Habilitation à diriger des recherches

INSTITUT DE RECHERCHE MATHÉMATIQUE AVANCÉE

UMR 7501

Strasbourg

Université de Strasbourg
Spécialité MATHÉMATIQUES

Pierre Guillot

Representations and Cohomology of Groups

Soutenue le 2 octobre 2012
devant la commission d'examen

Hans-Werner Henn, garant
Alejandro Ádem, rapporteur
Fabien Morel, rapporteur
Pierre Vogel, rapporteur
Vladimir Fock, examinateur

www-irma.u-strasbg.fr

Institut de Recherche Mathématique Avancée

UNIVERSITÉ DE STRASBOURG

Contents

Foreword

What is this document?

The *habilitation*, for some, is the occasion to write up a survey of one's area of expertise, perhaps with a personal perspective. Though I have always kept an eye on algebraic topology, my own research has taken me into various directions since it started about ten years ago, and I feel that there is not a single subject which is *what I do*. As a result I have not found it appropriate to write this thesis in the state-of-the-art style.

If I have had a guiding principle during the preparation of this document, it was one of *usefulness*. That is, to a reader who is interested in learning about my research, this work is supposed to be useful, and a time-saver. (Likewise, reading this introductory words to the end should help.)

With this purpose in mind, I have decided to group the chapters according to the technical tools that they require the reader to know. Chapter 1 and chapter 2 have, all in all, very different objectives; however since they both involve Steenrod operations, I can imagine the reader, after brushing up on these, willing to read them in succession. Likewise chapter 3 on links will discreetly guide the reader towards R-matrices, which show up in the final chapter for considerably different reasons. Hopefully such an organization will give this document, which was running the danger of becoming a collection of unrelated results, some of the *marabout-bout de ficelle-selle de cheval* harmony.

Let me add that you will find in the text a certain number of paragraphs reproduced from my papers with little or no changes. To me for example chapter 3 looks very much like the paper [CG] with all proofs removed. For some other sections, the presentation differs significantly from that in the original sources. Again, the goal is efficiency, and the motto is *read this first*.

How are the chapters organized?

My different papers are not given equal consideration in this thesis. Priority has been given to the more recent ones. In order to discuss this it will be helpful to have the list of my publications at hand, with the journals and other useful details relegated to the bibliography.

[Gui04] *Chow rings and cobordism of Chevalley groups*, 2004.

[Gui05] *Steenrod operations on the Chow ring of a classifying space*, 2005.

[Gui07a] *The Chow rings of G_2 and $Spin_7$*, 2007.

[Gui07c] *The representation ring of a simply connected Lie group as a λ-ring*, 2007.

[Gui07b] *Geometric methods for cohomological invariants*, 2007.

[Gui10] *The computation of Stiefel-Whitney classes*, 2009.

[GK10] (with C. Kassel) *Cohomology of invariant Drinfeld twists on group algebras*, 2010.

[GKM12] (with C. Kassel and A. Masuoka) *Twisting algebras using non commutative torsors*, 2012.

[CG] (with G. Collinet) *A link invariant with values in the Witt ring*, to appear.

[GM] (with J. Mináč) *Milnor K-theory and the graded representation ring*, preprint.

[Gui12] *Examples of quantum algebra in positive characteristic*, preprint.

This document has four numbered chapters, each dedicated to the description of a single paper, namely [Gui10], [GM], [CG], [GK10], in this order. Chapter 4 also incorporates the improvements obtained recently in [Gui12].

In addition, there are two appendices giving background information (on classifying spaces and braids, respectively). These are not specifically related to my own work, and are here for convenience.

What about the other papers?

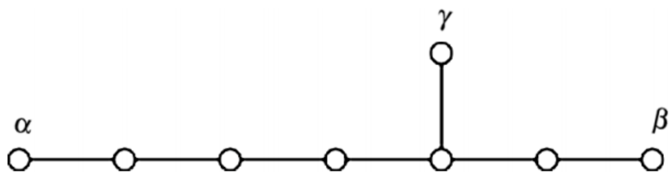
My early research dealt with Chow rings of classifying spaces. I have virtually turned away from that subject completely, and did not feel the desire to describe it in detail. Instead, they form the subject of the third appendix. Also in chapter 1 we mention [Gui05] briefly.

The paper [GKM12] is presented in appendix A. This special treatment is justified, in my view, by the high technicality of the main result in that article. Rather than indulge in the details, I have included an explicit example of application, which fitted well together with the material in this appendix.

Finally it seems that [Gui07c] has been entirely left out. Let me explain its main point:

$\longrightarrow$ Theorem 0.1 – *The representation ring of a compact Lie group is generated, as a λ-ring, by as many generators as there are branches in the Dynkin diagram.*

For example E_8 has the following Dynkin diagram:



So $R(E_8)$ has three generators as a λ-ring, and more precisely the result in *loc. cit.* specifies that

$$R(E_8) = \mathbb{Z}[\alpha, \lambda^2\alpha, \lambda^3\alpha\lambda^4\alpha, \beta, \lambda^2\beta, \gamma, \delta],$$

where δ can be taken to be any of $\lambda^5\alpha$, $\lambda^3\beta$, or $\lambda^2\gamma$.

What are the arrows for?

Some statements, such as theorem 0.1 above, are decorated with an arrow in the left margin. This is an indication that the result in question was obtained by myself, possibly in collaboration with a coauthor. The aim is to distinguish my own work from the background material, which is abundant.

Chapter 1

Steenrod operations & Stiefel-Whitney classes

In this chapter we describe the paper [Gui10]. We begin with a review of Steenrod operations, which are also intensively used in the next chapter. From the point of view of *loc. cit.*, that is, explicit computations, they are intimately related to Stiefel-Whitney classes.[1]

The reader may wish to consult appendix A for recollections on Stiefel-Whitney classes and classifying spaces.

§1. Background

Let us write $H^*(X)$ for the mod 2 cohomology $H^*(X, \mathbb{F}_2)$ of the topological space X. Then $H^*(X)$ is not just a commutative algebra, but also a module over the *Steenrod algebra* $\mathcal{A}$ (at the prime 2). This is the quotient of the free $\mathbb{F}_2$-algebra on generators $Sq^1, Sq^2, \ldots$, subject to the Ádem relations:

$$Sq^i Sq^j = \sum_{k=0}^{[i/2]} \binom{j-k-1}{i-2k} Sq^{i+j-k} Sq^k \qquad (\text{for } i < 2j).$$

For example the action of $Sq^1 \colon H^*(X) \to H^{*+1}(X)$ is the map coming from the long exact sequence induced by the short exact sequence of coefficients

$$0 \longrightarrow \mathbb{Z}/2 \longrightarrow \mathbb{Z}/4 \longrightarrow \mathbb{Z}/2 \longrightarrow 0.$$

In general Sq^i raises degrees by i.

In a sense $\mathcal{A}$ is as large as possible, for it can be shown that any natural operation on mod 2 cohomology which commutes with the isomorphism $H^{*+1}(SX) \cong H^*(X)$ (where SX is the suspension of X) is in fact given by a Steenrod operation. Let us also mention that there is a Steenrod algebra $\mathcal{A}_p$ related to the mod p cohomology of spaces, but we shall barely mention it in this work.

This extra structure on mod 2 cohomology is a powerful tool. It is a classical example that $S^2 \vee S^4$ has the same cohomology as $\mathbf{P}^2(\mathbb{C})$ (with any coefficients), but that the Steenrod operations allow us to distinguish between these two spaces. Combined with a description of $\mathbf{P}^2(\mathbb{C})$ as a 4-ball attached to a 2-sphere via the Hopf map, this leads to an easy proof that all the suspensions of the Hopf map are homotopically non-trivial, so that $\pi_{n+1}(S^n) \neq 0$ for $n \geq 2$ ([Bre97], corollary 15.4).

§2. Example: algebraic cycles

Let us digress to describe briefly an application of Steenrod operations which made its appearance in my early paper [Gui05]. It seems reasonably typical

[1] This, independently of the possible *definition* of Stiefel-Whitney classes from the Steenrod operations as in [Bre97], Definition 17.1.

of the type of things one can do with the extra information provided by the operations.

Whenever X is a complex variety, there is a *cycle map*

$$CH^*X \longrightarrow H^*(X,\mathbb{Z})$$

sending a subvariety of X to the cohomology class that is Poincaré dual to its fundamental class (in Borel-Moore homology). Computing the image of the cycle map is nothing but the natural question of describing which cohomology classes have a geometrical interpretation.

Steenrod operations are instrumental in describing the corresponding map $CH^*X \otimes \mathbb{F}_2 \to H^*(X)$ modulo 2. Indeed, from the description of Sq^1 given above, we can at least see that cohomology classes coming from the reduction mod 2 of integral classes – that is classes in $H^*(X,\mathbb{Z})$, including those coming from CH^*X – must be killed by Sq^1. Much more is true, however, since Brosnan has shown ([Bro03]) that $CH^*X \otimes \mathbb{F}_2$ is also a module over $\mathcal{A}$, in a way that is compatible with the cycle map. For the formulae to work out, one has to see $CH^nX \otimes \mathbb{F}_2$ as being in cohomological degree $2n$, and the Steenrod operations of odd degree must vanish. In turn, a Steenrod operation has odd degree if and only if it belongs to the two-sided ideal generated by Sq^1 in $\mathcal{A}$.

In summary, we have the following observation.

$\longrightarrow$ Lemma 1.1 – *Let $\alpha \in H^*(X)$ be a cohomology class in the image of the cycle map $CH^*X \otimes \mathbb{F}_2 \longrightarrow H^*(X)$. Then α is killed by the Steenrod operations in the two-sided ideal generated by Sq^1.*

In [Gui10] we prove in fact that this condition is equivalent to demanding that $Q_i(\alpha) = 0$ for all $i \geq 1$, where Q_i is the i-th "Milnor derivation". This makes it obvious that the classes identified by the lemma form a ring.

The standard notation for the ring of even-degree cohomology classes killed by odd-degree Steenrod operations is $\tilde{\mathcal{O}}H^*(X)$ (the functor $\tilde{\mathcal{O}}(-)$ is adjoint to the forgetful functor, from $\mathcal{A}$-modules concentrated in even degrees to $\mathcal{A}$-modules; so one has to assume that the letter $\mathcal{O}$ comes from the French "oubli").

$\longrightarrow$ Example 1.2 – Let $X = BG$ where $G = (\mathbb{Z}/2)^n$ is elementary abelian. Then

$$H^*(BG) = \mathbb{F}_2[t_1, \ldots, t_n],$$

while

$$CH^*BG \otimes \mathbb{F}_2 = \tilde{\mathcal{O}}H^*(BG) = \mathbb{F}_2[t_1^2, \ldots, t_n^2].$$

However $\tilde{\mathcal{O}}H^*(BG)$ is not the even-degree part of $H^*(BG)$ (which contains extra classes such as t_1t_2).

In [Gui05] we prove the following.

$\longrightarrow$ Theorem 1.3 – *Let S_n denote the symmetric group on n letters. Then*

$$CH^*BS_n \otimes \mathbb{F}_2 \cong \tilde{\mathcal{O}}H^*(BS_n).$$

The analogous statement at odd primes also holds.

The same paper contains results about Chevalley groups which are similar to this one, when properly understood, but they are also harder to state. See appendix C for more on this.

§3. Position of the problem

We turn to the description of the paper [Gui10].

Goal. One of the motivations behind the paper is to address the following question: how are we to compute the effect of Sq^i on the ring $H^*(X)$, concretely? The usual definitions of Steenrod operations are too complicated to allow a direct approach; in §6 below we comment on this. Simple-minded as this will seem, we shall rely entirely on *Wu's formula* instead, which gives the answer in the case $X = BO_n$. Recall that

$$H^*(BO_n) = \mathbb{F}_2[w_1, \ldots, w_n];$$

one has then:

$$Sq^i(w_j) = \sum_{t=0}^{i} \binom{j+t-i-1}{t} w_{i-t} w_{j+t}\,.$$

(See [MS74], Problem 8-A.) This formula is universal in the sense that it tells us something about the cohomology of any space. Indeed, if E is a real vector bundle of rank n over X, then it is classified by a map $f\colon X \to BO_n$, and the map f^* is compatible with the Steenrod operations. Thus if we write $w_i(E) = f^*(w_i)$ as is traditional, we have

$$Sq^i(w_j(E)) = \sum_{t=0}^{i} \binom{j+t-i-1}{t} w_{i-t}(E) w_{j+t}(E)\,.$$

So the action of the Steenrod algebra is easy to determine on the subring of $H^*(X)$ generated by Stiefel-Whitney classes (there are simple expressions for the action of Sq^i on a product or a sum). Fortunately, there are many spaces for which the *entire* cohomology ring is generated by such classes. Thus we should look for a way to compute concretely the Stiefel-Whitney classes, and our original problem will be to a large extent solved.

This is the official goal of [Gui10]. Our emphasis is on a calculation method which would be algorithmic, so that we could trust a computer to carry it out for us on dozens of spaces, and perhaps unsurprisingly we would like to start with classifying spaces of finite groups.

Cohomology and computers. It has been known for a while that computers could deal with the cohomology of finite groups in finite time ([Car99], [Car01], [Ben04]). They can produce a presentation in terms of generators and relations, from which of course one can determine the nilradical, the Krull dimension, etc. However, Stiefel-Whitney classes are usually not computed, nor are Steenrod operations, and this makes the output a little different than that which would be produced by a human.

To illustrate this discussion, let us focus on the example of Q_8, the quaternion group of order 8. On Jon Carlson's webpage, or David Green's or Simon King's, one will find that $H^*(BQ_8)$ is an algebra on generators z, y, x of degree $1, 1, 4$ respectively, subject to the relations $z^2 + y^2 + zy = 0$ and $z^3 = 0$. On the other hand, if we look at the computation by Quillen of the cohomology of extraspecial groups (see [Qui71]), one finds in the case of Q_8 (with a little rewriting):

Proposition 1.4 – *There are 1-dimensional, real representations r_1 and r_2 of Q_8, and a 4-dimensional representation Δ, such that $H^*(BQ_8, \mathbb{F}_2)$ is generated by $w_1(r_1)$, $w_1(r_2)$ and $w_4(\Delta)$. The ideal of relations is generated by $R = w_1(r_1)^2 + w_1(r_2)^2 + w_1(r_1)w_1(r_2)$ and $Sq^1(R)$.*

Finally, $Sq^1(\Delta) = Sq^2(\Delta) = Sq^3(\Delta) = 0$.

(Recall that the action of the Steenrod algebra on $w_1(r_i)$ need not be spelled out, for we always have $Sq^1(x) = x^2$ and $Sq^i(x) = 0$ for $i > 1$, whenever x is a cohomology class of degree 1.)

Clearly this is better. Note also that Stiefel-Whitney classes give some geometric or representation-theoretic meaning to the relations in the cohomology of a group, in good cases. In the case of Q_8 thus, there is a relation between the representations mentioned in proposition 1.4, namely:

$$\lambda^2(\Delta) = r_1 + r_2 + r_1 \otimes r_2 + 3$$

(here "+3" means three copies of the trivial representation, and λ^2 means the second exterior power). There are formulae expressing the Stiefel-Whitney classes of a direct sum, a tensor product, or an exterior power. In the present case, they give $w_2(r_1 + r_2 + r_1 \otimes r_2 + 3) = w_1(r_1)^2 + w_1(r_2)^2 + w_1(r_1)w_1(r_2)$, while $w_2(\lambda^2(\Delta)) = 0$. The latter takes into account the fact that $w_1(\Delta) = w_2(\Delta) = w_3(\Delta) = 0$, which in turn is a formal consequence of the fact that Δ carries a structure of $\mathbb{H}$-module, where $\mathbb{H}$ is the algebra of quaternions. Putting all this together, we get an "explanation" for the relation $R = 0$ based on representation theory.

§4. Strategy

Our goal is thus the computation of Stiefel-Whitney classes, and of Steenrod operations as a result. Again we point out that a direct approach using the definitions is hardly possible (see §6), so we are looking for an alternative way to get at the answer. Here is now an outline of the method which we describe in [Gui10].

Given a group G, we shall always assume that we have a presentation of $H^*(BG)$ as a ring available. We shall then define a ring $\mathcal{W}_F(G)$ as follows. As a graded $\mathbb{F}_2$-algebra, $\mathcal{W}_F(G)$ is to be generated by formal variables $w_j(r_i)$ where the r_i's are the irreducible, real representations of G. Then we impose all the relations between these generators which the theory of Stiefel-Whitney classes predicts: relations coming from the formulae for tensor products and exterior powers, rationality conditions, and so on. (It is perhaps more accurate to say that we impose all the relations that we can think of.)

Then one has a map[2] $a : \mathcal{W}_F(G) \to H^*(BG)$ sending $w_i(r_j)$ to the element with the same name in $H^*(BG)$. This map has good properties: namely, it is an isomorphism in degree 1, and turns the cohomology of G into a *finitely generated* module over $\mathcal{W}_F(G)$. The key point is that, in fact, there are *very few* maps between these two rings having such properties (in practice, there are so many relations in $\mathcal{W}_F(G)$ that there are few well-defined maps out of this ring anyway).

The slight twist here is that, unlike what you might expect, *we do not compute the effect of the map a*. Rather, we write down an exhaustive list of all the maps $\mathcal{W}_F(G) \to H^*(BG)$ having the same properties as a, and it turns out, most of the time, that all these maps have the same kernel and "essentially" the same image. More often than not, all the maps are surjective; let us assume in this outline that it is so for a given G, ignoring the more difficult cases. Since a is among these maps (without our knowing which one it is!), we know its kernel, and we have a presentation of $H^*(BG)$ as a quotient of $\mathcal{W}_F(G)$, that is a presentation in terms of Stiefel-Whitney classes. The computation of Steenrod operations becomes trivial.

As a toy example, we may come back to $G = Q_8$. In this case one has

$$\mathcal{W}_F(G) = \frac{\mathbb{F}_2[w_1(r_1), w_1(r_2), w_4(\Delta)]}{(R, Sq^1(R))}$$

where $R = w_1(r_1)^2 + w_1(r_2)^2 + w_1(r_1)w_2(r_2)$. It is apparent that $\mathcal{W}_F(G)$ is abstractly isomorphic with $H^*(G)$; Quillen's theorem states much more specifically that the map a is an isomorphism. Our approach, reducing to something trivial here, is to note that there are only two classes in degree 4 in the cohomology ring, namely 0 and an element x which generates a polynomial ring. If the image under a of the Stiefel-Whitney class $w_4(\Delta)$ were 0, then $H^*(G, \mathbb{F}_2)$

[2] The letter a was for "actual", but I regret this choice now.

could not be of finite type over $\mathcal{W}_F(G)$. Thus $a(w_4(\Delta)) = x$. Since a is an isomorphism in degree 1, it must be surjective; for reasons of dimensions it is an isomorphism. In this fashion we recover Quillen's result from a presentation of the cohomology ring and a simple game with $\mathcal{W}_F(G)$, and this (in spirit if not in details) is what our program will do. Now, describing $\mathcal{W}_F(G)$ explicitly is extremely long if one proceeds manually, but it is straightforward enough that a computer can replace us.

