to H^1(k, O_n) \). If we define \( \tilde{c} \in \text{Inv}((\mathbb{Z}/2)^m, M)^S \) as above, we compute

\[
\text{res}^P_{O_n}(\tilde{c})(a_1, \ldots, a_m) = \sum_{l \in [1, [m]]} b(a_l) + \left( \sum_{l \in [1, [m]]} \sum_{[l] = [k]} b(a_l, 1, \ldots, 1) \right) + \left( \sum_{l \in [1, [m]]} \sum_{[l] = [k]} b(a_l, 2, 1, \ldots, 1) \right).
\]

Again we see that \( a - \text{res}^P_{O_n}(\tilde{c}) \in \text{Inv}(P, M)^N \) is a sum of invariants of order \( < d \). \( \square \)

**Example 2.7.3.** Suppose \( M \) is a \( \mathbb{Z} \)-graded \( A^1 \)-module with \( K^W \)-structure. Then \( \text{Inv}^r(P, M) \) is a free \( M(k_0) \)-module with basis \( \{x_l \}_{I \subseteq [1, [m]]} \). The action of \( N \) on \( \text{Inv}^r(P, M) \) permutes the \( x_l \) and the orbits of this action are given by \( B_0, \ldots, B_m \) where \( B_d = \{x_l \mid [l] = [d] \} \). By 2.6.3, \( \text{Inv}^r(P, M) \) is a free \( M(k_0) \)-module with basis \( \{\sum_{l \in [1, [m]]} x_l \}_{0 \leq d \leq m} \). But the modified Stiefel-Whitney classes \( \overline{w}_d \) defined in 2.6.6 satisfy \( \text{res}^P_{S_n}(\overline{w}_d) = \sum_{l \in [1, [m]]} x_l \). By abuse of notation, we will denote the restriction of the \( \overline{w}_d \) to \( S_n \) that still by \( \overline{w}_d \). Thus \( \text{Inv}^r(S_n, M) \) is a free \( M(k_0) \)-module with basis \( \{\overline{w}_d \}_{0 \leq d \leq m} \).

**Remark 2.7.4.** The relation 2.6.1 holds also for the modified Stiefel-Whitney classes: Write \( r = \sum_{i \in \mathcal{R}} 2^i \), \( s = \sum_{i \in \mathcal{S}} 2^i \) for some \( R, S \subset \{0, 1, 2, \ldots \} \) and put \( m := \sum_{i \in \mathcal{R} \cup S} 2^i \). Then we have

\[
\overline{w}_r \cdot \overline{w}_s = \{1\}^m \cdot \overline{w}_{r+s-m} \in \text{Inv}^{r+s}(S_n, M).
\]

(It is enough to prove this after restricting to \( P \); then we can use the same proof as in 2.6.1)

45
Remark 2.7.5. We promised to show that the usual/unmodified Quillen map (i.e. the one obtained by considering all elementary abelian 2-subgroups) is in general not surjective for the group $S_4$. Let $k_0$ be any field, such that $\text{char}(k_0) \neq 2$ and $-1 \in k_0^{\times 2}$; we use $K^M/2$ as coefficients. First observe that the restriction of the invariant $x_{(1,2)} \in \text{Int}^r((\mathbb{Z}/2)^2, K^M/2)$ to any proper subgroup of $(\mathbb{Z}/2)^2$ is zero. Indeed, let $\iota_1, \iota_2, \iota_3 : \mathbb{Z}/2 \rightarrow \mathbb{Z}/2 \times \mathbb{Z}/2$ be the inclusion into the first factor, the inclusion into the second factor and the diagonal and let $\alpha \in k^\times/k^2\times$ be any $\mathbb{Z}/2$-torsor. Then we compute

$$
\iota_1^*(x_{(1,2)})(\alpha) = |\alpha||1| = 0
\iota_2^*(x_{(1,2)})(\alpha) = |1|\alpha = 0
\iota_3^*(x_{(1,2)})(\alpha) = |\alpha|\alpha = [-1]|\alpha| = 0.
$$

$S_4$ has the maximal elementary abelian 2-subgroups $\langle (12), (34) \rangle, \langle (13), (24) \rangle, \langle (14), (23) \rangle$; we denote them by $\langle \iota_1 \rangle, \langle \iota_2 \rangle, \langle \iota_3 \rangle$. The first three are conjugated, while the last one is a normal subgroup in $S_4$. Now define an element $z = (z_P)_{P\leq Q(S_4)_{\text{hom}}(\eta)} = \prod P \leq Q(S_4)_{\text{hom}} \text{Int}^2(S_4, K^M/2)$ by setting $z_P := x_{(1,2)}(P)$ and $z_P := 0$ if $P \neq Q$. Then this is in fact an element of

$$
\lim_{P \leq Q(S_4)_{\text{hom}}} \text{Int}^2(P, K^M/2).
$$

Indeed, there are two types of arrows ending in $Q$. Either it is an arrow which factors through a proper subgroup $\mathcal{P}$ of $Q$; and we checked above that the image of $z_{\mathcal{P}}$ under the induced morphism is then automatically 0. Or it is an arrow of the form $\phi : Q \rightarrow Q$. We claim that $\phi^*(x_{(1,2)}) = x_{(1,2)}$ for all those $\phi$. To prove this, first put $f_1 := (12)(34), f_2 := (13)(24), f_3 := f_1 \circ f_2 = (14)(23)$. Then we have 6 automorphisms of $Q$ determined by first choosing one of the elements $\{f_1, f_2, f_3\}$ as the image of $f_1$ and then choosing one of the remaining two elements as the image of $f_2$. It is now easy to check by hands that $x_{(1,2)}$ is fixed by all those automorphisms. For instance consider the map $\phi$ mapping $f_1$ to $f_1$ and $f_2$ to $f_1 \circ f_2$. For all $(\alpha, \beta) \in k^\times/k^2$ we compute

$$
\phi^*(x_{(1,2)})(\alpha, \beta) = x_{(1,2)}(\alpha \cdot \beta, \beta)
= |\alpha \cdot \beta||\beta|
= |\alpha||\beta|
= x_{(1,2)}(\alpha, \beta).
$$

After having checked all possible $\phi$, we conclude that $z$ is indeed an element of

$$
\lim_{P \leq Q(S_4)_{\text{hom}}} \text{Int}^2(P, K^M/2).
$$

However, $z$ can not come from $\text{Int}^2(S_4, K^M/2)$: indeed, any such invariant necessarily had to vanish identically, since its restriction to the maximal elementary abelian 2-subgroup generated by reflections $\langle (12), (34) \rangle$ is 0.

2.7.2 $H_3$

Our assumptions on $k_0$ are $\text{char}(k_0) \neq 2, 3, 5$ and $-1 \in k_0^{\times 2}$. $M$, is a $\mathbb{Z}$-graded $\mathbb{A}^1$-module with $K^M/2$-module structure.

Let $\sqrt{5} \in k_0$ be a fixed choice of one of the two elements whose square is 5. Furthermore, define

$$
a := \frac{1 + \sqrt{5}}{4}, \quad b := \frac{-1 + \sqrt{5}}{4}.
$$

By 2.4.5 we have $\Omega(W(H_3)) = \{[P]\}$, where $P := P(e_1, e_2, e_3)$. Next observe that $\gamma := s_{e_1+e_2} + s_{e_3} : S_{e_1+e_2+e_3}$ is the linear map determined by $e_1 \mapsto e_3, e_2 \mapsto e_1, e_3 \mapsto e_2$. Thus $\gamma$ normalizes $P$. It is not hard to show that the orbits of the basis $\{x_{i_1 e_1 e_2} e_3 \}$ of $\text{Int}^r(P, K^M/2)$ under $\{\gamma\}$ are given by $B_0, B_1, B_2, B_3$ , where $B_i = \{x_{i} \mid [i] = i\}$. By 2.6.4 the image of the restriction $\text{Int}^r(W(H_3), M) \rightarrow \text{Int}^r(P, M)$ is contained in the free $M, (k_0)$-submodule with basis $\{\sum_{i,j \leq 3} x_{i_1 e_1 e_2} e_3 \}$. The embedding $W(H_3) \subset O_3$ gives us invariants $\text{Res}_{W(H_3)}^O(\eta_i) \in \text{Int}^d(W(H_3), K^M/2)$; we will denote them again by $w_i$. Let $k \in F_{-4}$ and $x(e_1, e_2, e_3) \in (k^\times/k^2)^3$ be an arbitrary $P$-torsor. Then the quadratic form induced by this torsor under the map $P \rightarrow W(H_3)$ is normalized by $\{e_1, e_2, e_3\}$, thus its total Stiefel-Whitney class is $\prod_{i=1}^3 (1 + [e_i])$. We conclude that $\text{Res}_{W(H_3)}^P(\eta_i) = \sum_{i \leq 3} x_{i_1 e_1 e_2} e_3$. This shows that $\text{Int}^r(W(H_3), M)$ is a free $M, (k_0)$-module with basis $\{w_i\}_{0 \leq i \leq 3}$.
2.7.3 $H_4$

Again we require $\text{char}(k_0) \neq 2, 3, 5$ and $5 \in k_0^\times$. $M$ is a $\mathbb{Z}$-graded $A^1$-module with $K^M/2$-module structure. As in the previous section, we define

$$a := \frac{1 + \sqrt{5}}{2}, \ b := \frac{-1 + \sqrt{5}}{4}.$$  

By 2.4.3 $W(H_4)$, we have $\Omega(W(H_4)) = \{[P]\}$, where $P := P(e_1, e_2, e_3, e_4)$. Thus, the restriction $\text{Inv}^*(W(H_4), M) \to \text{Inv}^*(P, M)$ is an injection.

As in the $H_2$ case, by notation $g := s_{-\pi}, h := s_{\pi}$ is the linear map determined by $e_1 \mapsto e_3, e_3 \mapsto e_1, e_2 \mapsto e_2, e_4 \mapsto e_4$. In the same spirit, $\hat{h} := s_{-\pi} \cdot s_{\pi}$ is the linear map induced by $e_1 \mapsto e_4, e_4 \mapsto e_1, e_2 \mapsto e_2, e_3 \mapsto e_3$. Thus $g, h$ normalize $P$ and so the group $\langle g, h \rangle$ acts on $\text{Inv}^*(P, M)$. Again, it is not hard to show that the orbits of the basis $\{x_i\}_{i \in \{1, 2, 3, 4\}}$ of $\text{Inv}^*(W(H_4), K^M/2)$ are given by $[B_i] | 0 \leq i \leq 4$, where $B_i = [x_i] | [1] = i$. By 2.6.3, the image of the restriction $\text{Inv}^*(W(H_4), M) \to \text{Inv}^*(P, M)$ is contained in the free $M, (k_0)$-submodule with basis $\{\sum_{i=1}^{4} x_i\}$. Now it is easy to check that $\tau, \sigma$ act on $\text{Inv}^*(W(H_4), M) \to \text{Inv}^*(P, M)$ in fact an isomorphism.

Remark 2.7.6. As abstract groups, we have in fact $W(G_2) \cong W(I_2(6))$. However, in contrast to $I_2(6)$ the root system of $G_2$ is defined over any field of $\text{char}(k) \neq 2, 3$.

2.7.4 $G_2$

Let $\text{char}(k_0) \not\equiv 2, 3$. Let $M$ be any unramified $A^1$-invariant sheaf satisfying convention (C). Then it is easy to show that $\Omega(W(G_2)) = \{[P]\}$, where $P := P(e_1 - e_2, 2e_3 - e_1 - e_2)$. Thus the restriction map $\text{Inv}(W(G_2), M) \to \text{Inv}(P, M)$ is injective. Furthermore, $W(G_2)$ has a unique 3-Sylow subgroup $U$; therefore $W(G_2) \cong \mathbb{Z} \rtimes U$; in fact $W(G_2)$ is just the dihedral group of order 12. We conclude that the inclusion $P \subset W(G_2)$ has a section. Thus the injective restriction map $\text{Inv}(W(G_2), M) \to \text{Inv}(P, M)$ is in fact an isomorphism.

2.7.5 $I_2(n)$

$I_2(n) \subset \mathbb{R}^2$ is the root system consisting of $\{(\cos(k\pi/n), \sin(k\pi/n)) | 0 \leq k \leq 2n - 1\}$ and $W(I_2(n))$ is its just the dihedral group of order $2n$. It is convenient to distinguish some cases; let us first assume that $4 \not| n$.

By 2.4.7 this root system is defined over any field $k_0$, such that $\text{char}(k_0) \not\equiv 2n$ and such that $i, \zeta \in k_0$, where $\zeta$ is a primitive $2n$-th root of unity and $j$ is a primitive $4$-th root of unity. Furthermore let $M$ be any unramified $A^1$-invariant sheaf of abelian groups satisfying convention (C). Observe that we have a permutational representation $W = W(I_2(n)) = \langle \sigma, \tau \rangle \subset S_n$, given by

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ 2 & 3 & \cdots & 1 \end{pmatrix}, \ \ \tau = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ n & n-1 & \cdots & 2 & 1 \end{pmatrix}.$$  

First let us consider the case, where $n$ is odd. Then $\Omega(W) = \{[\tau]\}$. We conclude that the restriction $\text{Inv}(W, M) \to \text{Inv}((\tau), M)$ is injective. Furthermore, we have $W \cong (\tau, \tau) \ltimes U$. Again, the map $\tau \mapsto (\tau, \tau) \ltimes U \mapsto (\tau, \tau)$ is the identity. This proves that the restriction map is in fact surjective.

The same trick works for the case $2 \mid n$ and $4 \not| n$, i.e. $n = 2m$ with $m$ odd. Put $\bar{\tau} = \sigma^m \tau$. Then we have $\tau = (1, n)(2, n-1)\cdots(m, m+1)$ and $\Omega(W) = \{[\tau, \bar{\tau}]\}$. Observe that $W$ contains a unique subgroup $U$ of order $m$. Thus we have $W \cong (\tau, \bar{\tau}) \ltimes U$. Again, the map $\tau \mapsto (\tau, \tau) \ltimes U \mapsto (\tau, \tau)$ is the identity. Thus the injection $\text{Inv}(W, M) \to \text{Inv}((\tau, \bar{\tau}), M)$ is already surjective. The hard part is to determine the invariants in the case $4 \mid n$.

So suppose now $n = 2m$ with $m$ even. In this case, we require that $\text{char}(k_0) \not| 2n$ and that $k_0$ contains an $n$-th root of unity $\zeta$ (and thus automatically also a 4-th root of unity $i$). As discussed in 2.4.7-- after rescaling half of the roots of $I_2(n)$--the root system $I_2(n)$ may be used to define $W$ as an orthogonal reflection group over $k_0$. Furthermore, we assume that $M$, is a $\mathbb{Z}$-graded $A^1$-module with $K^M/2$-module structure.

As $\zeta \in k_0$ by assumption, we have a closed immersion $\phi: W \to GL_2$ of algebraic groups over $k_0$ defined by

$$\sigma \mapsto \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix}, \ \ \tau_1 \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$  

where $\sigma = (12 \cdots n)$ and $\tau_1 = (2, n)(3, n-1)\cdots(m, m+2)$ (note that, of course, this embedding has nothing to do with the embedding $W \subset O_2$ coming from the structure of $W$ as orthogonal reflection group). $\phi$ determines an action of $W$ on $k_0[X, Y]$ given by $X = \zeta X, \ Y = \zeta^{-1} Y, \ ^{\tau}X = Y, \ ^{\tau}Y = X$. When we think of the regular $n$-gon as being embedded into $\mathbb{A}^2$ with the first vertex lying at coordinate $(1, 0)$, then $\sigma$ is
just a rotation by the angle $2\pi/n$ and $\tau_1$ is the reflection at the $x$-axis. It is not too hard to show that $k_0[X,Y]^W = k_0[X^n + Y^n, XY] \cong k_0[A,B]$ (where $A := X^n + Y^n$, $B := XY$). Fix the notation $E := k_0(X,Y)$, $K := k_0(X^n + Y^n, XY)$. Now we want to determine an open, $W$-invariant subset of $A^2$ on which the action induced by $\phi$ is free. By [2.11], it suffices to check what closed points we need to remove. To ensure that $g \in W$ acts freely, we need to remove the eigenvectors of $\phi(g)$ corresponding to the eigenvalue 1. It is not hard to see that only the elements $\phi(\sigma \tau_1)$ have eigenvalue 1; the eigenspace is generated by $(1, \zeta^n, \zeta^{2n})^T$. Thus $W$ acts freely on the open subscheme 

$$U := D \left( \prod_i (c^i X + Y) \right) = D(X^n - Y^n) = D((X^n - Y^n)^2) \subset A^2.$$ 

Computation yields 

$$U/W \cong \text{Spec}(k_0[X,Y,(X^n - Y^n)^2]^W) = \text{Spec}(k_0[X^n + Y^n, XY,(X^n - Y^n)^2]) \cong \text{Spec} \left( k_0 \left[ A, B, \frac{1}{A^2 - 4B^n} \right] \right).$$ 

It is not yet obvious how to compute $M_\ast(U/W)$; therefore, we first observe that for $V := D(B) \subset U/W$ we have 

$$V \cong \text{Spec} \left( k_0 \left[ A, B, B^{-1}, \frac{1}{A^2 - 4B^n} \right] \right) \cong \text{Spec} \left( k_0 \left[ A', B, B^{-1}, \frac{1}{A' - 2', A' + 2} \right] \right),$$

where the second isomorphism is induced by mapping $A'$ to $A/B^m$. By applying [1.4.9] twice, we obtain 

$$M_\ast(V) \cong M_\ast(k_0) \oplus \{ A/B^m - 2 \}M_{-1}(k_0) \oplus \{ A/B^m + 2 \}M_{-1}(k_0) \oplus \{ B \}M_{-1}(k_0) \oplus \{ B \} \{ A/B^m - 2 \}M_{-2}(k_0) \oplus \{ B \} \{ A/B^m + 2 \}M_{-2}(k_0).$$

$M_\ast(U/W)$ can be computed as the kernel of the boundary $\partial = \partial_B : M_\ast(V) \to M_{-1}(G_m)$. It is not hard to carry this out explicitly: Recall that $2 \mid m$. Thus, for $t \in M_\ast(k_0)$ we have 

$$\partial(t) = 0,$$

$$\partial((A/B^m \pm 2)t) = \partial((A \pm 2B^m)t) = [A]\partial(t) = 0,$$

$$\partial((B)t) = t,$$

$$\partial((B)(A/B^m \pm 2)t) = \partial((B)(A \pm 2B^m)t) = [A]\partial((B)t) = [A]t.$$

We conclude 

$$M_\ast(U/W) = M_\ast(k_0) \oplus \{ A/B^m - 2 \}M_{-1}(k_0) \oplus \{ A/B^m + 2 \}M_{-1}(k_0) \oplus \{ B \}M_{-1}(k_0) \oplus \{ A \}^{2}M_{-2}(k_0) \oplus \{ B \}^{2}M_{-2}(k_0).$$

Unfortunately, the codimension of $A^2 - U$ is only 1, so that we can not just apply Totaro’s result. However, we have at least an injection $\text{im}^\ast(W,M) \to M_\ast(U/W)$ induced by the evaluation at the versal torsor $\text{Spec}(E) \to \text{Spec}(K)$. We will now check that this is indeed a surjection by constructing invariants mapping to the three non-constant basis elements of $M_\ast(U/W)$. 