§5. Overview of results

The paper has a companion, in the form of a computer program. The source and the results of the computer runs can be consulted on my webpage. We encourage the reader to have a look at this page now; indeed, our main result is this very page.

It is in the nature of our algorithm that it does not work in all cases, but our basic method can be adjusted for specific groups and made to work in new cases by small, taylored improvements. Our original goal however was to constitute, if not a "database", at least a significant collection of examples (rather than deal with a handful of important groups). Let us try to condense some of it into a theorem.

⟶ Theorem 1.5 – *For the 5 groups of order 8, for 13 of the 14 groups of order 16, for 28 of the 51 groups of order 32, and for 61 of the 267 groups of order 64, the subring of the cohomology ring generated by Stiefel-Whitney classes is entirely described. All Stiefel-Whitney classes and Chern classes are given.*

There are only 13 of these groups for which this subring is not the whole cohomology ring. In all these cases, elements are explicitly given which are not combinations of Stiefel-Whitney classes.

For the remaining $107 - 13 = 94$ *groups, the Steenrod operations are entirely described.*

In other words, for 107 groups we have a statement similar to proposition 1.4, proved by a computer and located on my webpage.

Whenever we know the effect of the Steenrod operations, we can in principle compute the subring $\tilde{O}H^*(G)$, as in §2. In practice though, the computation sometimes just takes too long.

⟶ Theorem 1.6 – *For 62 of the above groups, the ring $\tilde{O}H^*(G)$ is completely computed. In 38 cases the classes in this ring are combinations of Chern classes, and it follows that the image of*

$$CH^*BG \otimes \mathbb{F}_2 \to H^*(BG)$$

is precisely $\tilde{O}H^*(G)$.

Having this little collection of cohomology rings at your disposal, it becomes possible to test your conjectures, or simply observe. For example, note the following.

⟶ Theorem 1.7 – *There exist two finite groups, one isomorphic to a semi-direct product $\mathbb{Z}/8 \rtimes \mathbb{Z}/4$ and the other isomorphic to a semi-direct product $\mathbb{Z}/4 \rtimes \mathbb{Z}/8$, and an isomorphism between their cohomology rings which is compatible with the Steenrod operations.*

(In other parlance, these rings are isomorphic "as unstable algebras".) So even with the help of Steenrod operations, these two groups cannot be distinguished by their mod 2 cohomology rings.

Examining the intermediate ring $\mathcal{W}_F(G)$ can be instructive, too. The relations which hold in this ring are certain to also hold in any ring for which we have a theory of Stiefel-Whitney classes satisfying the usual axioms. In the next chapter this will be used with the ring $\operatorname{gr} R(G)$, related to the representation ring. More precisely, the following rather technical statement revealed the feasibility of the whole of chapter 2, although the connection will seem to appear only at the very end of our presentation.

$\longrightarrow$ LEMMA 1.8 – *Consider the dihedral group D_4 of order 8. Let r_1 and r_2 be the non-trivial 1-dimensional real representations of D_4 whose Stiefel-Whitney classes satisfy*

$$w_1(r_1)\, w_1(r_2) = 0\,. \tag{*}$$

Then (*) holds in $\mathcal{W}_F(D_4)$. Thus it also holds in the ring $\operatorname{gr} R(D_4)$ of the next chapter, when $w_1(r_i)$ is understood in this ring.

§6. Open questions

PROBLEM. *Is it possible to identify more formal properties of the Stiefel-Whitney classes which, incorporated in the construction of $\mathcal{W}_F^*(G)$, make the natural map to $H^*(BG)$ injective?*

My guess is that the answer is no; in other words, that there are more relations in the cohomology ring, even just among Stiefel-Whitney classes, than can be formally predicted from representation theory. This is a difficult question.

Here is an obvious problem, which will appeal to the mathematician with an inclination for programming:

PROBLEM. *Can you compute algorithmically the Stiefel-Whitney classes in the cohomology of any finite group?*

Here we ask for a complete computation, say providing explicit cocycle representatives.

In the appendix to [Gui10] we study this problem. In particular we establish that the computation can be carried over in finite time, and propose several angles of attack: the Evens norm and formulae for the Stiefel-Whitney classes of an induced representation; a combinatorial version of the Thom isomorphism; the use of representations over finite fields and lifts to characteristic 0. We describe these with quite a lot of details.

Thus the answer to the question is yes in principle, but in practice the implementation is a challenge.

Chapter 2

K-theory, real and Milnor

Let us turn to [GM]. At the heart of this paper is a result in algebraic topology, which states that the mod 2 cohomology of any space X has a canonical subquotient, to be denoted by $\mathcal{W}^*(X)/\mathcal{I}_X$ in this chapter. This subquotient is the target of a map defined on a ring related to the real K-theory of X, and the situation is analogous, in a sense to be made precise, to that of the classical Chern character.

With this new tool at our disposal, we are able to compute certain graded rings associated to the representation rings of finite groups. Considering an absolute Galois group (which is profinite), we obtain an object which appears to be related to Milnor K-theory.

§1. The operations θ_n

We start with a question which on the surface appears to be purely computational. Let E be a real vector bundle over a space X. It has Stiefel-Whitney classes $w_1(E)$, $w_2(E)$, …, $w_n(E) \in H^*(X)$. We have not yet mentioned the fact that $H^1(X) = H^1(X, \mathbb{F}_2) = [X, \mathbf{P}^\infty(\mathbb{R})]$ = the group of line bundles over X, up to isomorphism. If $t \in H^1(X)$, and if L is the corresponding line bundle, one has $w_1(L) = t$, essentially by definition.

Here is a simple question: if $L_1, \ldots, L_n$ correspond to $t_1, \ldots, t_n$ respectively, and if

$$\rho = (L_1 - 1) \cdots (L_n - 1),$$

what are the Stiefel-Whitney classes of ρ, at least in low degrees? Here ρ lives in $K(X)$, the real K-theory of X, of which more later.

Example 2.1 – Here are some examples for small values of n. For $n = 1$ we have $w_1(L_1 - 1) = w_1(L) = t_1$. For $n = 2$, let $\rho = (L_1 - 1)(L_2 - 1)$, then $w_1(\rho) = 0$ and $w_2(\rho) = t_1 t_2$.

For $n = 3$, let $\rho = (L_1 - 1)(L_2 - 1)(L_3 - 1)$, then $w_1(\rho) = w_2(\rho) = w_3(\rho) = 0$ and

$$w_4(\rho) = t_1^2 t_2 t_3 + t_1 t_2^2 t_3 + t_1 t_2 t_3^2 = Sq^1(t_1 t_2 t_3).$$

For $n = 4$, let $\rho = (L_1 - 1)(L_2 - 1)(L_3 - 1)(L_4 - 1)$, then $w_i(\rho) = 0$ for $1 \le i \le 7$ and

$$\begin{aligned} w_8(\rho) &= t_1^4 t_2^2 t_3 t_4 + t_1^2 t_2^4 t_3 t_4 + t_1^4 t_2 t_3^2 t_4 + t_1 t_2^4 t_3^2 t_4 + t_1^2 t_2 t_3^4 t_4 + \\ & \quad t_1 t_2^2 t_3^4 t_4 + t_1^4 t_2 t_3 t_4^2 + t_1 t_2^4 t_3 t_4^2 + t_1^2 t_2^2 t_3^2 t_4^2 + t_1 t_2 t_3^4 t_4^2 + \\ & \quad t_1^2 t_2 t_3 t_4^4 + t_1 t_2^2 t_3 t_4^4 + t_1 t_2 t_3^2 t_4^4 \\ &= (Sq^3 Sq^1 + Sq^4)(t_1 t_2 t_3 t_4). \end{aligned}$$

These examples should make the following result plausible.

⟶ Theorem 2.2 – *The Stiefel-Whitney classes of* $\rho = (L_1 - 1) \cdots (L_n - 1)$ *satisfy* $w_i(\rho) = 0$

for $1 \le i < 2^{n-1}$, *and*

$$w_{2^{n-1}}(\rho) = \sum_{2^{r_1}+\cdots+2^{r_n}=2^{n-1}} t_1^{2^{r_1}} \cdots t_n^{2^{r_n}}\,.$$

In [GM] this is theorem 2.1 combined with lemma 2.5. Incidentally the proof of this lemma is one of my favourites.

⟶ Corollary 2.3 – *For* $n \ge 1$ *there exists a Steenrod operation* θ_n, *of degree* $2^{n-1} - n$, *such that*

$$w_{2^{n-1}}((L_1 - 1)\cdots(L_n - 1)) = \theta_n(t_1 t_2 \cdots t_n)\,.$$

To see that the corollary follows from the theorem, we are going to rely on Milnor's description of the dual $\mathcal{A}^*$ of the Steenrod algebra, see [Mil58]. Recall that

(1) $\mathcal{A}^*$ is polynomial on variables ζ_i in degree $2^i - 1$.

(2) For any space X, there is a map *of rings*

$$\lambda^* \colon H^*(X) \to H^*(X) \otimes \mathcal{A}^*\,,$$

such that, for any Steenrod operation θ and element $x \in H^*X$, we can recover θx by evaluating $\lambda^*(x)$ at θ.

(3) For $X = B\mathbb{Z}/2$, whose cohomology is $\mathbb{F}[t]$, one has

$$\lambda^*(t) = \sum t^{2^i} \otimes \zeta_i\,.$$

This allows the computation of $\lambda^*(t_1 \cdots t_n)$ in our situation. If we define

$$Sq(i_1, i_2, \ldots, i_k)$$

to be the Steenrod operation dual to $\zeta_1^{i_1} \cdots \zeta_k^{i_k}$, we may put

$$\theta_n = \sum Sq(i_1, \ldots, i_k)$$

where the sum runs over all the elements which have the right degree, that is $2^{n-1} - n$. It is clear that the corollary then holds.

It is apparent that the operations θ_n are not uniquely defined by the requirement of the corollary. However, these particular operations were considered in a different context in the work [BF91] by Benson and Franjou (see also the computations by Adams [Ada92]). Furthermore, we want to point out the following alternative description. The Steenrod algebra $\mathcal{A}$ is a Hopf algebra, and is equipped with an antipode $c \colon \mathcal{A} \to \mathcal{A}$. It turns out that

$$\theta_n = c(Sq^{2^{n-1}-n})\,,$$

see §7, corollary 6 in [Mil58].

§2. The ideal

We need a piece of notation to describe the most important consequence of the last theorem and corollary. Let $\mathcal{W}^*(X)$ denote the subring of $H^*(X)$ generated by all the Stiefel-Whitney classes of real vector bundles over X. When $X = BG$, we see that $\mathcal{W}^*(BG)$ is the image of the "formal" ring $\mathcal{W}_F^*(G)$ described earlier in the previous chapter (there is a little something to prove here, which was done in lemma 3.9 (1) in [GM]).

⟶ Theorem 2.4 – *Define*

$$\mathcal{I}_X = \{x \in \mathcal{W}^*(X) : \theta_{|x|}\, x = 0\}\,,$$

where $|x|$ *is the degree of* x. *Then* $\mathcal{I}_X$ *is an ideal in* $\mathcal{W}^*(X)$.

See corollary 2.8 in [GM]

⟶ Example 2.5 – Let $X = BG$ where $G = (\mathbb{Z}/2)^n$. Then $H^*(BG) = \mathcal{W}^*(BG)$ and this ring is polynomial on classes $t_1, t_2, \dots, t_n$ in degree 1. Then $\mathcal{I}_X$ is the ideal generated by the elements

$$t_i^2 t_j = t_i t_j^2 .$$

⟶ Example 2.6 – The ideal $\mathcal{I}_X$ is described in the case of

$$X = BO_\infty \times BO_\infty \times \cdots \times BO_\infty .$$

This yields universal relations belonging to $\mathcal{I}_X$ for any space X (proposition 2.11 in *loc. cit.*). For example, let E be any real vector bundle over X, and let n be an integer. Write n in base 2 as

$$n = \sum_s a_s 2^s .$$

Then one has

$$w_n(E) = \prod_s w_{2^s}(E)^{a_s} \qquad \mod \mathcal{I}_X .$$

For instance as $5 = 1 + 4$ one always has

$$w_5(E) = w_1(E) w_4(E) \qquad \mod \mathcal{I}_X .$$

§3. Real K-theory

The importance of the subquotient $W^*(X)/\mathcal{I}_X$ will be exposed when we relate it to real K-theory. Let us start however with a few recollections of classical results. As a reference for these, see [FL85].

Let $KU(X)$ be the *complex* K-theory of the space X. Complex vector bundles have Chern classes. By taking a suitable combination of these, one constructs the *Chern character*

$$Ch\colon KU(X) \longrightarrow H^{2*}(X, \mathbb{Q}),$$

which is a ring homomorphism.

When X is nice enough (eg when X is finite CW-complex, or an algebraic variety), the Chern character induces an isomorphism $KU(X) \otimes \mathbb{Q} \cong H^{2*}(X, \mathbb{Q})$. However this does not hold for $X = BG$ for a finite group G, for example. Besides, since we have $H^*(BG, \mathbb{Q}) = 0$ in degrees $* > 0$ in this case, this ring is uninteresting.

We will define an analogous map using real vector bundles, Stiefel-Whitney classes and mod 2 cohomology. Its target will be $W^*(X)/\mathcal{I}_X$. However, the source will not quite be $K(X) = KO(X)$, but a certain associated graded ring.

To describe it, start with any λ-ring K. Thus K has operations $\lambda^n\colon K \to K$, typically defined using exterior powers. We are of course thinking of the example $K = K(X)$, but we shall also be dealing with $K = R(G, \mathbb{K})$, the representation ring of the finite group G over the field $\mathbb{K}$.

Grothendieck has introduced another set of operations, with many good properties. Put

$$\gamma^n(x) = \lambda^n(x + n - 1) .$$

Also, define $\Gamma^n \subset K$ to be the abelian group generated by all the elements

$$\gamma^{i_1}(x_1) \cdots \gamma^{i_s}(x_s) \quad \text{with} \quad \sum_k i_k \geq n ,$$

where x_i has rank 0. It is easy to show that each Γ^n is an ideal in K. The associated graded ring $\operatorname{gr} K$ is defined to be

$$\operatorname{gr} K = \Gamma^0/\Gamma^1 \oplus \Gamma^1/\Gamma^2 \oplus \Gamma^2/\Gamma^3 \oplus \cdots$$

The source of our map will be $\operatorname{gr} K(X)$. In order to convince the reader that we are not straying far from the complex case, let us resume our review of the classical theory.

The *algebraic Chern classes* of $x \in K$ are defined by

$$c_i(x) = \gamma^i(x - \varepsilon(x)) \in \operatorname{gr}^i K = \Gamma^i/\Gamma^{i+1}\,.$$

Here $\varepsilon(x)$ is the rank of x. The axioms for the λ-operations have the following easy-to-remember consequence: the classes c_i obey the same rules as the usual (topological) Chern classes.

A classical theorem of Grothendieck's states that, under familiar assumptions on K, the algebraic Chern classes can be combined into a ring homomorphism

$$Ch\colon K \otimes \mathbb{Q} \longrightarrow \operatorname{gr} K \otimes \mathbb{Q},$$

which is an isomorphism, also called the Chern character. Appealing to both Chern characters, we see that there is an isomorphism

$$\operatorname{gr} KU(X) \otimes \mathbb{Q} \to H^{2*}(X, \mathbb{Q})$$

in good cases, and it sends $c_i(E) \in \operatorname{gr} KU(X) \otimes \mathbb{Q}$ to the element with the same name in $H^{2*}(X, \mathbb{Q})$. Our own map is an analog of *that*.

$\longrightarrow$ Theorem 2.7 – *Let $K(X) = KO(X)$ be the* real *K-theory of X. There exists a ring homomorphism*

$$\omega\colon \operatorname{gr} K(X) \otimes \mathbb{F}_2 \longrightarrow \mathcal{W}^*(X)/\mathcal{I}_X$$

which sends the algebraic Chern class $c_i(x)$ to the Stiefel-Whitney class $w_i(x)$.

See theorem 3.6 in [GM].

§4. Graded representation rings

In most applications, we shall exploit the natural map

$$R(G, \mathbb{R}) \longrightarrow K(BG),$$

sending a representation $\rho\colon G \to O_n$ to the vector bundle whose classifying map is $B\rho\colon BG \to BO_n$. As it is a map of λ-rings, we eventually get maps

$$\operatorname{gr} R(G, \mathbb{R}) \otimes \mathbb{F}_2 \longrightarrow \operatorname{gr} K(BG) \otimes \mathbb{F}_2 \xrightarrow{\omega} \mathcal{W}^*(BG)/\mathcal{I}_{BG}\,.$$

Let us comment that it would be unrealistic to hope for more, that is, to try and construct a reasonable map of rings from $\operatorname{gr} R(G, \mathbb{R})$ (or even from $R(G, \mathbb{R})$ itself) into $H^*(BG)$. Indeed, Quillen has shown that the 2-rank of G, that is the maximal r such that $(\mathbb{Z}/2)^r \subset G$, is equal to the Krull dimension of $H^*(BG)$. As a result, the cohomology ring is considerably larger than $\operatorname{gr} R(G, \mathbb{R})$, for which every graded piece has dimension less than the number of irreducible, real representations of G (corollary 3.3 in [GM]). So quotienting out by $\mathcal{I}_{BG}$ is necessary (to avoid trivialities).

$\longrightarrow$ Example 2.8 – When $G = (\mathbb{Z}/2)^r$, one has

$$\operatorname{gr} R(G, \mathbb{R}) \otimes \mathbb{F}_2 = \frac{\mathbb{F}_2[c_1(\rho_1), \ldots, c_1(\rho_r)]}{c_1(\rho_i)^2 c_1(\rho_j) = c_1(\rho_i) c_1(\rho_j)^2}\,,$$

where the ρ_i's are the "obvious" 1-dimensional representations. (The result holds with $\mathbb{R}$ replaced by any field of char $\neq 2$.) Indeed, it is elementary to check that the relations hold; what is more, the target of the "character" ω fits the description above, as we have seen in example 2.5. We conclude that ω is an isomorphism. There seems to be no proof avoiding use of the "character".

From this example one can deal with many others by studying elementary subgroups; the dihedral group D_4 of order 8, which plays a special role in what follows, can be studied in this fashion (proposition 3.12 in *loc. cit.*).

The rings $\operatorname{gr} R(G, \mathbb{K})$ seem to have independent interest (that is, independent from the application to Milnor K-theory which follows). They depend finely on the field $\mathbb{K}$, too. Let us briefly digress into the following example.

$\longrightarrow$ Example 2.9 – When G is cyclic, one has

$$\operatorname{gr} R(G, \mathbb{C}) \cong H^{2*}(G, \mathbb{Z}),$$

while

$$\operatorname{gr} R(G, \mathbb{R}) \otimes \mathbb{F}_2 \cong H^*(G, \mathbb{F}_2).$$

So over the complex numbers, the graded representation ring looks like integral cohomology, with degrees doubled; over the reals, it looks like mod 2 cohomology, with no doubling!

There very few, if any, computations available in the literature regarding these objects. Dealing with a cyclic group when $\mathbb{K} = \mathbb{Q}$ is a challenge.

§5. Application to Milnor K-theory

The (mod 2) Milnor K-theory of the field F (always assumed to have characteristic $\neq 2$) is a certain graded ring $k_*(F)$ defined by generators and relations (see [Mil70]). First, let $k_1(F)$ denote the $\mathbb{F}_2$-vector space $F^\times/(F^\times)^2$, written additively. The canonical map

$$\ell \colon F^\times/(F^\times)^2 \longrightarrow k_1(F)$$

satisfies thus $\ell(ab) = \ell(a) + \ell(b)$. Next, let $T^*(k_1(F))$ be the tensor algebra, and let M denote the ideal generated by the "Matsumoto relations":

$$\ell(a)\ell(b) = 0 \quad \text{for} \quad a + b = 1 .$$

Finally $k_*(F) = T^*(k_1(F))/M$. One can show that it is commutative.

Example 2.10 – Let $F = \mathbb{R}$. Then $k_1(\mathbb{R}) = \mathbb{R}^\times/(\mathbb{R}^\times)^2 = \mathbb{F}_2$, so in this case $T^*(k_1(\mathbb{R})) = \mathbb{F}_2[t]$.

When $a + b = 1$, one of a or b is > 0, and so it is a square. Thus one of $\ell(a)$ or $\ell(b)$ is 0, and the relation $\ell(a)\ell(b) = 0$ is trivial. In the end $k_*(\mathbb{R}) = \mathbb{F}_2[t]$.

There were two conjectures by Milnor, both theorems now ([Voe03], [Voe11]). Let $G = Gal(\bar{F}/F)$ be the absolute Galois group of F (it is profinite). The first states that there is an isomorphism

$$k_*(F) \xrightarrow{\cong} H^*(G, \mathbb{F}_2).$$

To state the second conjecture/theorem, let $W(F)$ be the Witt ring of F (defined in terms of quadratic forms over F, and a central player in a subsequent chapter). Let I be its fundamental ideal, and let $\operatorname{gr} W(F)$ denote the graded ring associated to the filtration by powers of I. Then there is an isomorphism

$$k_*(F) \xrightarrow{\cong} \operatorname{gr} W(F).$$

Let us offer a variant.

$\longrightarrow$ Theorem 2.11 – *Let $\mathbb{K}$ be a field of char $\neq 2$, typically $\mathbb{K} = \mathbb{Q}$. There is a natural map*

$$k_*(F) \longrightarrow \operatorname{gr} R(G, \mathbb{K}) \otimes \mathbb{F}_2$$

sending $\ell(a)$ to the 1-dimensional representation of $G = Gal(\bar{F}/F)$ given by

$$\sigma \mapsto \sigma(\sqrt{a})/\sqrt{a} = \pm 1 .$$

This is theorem 4.1 in [GM]. The proof requires computing $\operatorname{gr} R(\mathbb{Z}/4, \mathbb{K})$ and $\operatorname{gr} R(D_4, \mathbb{K})$. Studying this map requires more of the previous machinery.

Instead of $G = Gal(\bar{F}/F)$, there is an easier group to study, which contains all the information we want. Following [MS96], let E be the extension of F which is the compositum of all the extensions F'/F such that $Gal(F'/F)$ is either $\mathbb{Z}/2$, $\mathbb{Z}/4$ or D_4; and then let $\mathcal{G} = Gal(E/F)$. The group $\mathcal{G}$ is a quotient of G, and

$$H^*(G) = H^*(\mathcal{G})_{dec} \qquad (= k_*(F)).$$

(See [AKM99].) Thus the cohomological information is there within $\mathcal{G}$, but the point is that $\mathcal{G}$ has a "simple" structure. For example when $F^\times/(F^\times)^2$ is finite, the group $\mathcal{G}$ is also finite. Consider that when F is a finite field, we have $G = \hat{\mathbb{Z}}$, while $\mathcal{G} = \mathbb{Z}/4$.

$\longrightarrow$ Theorem 2.12 – *There is a natural map*

$$k_*(F) \longrightarrow (\operatorname{gr} R(\mathcal{G}, \mathbb{K}) \otimes \mathbb{F}_2)_{dec}$$

which is an isomorphism in degrees ≤ 2.

For $\mathbb{K} = \mathbb{Q}$ at least, the map in the theorem is an isomorphism in all degrees when:

- F is finite,
- F is formally real (eg $\mathbb{R} \cap \bar{\mathbb{Q}}$),
- F is local (eg $\mathbb{Q}_p$),
- F is global (eg a number field),
- ...

Proving these results always involves the character ω defined above. Note that there is no example yet for which this map is not an isomorphism.

§6. Open questions

Problem. *Is the map in theorem 2.11 always an isomorphism?*

It would be satisfactory to to know the answer in the case of number fields, for example.

Problem. *Is the map in theorem 2.12 always an isomorphism?*

For example we would like to be able to treat the case of fields whose W-group is $(\mathbb{Z}/4)^n$ (which we can deal with up to $n = 3$).

Problem. *Is there an analog of the above maps at an odd prime* p*?*

The prime 2 is of course special with respect to Milnor K-theory (which can be reduced mod p for any prime), or at least this is what is currently believed. Indeed, the isomorphism between Milnor K-theory and the graded Witt ring does not have an analog with p odd. Thus an answer to this last question would be exciting. Note that we have to look further than the representation ring, since we are after a *graded commutative* ring, rather than a graded ring which is commutative.

Problem. *Does the character* ω *have any analogs at all at odd primes?*

Problem. *Compute* $\operatorname{gr} R(\mathbb{Z}/n, \mathbb{Q})$ *for all* n.

Chapter 3

A link invariant with values in a Witt ring

In this chapter we give an overview of [CG], in which we define an isotopy invariant for oriented links by constructing a Markov function. We assume that the reader is familiar with braid groups and Markov functions; for convenience we propose a summary in appendix B. We use freely the notation from the appendix, which is standard, for example B_n, σ_i and $\hat{\beta}$ denote the braid group on n strands, the i-th standard generator, and the closure of the braid β respectively.

Since our invariant takes its values in a Witt ring, it is fit to start with a review of some classic definitions.

§1. Witt rings

A reference for all the results in this section is [MH73]. Let K be a field with involution σ. The definitions which follow can be adapted to any field, and indeed even to the case when K is a ring, but for simplicity in this document we throw in the extra assumption that K is a field of characteristic $\neq 2$.

Hermitian spaces in this context are K-vector spaces with a non-degenerate binary form h which is linear in one variable and satisfies $h(y,x) = \sigma(h(x,y))$.

Let $G(K)$ be the Grothendieck ring of this category. A *hyperbolic space* is by definition a hermitian space of the form $(V,h) \oplus (V,-h)$. Hyperbolic spaces form an ideal I in $G(K)$.

Definition 3.1 – The *hermitian Witt ring of* K is $WH(K,\sigma) = G(K)/I$. When σ is the identity, we write simply $W(K)$. ■

Remark that in the Witt ring, there is no ambiguity in writing $-V$: it is both the class of V with the opposite Hermitian form, and the opposite of the class of V. In symbols $-[(V,h)] = [(V,-h)]$.

Example 3.2 – Over $\mathbb{R}$, any bilinear form can be diagonalized with ± 1 on the diagonal. Moreover the form whose matrix is

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

is hyperbolic. As a result $W(\mathbb{R}) \simeq \mathbb{Z}$, the isomorphism being given by the signature.

Example 3.3 – As is turns out, the inclusion $\mathbb{Z} \to \mathbb{R}$ induces an isomorphism $W(\mathbb{Z}) \simeq W(\mathbb{R})$.

Example 3.4 – Let σ denote the usual conjugation in $\mathbb{C}$. Then one can show $WH(\mathbb{C},\sigma) \simeq W(\mathbb{R})$.

Example 3.5 – One has

$$W(\mathbb{F}_p) = \begin{cases} \mathbb{Z}/2 \text{ for } p = 2, \\ \mathbb{Z}/2 \times \mathbb{Z}/2 \text{ for } p \equiv 1(4), \\ \mathbb{Z}/4 \text{ otherwise}. \end{cases}$$

Example 3.6 – There is a split exact sequence

$$0 \longrightarrow W(\mathbb{Z}) \longrightarrow W(\mathbb{Q}) \longrightarrow \bigoplus_p W(\mathbb{F}_p) \longrightarrow 0.$$

More generally there is an analogous exact sequence with $\mathbb{Z}$ replaced by any principal ideal domain and $\mathbb{Q}$ by its field of fractions (and a 4-term exact sequence for any Dedekind domain). For example there is an exact sequence

$$0 \longrightarrow W(\mathbb{Q}[t]) \longrightarrow W(\mathbb{Q}(t)) \longrightarrow \bigoplus_{P \text{ irreducible}} W(\mathbb{Q}[t]/(P)) \longrightarrow 0.$$

Moreover one can show $W(\mathbb{Q}[t]) = W(\mathbb{Q})$.

Eventually the link invariant which we are about to define will take its values in the ring $W(\mathbb{Q}(t))$, and more precisely in the subring $WH(\mathbb{Q}(t), \sigma)$ where σ is the involution with $\sigma(t) = t^{-1}$.

Note that the general statement is that $WH(K, \sigma)$ injects into $W(k)$ where $k = K^\sigma$ is the fixed subfield (as in example 3.4). In the case $K = \mathbb{Q}(t)$, we have $k = \mathbb{Q}(u)$ with $u = t + t^{-1}$, so that k and K happen to be isomorphic.

§2. Maslov indices

Let V be a vector space over K. A map $h : V \times V \to K$ is called an *anti-hermitian form* when it is linear in one variable and satisfies $h(y, x) = -\sigma(h(x, y))$. The form h is called non-degenerate when the determinant of the corresponding matrix (in any basis) is non-zero.

Let V be anti-hermitian. A *lagrangian* is a subspace $\ell \subset V$ such that $\ell = \ell^\perp$. We say that V is *hyperbolic* when it is the direct sum of two lagrangians. (We could have taken this as the definition of "hyperbolic" in the hermitian case, too.)

Given a hyperbolic, non-degenerate, anti-hermitian space V with form h and three lagrangians ℓ_1, ℓ_2 and ℓ_3, we shall now describe their *Maslov index*, which is a certain element

$$\tau(\ell_1, \ell_2, \ell_3) \in WH(K, \sigma).$$

Namely, the Maslov index $\tau(\ell_1, \ell_2, \ell_3)$ is the non-degenerate space corresponding to the following hermitian form on $\ell_1 \oplus \ell_2 \oplus \ell_3$:

$$H(\mathbf{v}, \mathbf{w}) = h(v_1, w_2 - w_3) + h(v_2, w_3 - w_1) + h(v_3, w_1 - w_2).$$

(In other words, if this hermitian form is degenerate, we consider the non-degenerate space obtained by an appropriate quotient.) Historically the first example considered was with $W(\mathbb{R}) = \mathbb{Z}$, so that the Maslov "index" was originally an integer.

This construction enjoys the following properties:

(i) Dihedral symmetry:

$$\tau(\ell_1, \ell_2, \ell_3) = -\tau(\ell_3, \ell_2, \ell_1) = \tau(\ell_3, \ell_1, \ell_2).$$

(ii) Cocycle condition:

$$\tau(\ell_1, \ell_2, \ell_3) + \tau(\ell_1, \ell_3, \ell_4) = \tau(\ell_1, \ell_2, \ell_4) + \tau(\ell_2, \ell_3, \ell_4).$$

(iii) Additivity: if ℓ_1, ℓ_2 and ℓ_3 are lagrangians in V, while ℓ_1', ℓ_2' and ℓ_3' are lagrangians in V', then $\ell_i \oplus \ell_i'$ is a lagrangian in the orthogonal direct sum $V \oplus V'$ and we have

$$\tau(\ell_1 \oplus \ell_1', \ell_2 \oplus \ell_2', \ell_3 \oplus \ell_3') = \tau(\ell_1, \ell_2, \ell_3) + \tau(\ell_1', \ell_2', \ell_3').$$

(iv) Invariance: for any $g \in \mathbf{U}(V)$ (the unitary group), one has

$$\tau(g \cdot \ell_1, g \cdot \ell_2, g \cdot \ell_3) = \tau(\ell_1, \ell_2, \ell_3).$$

The term "cocycle condition" is employed because the map

$$c : \mathbf{U}(V) \times \mathbf{U}(V) \longrightarrow WH(K, \sigma)$$

defined by $c(g,h) = \tau(\ell, g{\cdot}\ell, gh{\cdot}\ell)$ is then a 2-cocycle on the unitary group $\mathbf{U}(V)$, for any choice of lagrangian ℓ. There is a corresponding central extension :

$$0 \longrightarrow WH(K, \sigma) \longrightarrow \widetilde{\mathbf{U}(V)} \longrightarrow \mathbf{U}(V) \longrightarrow 1\,,$$

in which the group $\widetilde{\mathbf{U}(V)}$ can be seen as the set $\mathbf{U}(V) \times WH(K, \sigma)$ endowed with the twisted multiplication

$$(g, a) \cdot (h, b) = (gh, a + b + c(g, h)).$$

We conclude these definitions with a simple trick. The constructions above, particularly the definition of the two-cocycle, involve choosing a lagrangian in an arbitrary fashion. Moreover, the anti-hermitian space V needs to be hyperbolic, while many spaces arising naturally are not. Thus it is useful to note the following. Starting with any anti-hermitian space (V, h), put $\mathcal{D}(V) = (V, h) \oplus (V, -h)$, where the sum is orthogonal. Then $\mathcal{D}(V)$ is non-degenerate if V is, and it is automatically hyperbolic. Indeed, for any $g \in \mathbf{U}(V)$, let Γ_g denote its graph. Then Γ_g is a lagrangian in $\mathcal{D}(V)$, and in fact $\mathcal{D}(V) = \Gamma_1 \oplus \Gamma_{-1}$. From now on, we will see Γ_1 as our preferred lagrangian. Note that there is a natural homomorphism $\mathbf{U}(V) \to \mathbf{U}(\mathcal{D}(V))$ which sends g to $1 \times g$.

§3. The main result

We are now in position to state the main result of [CG]. Start with the Burau representation

$$r_n \colon B_n \longrightarrow GL_n(\mathbb{Z}[t, t^{-1}]),$$

which is described in example B.4. Now apply to the matrix coefficients a map $\alpha \colon \mathbb{Z}[t, t^{-1}] \to K$, where K is a field with involution σ. The ring $\mathbb{Z}[t, t^{-1}]$ possesses the involution $t \mapsto t^{-1}$, and we assume that α is compatible with the involutions. The examples to keep in mind are $K = \mathbb{Q}$ or $\mathbb{R}$ or a finite field, with trivial involution and $\alpha(t) = -1$ on the one hand, and $K = \mathbb{Q}(t)$ with $\sigma(t) = t^{-1}$ and $\alpha(t) = t$ on the other.

The following lemma is crucial.

Lemma 3.7 – *The action of B_n via the Burau representation preserves the anti-hermitian form whose matrix is*

$$H = \begin{pmatrix} 0 & t^{-1}-1 & t^{-1}-1 & \cdots & t^{-1}-1 \\ 1-t & 0 & t^{-1}-1 & \cdots & t^{-1}-1 \\ 1-t & 1-t & 0 & \cdots & t^{-1}-1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1-t & 1-t & 1-t & \cdots & 0 \end{pmatrix}.$$

This form is non-denenerate for infinitely many values of n.

(In this statement we supress α from the notation.)

We end up with a map $B_n \to \mathbf{U}(V_n)$, where V_n is the anti-hermitian space over K described in the lemma. Compose with the map $\mathbf{U}(V_n) \to \mathbf{U}(\mathcal{D}(V_n))$ already mentioned, to obtain the representations

$$\rho_n \colon B_n \longrightarrow \mathbf{U}(\mathcal{D}(V_n))$$

which appear in the statement of our main theorem.

$\longrightarrow$ THEOREM 3.8 – *The two-cocycle on* $\mathbf{U}(\mathcal{D}(V_n))$ *afforded by the Maslov index, when pulled-back to* B_n *via* ρ_n*, is a coboundary. As a result, there is a homomorphism*

$$B_n \longrightarrow \mathbf{U}(\widetilde{\mathcal{D}(V_n)})$$

and so also a map $f_n\colon B_n \to WH(K,\sigma)$.

The collection $(f_n)_{n\geq 2}$ *is a Markov function, and thus defines a link invariant with values in* $WH(K,\sigma)$.

We should probably spell out this result in detail. We have defined a link invariant, which we write Θ_K. If $L=\hat{\beta}$ is the closure of the braid $\beta\in B_n$, then the invariant $\Theta_K(L)$ can be computed as $f_n(\beta)$, where f_n is defined inductively as follows. One has $f_n(\sigma_i)=0$, and for $\beta,\gamma\in B_n$ there is the relation

$$f_n(\beta\gamma) = f_n(\beta) + f_n(\gamma) + \tau(\Gamma_1, \Gamma_{r(\beta)}, \Gamma_{r(\beta\gamma)}). \tag{*}$$

Here $r=r_n\colon B_n\to \mathbf{U}(V_n)$ is the Burau representation after applying α to the matrix coefficients, and as above Γ_g is the graph of g. Should this appear a little heavy to compute, we add that we have made a SAGE script available which can take care of all the calculations (it returns a list of elements of K which are the entries of a diagonal matrix representing $\Theta_K(L)$ in the ring $WH(K,\sigma)$).

§4. Examples

Signatures. Let us start with the example of $K=\mathbb{R}$, with trivial involution, and $\alpha(t)=-1$. The above procedure yields a link invariant with values in $W(\mathbb{R})\cong\mathbb{Z}$.

However, Gambaudo and Ghys have proved in [GG05] that the invariant which is classically called *the signature of a link* is in fact given by a Markov function satisfying the relation (*) above (right after the statement of theorem 3.8). By uniqueness, $\Theta_{\mathbb{R}}(L)$ must always coincide with the signature of L.

An obvious refinement is obtained by taking $K=\mathbb{Q}$ (and still $\alpha(t)=-1$). The invariant $\Theta_{\mathbb{Q}}(L)$ lives in $W(\mathbb{Q})$. Recall the exact sequence

$$0\longrightarrow W(\mathbb{Z})\longrightarrow W(\mathbb{Q})\longrightarrow \bigoplus_p W(\mathbb{F}_p)\longrightarrow 0\,.$$

$\longrightarrow$ THEOREM 3.9 – *For each oriented link L, there is a set of primes which is an invariant of L, namely the set of those p for which* $\Theta_{\mathbb{Q}}(L)$ *maps to a non-zero element via the residue map* $W(\mathbb{Q})\to W(\mathbb{F}_p)$. *For each p the value in* $W(\mathbb{F}_p)$ *is also an invariant.*

It may be useful to point out that, even though the Burau representation at $t=-1$ only involves integer entries, the form given in lemma 3.7 does not have determinant 1, and the invariant we define does not come from $W(\mathbb{Z})$.