By [2.4.7] we can consider $W$ as an orthogonal reflection group over $k_0$. That is, we have an embedding $\psi : W \subset O_2$ of algebraic groups over $k_0$ given by 

$$\alpha \mapsto \begin{pmatrix} \frac{\zeta^{2n-1}}{2} & -\frac{\zeta^{2n-1}}{4} \\ \frac{\zeta^{2n-1}}{4} & \frac{\zeta^{2n-1}}{2} \end{pmatrix}, \quad \tau_1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. $$

48
Pulling back \( w_1, w_2 \in \text{Inv}'(O_2, K^M/2) \) along \( \psi \), we obtain elements in \( \text{Inv}'(W, K^M/2) \) that – by abuse of notation – we again denote by \( w_1, w_2 \). Let us first compute the value of \( w_1 \) at the versal torsor \( E/K \) constructed above. To do this, we note that the determinant of \( \psi(\sigma \tau_1) \) is \(-1\), while the determinant of \( \psi(\sigma') \) is \(1\). Now \( X^n - Y^n \in E \) is mapped to its negative by each reflection and is fixed by all of the \( \sigma' \). Thus the value of \( w_1 \) at \( E/K \) is just \((X^n - Y^n)^2 \) in \( K^M(K)/2 \).

Another invariant comes from the embedding \( W \subset S_n \). We may define \( v_1 := \text{res}_{S_n}^W(\tilde{w}_1) \). Again, let us try to compute the value of \( v_1 \) at \( E/K \). We note that \( \tilde{w}_1 \in \text{Inv}'(S_n, K^M/2) \) may be computed as follows. Start with an arbitrary \( x \in H^1(k, S_n) \); then \( \tilde{w}_1(x) = \text{sgn}(x) \in H^1(k, Z/2) \cong k^*/(k^*)^2 \cong K^M(k)/2 \). It is easy to see that the kernel of \( \text{sgn} \) consists exactly of the elements \( \sigma^2, \sigma^2 \tau_1 \) with \( \sigma, \tau_1 \) as above. Now we just need to observe that \( X^n - Y^n \) is fixed by this kernel and is mapped to its negative by \( \sigma \). Thus the value of \( v_1 \) at the versal torsor is \((X^n - Y^n)^2 \). Consequently evaluating \( w_1 - v_1 \) at the versal torsor yields \((X^n + Y^n)^2 \). But \((X^n - Y^n)^2 = \lambda - 2B^n \) and \((X^n + Y^n)^2 = \lambda + 2B^n \) in \( k_0(X^n + Y^n, XY) = k_0(A, B) \). Thus, it remains to find an invariant mapping to the basis \([B]([A^2 - 4B^n]) \) of \( M_1(U/W) \).

Let us compute the value of \( w_2 \in \text{Inv}'(W, K^M/2) \) at \( E/K \). First consider the elementary abelian \( 2 \)-subgroup generated by reflections \( P = \langle \tau_1, \tau_1' \rangle \), where \( \tau_1' = \sigma m \tau_1 \). Thus we have

\[
\psi(\tau_1) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \psi(\tau_1') = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.
\]

Now consider the versal \( P \)-torsor \( E/E^P = k_0(X, Y)/k_0(X^2 + Y^2, XY) \) (recall that the action of \( W \) on \( E \) is defined via \( \phi \)). \( \tau_1 \in P = \text{Gal}(E/E^P) \), acts via \( \tau_1(X) = Y, \tau_1(Y) = X \) and \( \tau_1' \) via \( \tau_1'(X) = -Y, \tau_1'(Y) = -X \). Thus this \((Z/2)^2\)-torsor over \( E^P \) is equivalently described by the pair \( ((X - Y)^2, (X + Y)^2) \in ((E^P)^*)^2 \). We conclude that the value of \( \text{res}_{E^P} w_2 \) at this \( P \)-torsor is \((X - Y)^2((X + Y)^2) \in K^M(E^P)/2 \).

By the computations above, we know that the value of \( \text{res}_{E^P} w_2 \) at \( E/K \) is of the form

\[
\alpha_1 + [(X^n - Y^n)^2] \alpha_2 + [(X^n + Y^n)^2] \alpha_3 + [XY][(X^n - Y^n)^2] \alpha_4 \in K^M(K)/2
\]

for some \( \alpha_1 \in K^M(k_0)/2, \alpha_2, \alpha_3 \in K^M(k_0)/2, \alpha_4 \in K^M(k_0)/2 \). Now consider the diagram

\[
\begin{array}{ccc}
H^1(K, W) & \xrightarrow{w_2} & K^M(K)/2 \\
\text{res}_{E^P}^W(E) \downarrow & & \downarrow \text{ind}^P_1 \\
H^1(E^P, W) & \xrightarrow{w_2} & K^M(E^P)/2 \\
& \downarrow \text{ind}^P_1 & \\
& H^1(E^P, P) &
\end{array}
\]

The square commutes by the definition of invariants. Denote by \( E \in H^1(K, W) \) the \( W \)-torsor \( E/K \) and denote by \( F \in H^1(E^P, P) \) the \( P \)-torsor \( E/E^P \). For instance by looking at the cocycles, we see that

\[
\text{ind}^P_1(E) = \text{res}_{E^P}^W(E) \in H^1(E^P, W).
\]

Using this and observing that \((X^n + Y^n)^2 \) is a square in \( E^P \), we obtain

\[
[(X - Y)^2][(X + Y)^2] = \alpha_1 + [(X^n - Y^n)^2] \alpha_2 + [XY][(X^n - Y^n)^2] \alpha_4 \in K^M(E^P)/2.
\]

As we have \((X^n - Y^n)/(X^2 - Y^2), (X^n - Y^n)/(X^2 - Y^2) \in E^P \), this means

\[
(X - Y)^2[(X + Y)^2] = \alpha_1 + [(X^2 - Y^2)^2] \alpha_2 + [XY][(X^2 - Y^2)^2] \alpha_4.
\]

If we put \( a := X^2 + Y^2 \) and \( b := XY \in E^P = k_0(X^2 + Y^2, XY) \), then we may rewrite this as

\[
|a - 2b| |a + 2b| = |a^2 - 4b^2| \alpha_2 + |b| |a^2 - 4b^2| \alpha_4.
\]

Using the lemma below, we obtain \( \alpha_1 = 1 \) and then we conclude immediately that \( \alpha_1 = \alpha_2 = 0 \). Thus the value of \( \omega_2 - \omega_3 \cdot (w_1 - v_1) \) at \( E/K \) is \([XY][(X^n - Y^n)^2]\) and all of the basis elements of \( M_1(U/W) \) are indeed images of elements of \( \text{Inv}'(W, K^M/2) \). We conclude that the injection \( \text{Inv}'(W, M) \to M_1(U/W) \) is in fact surjective. It only remains to prove the following lemma:

**Lemma 2.7.7.** Let \( k \) be a field such that \(-1 \in k^{x^2}\). Let \( a, b \in k^X \) such that \( b, a - 2b, a + 2b \neq 0 \). Then in \( K^M(k)/2 \) we have \([a - 2b] |a + 2b| = |b| |a^2 - 4b^2| \).
Proof.

\[
(a - 2b)(a + 2b) = \left\{ 4b \left( \frac{a - 2b}{4b} \right) \right\} \left\{ 4b \left( \frac{a - 2b}{4b} + 1 \right) \right\}
= [b] \left\{ \frac{a - 2b}{4b} + 1 + \left( \frac{a - 2b}{4b} \right) \right\} [b]
= [b] \left\{ \frac{a^2 - 4b^2}{16b^2} \right\}
= [b] \left\{ a^2 - 4b^2 \right\}.
\]

This finishes the computation of $\text{Inv}^r(W,M)$ and we obtain:

**Proposition 2.7.8.** If $4 \mid n$, then $\text{Inv}^r(W(I_2(n)), M_1)$ is a free $M(k_0)$-module with basis consisting of the invariants $[1, w_1, v_1, w_2]$ constructed above.

We want to end this section with a corollary of the proof which we will need for the $W(B_2)$-invariants:

**Corollary 2.7.9.** Let $P_1 = P(e_1, e_2)$ and $P_2 = P(e_1 - e_2, e_1 + e_2)$. Then we have

\[
\text{res}^{P_1}_{W(I_2(4))}(w_1) = x_{[e_1]} + x_{[e_2]},
\]

\[
\text{res}^{P_1}_{W(I_2(4))}(v_1) = x_{[e_1]} + x_{[e_2]},
\]

\[
\text{res}^{P_1}_{W(I_2(4))}(w_2) = x_{[e_1, e_2]}
\]

and

\[
\text{res}^{P_2}_{W(I_2(4))}(w_1) = x_{[e_1 - e_2]} + x_{[e_1 + e_2]},
\]

\[
\text{res}^{P_2}_{W(I_2(4))}(v_1) = 0,
\]

\[
\text{res}^{P_2}_{W(I_2(4))}(w_2) = x_{[e_1 + e_2, e_1 - e_2]} + \{2\} \cdot (x_{[e_1 - e_2]} + x_{[e_1 + e_2]}).
\]

**Remark 2.7.10.** This corollary can be used to show that for $G = W(I_2(4))$ the modified Quillen map is not surjective.

### 2.7.6 $B_n$

In this section, we assume that $\text{char}(k) \nmid [b_n]$ and $-1 \in k^\times$. Furthermore, we will assume that $M$ is a $Z$-graded $A^1$-module with $K^1/2$-module structure. The root system $B_n$ is the disjoint union $\Delta_1 \cup \Delta_2 \subset \mathbb{R}^n$, where $\Delta_1 = \{ \pm e_i \mid 1 \leq i \leq n \}$ are the short roots and $\Delta_2 = \{ \pm e_i \pm e_j \mid 1 \leq i < j \leq n \}$ are the long roots. This root system induces an orthogonal reflection group over any $k_0$ satisfying the above requirements. Furthermore, note that we have $W(B_n) \cong S_n \ltimes (Z/2)^n$ as abstract groups. Put $m := \left\lfloor \frac{n}{2} \right\rfloor$ and for $1 \leq i \leq n$ define $a_i := e_{2i-1} - e_{2i}$ and $b_i := e_{2i-1} + e_{2i}$. Then each $0 \leq L \leq m$ the elements of $X_L := \{ a_1, b_1, \ldots, a_L, b_L, e_{2L+1}, e_{2L+2}, \ldots, e_n \}$ are mutually orthogonal; put $P_L := P(X_L)$. Let us prove by induction on $m$ that $\Omega(W) = \{ [P_0], \ldots, [P_n] \}$.

The claim is clear for $n = 2$. In the general case, let $P$ be any maximal elementary abelian 2-subgroup generated by reflections. First assume that $P$ contains a short root. By 2.4.4 we may assume that this short root is $e_1$. Now observe that $\langle e_1 \rangle^2 \cap B_n = B_{n-1}$ and use induction. If $P$ contains a long root, we may (again by 2.4.4) assume this root to be $a_1$. Now we have $\langle a_1 \rangle \cap B_n = \{ \pm b_1 \} \cup B_{n-2}$, where we consider $B_{n-2}$ to be embedded in $\mathbb{R}^n$ using the last $n - 2$ coordinates. Now we may again use the induction hypothesis.

Unfortunately, before we can start to determine $\text{Inv}^r(B_n, M)$ there are a couple of notational issues to be addressed. We will denote $P_L$-torsors over a field $k$ by $(a_1, b_1, \ldots, a_L, b_L, e_{2L+1}, \ldots, e_n) \in (k^2/k^\times)^n$. From the $(Z/2)^n$-section, we already know that $\text{Inv}^r(P_L, M)$ is a free $M(k_0)$-module with basis $[x_1]_{[1, n]}$. However, for our purposes the parametrization by subsets of $[1, n]$ is quite inconvenient. Therefore we change the index set, so that it will be better adapted to our situation. Namely, let us introduce

\[
A_L^d := \{(A, B, C, E) \subset [1, L]^3 \times [2L + 1; n] \mid A, B, C \text{ pairwise disjoint }, |A| + |B| + 2|C| + |E| = d\}.
\]

We may reindex the $M(k_0)$-basis of $\text{Inv}^r(P_L, M)$ by defining for every $(A, B, C, E) \in A_L^d$

\[
\chi^{(d)}_{(A, B, C, E)} : H^1(k, P_L) \rightarrow K^1_2(k)/2
\]

\[
(a_1, b_1, \ldots, a_L, b_L, e_{2L+1}, \ldots, e_n) \mapsto \prod_{a \in A} [a_x] \cdot \prod_{b \in B} [b_x] \cdot \prod_{c \in C} [a_c] [b_c] \cdot \prod_{e \in E} [e_e].
\]
In the same spirit, we will also write
\[ P(A, B, C, E) := P(\{a_i\}_{i \in A} \cup \{b_i\}_{i \in B} \cup \{a_r, b_r\}_{r \in C} \cup \{e_s\}_{s \in E}). \]

Let us now construct a few \( W(B_a) \)-invariants. First consider the canonical projection \( \rho : W(B_a) \cong S_n \to (\mathbb{Z}/2)^n \). For \( 0 \leq d \leq m \), we have modified Stiefel-Whitney classes \( \tilde{w}_d \in \text{inv}^d(S_n, K^M/2) \) and we define \( u_d := \rho^*(\tilde{w}_d) \in \text{inv}^d(W(B_a), M) \). Let \( k \in \mathcal{F}_B \) and let \( (\alpha_1, \beta_1), \ldots, (\alpha_L, \beta_L) \in \mathbf{E}_{2l+1}, \ldots, e_n \) be an arbitrary \( P_L \)-torsor over \( k \). Observe that the map \( W(B_a) \to S_n \) sends both \( s_{\tilde{d}} \) to \((2i - 1, 2i)\) and \( s_{\tilde{t}} \) to the neutral element. Using \((1.3.41)\) and that \( [2][2] = 0 \), we see that the value of the total modified Stiefel-Whitney class at this torsor is \( \prod_{i=0}^L (1 + |\alpha_i|) \). Using the notation introduced above, we conclude
\[
\text{res}_W^{P_L}(u_{\tilde{d}}) = \sum_{(A, B, C) \in \mathcal{A}_L^L} x^{(L)}_{(A, B, C, E, \tilde{d})}. \tag{2.7.1}
\]

Next, we have an embedding \( W(B_a) \to S_{2n} \). It is defined by \( \sigma \cdot \prod_{i \in I} s_{\tilde{n}_i} \mapsto \sigma \cdot (\sigma + n) \cdot \prod_{i \in I}(\alpha_i + 1, \beta_i + n) \), where \( I \subset [1; n] \), \( \sigma \in S_n \) and \( \sigma + n \in S_{2n} \) is given by
\[
k \mapsto \begin{cases} 
0 & \text{if } k \leq n \\
\sigma(k - n) & \text{if } k > n. 
\end{cases}
\]

Again, we have the modified Stiefel-Whitney invariants \( \tilde{w}_d \in \text{inv}^d(S_{2n}, K^M/2) \) and we may then define \( v_d := \text{res}_W^{P_L}(u_{\tilde{d}}) \in \text{inv}^d(W(B_a), K^M/2) \) for \( 0 \leq d \leq n \).

**Lemma 2.7.11.**

\[
\text{res}_W^{P_L}(v_{\tilde{d}}) = \sum_{(0, 0, C, E) \in \mathcal{A}_L^L} x^{(L)}_{(0, 0, C, E, \tilde{d})}. \tag{2.7.2}
\]

**Proof.** Observe that the map \( W(B_a) \to S_{2n} \) sends
\[
\begin{align*}
s_{\tilde{d}} &\mapsto (2i - 1, 2i)(2i - 1 + n, 2i + n) \\
s_{\tilde{t}} &\mapsto (2i - 1, 2i + n)(2i, 2i - 1 + n) \\
s_{\tilde{v}} &\mapsto (\alpha_i + n, \beta_i + n).
\end{align*}
\]

Now we may use \((1.3.43)\) to conclude that the composition \( P_L \to W(B_a) \to S_{2n} \to O_{2n} \) maps a \( P_L \)-torsor to the quadratic form
\[
\langle (\alpha_1, -\beta_1) \rangle \oplus \cdots \oplus \langle (\alpha_n, -\beta_n) \rangle \oplus (\epsilon_1, \ldots, \epsilon_{2l+1}, \ldots, 2, 2\epsilon_n).
\]

We claim that the total modified Stiefel-Whitney class evaluated at this quadratic form is given by
\[
\prod_{i=1}^L (1 + |\alpha_i|) \prod_{i=2l+1}^n (1 + |\epsilon_i|).
\]

To see this, it is sufficient to check that \( w(2) \otimes \langle (\alpha, \beta) \rangle = 1 + |\alpha| \cdot |\beta| \). First observe that we have \( w(\langle (\alpha, \beta) \rangle) = 1 + |\alpha| \cdot |\beta| \), since \(-1 \in k_0^{+2}\). For the same reason all \( q \in H^1(k, O_n) \) satisfy
\[
w(2) \otimes q = \sum_{d=0}^n w_d(q) + [2] \sum_{0 \leq d < n, d \text{ odd}} w_d(q).
\]

Putting these two facts together proves \( w(2) \otimes \langle (\alpha, \beta) \rangle = 1 + |\alpha| \cdot |\beta| \). Now one only needs to translate this into the new notation to obtain \( \text{res}_W^{P_L}(v_{\tilde{d}}) = \sum_{(0, 0, C, E) \in \mathcal{A}_L^L} x^{(L)}_{(0, 0, C, E, \tilde{d})} \). \( \square \)

Our aim is to show that \( \text{inv}^d(W(B_a), M) \) is a free \( M_r(k_0) \)-module on the products \( [u_{d-r} \cdot v_{\max(0, 2d-r)}]_{r \leq d} \). To prove this, we need to understand the restriction of such products to \( P_L \). If we assume \((2.7.1)\) and \((2.7.2)\), the proof of the following lemma does not use \(-1 \in k_0^{+2}\). We work with this extra generality, so that the lemma may also be used in the \( D_r \)-section, where we do not assume \(-1 \in k_0^{+2}\).