We need not restrict ourselves to the case $\alpha(t)=-1$, however. For example we may take $K=\mathbb{C}$ with the usual complex conjugation, and $\alpha(t)=\omega$, a complex number of module 1. All of the above generalizes. We obtain a link invariant with values in $WH(\mathbb{C})\cong\mathbb{Z}$, whose value on L will be written $\Theta_\omega(L)$.

When ω is a root of unity at least, Gambaudo and Ghys also prove in *loc. cit.* that the so-called *Levine-Tristram signature* of a link is again given by a Markov function satisfying (*), so that it must agree with $\Theta_\omega(L)$. However we can obtain another refinement. Whenever ω is algebraic, the field $K=\mathbb{Q}(\omega)$ is a number field. There is an exact sequence

$$0\longrightarrow W(\mathcal{O})\longrightarrow W(K)\longrightarrow \bigoplus_{\mathfrak{p}} W(\mathcal{O}/\mathfrak{p})\,,$$

where $\mathcal{O}$ is the ring of integers in K, and the direct sum runs over the prime ideals $\mathfrak{p}$.

⟶ Theorem 3.10 – *Let $K = \mathbb{Q}(\omega)$ as above, and let $\mathcal{O}$ denote its ring of integers. For each oriented link L, there is a set of prime ideals in $\mathcal{O}$ which is an invariant of L. For each $\mathfrak{p}$ the value in $W(\mathcal{O}/\mathfrak{p})$ is also an invariant.*

Note that $\mathcal{O}/\mathfrak{p}$ is a finite field.

The paper by Gambaudo and Ghys cited twice just above has been tremendously influencial for us, and this was somewhat obfuscated by the angle of development which we have chosen in this chapter. For a little more, see the introduction to [CG].

The case $K = \mathbb{Q}(t)$. Our favorite example is that of $K = \mathbb{Q}(t)$ with $\sigma(t) = t^{-1}$ and $\alpha(t) = t$; in some sense we shall be able recover the signatures of the previous examples from this one. We shall go into more computational considerations than above. The reader who wants to know more about the technical details should consult the accompanying Sage script, available on the authors' webpages. Conversely, this section is a prerequisite for understanding the code.

In condensed form, we are going to describe the following.

⟶ Theorem 3.11 – *There is an oriented link invariant $\Theta_{\mathbb{Q}(t)}$ with values in the hermitian Witt ring $WH(\mathbb{Q}(t), \sigma)$, where σ is the involution satisfying $\sigma(t) = t^{-1}$.*

From $\Theta_{\mathbb{Q}(t)}(L)$ we can construct a palindromic Laurent polynomial, as well as a diagram in the shape of a camembert which summarizes the values of the various signatures of L.

Consider $\beta = \sigma_1^3 \in \mathcal{B}_2$ as a motivational example. Here $L = \hat{\beta}$ is the familiar trefoil knot (see the pictures on page 44).

When computing $\Theta_{\mathbb{Q}(t)}(L)$ we are led to perform additions in $WH(\mathbb{Q}(t), \sigma)$. Since a hermitian form can always be diagonalized, we can represent any element in the hermitian Witt ring by a sequence of scalars. In turn, these are in fact viewed in $k^\times/N(K^\times)$, where as above $k = K^\sigma$ and $N : K \to k$ is the norm map $x \mapsto x\bar{x}$. Summing two elements amounts to concatenating the diagonal entries.

Let us turn to the example of the trefoil knot. We relax the notation, and write f for f_n when n is obvious or irrelevant, and we write c for the two-cocycle $c(\beta, \gamma) = \tau(\Gamma_1, \Gamma_{r(\beta)}, \Gamma_{r(\beta\gamma)})$, so we have the formula $f(\beta\gamma) = f(\beta) + f(\gamma) + c(\beta, \gamma)$. Now:

$$\begin{aligned}\Theta_{\mathbb{Q}(t)}(L) = f(\sigma_1^3) &= f(\sigma_1) + f(\sigma_1^2) + c(\sigma_1, \sigma_1^2)\\ &= f(\sigma_1) + (f(\sigma_1) + f(\sigma_1) + c(\sigma_1, \sigma_1)) + c(\sigma_1, \sigma_1^2)\\ &= 0 + 0 + 0 + c(\sigma_1, \sigma_1) + c(\sigma_1, \sigma_1^2).\end{aligned}$$

Thus $\Theta_{\mathbb{Q}(t)}(L)$ is the sum of two Maslov indices, and direct computation shows that it is represented by

$$\left[-1, 1, \frac{2t^2 - 2t + 2}{t}, -1, 1, -2\right].$$

Now, the hermitian form given by the matrix

$$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

is hyperbolic and so represents the trivial element in the Witt ring. We conclude that $\Theta_{\mathbb{Q}(t)}(L)$ is represented by the form whose matrix is

$$\begin{pmatrix} \frac{2t^2-2t+2}{t} & 0 \\ 0 & -2 \end{pmatrix}.$$

Comparing elements in the Witt ring can be tricky. For example, we need to be able to tell quickly whether this last form is actually 0 or not. In general, link invariants need to be easy to compute and compare.

To this end, we turn to the construction of a Laurent polynomial invariant. There is a well-known homomorphism $D : WH(K,\sigma) \to k^\times/N(K^\times)$ given by the *signed determinant* : given a non-singular, hermitian $n\times n$-matrix A representing an element in the Witt ring, then $D(A) = (-1)^{n+1}\det(A)$. This defines a link invariant with values in $k^\times/N(K^\times)$, and for the trefoil we have

$$D(\Theta_{\mathbb{Q}(t)}(L)) = \frac{t^2 - t + 1}{t}.$$

(Note how we got rid of the factor $4 = N(2)$.) This happens to be the Alexander-Conway polynomial of L.

For definiteness, we rely on the following lemma.

Lemma 3.12 – *Any element in $k^\times/N(K^\times)$ can be represented by a fraction of the form*

$$\frac{D(t)}{t^d},$$

where $D(t)$ is a polynomial in t, of degree $2d$, not divisible by t, and which is also palindromic.

What is more, if D has minimal degree among such polynomials, then it is uniquely defined up to a square in $\mathbb{Q}^\times$.

Here is another simple invariant deduced from $\Theta_{\mathbb{Q}(t)}$. Suppose θ is a real number such that $e^{i\theta}$ is not algebraic (all real numbers but countably many will do). The assignment $t \mapsto e^{i\theta}$ gives a field homomorphism $\mathbb{Q}(t) \to \mathbb{C}$ which is compatible with the involutions (on the field of complex numbers we use the standard conjugation). There results a map

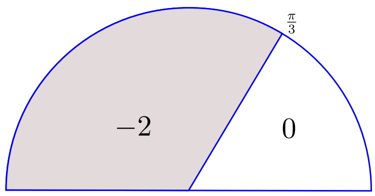
$$WH(\mathbb{Q}(t),\sigma) \longrightarrow WH(\mathbb{C}) \cong \mathbb{Z},$$

which we call the θ-signature.

Looking at the trefoil again, we obtain the form over $\mathbb{C}$

$$\begin{pmatrix} 4\cos(\theta) - 2 & 0 \\ 0 & -2 \end{pmatrix}$$

whose signature is 0 if $0 < \theta < \frac{\pi}{3}$ and -2 if $\frac{\pi}{3} < \theta < \pi$ (the diagonal entries are always even functions of θ, so we need only consider the values between 0 and π.) We may present this information with the help of a camembert :



This figure is a link invariant.

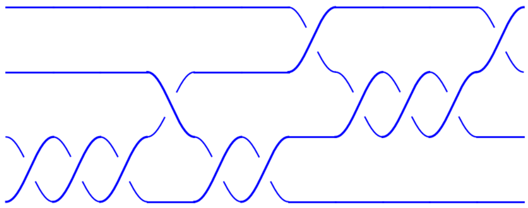
We may get rid of the restriction on θ. Given an element in $WH(\mathbb{Q}(t))$, pick a diagonal matrix as representative, and arrange to have Laurent polynomials as entries. Now substitute $e^{i\theta}$ for t, obtaining a hermitian form over $\mathbb{C}$, and consider the function which to θ assigns the signature of this form. This is a step function s, which is even and 2π-periodic.

Now, whenever θ is such that $e^{i\theta}$ is not algebraic, then $s(\theta)$ is intrinsically defined by the procedure above, and thus does not depend on the choice of representative. Since such θ are dense in $\mathbb{R}$, the following is well-defined:

$$\hat{s}(\theta) = \lim_{\alpha\to\theta, \alpha>\theta} s(\alpha).$$

It is clear by construction that $\hat{s}(\theta)$ agrees with the $e^{i\theta}$-signature of the link, presented above, for almost all θ.

To give a more complicated example, take $\sigma_1^3\sigma_2^{-1}\sigma_1^2\sigma_3^1\sigma_2^3\sigma_3^1 \in B_4$. The braid looks as follows:

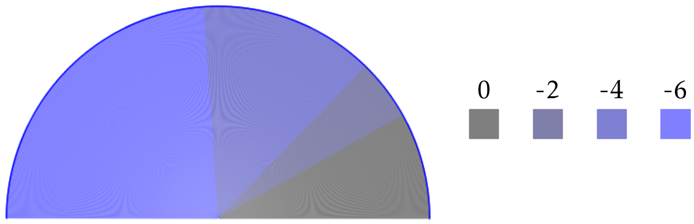


The signed determinant is

$$\frac{3t^6 - 9t^5 + 15t^4 - 17t^3 + 15t^2 - 9t + 3}{t^3},$$

where the numerator has minimal degree.

The camembert is



On my webpage the reader will find many examples of links for which the corresponding camemberts and polynomials are given.

§5. Open questions

Problem. *Generalize the construction to coloured links.*

Recall that a coloured link is one for which the connected components are distinguished. The above problem involves braid groupoids rather than braid groups, and is more technical as a result. Partial results indicate that a generalization is possible, though.

Problem. *Generalize the construction to $K = \mathbb{Z}[\frac{1}{2}, t, t^{-1}]$ rather than a field.*

Again this would be more technical. There is a reward: such an invariant would specialize to give all the other invariants Θ_K whenever K is a field of characteristic $\neq 2$. It is already apparent from the above that our invariants unify many others; a construction over $\mathbb{Z}[\frac{1}{2}, t, t^{-1}]$ would push this even further.

Chapter 4

Cohomology of Hopf algebras

In this chapter we turn to the paper [GK10], and the complements to it afforded by [Gui12]. Briefly, given a Hopf algebra $\mathcal{H}$, we are going to study a certain cohomology group $H^2_\ell(\mathcal{H})$; on the one hand, it generalizes familiar cohomological constructions, while on the other hand it is closely related to R-matrices, and thus in principle with braids. Note that we assume familiarity with the theory of R-matrices; see appendix B for a review if needed.

§1. Sweedler cohomology

Sweedler cohomology was defined in [Swe68]. Given a *cocommutative* Hopf algebra $\mathcal{H}$ and a commutative $\mathcal{H}$-module algebra A, Sweedler defines groups which we write $H^n_{sw}(\mathcal{H}, A)$ for $n \geq 0$.

How does one verify if a definition of a cohomology theory is sound? A first, shallow answer is that Sweedler's cohomology is built by imitating the classical bar construction, which in all its guises is known to produce interesting results. Also, there are long exact sequences available (and a relative version).

Perhaps more seriously, Sweedler proves that $H^2_{sw}(\mathcal{H}, A)$ classifies the extensions of $\mathcal{H}$ by A, suitably defined (note that in [Swe68] Sweedler calls them extensions of A by $\mathcal{H}$, which is confusing). This is of course a desirable property of any cohomology theory.

Finally, in the case when $\mathcal{H} = k[G]$ is the group algebra of the finite group G, one has $H^*_{sw}(\mathcal{H}, k) = H^*(G, k^\times)$ (there is a similar result for a general A and one may recover the usual cohomology of G with any coefficients by using relative Sweedler cohomology). Likewise when $\mathfrak{g}$ is a Lie algebra and $\mathcal{H} = U(\mathfrak{g})$, the universal enveloping algebra, one has $H^*_{sw}(\mathcal{H}, k) = H^*(\mathfrak{g}, k)$. So Sweedler cohomology unifies this two classical theories. It is interesting however to note that, both in the group algebra case and the universal enveloping algebra case, the cohomology groups are *Ext* functors, and so depend only on the *algebra* $\mathcal{H}$, and not on the comultiplication. Sweedler's cohomology groups on the other hand are altered if $\mathcal{H}$ is, say, isomorphic to $k[G]$ as an algebra but is endowed with a different comultiplication.

The details of the definition can be given quite compactly, so let us do so in the case $A = k$, viewed as an $\mathcal{H}$-module algebra via the augmentation map. (We shall not mention other examples for A from now on.) For each integer $n \geq 1$, we form the coalgebra $\mathcal{H}^{\otimes n}$ and define faces and degeneracies by the following formulae:

$$d_i(x_0 \otimes \cdots \otimes x_n) = \begin{cases} x_0 \otimes \cdots \otimes x_i x_{i+1} \otimes \cdots \otimes x_n & \text{for } i < n\,, \\ x_0 \otimes \cdots \otimes x_{n-1}\,\varepsilon(x_n) & \text{for } i = n\,, \end{cases}$$

and

$$s_i(x_0 \otimes \cdots \otimes x_n) = x_0 \otimes \cdots \otimes x_i \otimes 1 \otimes x_{i+1} \otimes \cdots \otimes x_n\,.$$

We are thus in the presence of a simplicial coalgebra. We may consider the monoid $Hom(\mathcal{H}^{\otimes n}, k)$, equipped with the "convolution product", which contains the group $R^n(\mathcal{H}) = Reg(\mathcal{H}^{\otimes n}, k)$ (comprised of all the invertible elements in $Hom(\mathcal{H}^{\otimes n}, k)$). Since $Reg(-, k)$ is a functor, we obtain a cosimplicial group $R^*(\mathcal{H})$ (sometimes written R^* for short in what follows).

Whenever $\mathcal{H}$ is cocommutative, R^* is a cosimplicial abelian group. Thus it gives rise to a cochain complex (R^*, d) whose differential is

$$d = \sum_{i=0}^{n+1} (-1)^i d^i$$

in additive notation, or (as we shall also encounter it)

$$d = \prod_{i=0}^{n+1} (d^i)^{(-1)^i} = d^0 (d^1)^{-1} d^2 (d^3)^{-1} \cdots$$

in multiplicative notation.

The cohomology $H^*(R^*, d)$ is by definition the Sweedler cohomology of the cocommutative Hopf algebra $\mathcal{H}$ with coefficients in k, denoted by $H^*_{sw}(\mathcal{H})$ for short.

Now suppose that $\mathcal{H}$ is a finite-dimensional Hopf algebra. Then its dual $\mathcal{K} = \mathcal{H}^*$ is again a Hopf algebra. In this situation, the cosimplicial group associated to $\mathcal{H}$ by Sweedler's method may be described purely in terms of $\mathcal{K}$, and is sometimes easier to understand when we do so.

In fact, let us start with any Hopf algebra $\mathcal{K}$ at all. We may construct a cosimplicial group directly as follows. Let $A^n(\mathcal{K}) = (\mathcal{K}^{\otimes n})^\times$ and let the cofaces and codegeneracies be defined by

$$d^i = \begin{cases} 1 \otimes id^{\otimes n} & \text{for } i = 0, \\ id^{\otimes (i-1)} \otimes \Delta \otimes id^{\otimes (n-i)} & \text{for } i = 1, \ldots, n-1, \\ id^{\otimes n} \otimes 1 & \text{for } i = n, \end{cases}$$

and

$$s^i = \begin{cases} \varepsilon \otimes id^{\otimes (n-1)} & \text{for } i = 0, \\ id^{\otimes (i-1)} \otimes \varepsilon \otimes id^{\otimes (n-i)} & \text{for } i = 1, \ldots, n-1, \\ id^{\otimes (n-1)} \otimes \varepsilon & \text{for } i = n. \end{cases}$$

When $\mathcal{K}$ is commutative, then $A^*(\mathcal{K})$ is a cosimplicial abelian group, giving rise to a cochain complex (A^*, d) in the usual way. Its cohomology $H^*(A^*, d)$ is what we call the *twist cohomology* of $\mathcal{K}$, written $H^*_{tw}(\mathcal{K})$. This terminology comes from the description of elements of degree 2, and will be justified below (see equation (†)).

Coming back to the case $\mathcal{K} = \mathcal{H}^*$ for a finite-dimensional Hopf algebra $\mathcal{H}$, it is straightforward to check that $R^*(\mathcal{H})$ can be identified with $A^*(\mathcal{K})$ (see Theorem 1.10 and its proof in [GK10] for some help; in degree 2 we have given the correspondence explicitly on page 41).

In this chapter we are chiefly interested in computing the Sweedler cohomology of $\mathcal{O}(G)$, the algebra of k-valued functions on the finite group G. This is cocommutative only when G is abelian, but we explain below what we can do with the general case. By the above, we need to look at the cosimplicial group $R^*(\mathcal{O}(G))$, which is the same as $A^*(k[G])$. It turns out to be easier to work with the latter.

§2. Lazy cohomology

When $\mathcal{H}$ is not cocommutative Sweedler's cohomology is not defined, but there is a general definition of low-dimensional groups $H^i_\ell(\mathcal{H})$ for $i = 1, 2$, called the *lazy* cohomology groups of $\mathcal{H}$, for any Hopf algebra $\mathcal{H}$: this definition is originally due to Schauenburg and is systematically explored in [BC06]. Of course when $\mathcal{H}$ happens to be cocommutative, then $H^i_\ell(\mathcal{H}) = H^i_{sw}(\mathcal{H})$. This is perfectly analogous to the construction of the non-abelian H^1 in Galois cohomology – note that $H^2_\ell(\mathcal{H})$ may be non-commutative, which is one of the highlights of [GK10].

When $\mathcal{H}$ is finite-dimensional, there is again a description of $H^i_\ell(\mathcal{H})$ in terms of the dual Hopf algebra $\mathcal{K}$. Since this is the case of interest for us, we only give the details of the definition in this particular situation (using results from [GK10], §1). Quite simply, $H^1_\ell(\mathcal{H})$ is the (multiplicative) group of central group-like elements in $\mathcal{K}$. The group $H^2_\ell(\mathcal{H})$ is defined as a quotient. Consider first the group Z^2 of all invertible elements $F \in \mathcal{K} \otimes \mathcal{K}$ satisfying

$$\Delta(a)F = F\Delta(a)$$

(here Δ is the diagonal of $\mathcal{K}$ – one says that F is *invariant*), and

$$(F \otimes 1)(\Delta \otimes id)(F) = (1 \otimes F)(id \otimes \Delta)(F) \tag{†}$$

(which says that F is a *Drinfeld twist*, as encountered in appendix A, see page 41). The group Z^2 contains the central subgroup B^2 of so-called trivial twists, that is elements of the form $F = (a \otimes a)\Delta(a^{-1})$ for a central in $\mathcal{K}$. Then $H^2_\ell(\mathcal{H}) = Z^2/B^2$.

The main topic of this chapter is the computation of the group $H^2_\ell(\mathcal{O}(G))$ for a finite group G. There are relatively few examples of calculations with lazy cohomology in the literature, so $\mathcal{O}(G)$ for non-abelian G seemed the most natural example of a non-cocommutative Hopf algebra. Before we explain our results though, we wish to say a word about Drinfeld twists, to put things in perspective.

In addition to the "torsor" point of view considered in appendix A, invertible elements $F \in \mathcal{K}\otimes\mathcal{K}$ satisfying (†) were introduced by Drinfeld in the context of R-matrices. The basic observation is that, if $\mathcal{K}$ is a Hopf algebra with R-matrix R, and if F is a Drinfeld twist, then one has another Hopf algebra $\mathcal{K}^F$ which also carries an R-matrix; one defines $\mathcal{K}^F$ to be $\mathcal{K}$ as an algebra, but endows it with the comultiplication

$$\Delta^F(x) = F\Delta(x)F^{-1}.$$

Then if we put

$$R_F = \tau_{\mathcal{K},\mathcal{K}}(F)\,R\,F^{-1},$$

one checks that R_F is an R-matrix for $\mathcal{K}^F$.

Whenever F is invariant in the above sense, one has $\mathcal{K}^F = \mathcal{K}$ as Hopf algebras, but R_F will still be different from R in general, and indeed it will mostly determine F in $H^2_\ell(\mathcal{H})$, at least when $\mathcal{H} = \mathcal{O}(G)$. We will expand on this in the rest of the chapter. For the time being, note the following: for $\mathcal{K} = k[G]$, we may take $R = 1 \otimes 1$ so that $R_F = F_{21}F^{-1}$ (with F_{21} the standard shorthand); then it is clear that $R_F = 1 \otimes 1$ whenever F is "trivial", as above, and indeed that $R_F = R_{F'}$ if F and F' represent the same class in Z^2/B^2. There is some sort of converse to this, as we will see.

Example 4.1 – Let us illustrate the above definitions in the case of an *abelian* group G, and for $k = \mathbb{C}$. Suppose we wish to compute the second Sweedler cohomology group of $\mathcal{O}(G)$ or the second twist cohomology group of $\mathbb{C}[G]$, which is the same. Then we may use the *discrete Fourier transform*, which is the isomorphism of Hopf algebras given by

$$\mathbb{C}[G] \xrightarrow{\cong} \mathcal{O}(\widehat{G}), \qquad g \mapsto \big(\chi \mapsto \chi(g^{-1})\big).$$

Here $\widehat{G} = Hom(G, \mathbb{C}^\times)$ is the Pontryagin dual of G. Applied to the group $\widehat{G}$, the discrete Fourier transform gives also an isomorphism $\mathbb{C}[\widehat{G}] \cong \mathcal{O}(G)$, and we conclude at once that

$$H^2_{tw}(\mathbb{C}[G]) = H^2_{sw}(\mathcal{O}(G)) \cong H^2_{sw}(\mathbb{C}[\widehat{G}]) \cong H^2(\widehat{G}, \mathbb{C}^\times). \tag{*}$$

(For the last isomorphism, recall that Sweedler cohomology of a group algebra is regular cohomology.)

However we can make things more explicit. Indeed a direct computation (rather than an abstract argument) shows that a twist $F \in \mathbb{C}[G] \otimes \mathbb{C}[G]$ is the same thing as a two-cocycle c on $\widehat{G}$ under the Fourier transform for the group $G \times G$; two twists define the same element in "twist cohomology" if and only if the corresponding two-cocycles differ by a coboundary. This gives (*) at once. But it gets better: an R-matrix on $\mathbb{C}[G] \otimes \mathbb{C}[G]$ corresponds to a bilinear form $\widehat{G} \times \widehat{G} \to \mathbb{C}^\times$, as is also observed in example B.8. The passage from F to $R_F = F_{21}F^{-1}$, in turn, corresponds to $c \mapsto b_c$, where b_c is the bilinear form $b_c(\sigma, \tau) = c(\tau, \sigma)c(\sigma, \tau)^{-1}$ measuring the commutativity default of c.

This we can tie up with classical results in group cohomology. When A is finite and abelian, one has

$$H_2(A, \mathbb{Z}) \cong \Lambda^2_{\mathbb{Z}}(A),$$

so that $Hom(H_2(A, \mathbb{Z}), B)$ is the set of alternating, bilinear forms on A with values in the arbitrary abelian group B. What is more, for $B = \mathbb{C}^\times$ the universal coefficients theorem gives

$$H^2(A, \mathbb{C}^\times) \cong Hom(\Lambda^2_{\mathbb{Z}}(A), \mathbb{C}^\times). \tag{**}$$

It is classical that a two-cocycle c on the left-hand side of (**) corresponds to the bilinear form b_c defined precisely as above – note that the latter is indeed alternating.

To sum up what we have learned from the abelian case: the class of a twist $F \in \mathbb{C}[G] \otimes \mathbb{C}[G]$ in $H^2_{tw}(\mathbb{C}[G])$ determines, and is determined by, a certain alternating bilinear form on the Pontryagin dual of G. Under the Fourier transform, this bilinear form is the R-matrix R_F. These remarks motivate our main theorem.

§3. The main result

We are encouraged to consider the map $F \mapsto R_F$, which is well-defined on the group $H^2_{tw}(k[G])$. Our main theorem describes its image and fibres.

So let G be a finite group. Let $\mathcal{B}(G)$ denote the set of all pairs (A, b) where A is an abelian, normal subgroup of G of order prime to the characteristic of k, and $b\colon \widehat{A} \times \widehat{A} \to k^\times$ is an alternating bilinear form on $\widehat{A}$ which is non-degenerate and G-invariant. The set $\mathcal{B}(G)$ has a distinguished element written 1, corresponding to $A = \{1\}$.

Next, let $\mathrm{Int}_k(G)$ denote the group of automorphisms of G which are induced by conjugation by elements of the normalizer of G within $k[G]^\times$. The group $\mathrm{Int}_k(G)/\mathrm{Inn}(G)$ is a subgroup of $\mathrm{Out}(G) = \mathrm{Aut}(G)/\mathrm{Inn}(G)$.

⟶ Theorem 4.2 – *Let G be any finite group, and let k be an algebraically closed field. There is a map of sets*

$$\Theta\colon H^2_{tw}(k[G]) \longrightarrow \mathcal{B}(G)$$

such that

1. *The pre-image $\Theta^{-1}(1)$ is a normal subgroup isomorphic to $\mathrm{Int}_k(G)/\mathrm{Inn}(G)$.*

2. *The fibres of Θ are the cosets of $\mathrm{Int}_k(G)/\mathrm{Inn}(G)$.*

3. *The image of Θ contains at least all the pairs (A, b) for which the order of A is odd. In particular Θ is surjective if either G has odd order or k has characteristic 2.*

The consequences of this Theorem will be explored in the next section, though we cannot delay the following

⟶ Corollary 4.3 – *The group $H^2_{tw}(k[G])$ is finite.*

Proof. The image and the fibres of Θ are finite. □

Let us say a word about the proof. The construction of Θ goes along the following steps (of course the details are to be found in [GK10]):

- To each twist F we associate the R-matrix R_F. This is well-defined.
- By a Theorem of Radford's on R-matrices ([Rad93]), there is an abelian, normal subgroup A of G such that $R_F \in k[A] \otimes k[A]$.
- By the abelian case already considered, R_F corresponds to a bilinear form b on $\widehat{A}$. Choosing A minimal in the previous step garantees that b is non-degenerate. It is obviously G-invariant.
- Consideration of the Drinfeld element of R_F shows that b is alternating.

Thus we can set $\Theta(F) = (A, b)$. In example 4.1, we have seen that R_F, and indeed any R-matrix for $k[A]$, must correspond to a twist $J \in k[A] \otimes k[A]$. However this element need not be G-invariant even if the R-matrix is. This accounts for the non-surjectivity of Θ in general. When A has odd order, we can use a trick to define c from b_c (in the notation of example 4.1).

Now let us consider the fibres of Θ. The prime question is: what can we say of F when $R_F = 1 \otimes 1$, that is when F is symmetric ($F_{21} = F$) ? The answer is in the following Lemma, which is due to Etingof.

Lemma 4.4 – *Let k be an algebraically closed field, and let $F \in k[G] \otimes k[G]$ be a symmetric twist. Then $F = (a \otimes a)\Delta(a)^{-1}$ for some $a \in k[G]$.*

Sketch. Consider the functor $\mathcal{F}$ from the symmetric monoidal category of $k[G]$-modules to that of k-vector spaces, which is defined as follows: $\mathcal{F}$ is the identity on objects and morphisms, but it sends the usual symmetry map $V \otimes W \to W \otimes V$ (defined by $v \otimes w \mapsto w \otimes v$) to the map $v \otimes w \mapsto Fw \otimes v$.

Since F is symmetric, the functor $\mathcal{F}$ is a symmetric monoidal functor, and indeed it is what Deligne calls a "fibre functor on the Tannakian category of $k[G]$-modules". Such functors form a G-torsor. Since k is algebraically closed, any torsor must be trivial. An isomorphism from $\mathcal{F}$ to the forgetful functor then yields the element a when all definitions are spelled out. □

We hasten to add that the element a in the Lemma needs not be central. So in case F is an invariant twist representing an element of $H^2_{tw}(k[G])$, we cannot quite infer from $R_F = 1 \otimes 1$ that F is "trivial". The group $\mathrm{Int}_k(G)/\mathrm{Inn}(G)$ appears precisely as a measure of this subtlety.

The attentive reader will have noticed a couple of improvements in the statement of the Theorem as we have just given it, compared to the original in [GK10]. The first is the remark that $N = \mathrm{Int}_k(G)/\mathrm{Inn}(G)$ is a *normal* subgroup. In *loc. cit.* this was left out, though we did establish the hard part, which is the fact that the fibres of Θ are the *left* cosets of N; that is if $\Theta(J_1) = \Theta(J_2)$ then $J_2 = FJ_1$ for $F \in N$. However a trivial calculation shows that $R_{JF} = J_{21} R_F J^{-1}$, from which it follows that $R_{JF} = R_J$ if $F \in N$. As a result, the right cosets of N are included in left cosets, and N must be normal.

A little more serious is the fact that subgroups A whose order is not prime to p can be discarded in the construction of $\mathcal{B}(G)$. This was proved in [Gui12], and follows from:

⟶ Theorem 4.5 – *Let k be a field of characteristic p, and let A be a finite abelian p-group. Then the only R-matrix for the Hopf algebra $k[A]$ is $R = 1 \otimes 1$.*

Ultimately the proof relies on the fact that $k[A]$ is indecomposable under the stated assumptions.

§4. Examples

The group $\mathrm{Int}_k(G)/\mathrm{Inn}(G)$ appearing in the main theorem is a delicate thing. To see how tricky it is to find a group G such that $\mathrm{Int}_k(G)/\mathrm{Inn}(G)$ is non-trivial, think of the case $k = \mathbb{C}$, and consider to elements g and h of G such that $h = \alpha(g)$ for some $\alpha \in \mathrm{Int}_k(G)$. By definition, this means that $h = xgx^{-1}$ for some $x \in \mathbb{C}[G]^\times$. It follows that g and h are conjugate in any representation of G, and so have the same trace there. In other words, the characters of G cannot distinguish between g and h, and the classical theory tells us that g and h are conjugate *within* G: for some $c = c_g \in G$, we have $h = cgc^{-1}$.

For α to be non-trivial in $\mathrm{Int}_k(G)/\mathrm{Inn}(G)$, it must not be inner, even though it is given by a conjugation "element-wise". Clearly a group G with such automorphisms is not so easy to find.

There are some general results. For example, when G is simple, or a symmetric group, then $\mathrm{Int}_k(G)/\mathrm{Inn}(G) = 1$: this follows mostly from [FS89], as explained in §7.1 of our paper. (Clearly this also holds when G is abelian, by the way.) The following is then an almost immediate consequence of Theorem 4.2.

$\longrightarrow$ Proposition 4.6 – *Let G be a simple group, or a symmetric group. Then*

$$H^2_\ell(\mathcal{O}(G)) = 1\,.$$

On the other hand, $\mathrm{Int}_k(G)/\mathrm{Inn}(G)$ has been much studied by group theorists. In [Sah68] , it is proved that there exists a group G of order 2^{15} such that $\mathrm{Int}_k(G)/\mathrm{Inn}(G)$ is non-abelian. As a result:

$\longrightarrow$ Proposition 4.7 – *There exists a Hopf algebra $\mathcal{H}$ with $H^2_\ell(\mathcal{H})$ non-abelian. Namely, one can take $\mathcal{H} = \mathcal{O}(G)$ where G is Sah's group.*

In between these extreme cases, there are examples for which $H^2_\ell(\mathcal{O}(G))$ can be worked out explicitly. The following is deduced from Theorem 4.2 with some specific work in each case.

$\longrightarrow$ Proposition 4.8 – *Let $k = \mathbb{C}$.*

1. *Let G be a wreath product $\mathbb{Z}/p \wr \mathbb{Z}/p$, for an odd prime p. Then*

$$H^2_\ell(\mathcal{O}(G)) = (\mathbb{Z}/p)^{\frac{p-1}{2}}\,.$$

2. *Let G be the wreath product $\mathbb{Z}/2 \wr \mathbb{Z}/2$ (which is also the dihedral group). Then*

$$H^2_\ell(\mathcal{O}(G)) = 1\,.$$

3. *Let $G = A_4$ be the alternating group on 4 letters. Then*

$$H^2_\ell(\mathcal{O}(G)) = \mathbb{Z}/2\,.$$

We point out that Theorem 4.2 guides us towards an *explicit* description of $H^2_\ell(\mathcal{O}(G))$. Consider the case $G = A_4$ above. We are led to pay attention to the normal subgroup $V = \mathbb{Z}/2 \times \mathbb{Z}/2$ and to the non-trivial alternating, bilinear forms on its Pontryagin dual: there is just one, which is essentially the determinant (a pair of elements of $\widehat{V}$ being considered as a 2×2 matrix over the field with two elements). Then one looks for a cocycle c whose associated bilinear form is precisely this one, and which is A_4-invariant. This is straightforward with the help of a computer, and we can give a representative F for the non-zero element in $H^2_\ell(\mathcal{O}(A_4))$, namely:

$$\begin{aligned}4F = 1 \otimes 1 &- (e_1 \otimes e_1 + e_2 \otimes e_2 + e_3 \otimes e_3)\\ &+ (1 \otimes e_1 + e_1 \otimes 1) + (1 \otimes e_2 + e_2 \otimes 1) + (1 \otimes e_3 + e_3 \otimes 1)\\ &+ (e_1 \otimes e_2 - e_2 \otimes e_1) + (e_2 \otimes e_3 - e_3 \otimes e_2) + (e_3 \otimes e_1 - e_1 \otimes e_3)\,.\end{aligned}$$

(Here the elements of $V = \mathbb{Z}/2 \times \mathbb{Z}/2$ are $1, e_1, e_2, e_3$ and this equation is in $k[V] \otimes k[V]$.) This is the F considered in appendix A during our discussion of torsors (on pp. 39–40).

§5. Rationality questions

Theorem 4.2 is about algebraically closed fields. The following extends the result to the case of *splitting fields* for G: restricting the discussion to fields of characteristic 0 for simplicity, a field k is a splitting field for G when all the complex representations of G can in fact be realized over k. For example any field is a splitting field for $G = \mathbb{Z}/2$, since we only need ± 1 to realize all the irreducible modules in this case. The same is true for the dihedral group of order 8, by inspection. It is a harder result, but a beautiful one, that any field at all is a splitting field for the symmetric group S_n. In general a splitting field may be obtained from any field k by adjoining some m-th roots of unity, where m is the exponent of G.

$\longrightarrow$ Theorem 4.9 – *Let k be a splitting field for G of characteristic zero. Then there is an exact sequence*

$$1 \longrightarrow H^1(k, Z(G)) \longrightarrow H^2_\ell(\mathcal{O}_k(G)) \longrightarrow H^2_\ell(\mathcal{O}_{\bar{k}}(G)) \longrightarrow 1\,,$$

where $Z(G)$ is the centre of G.

This is Theorem 6.3 in [GK10].

Example 4.10 – Let $G = \mathbb{Z}/2$ and $k = \mathbb{Q}$. It follows from Theorem 4.2 that $H^2_\ell(\mathcal{O}_{\bar{\mathbb{Q}}}(G)) = 1$, so that

$$H^2_\ell(\mathcal{O}_{\mathbb{Q}}(\mathbb{Z}/2)) \cong H^1(\mathbb{Q}, \mathbb{Z}/2) = \mathbb{Q}^\times/(\mathbb{Q}^\times)^2\,.$$

§6. Higher degrees

When G is commutative, the algebra $\mathcal{O}_k(G)$ is cocommutative, so the groups $H^n_{sw}(\mathcal{O}_k(G))$ are defined for all $n \geq 1$. As we have indicated in example 4.1, when k is algebraically closed of characteristic 0 the Fourier transform gives an isomorphism $\mathcal{O}_k(G) \cong k[\widehat{G}]$, and the Sweedler cohomology groups of group algebras are known. However when k has positive characteristic the Fourier transform is not available.

In [Gui12] we investigate the the group $G = \mathbb{Z}/2$. Over any field k of characteristic zero or $p > 2$, we have $\mathcal{O}(\mathbb{Z}/2) \cong k[\mathbb{Z}/2]$, so $H^n_{sw}(\mathcal{O}(\mathbb{Z}/2)) = H^n(\mathbb{Z}/2, k^\times)$. The latter is $k^\times/(k^\times)^2$ when n is even, and $\{\pm 1\}$ when n is odd. When k has characteristic 2, by contrast, we obtain the following result.

$\longrightarrow$ Theorem 4.11 – *Let k be a field of characteristic 2. The Sweedler cohomology of $\mathcal{O}_k(\mathbb{Z}/2)$, is given by*

$$H^n_{sw}(\mathcal{O}_k(\mathbb{Z}/2)) = \begin{cases} 0 \text{ for } n \geq 3\,, \\ \\ k/\{x + x^2 \mid x \in k\} \text{ for } n = 2\,, \\ \\ \mathbb{Z}/2 \text{ for } n = 1\,. \end{cases}$$

In particular when k is algebraically closed then these groups vanish in degrees ≥ 2.