**Lemma 2.7.12.** We have
\[
\text{res}_W^{P_L}(u_{\tilde{d}}) \cdot \text{res}_W^{P_L}(v_{\tilde{e}}) = \sum_{(A, B, C, E) \in \mathcal{A}_L^L} x^{(L)}_{(A, B, C, E, \tilde{d})} \cdot x^{(L)}_{(A, B, C, E, \tilde{d})}.
\]
Proof. First observe that we have \( x^{(l)}_{(A,B,0,\emptyset)} \cdot x^{(l)}_{(0,0,C,E)} = (-1)^{|A \cap C| + |B \cap C|} \cdot x^{(l)}_{(A-\{C\},B,C,E)} \). Using this relation we can write

\[
\left( \sum_{(A,B,0,\emptyset) \in \Lambda^d_L} x^{(l)}_{(A,B,0,\emptyset)} \right) \cdot \left( \sum_{(0,0,C,E) \in \Lambda^d_L} x^{(l)}_{(0,0,C,E)} \right) = \sum_{k \geq 0} \sum_{(A,B,0,\emptyset) \in \Lambda^d_L} \sum_{|A \cap C| + |B \cap C| = k} \cdot (-1)^k x^{(l)}_{(A-\{C\},B,C,E)}.
\]

We want to show that the second sum vanishes. Fix \( k \geq 1 \) and \((A',B',C',E') \in \Lambda^{d+f-k}_L\). Then define

\[
S := \{(A,B) \mid (A,B,0,\emptyset) \in \Lambda^d_L \text{ and } A - C' = A' \text{ and } B - C' = B'\}.
\]

Observe that we have \( S = \{(A' \cup U, B' \cup V) \mid U, V \subset C' \text{ and } U \cap V = \emptyset \text{ and } |U| + |V| = k\}. \) Using this description, we conclude \( |S| = \binom{|C|}{k} \cdot 2^k \). Since \( k \geq 1 \), this is even and we obtain the desired vanishing of the second sum.

Before we can determine the structure of \( Inv'(W(B_n), M) \), it is helpful to know something about the image of the restriction maps \( Inv'(W(B_n), M) \to Inv'(P_L, M) \). Let \( d, k, \ell, L \) be non-negative integers, \( L \leq m \). Then define

\[
\phi^d_{L,k,\ell} := \sum_{(A,B,C,E) \in \Lambda^d_L} x^{(l)}_{(A,B,C,E)} \in Inv^d(P_L, K^M / 2).
\]

Note that this is \( \neq 0 \), iff there exists \((A,B,C,E) \in \Lambda^d_L\) such that \(|C| = k\) and \(|E| = \ell\).

**Lemma 2.7.13.** The image of the restriction map \( Inv'(W(B_n), M) \to Inv'(P_L, M) \) is contained in the free \( M.(k_0)\)-submodule with basis

\[
\left\{ \phi^d_{L,k,\ell} \mid 0 \leq k, \ell, \ 0 \leq d \leq n, \ 2k + \ell \leq d, \ 2(d - k - \ell) \leq 2L \leq n - \ell \right\}.
\]

**Proof.** Let us first show that \( \phi^d_{L,k,\ell} \neq 0 \) iff \( 0 \leq k, \ell, \ 0 \leq d \leq n, \ 2k + \ell \leq d \) and \( 2(d - k - \ell) \leq 2L \leq n - \ell \). Clearly, the conditions \( 2k + \ell \leq d \) and \( 2L \leq n \) are necessary. Furthermore, from the pairwise disjointness of \( A, B, C \), we conclude \(|A| + |B| + |C| \leq L\). This is equivalent to \( d - (2k + \ell) \leq k \leq L \). Clearly \( d - k - \ell \leq L \) is also a necessary condition. Now let us check sufficiency. Suppose, we are given \( L, k, \ell, d \) satisfying the restrictions; then we have \([(1; d - \ell - 2k), \emptyset, [d - \ell - 2k + 1; d - \ell - k], [2L + 1; 2L + \ell)] \in \Lambda^d_L\). Thus \( \phi^d_{L,k,\ell} \neq 0 \). Next we check that the image of the restriction map is indeed contained in the submodule generated by the \( \phi^d_{L,k,\ell} \cdot M.(k_0) \).

Observe that all of the following elements normalize \( P_L \):

(i) \( s_{(2i-1)\rightarrow(2i-1)} \cdot s_{(2i)\rightarrow(2i)} \) for \( i \leq L \)
(ii) \( s_{(2i)\rightarrow(2i-1)} \) for \( i, j \geq 2L + 1 \)
(iii) \( s_{(2i)\rightarrow(2i)} \) for any \( 1 \leq i \leq L \)

Let \( N_L \subset N_{W(B_n)}(P_L) \) be the subgroup generated by these elements. We claim that \( N_L \) permutes the \( x^{(l)}_{(A,B,C,E)} \). Applying \( s_{(2i-1)\rightarrow(2i-1)} \cdot s_{(2i)\rightarrow(2i)} \) for \( i, j \leq L \) to a \( P_L \)-torsor \((\alpha_i, \ldots, \alpha_L, \beta_1, \ldots, \beta_L, \epsilon_{2L+1}, \ldots, \epsilon_n)\) will interchange \( \alpha_i \leftrightarrow \alpha_j \) and \( \beta_i \leftrightarrow \beta_j \). Thus \( x^{(l)}_{(A,B,C,E)} \) is mapped to \( x^{(l)}_{(A',B',C',E')} \) where \( A'/B'/C' \) is obtained from \( A/B/C \) by applying the transposition \((i, j)\) to the respective sets. Similarly, we see that swapping the \( i \)-th and the \( j \)-th coordinate for \( i, j \geq 2L + 1 \) maps \( x^{(l)}_{(A,B,C,E)} \) to \( x^{(l)}_{(A,B,C,E')} \) where \( E' \) is obtained from \( E \) by applying to it the transposition \((i, j)\). Finally changing the 2i-th sign will map \( x^{(l)}_{(A,B,C,E)} \) to \( x^{(l)}_{(A',B',C,E')} \), where \( A' = (A-\{i\}) \cup (B \cap \{i\}) \) and \( B' = (B \setminus \{i\}) \cup (A \cap \{i\}) \) (i.e. if \( i \in A \) we remove it from \( A \) and put it into \( B \) and vice versa).

Iteratively applying these operations to an arbitrary element \((A_0, B_0, C_0, E_0) \in \Lambda^d_L\), we see that its orbit under \( N_L \) is equal to \( \{(A, B, C, E) \in \Lambda^d_L \mid |C| = |C_0|, |E| = |E_0|\} \). Now the lemma follows from 2.6.4. \( \square \)
By Lemma 2.1.15, the injection $\text{Inv}^r(W(B_n), M) \to \prod_{i=0}^{n} \text{Inv}^r(P_L, M)$ has its image inside $\prod_{i=0}^{n} \text{Inv}^r(P_L, M)$ and the previous lemma gives a good description of this object. However, for two reasons it would be foolish to believe that this map is already surjective.

The first one is rather obvious. Up to now, we haven’t paid any attention to the compatibility relations between the various $P_L$. If an element $(z_i)_i$ of the right hand side comes from a $W(B_n)$-invariant, then certainly the restrictions of $z_i$ and $z_i'$ to $P_L \cap P_L'$ must coincide. For the second obstruction, we observe that $W(B_2)$ is the dihedral group of order 8. The Quillen map is not surjective for $W(B_2) = W(4)$ and this obstruction does in fact propagate to $W(B_n)$. Taking these facts into account, we can prove the following refined lemma:

**Lemma 2.7.14.** The image of $\text{Inv}^r(W(B_n), M) \to \prod_{i=0}^{n} \text{Inv}^r(P_L, M)$ lies in the subgroup $Q$ generated by \{\sum_{d \leq n} \phi^d_{L, k, \ell} \}, where $Q := \{ \sum_{d \leq n} \phi^d_{L, k, \ell} : 0 \leq d \leq n, \max(0, 2d - n) \leq r \leq d \} \subset \prod_{i=0}^{n} \text{Inv}^r(P_L, K^0/2)$. In fact $Q$ is a free $M_{(k_0)}$-module with basis $S$.

**Proof.** From the previous lemma, we conclude that the elements of $S$ are all non-zero. But then, it follows that $Q$ is indeed a free $M_{(k_0)}$-module with basis $S$. So it remains to show that the image of the restriction maps lies in $Q$. Let $z \in \text{Inv}^r(W(B_n), M)$ be an arbitrary homogeneous invariant and let $z = (z_i)_i \in \prod_{i=0}^{n} \text{Inv}^r(P_L, M)$ be the image of $z$ under the restriction maps. By the previous lemma, we can write $z = \{ \sum_{d \leq n} \phi^d_{L, k, \ell} m_{i, d, k, \ell} \}$ for some $m_{i, d, k, \ell} \in M_{-d(k_0)}$, where the sums are over all those $d, k, \ell$ such that $\phi^d_{L, k, \ell} \neq 0$.

Our first goal is to show that $m_{i, d, k, \ell}$ is independent of $L$ in the sense that $m_{i, d, k, \ell} = m_{i, d, k, \ell'}$ if $\phi^d_{L, k, \ell} \neq 0$ and $\phi^d_{L', k, \ell} \neq 0$; we will then denote by $m_{i, d, k, \ell}$ the common value. Observe that if we define

$$(A_0, B_0, C_0, E_0) := ([1; d - \ell - 2k], 0, [d - \ell - 2k + 1; d - \ell - k], [n - \ell + 1; n]),$$

then we have $(A_0, B_0, C_0, E_0) \in \Lambda_{L} \cap \Lambda_{L'}$. Since $z$ comes from an invariant of $W(B_n)$, we have

$$\text{res}_{P_L}^{P(A_0, B_0, C_0, E_0)}(z_i) = \text{res}_{P_{L'}}^{P(A_0, B_0, C_0, E_0)}(z_i).$$

If we compare the coefficients of the $x_{(A_0, B_0, C_0, E_0)}$-components of both sides, we obtain $m_{i, d, k, \ell} = m_{i, d, k, \ell'}$.

Now let us have a look at the second obstruction. We want to prove $m_{i, d, k, \ell} = m_{i, d, k, \ell'}$, if $2k + \ell = 2k' + \ell'$ and if there exist $L, L'$ such that $\phi^d_{L_k, k', \ell} \neq 0$ and $\phi^d_{L_k, k', \ell} \neq 0$. It suffices to prove this in the case $k' = k = 1$. Choose any $L$ such that $\phi^d_{L, 1, k', \ell} \neq 0$ (the existence of such an $L$ can be deduced from the existence of $L$, $L'$ satisfying $\phi^d_{L, 1, k', \ell} \neq 0$).

Let $y$ be the restriction of $z$ to $P([1; d - \ell - 2k], 0, [L - k + 1; L], [2L + 3; 2L + \ell]) \times W(B_2)$, where $B_2$ is embedded via the $2L + 1$-th and the $2L + 2$-th coordinates. By the formula 2.1.16 for the structure of the invariants of a cartesian product of two groups, $y$ can be written as

$$y = \sum_{A \in \{1, 2d - 2k \}, C \in \{L - k + 1; L\}, E \in \{2L + 3, 2L + \ell\}} x_{(A, B, C, E)}^{(L)} \cdot y_{(A, C, E)}$$

for certain uniquely determined $y_{(A, C, E)} \in \text{Inv}^{r(A, 0, 2(C - |E|)}(W(B_2), M)$. Furthermore, by the results of section 2.7.3, we have

$$y_{(A, C, E)} = m_{0}^{(A, C, E)} + w_{1} m_{1}^{(A, C, E)} + w_{2} m_{2}^{(A, C, E)}$$

for certain uniquely determined $m_{0}^{(A, C, E)} \in M_{-|A| - 2(C - |E|)(k_0)}$, $m_{1}^{(A, C, E)} \in M_{-|A| - |E| - 1(k_0)}$, $m_{2}^{(A, C, E)} \in M_{-|A| - 2(C - |E|) - 2(k_0)}$. Restricting $y$ further to $P([1; d - \ell - 2k], 0, [L - k + 1; L], [2L + 1; 2L + \ell])$ and considering the $x_{([1, d - 2k - \ell], [L - k + 1; L], [2L + 1; 2L + \ell] \cdot \text{-component}}$, we obtain from 2.7.4 that

$$m_{d, k, \ell} = m_{2}^{(A, C, E)}$$

On the other hand, restricting $y$ to $P([1; d - \ell - 2k], 0, [L - k + 1; L + 1], [2L + 3; 2L + \ell])$ and considering the $x_{([1, d - 2k - \ell], [L - k + 1; L + 1], [2L + 3; 2L + \ell] \cdot \text{-component}}$, we obtain from 2.7.9 that

$$m_{d, k, \ell} = m_{2}^{(A, C, E)}$$

This proves the lemma. □

From 2.7.12 we thus deduce

\[ 53 \]
Corollary 2.7.15. \( \text{Inv}'(W(B_n), M) \) is a free \( M_*(k_0) \)-module with basis \( \{ u_{d-r} v_r \mid 0 \leq d \leq n, \max(0, 2d - n) \leq r \leq d \} \).

Since the \( v_d, u_d \) are both induced by modified Stiefel-Whitney classes of symmetric groups, we also know the multiplicative structure:

Lemma 2.7.16. Write \( r = \sum_{i \in \mathbb{R}} 2^i, s = \sum_{i \in \mathbb{R}} 2^i \) for some \( R, S \subseteq \{ 0, 1, 2, \ldots \} \) and put \( t := \sum_{i \in R \cap S} 2^i \). Then we have \( u_r \cdot u_s = u_{r+t} \cdot [-1]^t \) and \( v_r \cdot v_s = v_{r+t} \cdot [-1]^t \).

2.7.7 \( F_4 \)

We assume that \( -1 \in k_0^{\times 2} \) and \( \text{char}(k_0) \nmid |F_4| = 2^2 \cdot 3^2 \), i.e. \( \text{char}(k_0) \neq 2, 3 \). \( M \) is required to be a \( \mathbb{Z} \)-graded \( A^1 \)-module with \( kM/2\)-module structure.

The root system \( F_4 \) is the disjoint union \( \Delta_1 \cup \Delta_2 \cup \Delta_3 \subset \mathbb{R}^4 \), where

\[
\Delta_1 := \{ \pm e_i \mid 1 \leq i \leq 4 \}, \quad \Delta_2 := \{ 1/2(\pm e_1 \pm e_2 \pm e_3 \pm e_4) \}
\]

are the short roots and

\[
\Delta_3 := \{ \pm e_i \pm e_j \mid 1 \leq i < j \leq 4 \}
\]

are the long roots.

We have \( \Omega(W(F_4)) = \{ [P_0], [P_1], [P_2] \} \), where

(i) \( P_0 := P(e_1, e_2, e_3, e_4) \)
(ii) \( P_1 := P(a_1, b_1, c_3, e_4) \)
(iii) \( P_2 := P(a_1, b_1, a_2, b_2) \)

Indeed, the set of long roots of \( F_4 \) is the root system \( D_4 \), which up to conjugacy has a unique maximal set of pairwise orthogonal vectors, namely \( a_1, b_1, a_2, b_2 \). On the other hand, if we have a maximal set of pairwise orthogonal roots containing a short root, we can wlog (by \( \Delta_2 \)) assume this root to be \( e_4 \). But \( \{ e_4 \} \cap F_4 = B_3 \). We have determined before that up to conjugacy \( B_3 \) contains two maximal sets of pairwise orthogonal roots; namely \( \{ e_1, e_2, e_3 \} \) and \( \{ a_1, b_1, e_3 \} \).

Furthermore, observe that we have inclusions \( P_1 \subset W(B_4) \subset W(F_4) \). Thus the restriction map \( \text{Inv}'(W(F_4), M) \to \text{Inv}'(W(B_4), M) \) is injective. Recall that \( \text{Inv}'(W(B_4), M) \) is a free \( M_*(k_0) \)-module with the following basis:

(i) \( 1 \)
(ii) \( u_1, v_1 \)
(iii) \( u_2, v_1 u_1, v_2 \)
(iv) \( v_4 \)

Before we construct some invariants, let us first derive another restriction in degree 2. Note that \( \text{res}^2_{W(F_4)}(v_1) = \text{res}^2_{W(B_4)}(v_3) = 0 \), so that the image of the restriction \( \text{Inv}'(W(F_4), M) \to \text{Inv}'(P_2, M) \) is contained in the free \( M_*(k_0) \)-submodule \( S \subset \text{Inv}'(P_2, M) \) with basis \( \{ 1, y_1, y_2, y'_2, y_3, y_4 \} \), where \( y_1 = \text{res}^2_{W(B_4)}(u_1) \), \( y_2 = \text{res}^2_{W(B_4)}(u_2) \), \( y'_2 = \text{res}^2_{W(B_4)}(v_2) \), \( y_3 = \text{res}^2_{W(B_4)}(v_1 u_1) \) and \( y_4 = \text{res}^2_{W(B_4)}(v_4) \).

Now let \( a \in \text{Inv}'(P_2, M) \) be an invariant which comes from \( \text{Inv}'(W(F_4), M) \). Then we can find unique \( m_d \in M_{-d}(k_0), m_2, m'_2 \in M_{-2}(k_0) \) such that

\[
a = \sum_{0 \leq d \leq 4} \left( \sum_{(A,B,C) \in \Lambda^3} x_{(A,B,C)} m_d \right) + \left( \sum_{(A,B) \in \Lambda^2} x_{(A,B)} m_2 \right) + \left( \sum_{(B,B,C) \in \Lambda^2} x_{(B,B,C)} m'_2 \right).
\]

Note that \( s_{1,2,3,4} \) lies in the normalizer of \( P_2 \). This element leaves \( a_1, a_2 \) fixed, but maps \( b_1 \) to \( -b_2 \) and vice versa. Since \( a \) comes from \( \text{Inv}'(W(F_4), M) \), it is invariant under the action of \( s_{1,2,3,4} \). Hence we also have

\[
a = \sum_{0 \leq d \leq 4} \left( \sum_{(A,B,C) \in \Lambda^3} x_{(A,B,C)} m_d \right) + \left( x_{(a_1,2,2)} + x_{(b_1,b_2)} + x_{(a_1,1,4)} + x_{(a_2,b_2)} \right) m_2 + \left( x_{(a_1,1,2)} + x_{(a_2,2,1)} \right) m'_2.
\]

Comparing coefficients yields \( m_2 = m'_2 \).

Thus the image of the restriction map \( \text{Inv}'(W(F_4), M) \to \text{Inv}'(P_2, M) \) is actually contained in the free \( M_*(k_0) \)-submodule with basis \( \{ 1, y_1, y_2 + y'_2, y_3, y_4 \} \). But from this, we conclude that the image of the restriction map \( \text{Inv}'(W(F_4), M) \to \text{Inv}'(W(B_4), M) \) is contained in the free \( M_*(k_0) \)-module with basis

54
(0) 1

(i) \( u_1, v_1 \)

(ii) \( u_2 + v_2, v_1 u_1 \)

(iii) \( v_2 u_1, v_3 \)

(iv) \( v_4 \)

Now, we need to construct \( F_4 \)-invariants which restrict to these elements. First observe that we have \( D_3 \subset F_4 \) and that \( W(F_4) \) stabilizes \( D_3 \). Thus any \( g \in W(F_4) \) maps the simple system \( S = \{ e_1 - e_2, e_2 - e_3, e_3 - e_4, e_4 \} \) to another simple system \( S' \subset D_3 \). Since all simple systems are conjugate, we conclude from \( 2.4.4 \) that there exists a unique \( h \in W(D_4) \) mapping \( S' \) to \( S \). This procedure induces a permutation of the 3 outer vertices \( \{ e_1 - e_2, e_2 - e_4, e_3 + e_4 \} \) of the Coxeter graph and we obtain a map \( \psi : W(F_4) \rightarrow S_3 \) (which is easily seen to be a group homomorphism).

Thus we can define \( \gamma = \psi(\omega_i) \), where \( \omega_i \in \text{Inv}^*(S_3, K^M/2) \) is the first (modified) Stiefel-Whitney class. Again, if \( 2 \) is not a square in \( k_0 \), then these invariants will not have a nice form, when restricted to the \( P_1 \); therefore we will change them a little and define invariants \( \tilde{\omega_i} \). Let \( (\alpha_1, \ldots, \alpha_L, \beta_1, \ldots, \beta_L, \varepsilon_{2L+1}, \ldots, \varepsilon_4) \) be a \( P_1 \)-torse. Its image in \( H^1(k, O_4) \) induced by the map \( P_1 \subset W(F_4) \subset O_4 \) may be computed by using \( 1.3.39 \). It is given by \( (2\alpha_1, 2\beta_1, \ldots, 2\alpha_L, 2\beta_L, \varepsilon_{2L+1}, \ldots, \varepsilon_4) \). We would like to have

\[
\text{res}_{W(F_4)}^{P_1}(\omega_d) = \sum_{(A,B,C)\in\Lambda^1_x} x_{(A,B,C),d}^{(l)}
\]

To check the computations below, observe that we have \( |x| |x| = 0 \), since \( -1 \in k_0^{22} \) by assumption. It is easy to see that the restriction of \( \omega_1 \) to \( P_1 \) is already given by \( \sum_{(A,B,C)\in\Lambda^1_x} x_{(A,B,C)}^{(l)} \). Thus, we just put \( \omega_1 := \omega_1 \). For \( d = 2 \), we have

\[
\text{res}_{W(F_4)}^{P_1}(\omega_2) = \sum_{(A,B,C)\in\Lambda^1_x} x_{(A,B,C),d}^{(l)} + \sum_{(A,B,B)\in\Lambda^1_x} [2] \cdot x_{(A,B,B),1}^{(l)}
\]

Thus, \( \omega_2 := \omega_2 - [2] \cdot (\omega_1 - v_1) \) will have the desired property. The restriction of \( \omega_3 \) to \( P_1 \) is

\[
\text{res}_{W(F_4)}^{P_1}(\omega_3) = \sum_{(A,B,C)\in\Lambda^1_x} x_{(A,B,C),d}^{(l)} + \sum_{(A,B,B)\in\Lambda^1_x} [2] \cdot x_{(A,B,B),1}^{(l)}
\]

Thus, we set \( \omega_3 := \omega_3 - [2] \cdot (\omega_1 - v_1) \cdot v_1 \). Finally, the restriction of \( \omega_4 \) to \( P_1 \) is

\[
\text{res}_{W(F_4)}^{P_1}(\omega_4) = \sum_{(A,B,C)\in\Lambda^1_x} x_{(A,B,C),d}^{(l)} + \sum_{(A,B,B)\in\Lambda^1_x} [2] \cdot x_{(A,B,B),1}^{(l)}
\]

Thus, we set \( \omega_4 := \omega_4 - [2] \omega_2 (\omega_1 - v_1) \). Furthermore define \( u_1 := \omega_1 - v_1 \in \text{Inv}^*(W(F_4), K^M/2) \).

Now let us see, what we obtain when restricting the invariants just constructed to \( W(B_2) \). We claim that \( v_1, u_1 \in \text{Inv}^*(W(B_4), K^M/2) \) restrict to \( v_1, u_1 \in \text{Inv}^*(W(B_4), K^M/2) \), that \( u_1 v_1, (\bar{\omega}_2 - u_1 v_1) \in \text{Inv}^2(W(F_4), K^M/2) \) restrict to \( v_1 u_1, (\bar{\omega}_2 - \bar{\omega}_2) \in \text{Inv}^2(W(F_4), K^M/2) \) restrict to \( v_1 u_1, v_3 \in \text{Inv}^3(W(B_4), K^M/2) \). Finally \( \bar{\omega}_4 \in \text{Inv}^4(W(F_4), K^M/2) \) restricts to \( v_4 \in \text{Inv}^4(W(B_4), K^M/2) \). To prove all these claims, we only need to consider the restrictions to \( \text{Inv}^*(P_1, K^M/2) \) and there the identities are clear by construction. Thus \( \text{Inv}^*(W(F_4), M) \) is a free \( M,(k_0) \)-module with basis \( \{ 1, \omega_1, v_1, v_2, v_1 w_1, w_3, v_1 w_2, w_4 \} \).

By construction of the \( \bar{\omega}_i \) we also have the following:

**Proposition 2.7.17.** \( \text{Inv}^*(W(F_4), M) \) is a free \( M,(k_0) \)-module with basis \( \{ 1, w_1, v_1, w_2, v_1 w_1, w_3, v_1 w_2, w_4 \} \).
2.7.8 $D_n$

In this section, we assume that $\text{char}(k_0) \nmid |D_n|$. Furthermore, $M_n$ is assumed to be a $\mathbb{Z}$-graded $A^1$-module with $K^M/2$-module structure. The root system $D_n$ is the subset of $\mathbb{R}^n$ consisting of the elements

$$D_n = \{ \pm e_i \pm e_j | 1 \leq i < j \leq n \}.$$ 

Let $m := [n/2], a_i := e_{2i-1} - e_{2i}, b_i := e_{2i-1} + e_{2i}$. We know that this root system defines an orthogonal reflection group over all $k_0$ such that $\text{char}(k_0) \neq 2$. It follows from \[2.4.3\] that $|\Omega(W(D_n))| = 1$ and it is easy to check that $\rho := \rho(a_1, b_1, \ldots, a_m, b_m)$ is in fact a maximal elementary abelian 2-group generated by reflections. In the following, we will always assume $n \geq 2$ (if $n = 1$, then $W(D_1) \cong \mathbb{Z}/2$ and we already know everything about it). From the root system, it is clear that $W(D_n)$ is a subgroup of $W(B_n)$; more precisely, we have $W(D_n) = \{ u \cdot \prod s_a \in S_n \mid (\mathbb{Z}/2)^n \cong W(B_n) \mid | | \text{even} \}$.

Similarly to the $B_n$-section, we define

$$A^d := \{(A, B, C) \in [1, m]^3 \mid A, B, C \text{ are pairwise disjoint, } |A| + |B| + 2|C| = d \}$$

and

$$x_{(A,B,C)} : H^1(k, P) \to K^M_d(k)/2$$

$$(a_1, b_1, \ldots, a_m, b_m) \mapsto \prod_{(a \in A)} x_a \cdot \prod_{(b \in B)} x_b \cdot \prod_{(c \in C)} x_c.$$ 

The invariants constructed in the $B_n$-section are useful in the current situation, too. However, we quickly recall their construction, since we do not want to assume $-1 \in k_0^{\times 2}$ (as we did in the $B_n$-case). First observe that we have a morphism $p : W(D_n) \subset W(B_n) \to S_n$. Now define $u_{\alpha} := \rho^*(\bar{\alpha}) \in \text{Inv}^{2d}(W(D_n), K^M/2)$. As before, we have $res_{W(B_n)}^{p^*(u_{\alpha})}(x_{(A,B,C)}) = \sum x_{(A,B,C)}$.

Furthermore - just as in the $B_n$-case - we have an embedding $W(D_n) \subset W(B_n) \subset S_{2n}$. Starting with a $W(D_n)$-torsor $x \in H^1(k, W(D_n))$, we may consider its image $q_x \in H^1(k, O_{2n})$ induced by the map $W(D_n) \to S_{2n} \to O_{2n}$. Observe that $W(D_n) \to S_{2n}$ sends

$$s_{\alpha} \mapsto (2i-1, 2i)(2i-1, 2i+n)$$

$$s_{\beta} \mapsto (2i-1, 2i+n)(2i, 2i-1+n).$$

Thus, if we start with a $P$-torsor $(a_1, \ldots, a_m, b_1, \ldots, b_m)$, then we may apply \[1.3.43\] to see that under the composition $P \to W(D_n) \to S_{2n} \to O_{2n}$ this torsor is mapped to $\langle -\alpha_1, -\beta_1 \rangle \oplus \cdots \oplus \langle -\alpha_m, -\beta_m \rangle(\oplus(1,1))$. Here the expression in parentheses only appears, if $n$ is odd.

We would like to have an element $\nu \in \text{Inv}^{2d}(W(D_n), K^M/2)$ such that $res_{W(D_n)}^{P}(\nu)$ is given by

$$H^1(k, P) \to K^M_d(k)/2$$

$$(a_1, \ldots, a_m, b_1, \ldots, b_m) \mapsto (1 + |a_1|\langle b_1 \rangle) \cdots (1 + |a_m|\langle b_m \rangle).$$

We will construct the homogeneous components $\nu_i$ of $\nu$ by induction on $d$. Clearly, we may take $\nu_0 = 1$ constant. Now suppose $\nu_0, \ldots, \nu_{d-1}$ have already been constructed. If $d$ is odd, we may just take $\nu_d = 0$; so suppose $d = 2d'$ is even. Let us first compute the value of the total Stiefel-Whitney class $\nu \in \text{Inv}^{2d}(O_{2n}, K^M/2)$ at a 2-fold Pfister form:

$$w(\langle -\alpha, -\beta \rangle) = (1 + |\alpha|)(1 + |\beta|)(1 + |\alpha| + |\beta|)$$

$$= 1 + |\alpha| + |\beta| + |\alpha| \cdot |\beta|$$

$$= 1 + |\alpha| + |\beta|.$$ 

Put $\nu' := res_{O_{2n}}^{W(D_n)}(\nu)$ and let $y = (a_1, \ldots, a_m, b_1, \ldots, b_m)$ be an arbitrary $P$-torsor. Then we compute

$$res_{W(D_n)}^{P}(\nu')(y) = w(\langle -\alpha_1, -\beta_1 \rangle \oplus \cdots \oplus \langle -\alpha_m, -\beta_m \rangle)(\oplus(1,1))$$

$$= \prod_{i=1}^{m} (1 + |\alpha_i| + |\beta_i|) + |\alpha_i| |\beta_i|).$$

Thus the degree $d$ part of $res_{W(D_n)}^{P}(\nu')$ is $\sum_{j=0}^{d} \sum_{(A,B,C) \in A^d} x_{(A,B,C)}$ for all $j$. Observe that \[2.7.12\] holds also in our situation (we may copy the proof, as we didn’t use $-1 \in k_0^{\times 2}$). Thus we have

$$\sum_{(A,B,C) \in A^d} x_{(A,B,C)} = \left( \sum_{(A,B) \in A^{d'}} x_{(A,B)} \right) \cdot \left( \sum_{(B,C) \in A^{d-2}} x_{(B,C)} \right).$$

56
Taking $v_d := v_d' - \sum_{j=1}^{p} |u_j|u_{d-2j}$ completes the induction step.

Furthermore, note that we have

$$v_d = \sum_{(\emptyset, C) \in A'} x_{(\emptyset, C)}$$

and (by 2.7.12)

$$\text{res}_{W(D_n)}^P(u_d) \cdot \text{res}_{W(D_n)}^P(v_2) = \sum_{(A, B, C) \in A''} x_{(A, B, C)}.$$  

Now suppose that $n = 2m$ is even. In this case, we need to construct one further invariant. Since $W(D_n) \cong S_n \ltimes (\mathbb{Z}/2)^{n-1}$, we have an embedding $S_n \subset W(D_n)$ such that $|W(D_n)/S_n| = 2^{n-1}$. More precisely, $|W(D_n)/S_n|$ consists of the cosets $g_1S_n$, where $g_1 := \prod_{i \in I} g_i$ and where $I \subset \{1; n\}$ has even cardinality. The left action of $W(D_n)$ on these cosets induces a map $W(D_n) \to S_{2n-1} \to O_{2^{n-1}}$. Thus for any $k \in \mathbb{F}_k$ and any $y \in H^1(k, W(D_n))$, we obtain a quadratic form $\Delta_y \in H^1(k, O_{2^{n-1}})$. This gives us an invariant $\omega \in \text{Inv}(W(D_n), W)$. In fact, we claim that $\omega \in \text{Inv}(W(D_n), L^m)$ (here $l(k) \subset W(k)$ is the fundamental ideal).

To prove this, we start by showing that $\text{res}_{W(D_n)}^P(\omega) \in \text{Inv}(P, I^m)$. It is convenient to have a good understanding of the map $W(D_n) \to S_{2n-1}$ on the subgroup $P$:

Lemma 2.7.18. Let $L = \{[2i - 1, 2i] \mid 1 \leq i \leq m\}$ and define

$$f : 2^{1\ldots n-1} \to 2^L$$

$$l \mapsto ([2i - 1, 2i] \mid \text{either } 2i - 1 \in I \text{ or } 2i \in I, \text{ but not both}).$$

Then we have the following:

(i) The action of $P$ on $W(D_n)/S_n$ has the $2^{m-1}$ orbits $O_{f} := \{g_1 \cdot S_n \mid f(l) = J\}$, $J \subset L$, $|J|$ even.

(ii) Let $O_f$ be an arbitrary orbit from (i). Put $A_f := \{i \in [1; m] \mid [2i - 1, 2i] \in J\}$ and $B_f := \{i \in [1; m] \mid [2i - 1, 2i] \notin J\}$. Then $P([a_i]_{i \in A_f} \cup [b_i]_{i \in B_f})$ acts trivially on $O_f$ and the action of $P_f := P([a_i]_{i \in A_f} \cup [b_i]_{i \in B_f})$ on $O_f$ is simply transitive.

Proof. (i) Let $l \subset [1; n]$. If $[2i - 1, 2i] \notin f(l)$, then $s_{a_i}g_1 = g_1s_{b_i}$ and $s_{b_i}g_1 = g_1s_{a_i}$, where $\Delta$ is the symmetric difference operation. On the other hand, if $[2i - 1, 2i] \in f(l)$, then $s_{a_i}g_1 = g_1s_{a_i}$ and $s_{b_i}g_1 = g_1s_{b_i}$.

(ii) Clearly, it follows from the previous lines that $P([a_i]_{i \in A_f} \cup [b_i]_{i \in B_f})$ acts trivially on $O_f$. For the second assertion, it suffices to show that the action of $P([a_i]_{i \in A_f} \cup [b_i]_{i \in B_f})$ on $O_f$ is free (indeed, we have $P([a_i]_{i \in A_f} \cup [b_i]_{i \in B_f}) \cong 2^{m} = |O_f|$). So suppose, we have $I \subset [1; n]$, $M \subset A_f$ and $N \subset B_f$ such that $f(l) = J$ and $g := \prod_{i \in M} s_{a_i} \cdot \prod_{j \in N} s_{b_j}$ fixes $g_1S_n$. But using the relations considered above, we have $g : g_1S_n = g_1S_n$, where $l' = \Delta(\Delta^{(2i - 1; 2i)}(g_1S_n))$ denotes the iterated symmetric difference indexed over all elements of $M$ and $N$. Now observe $l' = I$ $\iff$ $M = N = \emptyset$, which shows that the action is free.

Using this lemma, we can now conclude the following: Let $y = (\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_m) \in H^1(k, P)$ be arbitrary and let $q_y \in H^1(k, O_{2^{n-1}})$ be the quadratic form induced by the composition $P \to W(D_n) \to S_{2n-1} \to O_{2^{n-1}}$. By 1.3.42 the decomposition of the action of $P$ into orbits of $O_f$ induces a decomposition of $q_y$ as $q_y \cong \oplus_{f \in F} q_{f}$. More precisely, the action of $P_f$ on $O_f$ induces a map $P_f \to S_{2n}$ and $q_y$ is defined to be the image of $y \in H^1(k, P)$ under the composition $P \to S_{2n} \to O_{2^{n-1}}$. By the lemma, this composition factors through the projection $P \to P_f$. Using 1.3.45 it’s remark and the above lemma, we can then conclude that

$$q_y \cong (2^m) \otimes \bigotimes_{i \in A_f} (\langle -\alpha_i \rangle) \otimes \bigotimes_{j \in B_f} (\langle -\beta_j \rangle).$$

In particular the image of $q_y \otimes g_{\mathbb{F}_k}$ in $W(k)$ lies in $I^m(k)$. This proves $\text{res}_{W(D_n)}^P(\omega) \in \text{Inv}(P, I^m)$.

Now we need to pass from the subgroup $P$ to $W(D_n)$. Observe that there is a map from $W$ to $(I^m/I^{m+1})_0 = W/I$. Thus $\omega$ induces an invariant $\overline{\omega} \in \text{Inv}^0(W(D_n), I^m/I^{m+1})$. Since the image of $\text{res}_{W(D_n)}^P(\omega)$ lies in $I^m \subset I$, we conclude that $\text{res}_{W(D_n)}(\omega) = 0$. But (up to conjugation), $P$ is the unique maximal elementary abelian $2$-subgroup of $W(D_n)$ generated by reflections. From 2.3.13 we then conclude that $\overline{\omega} = 0 \in \text{Inv}^0(W(D_n), I^m/I^{m+1})$. But this is another way of saying that $\omega \in \text{Inv}(W(D_n), I)$.

Iterating this procedure $m$ times, we obtain $\omega \in \text{Inv}(W(D_n), I^m)$. As we recalled in 2.3.14 there exists an invariant $e_m : I^m(k) \to K_m^M(k)/2$ satisfying

$$e_m(\langle \alpha_1 \rangle) \otimes \ldots \otimes (\langle \alpha_m \rangle) = \prod_{i=1}^{m} \langle a_i \rangle.$$
Then \( y \mapsto e_n((2^n) \otimes \omega(y)) \) defines an element of \( \text{Inv}^m(W(D_n), K\mathbb{M}/2) \); let us denote this element by \( \widetilde{e}_m \) for the moment. Our computations show that its restriction to \( P \) is given by

\[
\text{res}^P_{W(D_n)}(\widetilde{e}_m) = \sum_{(A,B,B) \in \Lambda^m, |A| \text{ even}} x_{(A,B,B)} + \sum_{(A,B,B) \in \Lambda^{m+1}} x_{(A,B,B)}.
\]

Thus, if we put \( e_m := \widetilde{e}_m - (-1)^m e_{m-1} \), we have \( \text{res}^P_{W(D_n)}(e_m) = \sum_{(A,B,B) \in \Lambda^m} x_{(A,B,B)} \).