Of course the fact that $H^2_{sw}(\mathcal{O}_k(G)) = 0$ when k is algebraically closed was predicted by theorem 4.2.

§7. Open questions

The most obvious challenge is the following.

Problem. *Give a version of theorem 4.2 for other classes of Hopf algebras (universal enveloping algebras, Drinfeld-Jimbo quantum groups, compact quantum groups in the sense of Woronowicz, quantum permutation groups...).*

It seems interesting also to generalize "lazy cohomology" to higher degrees.

Problem. *For any Hopf algebra $\mathcal{H}$, give a definition of cohomology groups $H^n_\ell(A)$ for $n \geq 1$ which agree with Sweedler's cohomology groups whenever $\mathcal{H}$ is cocommutative, and which generalize the above definitions for $n = 1, 2$.*

As we have seen in §1, things come down to associating cohomology groups to any cosimplicial group, generalizing the usual construction for cosimplicial *abelian* groups. One can show that such a theory could *not* exist if we required it to enjoy the usual properties, such as that of providing long exact sequences in cohomology given a short exact sequence of cosimplicial groups[1]; so we will have to settle for less.

We point out that, in the same way that for $n = 2$ the group $H^n_\ell(\mathcal{H})$ is related to Drinfeld twists (on the dual Hopf algebra), a putative candidate for $H^3_\ell(\mathcal{H})$ would be related to *Drinfeld associators* (you may see this by inspection of the cosimplicial group $A^*(\mathcal{K})$ of §1). And just as Drinfeld twists were not expected to form a group when they were first defined, and indeed do not form a group unless you restrict to invariant ones, Drinfeld associators are not traditionally thought of as the elements of a group.

[1] This was pointed out to me by Tom Goodwillie on the MathOverFlow website.

Appendix A

Bundles, torsors, and classifying spaces

In this appendix we review the three terms in the title in various contexts: algebraic topology, algebraic geometry, and non-commutative geometry (in a very elementary sense). Many readers will skip a good deal of these prerequisites, but presumably they will also find something new in some section or other (and they may enjoy the pictures).

The first objective is to motivate the use of classifying spaces of finite groups as the prime examples of topological spaces in the text. Second, the section on algebraic geometry is useful preparation for appendix C. Finally, the torsors in the non-commutative setting also show up in chapter 4, or rather the devices with which one can define them easily (two-cocycles, Drinfeld twists). We felt it most natural to introduce them here next to their classical counterparts.

On the other hand almost *all* of the material in this appendix is needed to appreciate [GKM12], of which we can finally say a word.

Topology

Basics. When G is a topological group, a *G-principal bundle* is a quotient map $p\colon Y \longrightarrow X = Y/G$ of the nicest possible type. Namely, it is required that p be locally trivial in the sense that X is covered by open sets U such that $p^{-1}(U) \cong U \times G$, so that p corresponds to the projection onto U; the transitions between two such trivializations are assumed to be given on each fibre by a translation by an element of G. In particular, the action of G on Y must be free.

For example, a $GL_n(\mathbb{C})$-principal bundle is essentially the same thing as a complex vector bundle of rank n over X (replace $U \times GL_n(\mathbb{C})$ by $U \times \mathbb{C}^n$ and glue these trivial pieces with the given transition maps to get a complex vector bundle in the classical sense). Likewise, there is a one-one correspondence between $GL_n(\mathbb{R})$-principal bundles and real vector bundles of rank n over the same base. Moreover, the use of Riemannian metrics (when the base is reasonable, say paracompact) shows that $GL_n(\mathbb{R})$-principal bundles are in bijection with O_n-principal bundles.

The word *torsor* is seldom used in topology (at least in the sense which follows). We define a torsor for G to be a principal bundle over the space reduced to a single point. So a G-torsor is simply a topological space with a G-action which is homeomorphic to G with the translation action on itself (say on the left), but *no such homeomorphism is specified*; two choices differ by a self-homeomorphism of G given by a translation (on the right). In other contexts the notion is more interesting (it is certainly the case, with our current definitions, that there is only one G-torsor up to isomorphism!). Note that for $GL_n(\mathbb{C})$ it is apparent that choosing a torsor amounts to choosing a complex vector space of dimension n, with no preferred basis.

Universal objects. A map $f: X_1 \to X_2$ allows us to pull-back any G-principal bundle $Y_2 \to X_2$ into $f^*(Y_2) \to X_1$. One can show that the bundle $f^*(Y_2)$ depends only on the homotopy class of f, up to isomorphism (we abuse notation and refer to a bundle by the name of its "total space"). A *universal* G-principal bundle is one of the form $EG \to BG$ with the property that *any* G-principal bundle over any reasonable space X is uniquely a pull-back of EG, that is, is isomorphic to a bundle of the form $f^*(EG)$ for some map $f: X \to BG$, unique up to homotopy; in other words, we require that the isomorphism classes of bundles over X be in one-one correspondence with $[X, BG]$. From this we see that a G-principle bundle, if it exists at all, must be unique. The space BG, which is then well-defined up to homotopy, is called the *classifying space* of G.

Existence is of course a classical result (see [Ste99]). In fact one can show that a bundle $Y \to X$ is universal if and only if the total space Y is contractible. It follows that, given a universal bundle for G and a subgroup $H \subset G$, one can consider the map $Y \to Y/H$ to get a universal principal bundle for H; the local triviality will be guaranteed if the map $G \to G/H$ is itself locally trivial. One can thus directly treat the case of $GL_n(\mathbb{C})$ using Grassmann manifolds (see [MS74], §5 and §14), and thereby establish the existence of a universal principal bundle for any compact Lie group.

Also note that whenever G is discrete, the fact that EG is contractible combined with the long exact homotopy sequence of a fibration shows that $\pi_n(BG) = 0$ for $n \neq 1$ while $\pi_1(BG) = G$; conversely these conditions on a space BG imply that the universal cover EG is contractible and may be taken as the total space of a universal G-bundle. One can construct BG directly by "killing homotopy groups", and we shall come back to this.

Nowadays though, topologists like to prove the existence of a classifying space with one sentence: take the nerve of the (topological) category with one object, and whose arrows are the elements of G. Should you look for a definition of EG, you can be told to take the nerve of the obvious category whose objects and arrows are both given by the elements of G (see [DH01], Part I, §5.9). Below we will draw some pictures.

Classifying spaces play an important rôle in what follows. Whenever we need a topological space to illustrate a result, we tend to pick BG for some group G. Why are these spaces so popular?

The first answer commonly heard is algebraic. Assume that G is discrete, and that EG and BG are CW-complexes. Then the cellular complex of EG is really a complex of free $\mathbb{Z}[G]$-modules (on a basis which is in bijection with the cells of BG). Since EG is contractible, this complex is exact, ie we get a resolution of $\mathbb{Z}$ by $\mathbb{Z}[G]$-modules, which is what the algebraist requires in order to compute the cohomology of G. If you take for granted that the cohomology of groups is an important matter, for your own algebraic reasons, then you see the point of understanding spaces of the form BG. In particular $H^*(BG, k) = H^*(G, k)$ for any ring k.

Another answer takes a more topological viewpoint, though the crux of the matter is still that the group cohomology of G can be "realized" as that of a space. Leaving aside the hope of writing down explicit chain complexes, we can make the following remark. If X is any space with a G-action, the *Borel construction* on X is the formation of the space $X_G = (EG \times X)/G$. There is a fibration

$$X \longrightarrow X_G \longrightarrow BG$$

and a map

$$X_G \longrightarrow X/G$$

whose fibres are classifying spaces of stabilizers of points of X. The various spectral sequences at our disposal (namely the Leray, and the Leray-Serre, spectral sequences) give strong constrains on the action, involving the cohomology of G and its subgroups as well as that of X. For example such considerations have led to the proof that whenever a finite group acts freely on a sphere, then all the Sylow subgroups must be cyclic (or generalized quaternion at $p = 2$), see [AM04]. These applications show the relevance of the above fibrations, and thus demonstrate that classifying spaces appear naturally when studying G-actions.

Before you think that group theory can be swallowed by topology via the classifying space construction, consider the following: for *any* topological space X there exists a discrete group G and a map $BG \to X$ which is an isomorphism in homology (this is the Kan-Thurston Theorem, see [KT76]). So as far as the eyes of homology can see (and that is quite far), topology is subsumed by group theory. More seriously, this result indicates that, in principle at least, restricting attention to classifying spaces is hardly a restriction. Note that this Theorem was explicitly used, for example by Dwyer in [Dwy96] to construct a transfer map for fibrations, so it is more than a curiosity.

Characteristic classes. By definition, a characteristic class α for G-bundles assigns an element $\alpha(Y) \in H^*(X)$ to each principal bundle $Y \to X$ (the cohomology may be taken with various coefficients). The assignment is required to be natural with respect to pull-backs. It is then tautological that characteristic classes form a ring which is identified with $H^*(BG)$. Experience shows that these classes are very useful in the study of G-bundles. For example, it is well-known that

$$H^*(BGL_n(\mathbb{C}), \mathbb{Z}) = \mathbb{Z}[c_1, c_2, \ldots, c_n],$$

with c_i of degree $2i$. This gives rise to the *Chern classes* of complex vector bundles. Likewise

$$H^*(BO_n, \mathbb{F}_2) = \mathbb{F}_2[w_1, w_2, \ldots, w_n],$$

with w_i of degree i, giving rise to the theory of *Stiefel-Whitney classes* which are important in the sequel.

Recreation: Cayley graphs

Is it possible to draw pictures of classifying spaces? Well, we can do the following. Let G be a discrete group. Suppose we try to attach cells together so as to form a space X with $\pi_1(X) = G$ and $\pi_n(X) = 0$ for $n \neq 1$. Then X will have the homotopy type of BG, as indicated above, and even though this will not be the most functorial construction it will have the advantage of using few cells and thereby allow us to visualize the situation a little better.

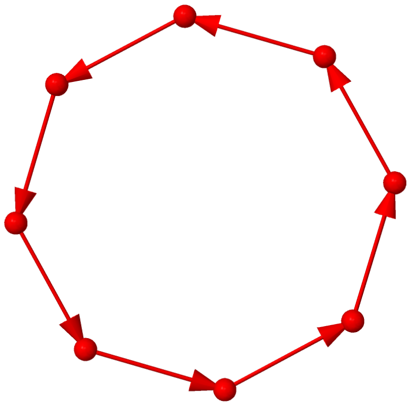
Suppose we are given a *presentation* of G, that is a set of generators S, assumed finite for simplicity, and a set R of words in the free group $\mathcal{F}(S)$ on S, such that G is isomorphic to $\mathcal{F}(S)/\langle R\rangle$ (here $\langle R\rangle$ is the *normal* subgroup generated by R).

Then we can start building BG by taking a single point, to which we attach a bouquet of circles in bijection with S; call this X_1. Then we attach a 2-cell for each relation in R, which dictates the "attaching map" of the cell. The resulting complex X_2 has $\pi_1(X_2) = G$ (say, by Van Kampen's Theorem).

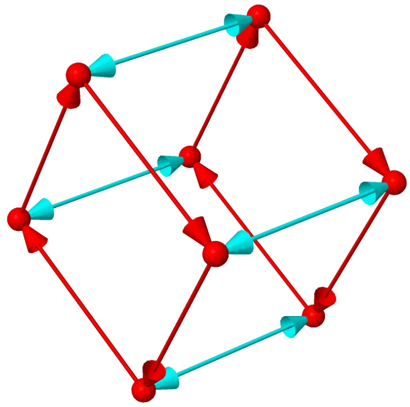
The rest of the construction would involve glueing more cells to kill successively the higher homotopy groups, but let us stop here. Eventually we would take EG to be the universal cover of BG, and we can at once describe E_1 and E_2, the pre-images of X_1 and X_2 respectively in EG.

We note that E_1 is really (the topological space underlying) a directed, coloured graph, called the *Cayley graph* of (G, S) (it does not depend on R). The space E_2 is sometimes called the Cayley complex, or presentation complex, of (G, S, R). So the Cayley graph of (G, S) has one vertex for each element of G, and for each $s \in S$ it has one edge coloured by s from g to sg. Better pictures are obtained when we choose S containing at most one of s, s^{-1} for each $s \in G$; assuming this, the only "back-and-forth paths" between two vertices are obtained for generators s satisfying $s = s^{-1}$, in which case we usually draw just one edge with a double arrow.

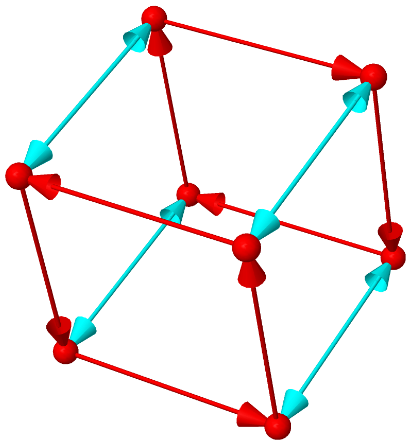
Let us try a few groups of order 8. When $G = \mathbb{Z}/8$, with $S = \{1\}$, the Cayley graph looks as follows.



If we consider now $G = \mathbb{Z}/4 \times \mathbb{Z}/2$, with $S = \{(1,0),(0,1)\}$, we obtain the following picture.

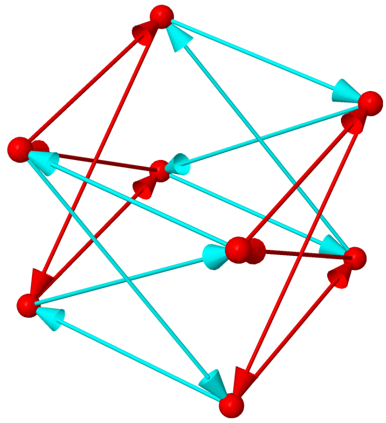


Notice the difference between this and the Cayley graph for the dihedral group of order 8, that is $G = \langle r, s : r^4 = s^2 = 1, s^{-1}rs = r^{-1} \rangle$ with $S = \{r, s\}$:

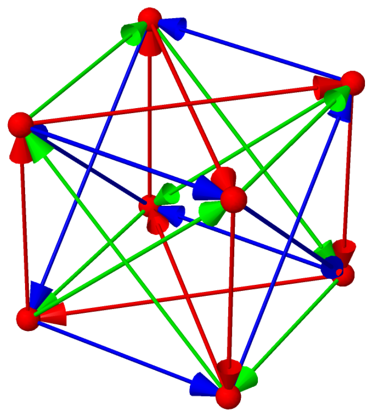


Of course the last two graphs are identical *as undirected, uncoloured* graphs, though the extra decorations tell you something about the action of G (which can be recovered as the group of directed, coloured graph automorphisms). On this last picture, to get the Cayley complex you would glue eight discs corresponding to $r^4 = 1$, four on each "red face", with a quarter of a turn between them, and eight more discs corresponding to $r^2 = 1$, paired around the double green edges (recall that the edges with double arrows are really two edges each).

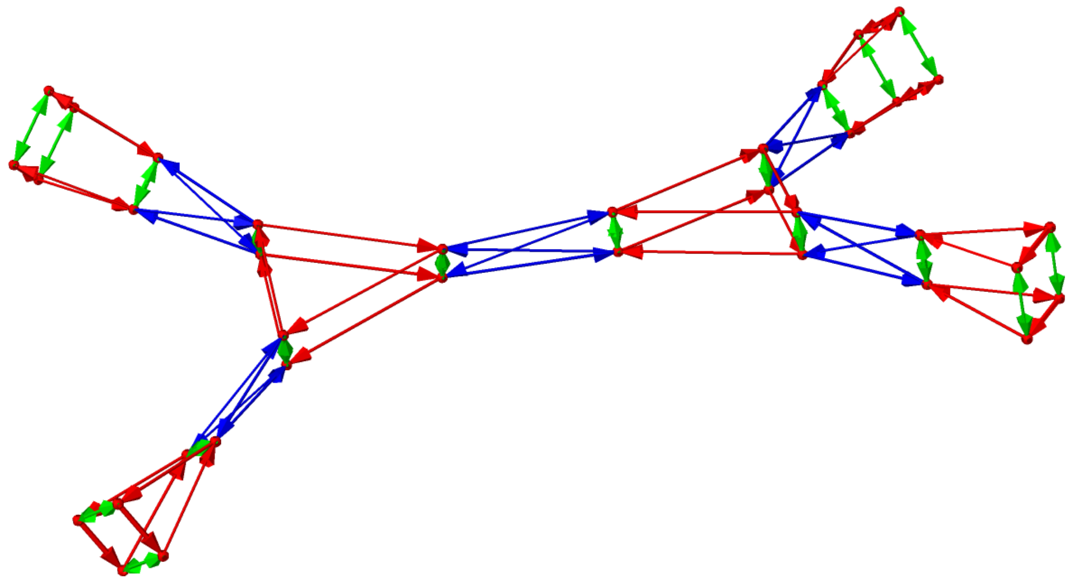
Here is the picture for the quaternion group $G = \langle i, j, k : i^2 = j^2 = k^2 = ijk = -1 \rangle$ and $S = \{i, j\}$:



One may be disappointed that the $\mathbb{Z}/3$ symmetry is hard to see on this picture. You may prefer the choice $S = \{i, j, k\}$:



Infinite groups can also be considered. Particularly when G is finitely presented (that is when S and R are both finite) then all relevant information about the graph can be seen on a finite portion. It does not matter which, since the Cayley graph has a transitive group of automorphisms, namely G itself. Below we picture $G = SL_2(\mathbb{Z})$.



We have chosen three generators, the green one corresponding to $-Id$. Quotienting by the central subgroup $\{\pm Id\}$ yields the group $PSL_2(\mathbb{Z})$, whose Cayley graph is obtained from the above by identifying two nodes when they are joined by a green arrow. It is then visible that $PSL_2(\mathbb{Z})$ is a free product of $\mathbb{Z}/2$ and $\mathbb{Z}/3$.

Algebraic geometry

Basics. Now let G be an affine algebraic group over a field k. Again a map of varieties $p\colon Y \to X$ will be called a G-principal bundle when $X = Y/G$ in some sense and p is nice enough. Let us be more precise. The first requirement is that the map $G \times Y \to Y \times Y$ given by $(g, y) \mapsto (y, g \cdot y)$ should be a closed immersion.

We state the second condition in the case when k is algebraically closed first. We require that (1) the fibres of p are the orbits of G; (2) p is surjective and open; (3) if U is open in Y, the map p induces an isomorphism between $\mathcal{O}_X(p(U))$ and the set of $f \in \mathcal{O}_Y(U)$ which are constant on the fibres of p.

For a general field k, we require that the above condition hold after extending the scalars to the algebraic closure $\bar{k}$. One can show that this property *descends*, in the sense that if one checks the condition with the scalars extended to *some* algebraically closed field K containing k, then it holds for *any* such field (see [Mum65], §2, remark 8 and proof of Proposition 0.9).