This was the hardest part of the section. Now we want to show that all other \( D_n \)-invariants can be obtained from the ones constructed above. Let us first introduce certain notations. For \( 0 \leq d \leq n \) and \( 0 \leq i \leq \left\lfloor \frac{d}{2} \right\rfloor \) put

\[
\phi^d_i := \sum_{(A,B,C) \in \Lambda^d, |C| = i} x_{(A,B,C)} \in \text{Inv}^d(P, K\mathbb{M}/2)
\]

and

\[
\psi_1 := \sum_{(A,B,B) \in \Lambda^d, |A| \text{ even}} x_{(A,B,B)}, \quad \psi_2 := \sum_{(A,B,B) \in \Lambda^d, |A| \text{ odd}} x_{(A,B,B)}.
\]

**Lemma 2.7.19.** The image of the restriction map \( \text{Inv}_k^\circ(W(D_n), M) \to \text{Inv}_k^\circ(P, M) \) is contained in the free \( M.(k_0) \)-module with basis

\[
S = \{\phi^d_i \mid 0 \leq d \leq n, \text{ max}(0,d-m) \leq i \leq \left\lfloor \frac{d}{2} \right\rfloor \cup R, \quad \text{where } R = \emptyset, \text{ if } n \text{ is odd and } R = \{\psi_1\}, \text{ if } n \text{ is even.}
\]

**Proof.** As in the \( B_{\varepsilon r} \)-section, it is easy to check that all the elements of \( S \) are non-zero. Now observe that the following elements normalize \( P \):

(i) \( S_{(2(r-1)-c(2(r-1))} \cdot S_{(2(r-1)-c(2r))} \)

(ii) \( S_{(2(r-1))} \cdot S_{(3(r-1))} \)

Let us denote by \( N_1, N_2 \subset N(P) \) the subgroups generated by the first, respectively second kind of elements and let us denote by \( N \) the subgroup generated by \( N_1 \) and \( N_2 \). At the torus level, conjugation by the first kind of elements will swap \( \alpha_i \leftrightarrow \alpha_j \) and \( \beta_i \leftrightarrow \beta_j \). Thus, if \( (A, B, C) \in \Lambda^d \) is an arbitrary element, then \( x_{(A,B,C)} \) maps to \( x_{(A',B',C')}, \) where \( A' = (i, j) A, B' = (i, j) B \) and \( C' = (i, j) C \). On the other hand, conjugation by the second kind of elements swaps \( \alpha_i \leftrightarrow \beta_i \) and \( \alpha_j \leftrightarrow \beta_j \). Thus, it maps \( x_{(A,B,C)} \) to \( x_{(A',B',C')} \), where \( A' = (A - (i, j)) \cup (B \cap (i, j)) \) and \( B' = (B - (i, j)) \cup (A \cap (i, j)) \) (i.e. if \( i \in A \), we remove it from \( A \) and put it into \( B \) and vice versa; then we do the same for \( j \)). Thus \( N \) acts on \( \text{Inv}^\circ(P, K\mathbb{M}/2) \) by permuting the \( x_{(A,B,C)} \) and hence we can apply (2.6.3). The next step is to determine the orbits of this action.

So let \( (A_0, B_0, C_0) \in \Lambda^d \) be arbitrary and let us determine the orbit of \( x_{(A_0, B_0, C_0)} \) under \( N \). First suppose that \( n \) is odd or that \( C_0 \neq \emptyset \) or that \( (n = 2m \text{ is even and } d < m) \). Then we claim that the orbit of \( x_{(A_0, B_0, C_0)} \) under \( N_2 \) is given by \( \{x_{(A, B, C)} \mid (A, B, C) \in \Lambda^d, A \cup B = A_0 \cup B_0 \} \). It suffices to show that for any \( n \in A_0 \), there exists an element of \( N_2 \) mapping \( x_{(A_0, B_0, C_0)} \) to \( x_{(A_0 - \{n\}, B_0, \{\{\} \})} \) (as soon as this is proven, one observes that the symmetric statement with \( B \) in \( B_0 \) also holds; iterating these operations, we indeed get the claimed orbit). If \( n \) is odd, then \( S_{(2(r-1))} \cdot S_{(n-1)} \) maps \( x_{(A_0, B_0, C_0)} \) to \( x_{(A_0 - \{n\}, B_0, \{\} \}) \). If \( C_0 \neq \emptyset \), then \( S_{(2(r-1))} \cdot S_{(n-1)} \) maps \( x_{(A_0, B_0, C_0)} \) to \( x_{(A_0 - \{n\}, B_0, \{\} \}) \). Finally, if \( n = 2m \) is even and \( d < m \), then there exists \( i \in \{1, m\} \) such that \( i \not\in A_0 \cup B_0 \cup C_0 \). The element \( S_{(2(r-1))} \cdot S_{(n-1)} \) does the trick. Thus the orbit of \( x_{(A_0, B_0, C_0)} \) under \( N_2 \) is indeed \( \{x_{(A, B, C)} \mid (A, B, C) \in \Lambda^d, A \cup B = A_0 \cup B_0 \} \). Furthermore, it is easy to check that for any \( (A_1, B_1, C_1) \in \Lambda^d \) the orbit of \( x_{(A_0, B_0, C_0)} \) under \( N_1 \) is given by \( \{x_{(A, B, C)} \mid (A, B, C) \in \Lambda^d, |A| = |A| \}, \{B|B|, \{|C| \} \} \). Putting these results together, we see that in this case, the orbit of \( x_{(A_0, B_0, C_0)} \) under \( N \) is given by \( \{x_{(A, B, C)} \mid (A, B, C) \in \Lambda^d, |A| = |A| \} \).

It remains to treat the case, where \( C_0 = \emptyset, n = 2m \) is even and \( d = m \). Then one can check that the orbit of \( x_{(A_0, B_0, C_0)} \) under \( N_2 \) is \( \{x_{(A, B, 0)} \mid (A, B, 0) \in \Lambda^d, A \cup B = A_0 \cup B_0, |B| = |B| \} \) is even. Then using that for any \( (A_1, B_1, C_1) \in \Lambda^d \) the orbit of \( x_{(A_0, B_0, C_0)} \) under \( N_1 \) is given by \( \{x_{(A, B, C)} \mid (A, B, C) \in \Lambda^d, |A| = |A| \}, \{B|B|, \{C|C| \} \} \), we see that the orbit of \( x_{(A_0, B_0, C_0)} \) under \( N \) is \( \{x_{(A, B, 0)} \mid (A, B, 0) \in \Lambda^d, |B| = |B| \} \) is even.

Applying (2.6.3) now proves the lemma (after observing \( \psi_1 + \psi_2 = \phi^d_0 \)). \( \square \)

It follows from our computations that we have \( \text{res}^P_{W(D_n)}(e_m) = \psi_1 \) and \( u_{d-2} \cdot \psi_2 = \phi^d_1 \) (using (2.6.4)). Thus we have

**Corollary 2.7.20.** \( \text{Inv}_k^\circ(W(D_n), M) \) is a free \( M.(k_0) \)-module with basis

\[
\{u_{d-2} \cdot \psi_2 \mid 0 \leq d \leq n, \text{ max}(0,d-m) \leq i \leq \left\lfloor \frac{d}{2} \right\rfloor \cup R, \quad \text{where } R = \emptyset, \text{ if } n \text{ is odd and } R = \{e_m\}, \text{ if } n \text{ is even.}
\]

58
Now let us determine the product structure. The $u_d$ are induced by the modified Stiefel-Whitney classes. Thus we have

Lemma 2.7.21. Write $r = \sum_{i \in R} 2^i, s = \sum_{i \in S} 2^i$ for some $R, S \subset \{0, 1, 2, \ldots\}$ and put $t := \sum_{i \in R \cup S} 2^i$. Then we have

$$u_r \cdot u_s = u_{r+s-t} \cdot [-1]^t.$$ 

For products of the form $v_{2r} \cdot v_{2s}$ we can give a very similar formula. Indeed, for $y = (\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_m) \in H^1(k, P)$ the value of $v_{2d} \cdot v_{2s}$ at $y$ is the degree $2d$-part of $(1 + [\alpha_1][\beta_1]) \cdots (1 + [\alpha_m][\beta_m])$. Thus for $r, s, t$ as above we have

$$\text{res}^P_{W(D_{2r})}(v_{2r}) \cdot \text{res}^P_{W(D_{2s})}(v_{2s}) = \text{res}^P_{W(D_{2t})}(v_{2r+s-2t} \cdot [-1]^{2t}).$$ 

Since the restriction to $P$ is an injection, we obtain

Lemma 2.7.22. Write $r = \sum_{i \in R} 2^i, s = \sum_{i \in S} 2^i$ for some $R, S \subset \{0, 1, 2, \ldots\}$ and put $t := \sum_{i \in R \cup S} 2^i$. Then we have

$$v_{2r} \cdot v_{2s} = v_{2r+s-2t} \cdot [-1]^{2t}.$$ 

It remains to understand the products involving the invariant $e_m$. As $e_m$ is homogeneous of degree $m$, we have $e_m^2 = [-1]^m e_m$.

Lemma 2.7.23. We have

$$e_m \cdot v_{2d} = \begin{cases} e_m & \text{if } d = 0 \\ [-1] u_{m-1} v_2 & \text{if } d = 1 \\ 0 & \text{if } d > 1 \end{cases}$$

Proof. The claim is clear for $d = 0$, so we only need to consider the cases, where $d > 0$. It is sufficient to prove this relation after restricting to $P$. We have $x_{(A, B, 0)} \cdot x_{(0, 0, C)} = [-1]^{|A \cap C| + |B \cap C|} \cdot x_{(A, B, C)}$. This implies

$$\sum_{(A, B, 0) \in \Lambda^m} x_{(A, B, 0), (A \cap C)} \cdot \sum_{(0, 0, C) \in \Lambda^d} x_{(0, 0, C)} = \sum_{(A, B, C) \in \Lambda^d} [-1]^d x_{(A, B, C)}.$$ 

Fix $(A', B', C') \in \Lambda^{d+m}$ such that $|C'| = d$. Then define

$$S := \{(A, B) \mid (A, B, 0) \in \Lambda^m, A - C' = A', B - C' = B', |A| \text{ even}\}.$$ 

We have $S = \{(A', \cup U, B' \cup V) \mid U, V \subset C', U \cap V = 0, U \cup V = C', |A'| + |U| \text{ even}\}$. Using this description, we conclude $|S| = 2^{d-1}$. For $d \geq 2$, this is even and thus the corresponding sum vanishes. For $d = 1$, this sum may be simplified to

$$\sum_{(A, B) \in \Lambda^{d+1}} [-1] x_{(A, B, C)} = [-1] \left( \sum_{(A, B, 0) \in \Lambda^{d-1}} x_{(A, B, 0)} \right) \cdot \left( \sum_{(0, 0, C) \in \Lambda^1} x_{(0, 0, C)} \right)$$

□

Lemma 2.7.24. Let $d > 0$. Then we have

$$e_m \cdot u_d = \binom{m}{d} [-1]^d e_m + \binom{m-1}{d-1} [-1]^{d-1} u_{m-1} v_2.$$ 

Proof. Again it is sufficient to prove this relation after restricting both sides to $P$. For $(A_1, B_2, 0) \in \Lambda^m$ we have $x_{(A_1, B_2, 0)} \cdot x_{(A_2, B_2, 0)} = [-1]^{|A_1 \cap A_2| + |B_1 \cap B_2|} \cdot x_{(A_1 \cup B_1, B_2 \cup (B_2 \cap A_2))}$. Thus we have

$$\sum_{(A_1, B_2) \in \Lambda^{d+1}} x_{(A_1, B_2, 0)} \cdot \sum_{(A_2, B_2) \in \Lambda^{d+1}} x_{(A_2, B_2, 0)} = \sum_{k \geq 0} \sum_{(A_1, B_2) \in \Lambda^{d-k}} x_{(A_1 \cup B_1, B_2 \cup (B_2 \cap A_2))} \cdot \sum_{(A_2, B_2) \in \Lambda^{d-k}} x_{(A_2 \cup B_2, A_1 \cap B_2)} = [-1]^k \sum_{k \geq 0} \sum_{(A_1, B_2) \in \Lambda^{d-k}} x_{(A_1 \cup B_1, B_2 \cup (B_2 \cap A_2))}.$$ 

59
Fix \( k \geq 0 \) and \( (A', B', C') \in \Lambda^{d+m-k} \) such that \(|C'| + k = d\). Then we have \(|A'| + |B'| = m - |C'|\). Now define

\[
S := \{(A_1, B_1, B_2) \mid (A_1, B_1, \emptyset) \in \Lambda^m, (A_2, B_2, \emptyset) \in \Lambda^d, A_1 - B_2 = A', B_1 - A_2 = B',
\]

\[
(A_1 \cap B_2) \cup (B_1 \cap A_2) = C', |A_1| \text{ even}.
\]

Then we have

\[
S = \{(A' \cup U_2, B' \cup V_1, U_1 \cup V_1, U_2 \cup V_2) \mid U_1 \subset A', V_2 \subset B', V_1 \subset C',
\]

\[
V_1 \cap U_2 = \emptyset, C' = V_1 \cup U_2, |A'| + |U_2| \text{ even}, |U_1| + |V_2| = d - |C'|.
\]

Now let us try to compute \(|S|\). Let us first do the case, where \(|C'| \geq 1\). Then we have

\[
|S| = 2^{|C'|-1} \cdot \left( \frac{|A'| + |B'|}{d - |C'|} \right) = 2^{|C'|-1} \cdot \left( \frac{m - |C'|}{d - |C'|} \right)
\]

This is 0 mod 2, unless \(|C'| = 1\). In this case, it is \(\binom{m-1}{d-1}\). On the other hand, if \(C' = \emptyset\) and \(|A'|\) is odd, then \(S = \emptyset\). If \(C' = \emptyset\) and \(|A'|\) is even, then we have \(|S| = \binom{m}{d}\). Thus we conclude

\[
\left( \sum_{(A_1, B_1, \emptyset) \in \Lambda^m, |A_1| \text{ even}} x_{(A_1, B_1, \emptyset)} \right) \cdot \left( \sum_{(A_2, B_2, \emptyset) \in \Lambda^d} x_{(A_2, B_2, \emptyset)} \right) = \sum_{k \geq 0} \sum_{(A_1, B_1, \emptyset) \in \Lambda^m, |A_1| \text{ even}} \sum_{(A_2, B_2, \emptyset) \in \Lambda^d, |A_1| \text{ even}} \sum_{|A_1| + |B_1| + |A_2| + |B_2| = k} \{-1\}^k x_{(A_1 - B_2, B_1 - A_3, (A_1 \cap B_2) \cup (A_3 \cap B_2))}
\]

\[
= \binom{m}{d} m! \sum_{(A, B, \emptyset) \in \Lambda^m, |A| \text{ even}} x_{(A, B, \emptyset)} + \binom{m-1}{d-1} \sum_{(A, B, C) \in \Lambda^m, |C| = 1} x_{(A, B, C)}
\]

2.7.9 \( E_6 \)

In this section, we require \(\text{char}(k_0) \not| |W(E_6)| = 2^7 \cdot 3^4 \cdot 5^3\), i.e. \(\text{char}(k_0) \not= 2, 3, 5\). \(M\), is a \(Z\)-graded \(A_1\)-module with \(K^M/2\)-module structure. By 2.4.5 we have \(|Q(W(E_6))| = 1\); a representative for this conjugacy class is for instance given by \(P := P(a_1, b_1, a_2, b_2)\). The injection \(\operatorname{Inv}^\vee(W(E_6), M) \to \operatorname{Inv}^\vee(P, M)\) factors through \(\operatorname{Inv}^\vee(W(D_5), M)\) and thus we obtain an injection \(\operatorname{Inv}^\vee(W(E_6), M) \to \operatorname{Inv}^\vee(W(D_5), M)\).

An \(M,(k_0)\)-basis of \(\operatorname{Inv}^\vee(W(D_5), M)\) is given by

\[(0) \quad 1,
\]

\[(i) \quad u_1,
\]

\[(ii) \quad u_2, v_2,
\]

\[(iii) \quad v_2 u_1,
\]

\[(iv) \quad v_4\]

So let \(a \in \operatorname{Inv}^\vee(P, M)\) be an invariant which comes from a \(W(E_6)\)-invariant. Since the inclusion \(P \subset W(E_6)\) factors through \(W(D_5) \subset W(E_6)\), \(a\) can be uniquely written as

\[
a = \sum_{0 \leq d \leq 5} \left( \sum_{(A, B, C) \in \Lambda^d} x_{(A, B, C)} \right) m_d + \left( \sum_{(A, B, \emptyset) \in \Lambda^2} x_{(A, B, \emptyset)} \right) m_2 + \left( \sum_{(0, B, C) \in \Lambda^2} x_{(0, B, C)} \right) m'_2
\]

for certain \(m_d \in M_{-d}(k_0), m_2, m'_2 \in M_{-2}(k_0)\). The element

\[
S := S_{\{\pm 1, -3, 4, 5, -6, -7, e_8\}} \cdot S_{\{-1, 2, 3, 4, 5, -6, -7, e_8\}} \cdot S_{\pm 1} \in W(E_6)
\]

lies in the normalizer of \(P\), since we have

\[
S \cdot s_{a_1} \cdot S^{-1} = s_{v_2},
\]

\[
S \cdot s_{b_1} \cdot S^{-1} = s_{v_1},
\]

\[
S \cdot s_{a_2} \cdot S^{-1} = s_{u_2},
\]

\[
S \cdot s_{b_2} \cdot S^{-1} = s_{u_1}.
\]
The induced action of $g$ on a $P$-torsor $(a_1, a_2, b_1, b_2)$ is thus given by swapping $a_1 \leftrightarrow b_2$, while leaving $a_2, b_1$ fixed. Therefore applying $g$ to the invariant $a$ yields

$$\sum_{0 \leq d \leq 4} \left( \sum_{(A,B,C) \in \Lambda^d} \chi(A,B,C) \right) m_d + (x_{[a_1,b_1]} + x_{[a_1,a_2]} + x_{[a_1,b_1]} + x_{[a_2,b_2]}) m_2 + (x_{[a_1,a_2]} + x_{[b_1,b_2]}) m'_2.$$ 

Since $a$ comes from an invariant of $W(E_6)$, it must be invariant under $g$ and comparing coefficients, we conclude that the image of the restriction $\text{Inv}'(W(E_6), M) \to \text{Inv}'(W(D_5), M)$ lies in the free $M.(k_0)$-submodule with basis

(i) $u_1$
(ii) $u_2 + v_2$
(iii) $v_2u_1$
(iv) $v_4$

Since $W(E_6)$ is an orthogonal reflection group, we have an embedding $W(E_6) \subset O_8$ and thus we may define invariants $\text{res}^{W(E_6)}_{O_8}(\bar{w}_d) \in \text{Inv}^d(O_8, K^M/2)$ which we will again denote by $\bar{w}_d$. Let $k \in \mathcal{F}_{k_0}$ be arbitrary and let $(a_1, b_1, a_2, b_2) \in (k^x/k^2)^4$ be an arbitrary $P$-torsor; using the map $P \to W(E_6) \subset O_8$ this induces the quadratic form

$$\langle 2a_1, 2b_1, 2a_2, 2b_2, 1, 1, 1, 1 \rangle.$$ 

Thus, the total modified Stiefel-Whitney class evaluated at this torsor is

$$(1 + [a_1])(1 + [a_2])(1 + [b_1])(1 + [b_2])(1 + \{2\}^4).$$

Now it is easy to compute that

$$\begin{align*}
\text{res}^{W(D_5)}_{W(E_6)}(u_1) &= \text{res}^{W(E_6)}_{W(E_6)}(\bar{w}_1) \\
\text{res}^{W(D_5)}_{W(E_6)}(u_2 + v_2) &= \text{res}^{W(E_6)}_{W(E_6)}(\bar{w}_2) \\
\text{res}^{W(D_5)}_{W(E_6)}(v_2u_1) &= \text{res}^{W(E_6)}_{W(E_6)}(\bar{w}_3) \\
\text{res}^{W(D_5)}_{W(E_6)}(v_4) &= \text{res}^{W(E_6)}_{W(E_6)}(\bar{w}_4 - \{2\}^4).
\end{align*}$$

This shows that the $[\bar{w}_d]_{0 \leq d \leq 4}$ form a basis of $\text{Inv}'(W(E_6), M_8)$ as $M.(k_0)$-module. The product structure can be deduced from the $W(D_5)$-case.