In this context, a *torsor* is a principal bundle over $Spec(k)$. Two other definitions are equivalent. A torsor can be defined to be a variety T with an action of G such that the map $G \times T \to T \times T$ is an isomorphism (of course this is the above definition, somewhat cleaned up). Or, one can define a torsor to be a variety T with an action of G, which becomes isomorphic to G itself with its translation action when the scalars are extended to $\bar{k}$.

Example – Let $G = O(q_0)$ denote the orthogonal group of the non-degenerate quadratic form q_0 defined over the k-vector space V. Given another non-degenerate quadratic form q defined on V, consider the variety T of all isometries from (V, q) to (V, q_0). (The forms q_0 and q must become isometric when scalars are extended to $\bar{k}$; if they are not isometric over k, then the variety T has no k-rational points, but is still well-defined.) The isomorphisms in T may be post-composed with the automorphisms in G, so T is a G-variety (on the right). It is in fact a G-torsor. Moreover all the G-torsors are of this form: there is a one-one correspondence between non-degenerate quadratic forms defined on V and G-torsors ([Ser02], III, §1.2, Proposition 4).

Whenever G is the automorphism group of some type of algebraic structure, it is frequently possible to show that G-torsors are in bijection with the isomorphism classes of that structure.

Example – Let K/k be a finite, Galois extension of fields, and let $G = Gal(K/k)$. The finite group G is thought of as an algebraic group over k, with coordinate ring $\mathcal{O}_k(G)$. The algebra K is a G-algebra, or an $\mathcal{O}_k(G)$-comodule algebra, so $Spec(K)$ is a G-variety (here we use the letter G for $Spec(\mathcal{O}_k(G))$, of course).

Let n denote the order of G. Write $K = k[P]/(P)$ where P is a separable, irreducible polynomial of degree n over k. The group G acts simply transitively on the roots of P.

When we form $K \otimes_k \bar{k} = \bar{k}[P]/(P)$, the Chinese Remainder Theorem tells us that the ring we have is a product of n copies of $\bar{k}$. Inspecting the G-action, we see that $K \otimes_k \bar{k}$ is really $\mathcal{O}_{\bar{k}}(G)$, the coordinate ring of $G_{\bar{k}}$. So $Spec(K)$ is a G-torsor.

This example explains the terminology *Galois object* which is sometimes used in lieu of *torsor*.

Universal objects. Universal bundles and classifying spaces, at first sight, seem not to exist. There exists a larger category than that of algebraic varieties in which we can mimick the topological construction (see [MV99]), but we will stick to elementary methods and describe Totaro's construction (taken from [Tot99]).

This is the observation that, given G as above, there exists a representation V such that the action of G is free outside of a Zariski closed subset S of arbitrary large codimension. Thus $V \setminus S$ is an approximation of EG, and $(V \setminus S)/G$ is an approximation of BG. We think of "BG in algebraic geometry" as being the colimit, somehow, of all the varieties $(V \setminus S)/G$ imaginable.

This collection of varieties is well-behaved. For starters, if $Y \to X$ is any G-principal bundle, one can find a variety X' with a map $X' \to X$ whose fibres are affine spaces, such that the bundle $Y' \to X'$ obtained by pull-back is also a pull-back of a bundle of the form $V \setminus S \longrightarrow (V \setminus S)/G$, for some V and S. This is of course analogous to the universality of BG in topology.

Another nice property of Totaro's varieties is as follows. Consider a "good" functor F^* from varieties to graded groups. What we need is that $F^*(E) \cong F^*(B)$ when $E \to B$ is a vector bundle, and that the F^*-theory comes equipped with some long exact sequences whenever we consider a closed subset of a variety. The examples to keep in mind are étale cohomology, ordinary cohomology when $k = \mathbb{C}$, and the Chow ring CH^*. Then Totaro's "double fibration argument" shows that $F^n((V \setminus S)/G)$ is independent of the choice of V and S, as long as the codimension of S in V is large enough. The common value is denoted $F^n(BG)$. Note that when $k = \mathbb{C}$ and we consider ordinary cohomology, one can show that this trick gives the "right" cohomology for BG.

Combining the remarks of the last two paragraphs, we see for example that CH^*BG is the ring of characteristic classes (with values in the Chow ring) for G-principal bundles. Computing CH^*BG explicitly on examples was a major theme in my early research. See appendix C for more on this.

Cohomological invariants. When discussing characteristic classes, we have so far considered all G-principal bundles involving varieties over a fixed field k. Many authors have investigated the following alternative class of objects. Let us focus attention on bundles over $Spec(K)$, for K a field containing k; more precisely, let us consider the class of all G_K-torsors, for all fields K containing k, where G_K is G with scalars extended to K. (Note that K may well not be finitely generated over k, so that $Spec(K)$ is not a "variety over k" under everyone's definition.) Then, consider the characteristic classes for these objects, with values in étale cohomology: they are the so-called *cohomological invariants* of G. Of course the étale cohomology of $Spec(K)$ is just the Galois cohomology of K, written $H^*(K)$ (with various coefficients available).

In more compact notation, the situation is as follows. Write $H^1(K,G)$ for the (pointed) set of all G_K-torsors (a notation which will be discussed later). Then a cohomological invariant is a transformation of functors

$$H^1(-,G) \longrightarrow H^*(-)$$

(again we do not specify coefficients). Such invariants form a graded ring written $Inv(G)$.

One may ask the question of universality in this context. Let us announce at once that there is no universal torsor yielding all the others by pull-back; and there is no field K such that $Inv(G) = H^*(K)$. However, the following holds. Let

$$p\colon (V \setminus S) \to (V \setminus S)/G$$

be one of Totaro's varieties, with S of codimension at least 2. Then any torsor over $Spec(K)$ is obtained as a fibre of p, that is a pull-back over some map

$$Spec(K) \longrightarrow (V \setminus S)/G.$$

There is no uniqueness statement regarding this map, and this is probably the reason why p is called *versal* (that is, universal without uniqueness).

Now let Ω be the field of rational functions on the variety $(V \setminus S)/G$. Then $Inv(G)$ can be identified with a certain subring of $H^*(\Omega)$. For more information see [GMS03].

I have contributed to the theory of cohomological invariants in [Gui07b]. Salient points are summarized in appendix C.

Non-commutative geometry

Basics. Suppose all the varieties in the previous section are taken to be affine. Then most results can be stated in terms of coordinate rings, which are commutative. It is natural curiosity to study the situation with all commutativity requirements removed.

There are in facts several ways to write down the definitions (just like in algebraic geometry there are several definitions of "quotient"). We shall give just one example. The group G will be replaced by a Hopf algebra $\mathcal{H}$ over k (think of $\mathcal{H} = \mathcal{O}(G)$), the variety Y will be replaced by an H-comodule algebra, and the quotient $X = Y/G$ will be replaced by

$$B = A^{co-H} = \{a \in A \mid \Delta_A(a) = a \otimes 1\},$$

where $\Delta_A \colon A \to A \otimes H$ is the map giving the coaction. Then the inclusion $B \subset A$ is called Galois when the map

$$A \otimes_B A \to A \otimes_k H, \qquad a \otimes b \mapsto (a \otimes A)\Delta_A(b)$$

is an isomorphism. This mimicks the fact that, in the classical case, the map $(g,y) \mapsto (y, g \cdot y)$ gives an isomorphism $G \times Y \cong Y \times_X Y$.

Then we further call the extension $B \subset A$ a *quantum $\mathcal{H}$-principal bundle* when B is contained in the centre of A, and A is faithfully flat as a B-module (this is the definition taken in [Kas04]).

We do not claim that this definition reduces to the classical one when applied to commutative algebras (rather, it seems to refer to a slightly larger class of objects). In some situations one may use alternative definitions. However, there is an agreement on the usefulness of the following rather technical requirement, which is automatically satisfied in the commutative case. The extension $B \subset A$ as above is called *cleft* when there exists a map of right H-comodules $\gamma \colon \mathcal{H} \to A$ (the "cleaving map") which has a convolution inverse in $Hom_k(\mathcal{H}, A)$.

Cleft quantum principal bundles with $B = k$ are definitely what we should call *torsors* for $\mathcal{H}$, although the usually accepted terminology is *cleft Galois objects for $\mathcal{H}$*.

To give just a little bit of intuition for the "cleft" condition, we mention that Kassel in [Kas04] proves for certain Hopf algebras, and conjectures for many Hopf algebras, that the cleftness of $B \subset A$ is equivalent to the existence of an isomorphism of this extension with $B \subset B \otimes H$ after a finite, étale extension and a homotopy (in some elementary sense). In algebraic geometry a torsor becomes trivial in a finite extension of the base field (since it is enough to find one rational point), so it certainly satisfies Kassel's condition.

The question of the existence of a universal principal bundle is not settled in the "quantum" world. Kassel and Aljadeff in [AK08] have studied *versal* bundles, on the other hand; see also the appendix to [GKM12]. Essentially for any torsor T in the above sense, there exists a quantum bundle whose fibres are torsors becoming isomorphic to T when the scalars are extended to a large enough field, and such that conversely all such torsors can be obtained as fibres. In the classical case all torsors become trivial over algebraically closed fields, so the versal bundles considered in the previous section are actually of this form, with $T = G$ trivial. The novelty in the quantum realm resides in the existence of non-trivial "torsors" over non-algebraically closed fields.

Examples. We would like to show non-commutative torsors in action. Rather than a torsor itself, we shall illustrate the associated twisting procedure. Recall the classical case. Given a torsor T for G, and a G-variety X, one may form

$$X_T = \frac{T \times X}{G}.$$

When $T = G$ is the trivial torsor, we have $X_T = X$; as a result, the twisting is always trivial over algebraically closed fields, and we see that X_T is another *form* of X.

Studying the analogous construction in the context of Hopf algebras and non-commutative geometry is the subject matter of [GKM12], in which we seek to give generators and relations for the algebra corresponding to X_T. Our main Theorem says that things are as simple as possible, in the sense that certain "obvious" relations in this algebra are in fact sufficient. The statement unfortunately is rather technical, and we shall be content with an example. As promised, it will show that there are non-trivial non-commutative torsors even over algebraically closed fields.

Let us work with the algebra of functions on the algebraic group SL_2, playing the rôle of X. We consider $\mathcal{H} = \mathcal{O}(G)$ for $G = \mathbb{Z}/2 \times \mathbb{Z}/2 = \langle e_1, e_2 \rangle$ acting on the algebra

$$A = SL(2) = k[a,b,c,d]/(ad - bc - 1)$$

by

$$e_1 \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} d & c \\ b & a \end{pmatrix} \quad \text{and} \quad e_2 \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & -b \\ -c & d \end{pmatrix}.$$

(Each matrix identity is shorthand for four identities in A.)

We need to pick a torsor for $\mathcal{H}$. In the next section we shall explain how to do this "combinatorially" (or at least computationally). Namely, to define a torsor it is sufficient to exhibit a Drinfeld twist as we have met them in chapter 4. More precisely let us take the twist F given on page 28. We denote the corresponding torsor also by the letter F.

By the procedure detailed in [GKM12], it defines a twisted algebra A_F, which we also denote by $SL_F(2)$. Let us give a presentation of the latter.

Set $x = (a+d)/2$, $y = (a-d)/2$, $z = (b+c)/2$ and $t = (b-c)/2$. These elements are eigenvectors for the action of G, and we have

$$SL(2) = k[x,y,z,t]/(x^2 - y^2 - z^2 + t^2 - 1).$$

From our main Theorem in *loc. cit.* it is an exercise to show the following.

PROPOSITION – *The algebra $SL_F(2)$ has a presentation with four generators X, Y, Z, T subject to the seven relations*

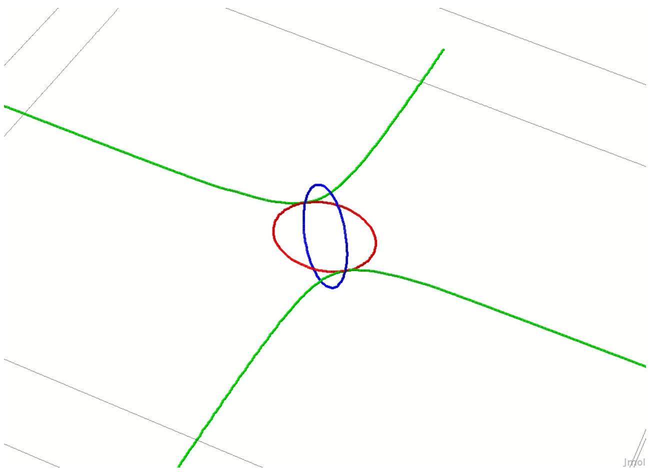
$$XY = YX, \quad XZ = ZX, \quad XT = TX,$$

$$YZ = -YZ, \quad YT = -TY, \quad ZT = -TZ,$$

$$X^2 + Y^2 + Z^2 - T^2 = 1.$$

As an illustration, we may take $k = \mathbb{R}$ and describe the set $Hom_{alg}(SL_F(2), \mathbb{R})$ of $\mathbb{R}$-points, which we denote by $SL_F(2, \mathbb{R})$.

COROLLARY – *The set $SL_F(2, \mathbb{R})$ consists of two circles and a hyperbola, all intersecting in two points.*



The algebra $SL(2)$ is a Hopf algebra with coproduct $\Delta : SL(2) \to SL(2) \otimes SL(2)$ given by

$$\Delta(x) = xx' + yy' + zz' - tt', \qquad \Delta(y) = xy' + yx' - zt' + tz',$$

$$\Delta(z) = xz' + yt' + zx' - ty', \qquad \Delta(t) = xt' + yz' - zy' + tx',$$

where x is identified with $x \otimes 1$ and x' with $1 \otimes x$ (similarly for the other variables).

The twisted algebra $SL_F(2)$ is a Hopf algebra "in the braided sense". That is, if we denote $(SL(2) \otimes SL(2))_F$ by $SL_F(2,2)$ for short, one can show that $SL_F(2,2)$ is the "tensor product" of $SL_F(2)$ with itself in some monoidal category, and there is a map $SL_F(2) \to SL_F(2,2)$.

Proposition – *The algebra $SL_F(2,2)$ is generated by eight generators X, Y, Z, T, X', Y', Z', T' subject to the following relations:*

- *the "left relations", which are as in the previous Proposition,*
- *the "right relations", which are obtained from the left relations by applying the substitutions $X \mapsto X'$, $Y \mapsto Y'$, $Z \mapsto Z'$, $T \mapsto T'$,*
- *the "composability conditions", namely X and X' commute with all other generators, and*

$$YZ' = -Z'Y, \quad YT' = -T'Y, \quad ZT' = -T'Z,$$

$$Y'Z = -ZY', \quad Y'T = -TY', \quad Z'T = -TZ'.$$

The map $\Delta : SL_F(2) \to SL_F(2,2)$ is given by the following formulas:

$$\Delta(X) = XX' - YY' - ZZ' + TT', \qquad \Delta(Y) = XY' + YX' - ZT' - TZ',$$

$$\Delta(Z) = XZ' - YT' + ZX' - TY', \qquad \Delta(T) = XT' + YZ' + ZY' + TX'.$$

When R is a *commutative* algebra, then the set $SL(2,R) = Hom_{alg}(SL(2),R)$ is a group; for a general algebra R however, the set $SL(2,R)$ has only a partially defined group law (essentially, one can only multiply two matrices if all the coordinates commute). A similar statement holds for $SL_F(2)$: two points of $SL_F(2,R) = Hom_{alg}(SL_F(2),R)$ are composable if and only if they satisfy the composability conditions of the Proposition.

We are now in position to describe the partially defined group law on the set $SL_F(2,\mathbb{R})$ of real points of $SL_F(2)$. Let $\mathcal{C}_1$, $\mathcal{C}_2$ denote the two circles and $\mathcal{H}$ the hyperbola.

Corollary – *Two points of $SL_F(2,\mathbb{R})$ can be composed if and only if they both belong to one of $\mathcal{C}_1$, $\mathcal{C}_2$ or $\mathcal{H}$. The groups $\mathcal{C}_1$ and $\mathcal{C}_2$ are isomorphic to the group of complex numbers of modulus 1, while $\mathcal{H}$ is isomorphic to the multiplicative group of non-zero real numbers.*

Combinatorial descriptions

We have written $H^1(k,G)$ for the set of G-torsors over the field k. Let us recall briefly a few definitions from [Ser02] which justify this otherwise surprising notation.

If A is any group with an action of $Gal(\bar{k}/k)$ by group automorphisms, a 1-cocycle is a continuous map $Gal(\bar{k}/k) \to A$ of the form $s \mapsto a_s$ with the property that $a_{st} = a_s s{\cdot}a_t$. Two 1-cocycles a and a' are cohomologous if there exists $b \in A$ such that $a'_s = b^{-1} a_s s \cdot b$. The set of 1-cocycles modulo cohomology is written $H^1(k,A)$. When A is abelian, the set $H^1(k,A)$ is a group and is indeed the first cohomology group of G with coefficients in A (that is, it is an *Ext* in an appropriate category).

It is then a theorem that for $A = G(\bar{k})$ the set $H^1(k, G(\bar{k}))$, more commonly written $H^1(k,G)$, is in bijection with the set of G-torsors over k. Briefly, given a cocycle a one starts with the trivial torsor, namely G itself or rather $G(\bar{k})$, and changes the Galois action to

$$s * x = a_s\, s \cdot x. \qquad (x \in G(\bar{k}),\ s \in Gal(\bar{k}/k))$$

This defines a new structure of k-variety on G, and this is the required torsor.

In the quantum setting there is also a combinatorial description of the torsors. We sketch this here and refer to [GKM12] for details. A *two-cocycle* for a Hopf algebra $\mathcal{H}$ over k is a convolution-invertible bilinear form $\sigma\colon \mathcal{H} \times \mathcal{H} \to k$ satisfying (in Sweedler's notation)

$$\sum_{(x),(y)} \sigma(x_1, y_1)\,\sigma(x_2 y_2, z) = \sum_{(y),(z)} \sigma(y_1, z_1)\,\sigma(x, y_2 z_2)$$

for all $x, y, z \in \mathcal{H}$. Given such a σ, we may endow $\mathcal{H}$ with a new multiplication defined by

$$x * y = \sum_{(x),(y)} \sigma(x_1, y_1)\, x_2 y_2 .$$

The algebra $\mathcal{H}$ with this twisted multiplication is a torsor (cleft Galois object) for $\mathcal{H}$, and all torsors are of this form. The two-cocycles σ and τ define the same torsor if and only if there is a convolution-invertible map $\lambda\colon \mathcal{H} \to k$ such that

$$\tau(x,y) = \sum_{(x),(y)} \lambda(x_1)\lambda(y_1)\sigma(x_2, y_2)\lambda^{-1}(x_3 y_3),$$

for all $x, y \in \mathcal{H}$. One says that they are equivalent.