### 2.7.10 $E_7$

We require that $\text{char}(k_0) \nmid |W(E_7)| = 2^{10} \cdot 3^4 \cdot 5 \cdot 7$, i.e. $\text{char}(k_0) \neq 2, 3, 5, 7$. $M$ is a $\mathbb{Z}$-graded $A^1$-module with $K^M/2$-module structure.

By Proposition 2.4.5 we have $\Omega(W(E_7)) = \{ [P] \}$, where $P := P(a_1, b_1, a_2, b_2, a_3, b_3, a_4)$. Looking at the root systems, we see that there is an inclusion $W(D_8) \times \langle s_{a_4} \rangle \subset W(E_7)$. By the same factorization argument as before, we see that the restriction map $\text{Inv}'(W(E_7), M) \to \text{Inv}'(W(D_8) \times \langle s_{a_4} \rangle, M)$ is injective. We will denote $P$-torsors by $(a_1, b_1, a_2, b_2, a_3, b_3, a_4) \in (k^x/k^2)^7$. Let us first recall that $\text{Inv}'(W(D_8) \times \langle s_{a_4} \rangle, M)$ is a free $M.(k_0)$-module with basis

(i) $u_1, x_{[a_4]}$
(ii) $u_2, v_2, u_1x_{[a_4]}$
(iii) $(u_3 - e_3), e_3, u_1v_2, u_2x_{[a_4]}, v_2x_{[a_4]}$
(iv) $u_2v_2, v_4, (u_3 - e_3)x_{[a_4]}, e_3x_{[a_4]}, u_1v_2x_{[a_4]}$
(v) $v_4u_1, u_3x_{[a_4]}, v_2x_{[a_4]}$
(vi) $v_6, v_4u_1x_{[a_4]}$
Let $k \in \mathcal{F}_k$ and $(a_1, \beta_1, \ldots, a_3, \beta_3, a_4) \in (k^x/k^c)^7$ be a $P$-torsor. The action of $g$ on this torsor is thus given by swapping $a_1 \leftrightarrow \beta_2, \beta_3 \leftrightarrow a_4$ while leaving $\beta_1, a_2, a_3$ fixed. Arguing just as in the $E_8$-case, we see that the image of $\text{Inv}^e(W(E_7), M) \to \text{Inv}^e(W(D_8) \times \langle \langle s_{a_4} \rangle, M \rangle$ lies in the free $M,(k_0)\text{-module with basis}$

\begin{enumerate}
  \item $1$
  \item $u_1 + x_{[a_4]}$
  \item $v_2 + u_2 + u_1 x_{[a_4]}$
  \item $v_4 (u_3 - e_3) + u_2 x_{[a_4]} + v_2 x_{[a_4]}$
  \item $u_4 v_2 + u_2 x_{[a_4]} + v_4 u_1$
  \item $v_6 x_{[a_4]}$
\end{enumerate}

Now we need to provide enough $W(E_7)$-invariants. First, the embedding $W(E_7) \subset O_8$ gives us invariants $\text{res}^e_{\text{Ch}}(\bar{w}_i) \in \text{Inv}^e(W(E_7), K^A/2)$ which we will again denote by $\bar{w}_i$. It is routine to check that we have

\[
\text{res}^e_{W(E_7)}(\bar{w}_1) = \text{res}^e_{W(D_8) \times \langle \langle s_{a_4} \rangle} (u_1 + x_{[a_4]})
\]
\[
\text{res}^e_{W(E_7)}(\bar{w}_2) = \text{res}^e_{W(D_8) \times \langle \langle s_{a_4} \rangle} (u_2 + v_2 + u_1 x_{[a_4]})
\]
\[
\text{res}^e_{W(E_7)}(\bar{w}_3) = \text{res}^e_{W(D_8) \times \langle \langle s_{a_4} \rangle} (u_3 + u_1 v_2 + u_2 x_{[a_4]} + v_2 x_{[a_4]})
\]
\[
\text{res}^e_{W(E_7)}(\bar{w}_4) = \text{res}^e_{W(D_8) \times \langle \langle s_{a_4} \rangle} (u_2 v_2 + v_4 + u_3 x_{[a_4]} + u_1 v_2 x_{[a_4]})
\]
\[
\text{res}^e_{W(E_7)}(\bar{w}_5) = \text{res}^e_{W(D_8) \times \langle \langle s_{a_4} \rangle} (v_4 u_1 + v_4 x_{[a_4]} + u_2 v_2 x_{[a_4]})
\]
\[
\text{res}^e_{W(E_7)}(\bar{w}_6) = \text{res}^e_{W(D_8) \times \langle \langle s_{a_4} \rangle} (v_6 x_{[a_4]})
\]
\[
\text{res}^e_{W(E_7)}(\bar{w}_7) = \text{res}^e_{W(D_8) \times \langle \langle s_{a_4} \rangle} (v_6 x_{[a_4]})
\]

So we still need some further basis invariants in degree 3 and 4. To construct the missing invariant in degree 3, we will mimic the construction of the invariant $e_9$ in the $D_n$-section. Let $U \cong S_6 \times \langle \langle s_{a_4} \rangle \subset W(E_7)$ be the subgroup generated by the reflections at $[e_1 + e_2, e_2 - e_1, e_3 - e_4, e_4 - e_5, e_5 - e_6, e_6 - e_7]$. Then $[U \setminus W(E_7)] = 2016$ and we obtain a map $W(E_7) \to S_{2016} \to O_{2016}$. To be more precise, there is a right action of $W(E_7)$ on the right cosets $U \setminus W(E_7)$ given by right multiplication. This induces an anti-homomorphism $W(E_7) \to S_{2016}$ and precomposing this map with $\bar{g} \mapsto \bar{g}^{-1}$, we obtain the desired homomorphism (we didn’t use left cosets, since right cosets are more convenient when doing computations in GAP). We need the following lemma which tells us that we are in a situation which is quite similar to the $D_n$-case:

**Lemma 2.7.25.** Let $k \in \mathcal{F}_k$ and $y \in H^1(k, P)$ be a $P$-torsor. Let $q_y$ be the quadratic form induced by $y$ under the composition $P \to W(E_7) \to S_{2016} \to O_{2016}$. Then the image of $q_y$ in $W(k)$ is contained in $P(k)$.

**Proof.** This can be checked by a computer; see appendix [3].
We can now argue exactly as in the $D_7$-case to obtain an invariant $f_2 \in \text{Inv}^3(W(E_7), K^M/2)$. In concrete terms, if $y$ is a $W(E_7)$-torsor, and $q_y$ is the quadratic form induced by $y$ under the composition $W(E_7) \to S_{2016} \to 0_{2016}$, then the image of $q_y$ in $W(k)$ is contained in $P(k)$ and we define $f_2(y) : = e_5((2^3) \otimes q_y)$. In the appendix we also describe how a computer may be used to compute that the restriction of $f_2$ to $P$ is

$$\text{res}_{W(D_8)}^{P}(u_1v_2 + u_3 - e_3 + u_2x_{[4]}).$$

Finally, observe that

$$(u_1 + x_{[4]})(u_1v_2 + (u_3 - e_3) + u_2x_{[4]}) = u_1^2v_2 + u_1(u_3 - e_3) + u_1u_2x_{[4]} + u_2x_{[4]} + (u_3 - e_3)x_{[4]} + u_2x_{[4]}^2 = [-1](u_1v_2 + u_2v_2 + [-1](u_3 - e_3) + u_3x_{[4]} + u_1u_2x_{[4]} + (u_3 - e_3)x_{[4]} + [-1]u_2x_{[4]} = u_2v_2 + u_1u_2x_{[4]} + e_3x_{[4]} + [-1](u_1v_2 + (u_3 - e_3) + u_2x_{[4]}).$$

Thus, $\text{Inv}^6(W(E_7), M)$ is a free $M_4(k_0)$-module with basis $\{\overline{w_d} | 0 \leq d \leq 7 \cup \{f_3, f_3 \cdot v_1\}$ and the product structure can be deduced from the $\text{Inv}^6(W(D_8))$-case.

### 2.7.11 $E_8$

We require that $\text{char}(k_0) \notin |W(E_8)| = 2^1 \cdot 3^5 \cdot 5^2 \cdot 7$, i.e. $\text{char}(k_0) \neq 2, 3, 5, 7$. $M$, is a $\mathbb{Z}$-graded $A_1$-module with $K^M/2$-module structure.

Observe that $P := P(a_1, b_1, a_2, b_2, a_3, b_3, a_4, b_4)$ is the (up to conjugacy) unique maximal elementary abelian subgroup generated by reflections in $W(E_8)$. By the same arguments as in the $E_8/E_7$-case, we obtain that the restriction map $\text{Inv}^6(W(E_8), M) \to \text{Inv}^6(W(D_8), M)$ is injective. We first recall that $\text{Inv}^6(W(E_8), M)$ is a free $M_4(k_0)$-module with the following basis:

- (0) 1
- (i) $u_1$
- (ii) $u_2, v_2$
- (iii) $u_3, v_2 u_1$
- (iv) $e_4, (u_4 - e_4), v_2 u_2, v_4$
- (v) $v_2 u_3, v_3 u_1$
- (vi) $v_4 u_2, v_6$
- (vii) $v_5 u_1$
- (viii) $v_8$

Again, we define $g \in W(E_8)$ as in the $E_6$ or $E_7$-case; again, we check that it normalizes $P$:

$$g \cdot s_{a_1} \cdot g^{-1} = s_{a_2}$$
$$g \cdot s_{b_1} \cdot g^{-1} = s_{b_1}$$
$$g \cdot s_{a_2} \cdot g^{-1} = s_{a_2}$$
$$g \cdot s_{b_2} \cdot g^{-1} = s_{b_1}$$
$$g \cdot s_{a_3} \cdot g^{-1} = s_{a_3}$$
$$g \cdot s_{b_3} \cdot g^{-1} = s_{b_3}$$
$$g \cdot s_{a_4} \cdot g^{-1} = s_{a_4}$$
$$g \cdot s_{b_4} \cdot g^{-1} = s_{b_4}.$$

The action of $g$ on a $P$-torsor $(a_1, b_1, a_2, b_2, a_3, b_3, a_4, b_4)$ is thus given by swapping $a_1 \leftrightarrow b_2, b_3 \leftrightarrow a_4$ while leaving $b_1, a_2, a_3, b_4$ fixed. Again, applying the same kind of arguments as in the $E_6$-case, we see that the image of the restriction map $\text{Inv}^6(W(E_8), M) \to \text{Inv}^6(W(D_8), M)$ is contained in the free $M_4(k_0)$-submodule with basis

- (0) 1

63
the subgroup generated by the reflections at $\{U_1, U_2, U_3, U_4\}$. Thus we conclude that $\text{Inv}(W) = \text{Inv}(V)$ and $\text{Inv}(W) = \text{Inv}(V)$.

Now we need to construct $W(E_8)$-invariants mapping to these basis elements. On the one hand, the inclusion $W(E_8) \subset O_8$ gives us modified Stiefel-Whitney classes $\tilde{w}_d \in \text{Inv}^d(W(E_8), K^M/2)$. Again one can check that

$$\text{res}_{W(E_8)}(\tilde{w}_1) = \text{res}_{W(D_8)}(u_1)$$
$$\text{res}_{W(E_8)}(\tilde{w}_2) = \text{res}_{W(D_8)}(u_2 + v_2)$$
$$\text{res}_{W(E_8)}(\tilde{w}_3) = \text{res}_{W(D_8)}(u_3 + u_1 v_2)$$
$$\text{res}_{W(E_8)}(\tilde{w}_4) = \text{res}_{W(D_8)}(u_4 + u_2 v_2 + v_4)$$
$$\text{res}_{W(E_8)}(\tilde{w}_5) = \text{res}_{W(D_8)}(v_2 u_3 + v_4 u_1)$$
$$\text{res}_{W(E_8)}(\tilde{w}_6) = \text{res}_{W(D_8)}(v_4 u_2 + v_6)$$
$$\text{res}_{W(E_8)}(\tilde{w}_7) = \text{res}_{W(D_8)}(v_6 u_1)$$
$$\text{res}_{W(E_8)}(\tilde{w}_8) = \text{res}_{W(D_8)}(v_8)$$

The situation is very similar to the $E_7$-case; this time we miss a basis invariant in degree 4. Let $U \subset W(E_8)$ be the subgroup generated by the reflections at $\{e_1 + e_2, e_2 - e_3, e_3 - e_4, e_4 - e_5, e_5 - e_6, e_6 - e_7, e_7 - e_8\}$. By observing that $U = S_8$ or by using a computer, we conclude $|U \setminus W(E_8)| = 17280$. As in the $E_7$-case, we obtain a map $W(E_8) \to S_{17280} \to O_{17280}$. Again we need the following lemma which we can only prove by making use of a computer:

**Lemma 2.7.26.** Let $k = F_{32}$ and $y \in H^1(k, P)$ be a $P$-torsor. Let $q_y$ be the quadratic form induced by $y$ under the composition $P \to W(E_8) \to S_{17280} \to O_{17280}$. Then the image of $q_y$ in $W(k)$ is contained in $I^4(k)$.

**Proof.** Again this can be checked by a computer and we give details in the appendix.

As in the $D_4$-case, we obtain from this an invariant $f_4 \in \text{Inv}^4(W(E_8))$. More precisely, if $y$ is a $W(E_8)$-torsor and $q_y$ is the quadratic form induced by $y$ under the composition $W(E_8) \to S_{17280} \to O_{17280}$, then the image of $q_y$ in $W(k)$ is contained in $I^4(k)$ and we define $f_4(y) = e_4(q_y)$.

To compute the restriction of $f_4$ to $P$, we may again ask the computer. He says (see appendix) that it is

$$\text{res}_{W(D_8)}(v_2 u_2 + (u_4 - e_4)).$$

Thus we conclude that $\text{Inv}(W(E_8), M)$ is a free $M,(k_0)$-module with basis $\{f_4 \cup \{\tilde{w}_d\}_{0 \leq d \leq 8}\}$ and the product structure can be deduced from the $\text{Inv}(W(D_8))$-case.

### 2.8 Summary and open questions

It is probably a good idea to summarize the piecemeal results obtained in the previous sections:

**Summary 2.8.1.** Let $M_\bullet$ be a $\mathbb{Z}$-graded $\mathbf{A}^1$-module with $K^M/2$-structure. Let $W$ be a finite Euclidean irreducible reflection group and let $k_0$ be a base field, which is nice enough (for Weyl groups, char($k_0$) $\nmid |W|$ and $-1 \in k_0^{\times 2}$ is certainly nice enough; see the respective sections for details). Then $\text{Inv}_{k_0}^\bullet(W, M)$ is a free $M,(k_0)$-module. Here is a list that gives for each possible type of $W$ such a basis:

- $W = W(A_n)$: $|\tilde{w}_d| \mid 0 \leq d \leq \left[ \frac{n+1}{2} \right]$.
- $W = W(B_n)$: $|u_{d-r}v_r| \mid 0 \leq d \leq n$, $\max(0, 2d - n) \leq r \leq d$.
• \( W = W(D_n) \):
  
  - \( 2 \nmid n \): \([u_d, v_d] \mid 0 \leq d \leq n, \max(0, 2d - n) \leq 2r \leq d \)
  
  - \( 2 \mid n \): \([u_d, v_d] \mid 0 \leq d \leq n, \max(0, 2d - n) \leq 2r \leq d \) \( \cup \{ e_m \} \)

• \( W = W(E_6) \): \([\overline{w_d}] \mid 0 \leq d \leq 4 \)

• \( W = W(E_7) \): \([\overline{w_d}] \mid 0 \leq d \leq 7 \) \( \cup \{ f_3, \overline{w_3} \} \)

• \( W = W(E_8) \): \([\overline{w_d}] \mid 0 \leq d \leq 8 \) \( \cup \{ f_4 \} \)

• \( W = W(F_4) \): \([w_d] \mid 0 \leq d \leq 4 \) \( \cup \{ v_1, w_1, v_2, w_2 \} \)

• \( W = W(G_2) \): \(\{1, x_{[r \rightarrow -2]}, x_{[2, c \rightarrow r \rightarrow -2]}, x_{[r \rightarrow -2, c \rightarrow r \rightarrow -2]}\} \)

• \( W = W(H_3) \): \([w_d] \mid 0 \leq d \leq 3 \)

• \( W = W(H_4) \): \([w_d] \mid 0 \leq d \leq 4 \)

• \( W = W(I_2(n)) \):
  
  - \( 2 \nmid n \): \(\{1, x_{[r]}\} \)
  
  - \( 2 \mid n \): \(\{1, x_{[r]}, x_{[2]}\} \)
  
  - \( 4 \mid n \): \(\{1, w_1, v_1, w_2\} \)

**Corollary 2.8.2.** Let \( \text{char}(k_0) \nmid |W| \) and \(-1 \not\in k_0^\times \). Let \( W \) be a Weyl group; let \( M \) be a \( \mathbb{Z} \)-graded \( \mathbb{A}^1 \)-module. Then \( \text{Inv}^\ast_{k_0}(W, M) \) is a free \( M_{(k_0)} \)-module.

**Proof.** This follows from the summary above and 2.1.16

**Corollary 2.8.3.** Let \( k_0 \) be perfect, \( \text{char}(k_0) \nmid |W| \) and \(-1 \not\in k_0^\times \). Let \( W \) be a Weyl group and \( M \) be a cycle module. Then \( h_0(B_{gm}(W)) = \mathbb{Z} \oplus \oplus K^M_0/2 \) for certain non-negative integers \( d \) and \( \text{Inv}^\ast_{k_0}(W, M) \cong M_{(k_0)} \oplus \oplus M_{-d(k_0)}(2) \).

**Proof.** This was observed in 2.8.1 (using the above summary).

Finally, we observe that this diploma thesis still leaves many open questions on the invariants of Euclidean reflection groups:

(i) What can we say about \( \text{Inv}^\ast_{k_0}(W(B_n), M) \) and \( \text{Inv}^\ast_{k_0}(W(F_4), M) \), if \(-1 \not\in k_0^\times \)?

(ii) Why does the modified Quillen map fail to be an isomorphism for reflection groups of type \( W(I_2(n)) \)?

   We can deduce this only by using an \textit{ad hoc} argument (i.e. by choosing a versal torsor which is quite nice from the computational point of view); a more conceptual explanation/obstruction would be desirable.

(iii) Find a way to determine the structure of \( \text{Inv}^\ast(W(E_7), M) \) and \( \text{Inv}^\ast(W(E_8), M) \) without using a computer!

(iv) Although Serre’s splitting principle holds for any unramified \( \mathbb{A}^1 \)-invariant sheaf, most of our computations are only valid for cycle modules or \( \mathbb{Z} \)-graded \( \mathbb{A}^1 \)-modules with \( K^M/2 \)-structure. For instance, it would be interesting to determine the structure of the invariants using Witt groups as coefficients.
A Miscellaneous facts on schemes

Proposition A.0.1. Let $S$ be a scheme $X, Y \in \text{Sch}/S$ and $\iota: X \to Y$ be a closed immersion. Let $T \in \text{Sch}/S$ and $f_1, f_2: T \to X$ be such that $\iota \circ f_1 = \iota \circ f_2$. Then we have $f_1 = f_2$.

Proof. The assertion is clear on the set-theoretic level. In particular, for any open affine $U \subset Y$ the open subschemes $f_1^{-1}(X \cap U), f_2^{-1}(X \cap U) \subset T$ agree. So there is no harm in supposing $Y = \text{Spec}(A)$ affine. Thus $X = \text{Spec}(A/I)$ for some ideal $I \subset A$. But then the proposition is reduced to the following statement:

If the composite maps

$$A \to A/I \xrightarrow{f_1^*(\text{Spec}(A/I))} \mathcal{O}_T(T)$$

$$A \to A/I \xrightarrow{f_2^*(\text{Spec}(A/I))} \mathcal{O}_T(T)$$

agree, then so do $f_1^*(\text{Spec}(A/I))$ and $f_2^*(\text{Spec}(A/I))$. This is clear. \(\square\)

Proposition A.0.2. Let $X_1, X_2, \ldots, X_n, Y$ be schemes and $\phi_i: X_i \to Y$ be closed immersions whose images are pairwise disjoint. Then the induced map $\phi: \bigsqcup X_i \to Y$ is a closed immersion.

Proof. Put $X := \bigsqcup X_i$. It is clear that $\phi$ is a closed embedding of topological spaces. So it remains to check that $\mathcal{O}_Y \to \phi_* \mathcal{O}_X$ is surjective. This question is local on $Y$, so we may assume $Y = \text{Spec}(A)$ affine. The $X_i$ are defined by pairwise coprime ideals $I_i \subset A$. Thus the map $A \to A/\prod_{i=1}^n I_i \cong \prod_{i=1}^n A/I_i$ is surjective by the Chinese remainder theorem. \(\square\)

Definition A.0.3 (Relative Dimension). Let $f: X \to Y$ be a flat morphism of schemes of finite type over a field. We say that $f$ is of relative dimension $d$ if the following two equivalent properties are satisfied

- For all irreducible closed subschemes $Z \subset Y$ and for all irreducible components $W$ of $f^{-1}(Z)$ we have $\dim(W) = \dim(Z) + d$.

- For all $y \in Y$ and for all generic points $x$ of $X_y$, we have $\dim([x]) = \dim([y]) + d$.

Proof. We begin by showing that the first point implies the second one. Let $y \in Y$ and define $Z := [y]$. Let $W_1, \ldots, W_n$ be the irreducible components of $f^{-1}(Z)$ and let $w_1, \ldots, w_n$ be their generic points. Since $f$ is flat, all the $W_i$ dominate $Z$. Thus $f(w_i) = y$. We conclude that the $X_y \cap W_i$ are the irreducible components of $X_y$ and that each generic point $x$ of $X_y$ coincides with one of the $w_i$.

On the other hand, suppose now the second property holds. Let $Z \subset Y$ be an irreducible closed subscheme and let $y$ be its generic point. Now we argue just as above. Let $W_1, \ldots, W_n$ be the irreducible components of $f^{-1}(Z)$ and let $w_1, \ldots, w_n$ be their generic points. Again, we have $f(w_i) = y$ and the $X_y \cap W_i$ are the irreducible components of $X_y$. In particular, $w_i$ is a generic point of $X_y$ and by assumption, we have $\dim(W_i) = \dim([w_i]) = \dim(Z) + d$. \(\square\)

We have

Proposition A.0.4. Let $f: X \to Y$ be a flat morphism of schemes of finite type over a field. Suppose that $Y$ is irreducible and that all irreducible components of $X$ have dimension $\dim(Y) + d$ (i.e. $X$ is equidimensional of dimension $\dim(Y) + d$). Then $f$ has relative dimension $d$.

Proof. [HN] Corollary 9.6] \(\square\)

Let us recall the definition of codimension:

Definition A.0.5 (Codimension). Let $X$ be a Noetherian scheme and let $Z \subset X$ be an irreducible closed subscheme. Then the codimension of $Z$ in $X$ – denoted by $\text{codim}_X(Z)$ – is defined to be the supremum of all lengths $n$ of ascending chains of irreducible subschemes starting at $Z$:

$$Z := Z_0 \subset Z_1 \subset \ldots \subset Z_n \subset X.$$  

If $Z \subset X$ is a closed (not necessarily irreducible) subscheme of $X$, then the codimension of $Z$ in $X$ is defined to be the infimum of the $\text{codim}_X(Z)$, where $Z_i$ is an irreducible component of $Z$.

Proposition A.0.6. Let $X, Y$ be of finite type over a field $k$ and assume $X$ equidimensional, $Y$ irreducible. Let $f: X \to Y$ be flat and let $Z \subset Y$ be a closed subscheme. If $f^{-1}(Z) \neq \emptyset$, then $\text{codim}_X(f^{-1}(Z)) \geq \text{codim}_Y(Z)$.
We conclude

\[ \text{codim} \]

we obtain

\[ \text{codim} \]

by reflections

GAP

For the computations in the

E

package

CHEVIE

We want to have some precise information on the orbit structure of the action of

U

All other simple systems are of the form

\{\]

The

dim

If

X

Proposition A.0.7.

Let

X

= \[ \dim (X_j) \]

1

\[ \dim (X) - \dim (W) \]

\[ \text{codim}_X(W) = \dim (X_i) - \dim (W) = \dim (X_i) - \dim (W) \]

This implies \( \text{codim}_X(W) = \dim (X) - \dim (W) \) and we obtain:

\[ \text{codim}_X(W) = \dim (X) - \dim (W) = \dim (X) - (d + \dim (Z_i)) = \dim (Y) - \dim (Z_i) = \text{codim}_Y(Z_i) \geq \text{codim}_Y(Z). \]

\[ \square \]

Proposition A.0.7. Let

X

Y

be of finite type over a field

k

and assume

X

equidimensional,

Y

irreducible. Furthermore,

let

U

be open,

let

f

be faithfully flat and put

V

= \( f(U) \) (this is an open subscheme, since

f

is flat and of finite type). Suppose furthermore that

U

\[ \text{codim}_X(X - U) \leq \text{codim}_Y(Y - V). \]

Proof.

Let

d

= \( \dim (X) - \dim (Y) \). By \[ A.0.4 \]

f

is of relative dimension

d

Let

Y

be of finite type over a field

k

and assume

X

equidimensional, \( Y \) irreducible. Furthermore,

let

W

be the irreducible components of

Y

- \( V \); let further

W_{ij}

be the irreducible components of \( f^{-1}(Y_i) \). Then the

W_{ij}

are the irreducible components of \( X - U \).

We conclude \( \text{codim}_X(X - U) \leq \text{codim}_Y(Y - V) \).

\[ \square \]

B Computation concerning \( W(E_7) \)

For the computations in the \( E_7 \) and \( E_8 \)-case, we use the computational algebra system GAP 3.4.4 and the GAP-package CHEVIE \[ \text{[CH].} \]

GAP 3.4.4 is available freely from \text{http://www.gap-system.org/}\] Currently,

the CHEVIE-package is not compatible with the new version GAP 4.

Let us recall the situation we are facing. We have a maximal elementary abelian subgroup generated by reflections \( P = P(a_1, b_1, a_2, b_2, a_3, b_3, a_4) \subset W(E_7) \) and a subgroup \( U = \langle s_{1+2}, s_{2+3}, s_{3+4}, s_{4+5}, s_{5+6}, s_{6+7}, s_{7-8} \rangle \).

We want to have some precise information on the orbit structure of the action of \( P \) on the set of right cosets \( U \setminus W(E_7) \). Let \( \{v_1, \ldots, v_7\} \) be the simple system of roots, introduced in \[ \text{[2.4].} \]

One can check that

\[ -a_1 = v_3 \]

\[ b_1 = v_2 \]

\[ -a_2 = v_5 \]

\[ b_2 = v_2 + v_3 + 2v_4 + v_5 \]

\[ -a_3 = v_7 \]

\[ b_3 = v_2 + v_3 + 2v_4 + 2v_5 + 2v_6 + v_7 \]

\[ -a_4 = 2v_1 + 2v_2 + 3v_3 + 4v_4 + 3v_5 + 2v_6 + v_7 \]

and

\[ e_1 + e_2 = v_2 \]

\[ e_3 - e_2 = v_4 \]

\[ e_4 - e_3 = v_5 \]

\[ e_5 - e_4 = v_6 \]

\[ e_6 - e_5 = v_7 \]

\[ e_8 - e_7 = 2v_1 + 2v_2 + 3v_3 + 4v_4 + 3v_5 + 2v_6 + v_7. \]

All other simple systems are of the form \( \{t(v_1), \ldots , t(v_8)\} \) for some \( t \in W(E_7) \) and the action of \( tPt^{-1} \) on \( tUt^{-1} \setminus W(E_7) \) is isomorphic to the action of \( P \) on \( U \setminus W(E_7) \). Thus the question we are interested in does not depend on the choice of a simple system. Now let us consider an example session in GAP:

```gap
gap> RequirePackage("chevie");
gap> Read("coxOrbit");
gap> W:= CoxeterGroup("E",7);
```

67
CoxeterGroup("E", 7)

The first command loads the CHEVIE-package and the second one the program which will do the computations we need. We continue the session:

gap> a:=[3,2,5,28,7,49,63];
[ 3, 2, 5, 28, 7, 49, 63 ]
gap> for u in a do Print(W.roots[u]);Print(" \n");od;
[ 0, 0, 1, 0, 0, 0, 0 ]
[ 0, 1, 0, 0, 0, 0, 0 ]
[ 0, 0, 0, 1, 0, 0 ]
[ 0, 1, 1, 2, 1, 0, 0 ]
[ 0, 0, 0, 0, 0, 1 ]
[ 0, 0, 0, 0, 0, 0, 1 ]
[ 2, 2, 3, 4, 3, 2, 1 ]

In CHEVIE each root is given as a linear combination of a fixed (but arbitrary) simple system. If \( W \) is a reflection group associated to a root system \( \Phi \), then \( W.\text{roots}[i] \) returns the \( i \)-th root of \( \Phi \) (in some ordering). Keeping in mind the above computations, we see that \( P \subset W(E_7) \) is generated by the reflections at the \( 3,2,5,28,7,49,63 \)-th roots of the root system \( E_7 \). Thus we do the following:

\[
\text{ReflectionSubgroup}(W,[3,2,5,28,7,49,63]);
\]

\[
\text{ReflectionSubgroup}(\text{CoxeterGroup}("E", 7), \text{[3, 2, 5, 28, 7, 49, 63]})
\]

\[
\text{Size}(P);
\]

\[
128
\]

\[
\text{IsElementaryAbelian}(P);
\]

\[
\text{true}
\]

The last two lines are quite reassuring, since they imply that \( P \) is in fact a maximal elementary abelian subgroup generated by reflections. Now we would really like to compute the orbit structure of the action of \( P \) on \( U/W(E_7) \). To do this, we use the procedure "fullCheckE7" from the "coxOrbit"-program:

\[
\text{fullCheckE7}([2,4,5,6,7,63],[3,2,5,28,7,49,63]);
\]

On a multi-user AMD dual core 3800+ this took about 10 seconds. So while the computer is working, let me explain what the procedure fullCheckE7 does for us. Its first parameter says that we want \( U \) to be the subgroup generated by reflections at positions \( [2,4,5,6,7,63] \) and the second parameter says that we want \( P \) to be the subgroup generated by the reflections at \( [3,2,5,28,7,49,63] \).

First, fullCheckE7 computes the action of \( P \) on \( U/W(E_7) \) and its orbits \( O_1, \ldots, O_r \). Then, for each orbit \( O_k \), it determines a subset \( M_k \subset \{ a_1, b_1, a_2, b_2, a_3, b_3, a_4 \} \), such that \( P(\{ a_1, b_1, a_2, b_2, a_3, b_3, a_4 \} - M_k) \) acts trivially on \( O_k \) and such that \( P(M_k) \) acts simply transitively on \( O_k \) (a priori, there is no reason that such a subset should exist, however – as checked by the program – it exists in the case we are considering). The return value \( X \) of the procedure fullCheckE7 is an array whose \( k \)-th entry is just the set \( M_k \). We can now argue as in the \( D_n \)-case. Let \( y \in H^1(k, P) \) be an arbitrary \( P \)-torsor and let \( q_y \) denote its image under the map induced by \( P \to W(E_7) \to S_{2016} \to O_{2016} \). Then the decomposition of \( |U/W(E_7)| \) into orbits \( O_1, \ldots, O_r \) under \( P \) induces a decomposition \( q_y \equiv \otimes_{i=1}^{r} q_{y_i} \). By \( \textbf{[3.48]} \) each \( q_k \) is a scaled \( |M_k| \)-fold Pfister form. If we want to show that the image of \( q_y \) in \( W(k) \) is contained in \( \tilde{P}(k) \), then it is sufficient to show that each \( M_k \) consists of at least 3 elements. Thus we ask

\[
gap> \text{for x in X do if Length(x)<3 then Print("Fail")fi;od;}
\]

and we are happy, since no \( \text{Fail} \)s appear. By the same arguments as in the \( D_n \)-section, we can therefore define an element \( f_3 \in \text{Inv}^3(W(E_7), K^M/2) \) by \( x \mapsto c_1((2^3) \otimes q_x) \).

Now we would like to determine \( \text{res}_{W(E_7)}^P(f_3) \). Let again \( y = (a_1, \beta_1, a_2, \beta_2, a_3, \beta_3, a_4) \) be an arbitrary \( P \)-torsor and let \( O_1, \ldots, O_r \) be the orbits of the action of \( P \) on \( U/W(E_7) \). As we have noted above, \( q_y \) decomposes as \( q_y \equiv \otimes_{i=1}^{r} q_{y_i} \), where the \( q_k \) are scaled \( |M_k| \)-fold Pfister forms. Let us fix some \( k \) and write \( M_k = \{ a_{i_1}, \ldots, a_{i_k}, b_{i_1}, \ldots, b_{i_k} \} \); then we have

\[
q_k \equiv (2^{M_k}) \otimes \langle (-a_{i_1}) \rangle \otimes \ldots \otimes \langle (-a_{i_k}) \rangle \otimes \langle (-\beta_{i_1}) \rangle \otimes \ldots \otimes \langle (-\beta_{i_k}) \rangle.
\]
Now observe that \( e \) vanishes on \( I^\ell \) for \( \ell \geq 4 \). Therefore we only need to consider those \( M_k \) with \( |M_k| < 4 \) (i.e. \( |M_k| = 3 \)). Let us first define this list

\[
\text{gap}\ Y:=\text{Filtered}(X, x \rightarrow \text{Length}(x) < 4);
\]

Now we can print this list:

\[
\begin{align*}
\{ & "a2", "a3", "a4" \} \\
\{ & "a1", "a3", "a4" \} \\
\{ & "a1", "b1", "b2" \} \\
\{ & "a1", "a2", "a4" \} \\
\{ & "b1", "a2", "b2" \} \\
\{ & "a2", "b3", "a4" \} \\
\{ & "b2", "a3", "a4" \} \\
\{ & "a2", "b2", "a3" \} \\
\{ & "b2", "b3", "a3" \} \\
\{ & "b1", "a2", "b3" \} \\
\{ & "b1", "b3", "a4" \} \\
\{ & "b1", "b2", "a4" \} \\
\{ & "b1", "a3", "a4" \} \\
\{ & "a1", "b1", "b3" \} \\
\{ & "a1", "a3", "b3" \} \\
\{ & "a1", "b1", "a3" \} \\
\{ & "b1", "a3", "b3" \} \\
\{ & "b1", "b2", "a3" \} \\
\{ & "b1", "a2", "a4" \} \\
\{ & "b2", "a2", "a4" \} \\
\{ & "a1", "a2", "a3" \} \\
\{ & "a1", "a2", "a4" \} \\
\{ & "a2", "a3", "a4" \}
\end{align*}
\]

We claim that the elements appearing in this list are exactly

\[
\{(A, B, C) \in \Lambda^3 \mid |C| = 1\} \cup \{(A, B, \emptyset) \in \Lambda^3 \mid |A| \text{ odd}\} \cup \{(A, B, \emptyset, a_4) \mid (A, B, \emptyset) \in \Lambda^2\}.
\]

This can be checked either by hands or one may also use the procedure “e7Correct”

\[
\text{gap}\ e7\text{Correct}(Y);
\]

If we do not see any “Fail”s, then everything is ok (internally e7Correct checks that \( Y \) does not contain elements which are not in the claimed set above; since \( Y \) and the claimed set both have 28 elements, this reasoning yields the claimed description of \( Y \)). One way or another, we conclude:

\[
\text{res}_{W(E_7)}^p(f_3) = \sum_{(A, B, C) \in \Lambda^3} x_{(A, B, C)} + \sum_{(A, B, \emptyset) \in \Lambda^3} x_{(A, B, \emptyset)} + \{-1\} \sum_{(A, B, \emptyset) \in \Lambda^2} x_{(A, B, \emptyset)}
\]

\[
= \sum_{(A, B, C) \in \Lambda^3} x_{(A, B, C)} + \sum_{(A, B, \emptyset) \in \Lambda^3} x_{(A, B, \emptyset)} + \sum_{(A, B, \emptyset) \in \Lambda^2} x_{(A, B, \emptyset)} \cdot x_{a_4}.
\]
But we also have
\[
\text{res}^W_{W(D_4) \times (W_8)}(u_1v_2 + (u_3 - e_3) + u_2x_{4d}) = \sum_{(A,B,C) \in \mathbb{A}^3} x_{(A,B,C)} + \sum_{(A,B,0) \in \mathbb{A}^3} x_{(A,B,0)} + \sum_{(A,B,0) \in \mathbb{A}^3} x_{(A,B,0)} \cdot x_{4d}.
\]
This shows that \( f_8 \) is indeed the invariant we sought.

### C Computation concerning \( W(E_8) \)

Also in the \( E_8 \)-case, we will use \textit{GAP} and \textit{CHEVIE} to do the computations. We have a maximal elementary abelian subgroup generated by reflections \( P = \langle a_1, b_1, a_2, b_2, a_3, b_3, a_4, b_4 \rangle \) and a subgroup \( U = \langle 5s_{v1}c_1, 5s_{v2}c_2, 5s_{v3}c_3, 5s_{v4}c_4, 5s_{v5}c_5, 5s_{v6}c_6, 5s_{v7}c_7, 5s_{v8}c_8 \rangle \). We want to have some precise information on the orbit structure of the action of \( P \) on the set of right cosets \( U \setminus W(E_8) \). We have \( |U \setminus W(E_8)| = 17280 \) and thus we obtain a map \( W(E_8) \to S_{17280} \to O_{17280} \). With the notation of section 2.4 we have

\[
\begin{align*}
-a_1 &= v_3 \\
-b_1 &= v_2 \\
-a_2 &= v_5 \\
-b_2 &= v_3 + 2v_4 + v_5 \\
-a_3 &= v_7 \\
-b_3 &= v_2 + v_3 + 2v_4 + 2v_5 + 2v_6 + v_7 \\
-a_4 &= 2v_1 + 2v_2 + 3v_3 + 4v_4 + 3v_5 + 2v_6 + v_7 \\
-b_4 &= 2v_1 + 3v_2 + 4v_3 + 6v_4 + 5v_5 + 4v_6 + 3v_7 + 2v_8
\end{align*}
\]

and

\[
\begin{align*}
e_1 + e_2 &= v_2 \\
e_3 - e_2 &= v_4 \\
e_4 - e_3 &= v_5 \\
e_5 - e_4 &= v_6 \\
e_6 - e_5 &= v_7 \\
e_7 - e_6 &= v_8 \\
e_8 - e_7 &= 2v_1 + 2v_2 + 3v_3 + 4v_4 + 3v_5 + 2v_6 + v_7.
\end{align*}
\]

Now let us start a \textit{GAP}-session:

```gap
gap> RequirePackage("chevie");
gap> Read("coxOrbit");
gap> W:=CoxeterGroup("E",8);
    CoxeterGroup("E", 8)
gap> a:=[3,2,5,32,7,61,97,120];
    [ 3, 2, 5, 32, 7, 61, 97, 120 ]
gap> for u in a do Print(W.roots[u]); Print( "\ n"); od;
0 1 0 0 0 0 0 0
0 1 0 0 0 0 0 0
0 0 0 0 0 0 0 0
0 1 1 2 1 0 0 0
0 0 0 0 0 0 0 1
0 1 1 2 2 1 0 0
2 2 3 4 3 2 1 0
2 3 4 6 5 4 3 2
gap> P:=ReflectionSubgroup(W,[3,2,5,32,7,61,97,120]);
    ReflectionSubgroup(CoxeterGroup("E", 8), [ 3, 2, 5, 32, 7, 61, 97, 120 ])
gap> Size(P);
    256
gap> IsElementaryAbelian(P);

70
```
Again, the above computations together with the above session show that \( P = P(a_1, b_1, a_2, b_2, a_3, b_3, a_4, b_4) \subset W(E_8) \) is the subgroup generated by the reflections at the roots at position 3, 2, 5, 32, 7, 61, 97 and 120; \( U \) is generated by the reflections at the roots at positions 2, 4, 5, 6, 7, 8, 97. So we enter:

```
gap> X:=fullCheckE8([2,4,5,6,7,8,97],[3,2,5,32,7,61,97,120]);
```

On a multi-user AMD dual core 3800+ this took about 7 minutes. After this we may enter:

```
gap> for x in X do if Length(x)<4 then Print("Fail");fi;od;
```

If you don’t see any \( \text{Fail} \)s, then we can conclude as in the case of \( E_7 \) that the image \( q_y \) of any \( P \)-torsor \( y \in H^1(k, P) \) under the map \( H^1(k, P) \rightarrow H^1(k, W(E_8)) \rightarrow H^1(k, S_{17280}) \rightarrow H^1(k, O_{17280}) \rightarrow W(k) \) lies in \( I^4(k) \). As before, we conclude that this is also true, if we take \( W(E_8) \) instead of \( P \)-torsors. Thus we can define an element \( f_4 \in \text{Im}^4(W(E_8), k^M/2) \) by \( x \mapsto e_4(q_x) \).

Now we want to determine \( \text{res}^P_{W(E_8)}(f_4) \). We proceed as in the \( E_7 \)-case and first define a new list

```
gap> Y:=Filtered(X,x->Length(x)<5);
```

We can print the list:

```
gap> for y in Y do Print(y);Print("n");od;
```

```
[ "a1", "b2", "b3", "b4" ]
[ "a1", "b2", "a3", "a4" ]
[ "a1", "a2", "b3", "a4" ]
[ "a2", "b2", "a4", "b4" ]
[ "a1", "b3", "a4", "b4" ]
[ "a1", "a2", "b2", "b3" ]
[ "a1", "b3", "a4", "b4" ]
[ "a1", "a2", "b2", "b3" ]
[ "a1", "b3", "a4", "b4" ]
[ "b1", "b2", "b3", "a4" ]
[ "a1", "b1", "b3", "a4" ]
[ "a1", "b1", "b2", "b3" ]
[ "a1", "b1", "b2", "a4" ]
[ "a1", "b1", "b2", "b4" ]
[ "a1", "b1", "a2", "a4" ]
[ "a1", "b1", "a2", "b4" ]
[ "a1", "b2", "b2", "b3" ]
[ "a1", "a2", "b2", "a3" ]
[ "b1", "b2", "b3", "b4" ]
[ "a1", "b1", "b2", "b3" ]
[ "a1", "b1", "b2", "a3" ]
[ "a1", "b1", "b2", "b4" ]
[ "a1", "b1", "a2", "a3" ]
[ "a1", "b1", "a2", "b4" ]
[ "a2", "b2", "b3", "b4" ]
[ "a2", "b2", "a3", "a4" ]
[ "b1", "b2", "a3", "b3" ]
[ "a1", "a2", "a3", "b3" ]
[ "b2", "a3", "b3", "b4" ]
[ "a2", "a3", "b3", "a4" ]
[ "a2", "b2", "a3", "b4" ]
[ "a2", "a3", "b3", "b4" ]
[ "b1", "a2", "a3", "b3" ]
```

71
Here is the source code of the program "coxOrbit" used in the computations:

```plaintext
D Sourcecode
end of the

We claim that the elements appearing in this list are precisely

\{(A, B, C) \in \Lambda^4 \mid |C| = 1\} \cup \{(A, B, \emptyset) \in \Lambda^4 \mid |A| \text{ odd}\).

Again this can be checked by hand or by using the s8Correct procedure.

Thus we have

\[
res_{E_8}(f) = \left( \sum_{(A, B, C) \in \Lambda^4} x_{(A, B, C)} + \sum_{(A, B, B) \in \Lambda^4} x_{(A, B, B)} \right) + \left( \sum_{(A, B, B) \in \Lambda^4} x_{(A, B, B)} + \sum_{|A| \text{ odd}} x_{(A, B, B)} \right)
\]

Using \(res_{E_8}(u_2 + (u_4 - e_4)) = \sum_{(A, B, C) \in \Lambda^4} x_{(A, B, C)} + \sum_{|A| \text{ odd}} x_{(A, B, B)}\) proves the desired claim stated at the end of the \(E_8\)-subsection.

D Sourcecode

Here is the source code of the program "coxOrbit" used in the computations:

```
# Determine the permutational representation of the basis elements of the maximal elementary abelian subgroup generated by reflections on the root system of $W$

for root in measgrRoots do
  Add(permuationMeasgr, Reflections(W)[root]);
od;

for orbit in orbits do

  # first determine those basis elements of the maximal elementary abelian subgroup gen. by reflections which do not fix the orbit pointwise
  movers := [];
  moversroots := [];
  for i in [1..measgrSize] do
    isMover := false;
    # check if the $i$-th basis element of the maximal elementary abelian subgroup gen. by reflections fixes the orbit pointwise
    refl := permutationMeasgr[i];
    for element in orbit do
      if not(isMover) and not(element * refl = element)
        then
          isMover := true;
        fi;
    od;
    if isMover then
      Add(movers, i);
      Add(moversroots, measgrRoots[i]);
    fi;
  od;

  # now check, if the operation of movers on the orbit is simply transitive
  Q := ReflectionSubgroup(W, moversroots);
  if (not(IsRegular(Q, orbit, OnRight))) then
    Print("Action not simply transitive! ");
  fi;
  Add(solution, movers);
od;
return solution;
end;

fullCheck := function (W, URoots, PRoots)
local U, RCosets, g, orr, Csize, P, X, Y;
U := ReflectionSubgroup(W, URoots);
P := ReflectionSubgroup(W, PRoots);
RCosets := RightCosets(W, U);
Print("RightCosets computed ");
Print("\n");
Csize := Length(RCosets);
Print("Number of Right cosets is ");
Print(Csize);
Print("\n");
orrr := Orbits(P, RCosets, OnRight);
Print("Orbits computed ");
Print("\n");
X := orbitStructure(W, orrr, RCosets, PRoots);
Print("orbitStructure computed ");
Print("\n");
return X;
end;
# Check if the list doesn't contain any invariants of type e_3 or v_2x{\alpha_4}

```
e7Correct:=function (invList)
  if ( (["b1","b2","b3"] in invList) or
          (["a1","a2","b3"] in invList) or
          (["a1","b2","a3"] in invList) or
          (["b1","a2","a3"] in invList) or
          (["a1","b1","a4"] in invList) or
          (["a2","b2","a4"] in invList) or
          (["a3","b3","a4"] in invList) ) then
    Print("Fail");
    return
  fi;
  Print("Ok"); Print("\n");
end;
```

# An input of "a1" gives back "b1"; an input of "b2" gives back "a2", etc.

```
partner:=function (root)
  if (root="a1") then return "b1"; fi;
  if (root="b1") then return "a1"; fi;
  if (root="a2") then return "b2"; fi;
  if (root="b2") then return "a2"; fi;
  if (root="a3") then return "b3"; fi;
  if (root="b3") then return "a3"; fi;
  if (root="a4") then return "b4"; fi;
  if (root="b4") then return "a4"; fi;
  Print("Input Fail");
end;
```

# Counts the number of partner-pairs contained in a list

```
partnerCount:=function (List)
  local element, counter, p;
  counter:=0;
  for element in List do
    p:=partner(element);
    if (p in List) then
      counter:=counter+1;
    fi;
  od;
  counter:=QuoInt(counter,2);
  return counter;
end;
```

# Counts the number of "a"-roots contained in a list

```
aCount:=function (List)
  local element, counter, aList;
  aList:=["a1","a2","a3","a4"];
  counter:=0;
  for element in List do
    if (element in aList) then counter:=counter+1; fi;
  od;
  return counter;
end;
```

# Check if the list doesn't contain any invariants of type e_4 or v_4

```
e8Correct:=function (InvList)
  local list;
  for list in InvList do
    if ( partnerCount(list)=2 or
           (partnerCount(list)=0 and
            ```
((aCount(list) mod 2) = 0) 
) then 
Print(“Fail”); 
return;
fi;
od; 
Print(“Ok”); Print(“\n”);
end;

e7Transcription := function (n)
local dictionary;
if (n>7) then Print(“Transcription Fail”); return; fi;
dictionary := ["a1","b1","a2","b2","a3","b3","a4"];
return dictionary[n];
end;

e7TranscriptionList := function (list)
local element, transcription, result;
result := [ ];
for element in list do
transcription := e7Transcription(element);
Add(result, transcription); 
od;
return result;
end;

e7TranscriptionListList := function (listList)
local list, transcriptionList, result;
result := [ ];
for list in listList do
transcriptionList := e7TranscriptionList(list);
Add(result, transcriptionList);
od;
return result;
end;

e8Transcription := function (n)
local dictionary;
if (n>8) then Print(“Transcription Fail”); return; fi;
dictionary := ["a1","b1","a2","b2","a3","b3","a4","b4"];
return dictionary[n];
end;

e8TranscriptionList := function (list)
local element, transcription, result;
result := [ ];
for element in list do
transcription := e8Transcription(element);
Add(result, transcription);
od;
return result;
end;

e8TranscriptionListList := function (listList)
local list, transcriptionListList, result;
result := [ ];
for list in listList do
transcriptionListList := e8TranscriptionListList(list);
Add(result, transcriptionListList);
od;
return result;
end;

fullCheckE7 := function (URoots, PRoots)
local W, X, Y;
W := CoxeterGroup("E", 7);
X := fullCheck(W, URoots, PRoots);
Y := e7TranscriptionListList(X);
return Y;
end;
ullnameE8 := function (URoots, PRoots)
local W, X, Y;
W := CoxeterGroup("E", 8);
X := fullCheck(W, URoots, PRoots);
Y := e8TranscriptionListList(X);
return Y;
end;
References

[BF] G. Berhuy and G. Favi, Essential Dimension: a Functorial Point of View (After A. Merkurjev), Documenta Math. 8, p. 279-330, 2003

[Bo] A. Borel, Linear Algebraic Groups, Graduate Texts in Mathematics 126, Springer, 1991

[Bos] S. Bosch, Algebra, fifth edition, Springer, 2004

[Bou1] N. Bourbaki, Éléments de mathématique. Algèbre, chapitres 4 à 7, Masson, 1981

[Bou2] N. Bourbaki, Éléments de mathématique. Groupes et algèbres de Lie, chapitres 4, 5 et 6, Masson, 1981.

[CH] M. Geck, G. Hiss, F. Lübeck, G. Malle, and G. Pfeiffer, CHEVIE – A system for computing and processing generic character tables for finite groups of Lie type, Weyl groups and Hecke algebras, Appl. Algebra Engrg. Comm. Comput. 7, p. 175-210, 1996

[Dég1] F. Déglise, Modules homotopiques avec transferts et motives génériques, PhD Thesis, Université Paris VII, 2002

[Dég2] F. Déglise, Modules homotopiques (Homotopy modules), preprint, arXiv: 0904.4747v2 [math.AG]

[DG] M. Demazure, P. Gabriel, Groupes algébriques, North-Holland, 1970

[Ei] D. Eisenbud, Commutative Algebra With a View Towards Algebraic Geometry, third corrected printing, Graduate Texts in Mathematics 150, Springer, 2004

[EGA I] A. Grothendieck and J. Dieudonné, Éléments de géométrie algébrique I. Le langage des schémas, Publications Mathématiques de l’IHÉS 4, 1960

[EGA II] A. Grothendieck and J. Dieudonné, Éléments de géométrie algébrique II. Étude globale élémentaire de quelques classes de morphismes, Publications Mathématiques de l’IHÉS 8, 1961

[EGA IV] A. Grothendieck and J. Dieudonné, Éléments de géométrie algébrique IV. Étude locale des schémas et des morphismes de schémas, Publications Mathématiques de l’IHÉS 20, 24, 28, 32, 1964-1967

[EKM] R. Elman, N. Karpenko, A. Merkurjev, The algebraic and geometric theory of quadratic forms, AMS Colloquium Publications vol. 56, American Mathematical Society, 2008

[EP] A.J. Engler and A. Prestel, Valued Fields, Springer Monographs in Mathematics, Springer, 2005

[Fu] W. Fulton, Intersection Theory, second edition, Springer, 1998

[GIT] D. Mumford, J. Fogarty, F. Kirwan, Geometric invariant theory, third enlarged edition, Springer, 1994

[GMS] S. Garibaldi, A. Merkurjev and J.-P. Serre. Cohomological invariants in Galois cohomology, AMS University Lecture Series vol. 28, American Mathematical Society, 2003

[Hh] R. Hartshorne, Algebraic Geometry, Graduate Texts in Mathematics 52, Springer, 1977

[Hu] J.E. Humphreys, Reflection Groups and Coxeter Groups, Cambridge Univ. Pr., 1990

[KMRT] M.-A. Knus, A. Merkurjev, M. Rost, J.-P. Tignol, The book of involutions, AMS Colloquium Publications vol. 44, American Mathematical Society, 1998.

[Lam] T.Y. Lam, The algebraic theory of quadratic forms, Benjamin, 1973

[Ma] H. Matsumura, Commutative ring theory, Cambridge Univ. Pr., 1986

[Mi] J. Milne, Étale cohomology, Princeton Univ. Pr., 1980

[Mo1] F. Morel, Sur les puissances de l’idéal fondamental de l’anneau de Witt, Comment. Math. Helv. 79(4), p. 689-703, 2004

[Mo2] F. Morel, A1-algebraic topology, International Congress of Mathematicians. Vol. II, pp. 1035-1059, 2006

[Mo3] F. Morel, A1-Algebraic Topology over a Field, Lecture Notes in Mathematics, 2052, Springer, 2012
[MV] F. Morel and V. Voevodsky, $A^1$-homotopy theory of schemes, Publications Mathématiques de l’IHÉS 90, p.45-143, 1999

[NK] J. Neukirch, Algebraische Zahlentheorie, Springer, 1992

[OVV] D. Orlov, A. Vishik and V. Voevodsky, An exact sequence for $K^M/2$ with applications to quadratic forms, Annals of Math. 165(1), p. 1-13, 2007

[Ro] M. Rost, Chow groups with coefficients, Documenta Math. 1, p. 319-393, 1996

[Se1] J.-P. Serre, Cohomologie Galoisienne, Lecture Notes in Math. 5, Springer, 1964

[Se2] J.-P. Serre, Corps locaux, fourth edition, Hermann, 1968

[SGA1] A. Grothendieck, Revêtements Étales et Groupe Fondamental, Lecture Notes in Math. 224, Springer, 1971

[SGA3] M. Demazure and A. Grothendieck et al., Schémas en Groupes, Lecture Notes in Math. 151, 152, 153, Springer, 1970

[St] J. R. Stembridge, coxeter/weyl version 2.4, Maple package, 2004, http://www.math.lsa.umich.edu/jrs/maple.html

[Sw] J.A. Swenson, The mod-2 Cohomology of Finite Coxeter Groups, PhD Thesis, University of Minnesota, 2006

[Voe] V. Voevodsky, Reduced power operations in motivic cohomology, Publications Mathématiques de l’IHÉS 98, p. 1-57, 2003