Now suppose that $\mathcal{H}$ is finite-dimensional, so that its dual $\mathcal{K}$ is again a Hopf algebra. A bilinear map σ on $\mathcal{H} \times \mathcal{H}$ defines a tensor $F \in \mathcal{K} \otimes \mathcal{K}$ via the requirement $\langle F, x \otimes y \rangle = \sigma(x, y)$. It is easily checked that σ is a two-cocycle if and only if F satisfies

$$(F \otimes 1)(\Delta \otimes id)(F) = (1 \otimes F)(id \otimes \Delta)(F)$$

in $\mathcal{K} \otimes \mathcal{K} \otimes \mathcal{K}$. One says that F is a *Drinfeld twist*. Drinfeld twists appear in chapter 4 in another context. Also, two twists F and F' correspond to equivalent two-cocycles if and only if

$$F' = (a \otimes a) F \Delta(a^{-1})$$

for some invertible $a \in \mathcal{K}$; one says that they are *gauge equivalent*. Again, this condition will pop up in chapter 4.

Appendix B

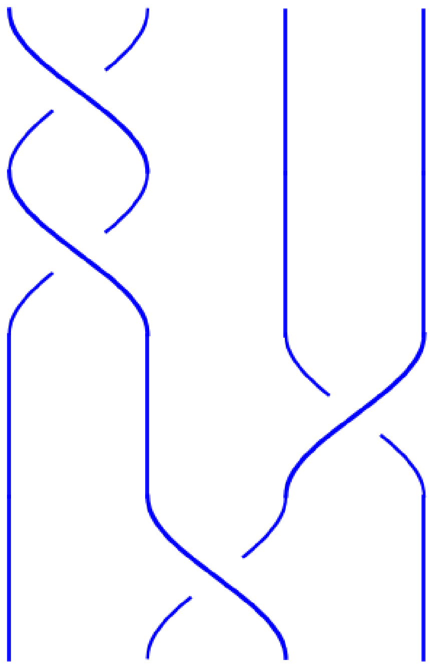
Braids and R-matrices

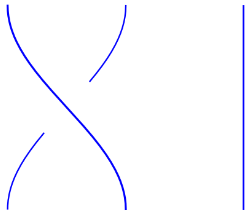
Braids, links and the apparatus of Markov functions are directly relevant to chapter 3, and we include a general discussion here. It turns out that the representations of the braid groups, much sought after in this theory, can be produced with the machinery of R-matrices on Hopf algebras. Since R-matrices will appear in chapter 4 (even if the relationship to braids will not be explicit then), it is convenient to introduce them in this appendix. We shall finish with a word about the Reshetikhin-Turaev Theorem, definitely not needed in the rest of this work but particularly enlightening at this point.

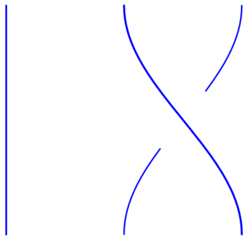
Braids

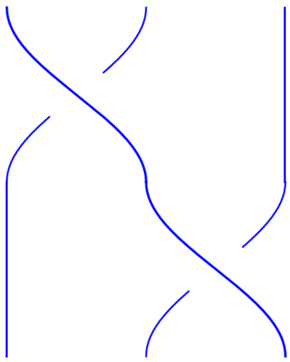
(A reference for the facts given without proof in the beginning of this appendix is [KT08].)

A geometric braid is something like what you see on the following picture. It is to be taken quite literally. The individual strands are homeomorphic to the unit interval $[0,1]$, and the scene takes place in $\mathbb{R}^3$. We think of such a braid as going "down" from n fixed starting points ($n = 4$ on the picture) to n end points, also fixed once and for all. The strands are not allowed to turn back up on their way down (if they did, they would be "tangles", to be described later).



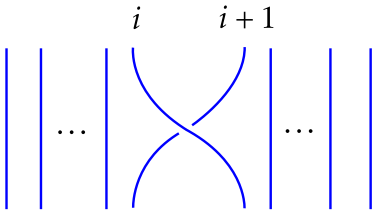
There is a composition law on the set of geometric braids, which briefly is "stack on top and rescale". In other words  composed with

 gives:



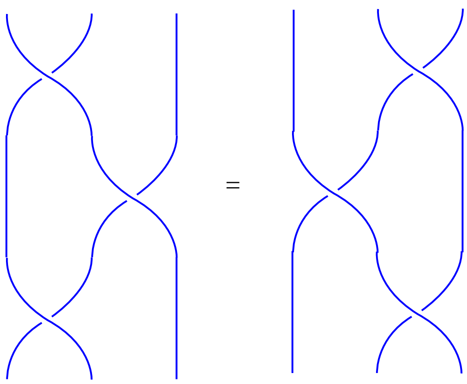
If we look at braids up to isotopy, then this composition gives a group law, with identity given by the "straight" braid, and inverses given by vertical mirror-images. The group formed by the isotopy classes of braids on n strands form the *braid group* B_n.

Let us give Artin's presentation of the braid group. First we introduce the braid $\sigma_i \in B_n$:



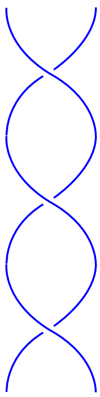
Theorem B.1 – *The group B_n is generated by the σ_i's. The relations between these all follow from $\sigma_i\sigma_j = \sigma_j\sigma_j$ when $|i-j| > 1$, and $\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}$.*

For example here is why $\sigma_1\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2$:

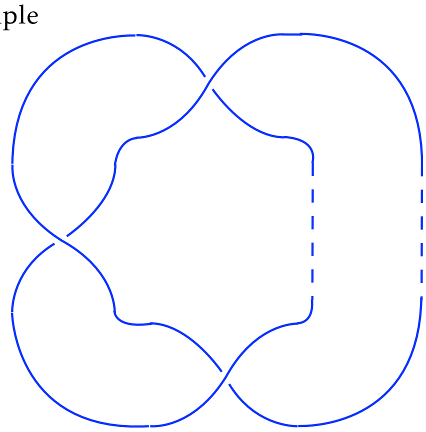


Links

Any braid β gives an oriented link $\hat{\beta}$ in $\mathbb{R}^3$ obtained by glueing its top and bottom, and called its *closure*. For example



gives

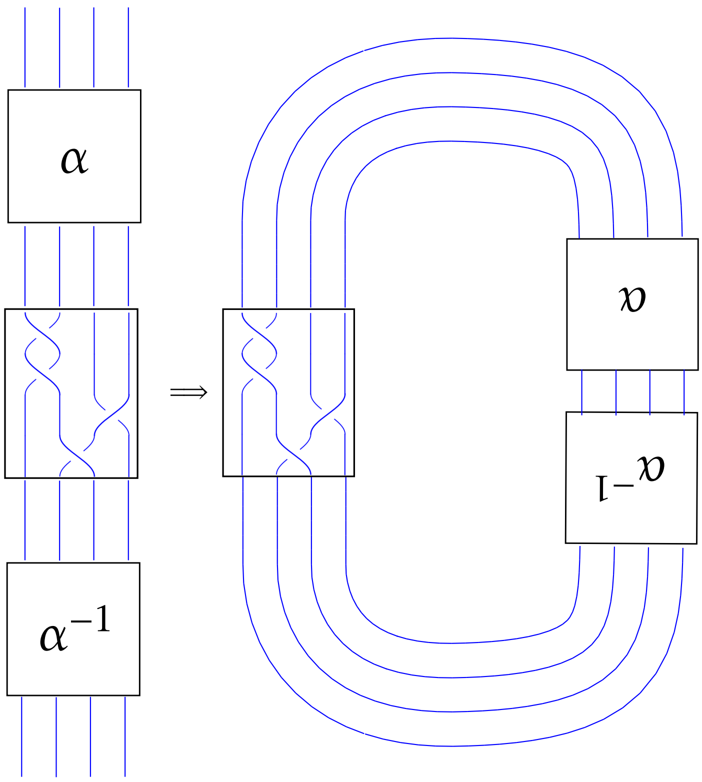


Alexander's celebrated Theorem is particularly easy to state:

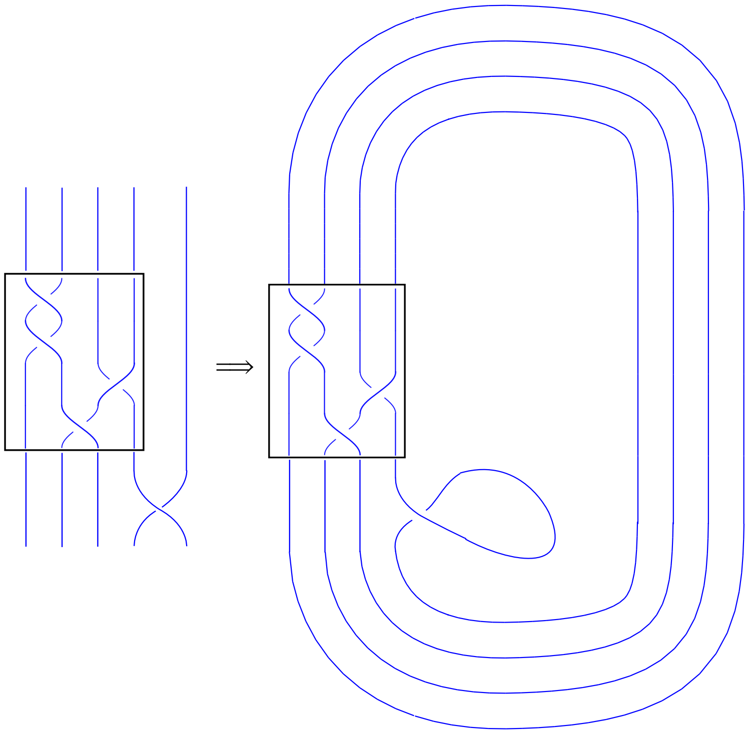
Theorem B.2 – *Any oriented link L in Euclidean 3-space is obtained as the closure $\hat{\beta}$ of some braid β.*

It would take a serious lack of curiosity not to ask: given two braids β and γ, when are $\hat{\beta}$ and $\hat{\gamma}$ isotopic ? This may well happen with $\beta \in B_n$ and $\gamma \in B_m$ with $n \neq m$.

For one thing, we have the formula $\widehat{\alpha\beta\alpha^{-1}} = \widehat{\beta}$, which is illustrated below.



Another simple observation is that $\widehat{\iota(\beta)\sigma_n^{\pm}} = \widehat{\beta}$, where $\iota\colon B_n \to B_{n+1}$ is the obvious inclusion (which adds a straight strand).



These are called the *Markov moves*, in reference to Markov's theorem, which is the following.

Theorem B.3 – *The two Markov moves generate the equivalence relation on $\coprod_n B_n$ which relates two braids when they have the same closure up to isotopy.*

In other words, let $f = (f_n)_{n\geq 2} : \coprod B_n \to S$ be any map to a set S. When f satisfies

1. $f_n(\gamma\beta\gamma^{-1}) = f_n(\beta)$,
2. $f_{n+1}(\iota(\beta)\sigma_n^{\pm 1}) = f_n(\beta)$ *for* $\beta \in B_n$,

and only in this case, then $f(\beta)$ depends only on the closure $\hat{\beta}$.

The collection $(f_n)_{n\geq 2}$ is called a Markov function. Thus defining a Markov function is tantamount to producing an isotopy invariant for oriented links in Euclidean 3-space.

A typical strategy to achieve this aim, on which we will expand quite a bit, is to look for representations $B_n \to GL(V_n)$ and define f_n to be a familiar function on the matrix group $GL(V_n)$ which is known to be conjugation-invariant, such as the trace or determinant. There remains to check condition (2) above, which is a requirement on the way one passes from the module V_n to V_{n+1}.

Example B.4 – Perhaps the most famous family of representations of the braid groups is the *Burau representation* (note that "Burau" is a German name whose pronounciation is nowhere near that of "bureau"). This is given by the the homomorphism $r_n : B_n \to GL_n(\mathbb{Z}[t, t^{-1}])$ defined by

$$\rho_n(\sigma_i) = \begin{pmatrix} I_{i-1} & 0 & 0 & 0 \\ 0 & 1-t & 1 & 0 \\ 0 & t & 0 & 0 \\ 0 & 0 & 0 & I_{n-i-1} \end{pmatrix}.$$

The determinant $d_n(\beta) = \det(\rho_n(\beta) - Id)$ is an element of $\mathbb{Z}[t, t^{-1}]$ for each braid $\beta \in B_n$. We write $D_n(\beta) \in \mathbb{Z}[s, s^{-1}]$ for this determinant evaluated at $t = s^2$.

If we put then

$$f_n(\beta) = (-1)^{n+1} \frac{s^{-\langle\beta\rangle}(s - s^{-1})}{s^n - s^{-n}} D_n(\beta),$$

then one can show that $(f_n)_{n\geq 2}$ is a Markov function; here $\beta \mapsto \langle\beta\rangle \in \mathbb{Z}$ is the *length* map, the only homomorphism $B_n \to \mathbb{Z}$ taking the value 1 on the generators σ_i. The associated link invariant is the *Alexander-Conway polynomial*.

R-matrices

In the next chapter we will define a link invariant following the strategy outlined above, and there are no further prerequisites for this chapter. However in chapter 4, we will refer to the machinery of R-matrices, which are best understood in view of their relations to braids. Thus this is the natural place to give an overview of this theory (although braids are not themselves mentioned in chapter 4).

Hopf algebras and R-matrices, in short, will show that there is a wealth of representations of the braid groups, and a systematic way of constructing them. A reference is [Kas95].

Definition B.5 – Let A be a Hopf algebra over the field k. A (universal) *R-matrix* for A is an invertible element $R \in A\otimes A$ such that

1. $\Delta^{op}(x) = R\Delta(x)R^{-1}$ for all $x \in A$,
2. $(\Delta\otimes id)(R) = R_{13}R_{23}$,
3. $(id\otimes\Delta)(R) = R_{13}R_{12}$,

where the following notation is used. The map $\Delta\colon A \to A\otimes A$ is the comultiplication (or diagonal) of A. For any A-modules V and W, we write $\tau_{V,W}$ for the flip $V\otimes W \to W\otimes V$ sending $v\otimes w$ to $w\otimes v$, and then $\Delta^{op} = \tau_{A,A}\circ\Delta$. Finally $R_{13} = (\tau_{A,A}\otimes id)(1\otimes R)$, while $R_{12} = R\otimes 1$ and $R_{23} = 1\otimes R$. ■

In order to illustrate what the axioms mean, we must at once introduce the maps
$$c_{V,W}\colon V\otimes W \longrightarrow W\otimes V$$
(one for each pair V, W of A-modules) defined by
$$c_{V,W}(v\otimes w) = \tau_{V,W}(Rv\otimes w).$$
The reader will observe that if we see $V\otimes W$ and $W\otimes V$ as A-modules in the usual way, then $c_{V,W}$ is a map of A-modules (from the first axiom). To get a feeling for the other two axioms, the best is to state the following.

Theorem B.6 – *Let A be a Hopf algebra with universal R-matrix. Then for any A-module V, the braid group B_n acts on $V^{\otimes n}$ by automorphisms of A-modules. The action of σ_i is given by*
$$id\otimes id\otimes\cdots\otimes id\otimes c_{V,V}\otimes id\cdots\otimes id\,,$$
where $c_{V,V}$ acts on the i-th and $i+1$-st factors.

In particular, on $V\otimes V\otimes V$ we have σ_1 acting as $R\otimes id$ and σ_2 acting as $id\otimes R$, in such a way that $\sigma_1\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2$. If one chooses a basis for V as a k-vector space and writes the above in terms of matrices, then one recovers the classical definition of R-matrices in terms of the "Yang-Baxter equation" (hence the name "universal R-matrix" for the element $R \in A\otimes A$).

Example B.7 – Whenever A is cocommutative (meaning $\Delta = \Delta^{op}$), one can take $R = 1\otimes 1$. In this situation the action on $V^{\otimes n}$ is particularly simple.

Note that there is a morphism of groups $B_n \to S_n$, where S_n is the symmetric group on n letters: simply assign to a braid the associated permutation of the end points. The kernel of this map is generated by the elements σ_i^2 (observe that σ_i corresponds to the transposition $(i, i+1)$). It follows that an action of B_n on $V^{\otimes n}$ factors through S_n if and only if $\tau_{A,A}(R) = R^{-1}$. (This is usually perceived as disappointing when it occurs, although in positive characteristic the representations of S_n are difficult to study and this procedure may very well give non-trivial results).

In the very particular case when $R = 1 \otimes 1$, the action of S_n is the obvious one, permuting the factors.

Example B.8 – Examples of Hopf algebras are, of course, provided by the algebras of functions (smooth, regular...), on a group (Lie, algebraic...). Let us stick to the simplest case and consider a finite group G and the algebra $A = \mathcal{O}(G)$ of all k-valued functions on it.

The elements of $A \otimes A$ are thus functions on $G \times G$. It is fun to check that an R-matrix in this situation is given by a map

$$G \times G \longrightarrow k^\times$$

which is *bilinear*.

In a similar vein, consider the case when A is commutative. Then the first axioms states that A must be cocommutative as well (for example $A = k[G]$, the group algebra of an abelian group G). We can then consider the group scheme $\mathbf{G}$ defined by $\mathbf{G}(K) = Hom_{k-alg}(A, K)$ for any k-algebra K (we hasten to add that we shall not use anything from the theory of group schemes in the argument that follows, beyond Yoneda's Lemma). Then an R-matrix corresponds to a map

$$\mathbf{G} \times \mathbf{G} \longrightarrow \mathbf{G}_m,$$

where $\mathbf{G}_m$ is the multiplicative group, that is $\mathbf{G}_m(K) = K^\times$, which is again bilinear in an appropriate sense.

The Reshetikhin-Turaev Theorem

We have now described all the material needed to read chapters 3 and 4. However, at this stage when we know how to produce lots of representations of the braid groups, the reader probably wonders whether one can go further and produce Markov functions from an appropriate Hopf algebra. The positive answer is given by the beautiful Theorem by Reshetikhin and Turaev stated below. This result is definitely not used in the following chapters, and we include it for fun. More details can be found in [KRT97] and the references therein.[1]

We need to switch to a categorical language. At the heart of the Theorem below is the definition of a *ribbon category*. Postponing a more formal definition, this is a monoidal category satisfying some simple-looking, linear-algebra-like axioms. The main point is the realization that, in spite of this modest initial description, such categories are intimately related to braids and links, in the following sense: given a collection of objects, there is a "free" ribbon category on those objects, and the latter is defined explicitly in terms of *tangles* (which generalize simultaneously braids and links).

Crucial to the applications is the fact that the category $\mathcal{C}$ of A-modules over a "nice" Hopf algebra A is ribbon. Thus there is a functor from the free ribbon category on the objects of $\mathcal{C}$ to $\mathcal{C}$ itself, and when we spell out what this means, we discover many (framed) link invariants (and much more).

Definition B.9 – A *ribbon category* is a category $\mathcal{C}$ equipped with a monoidal structure written $\otimes$, and endowed with the following extra structure.

1. *Commutativity constraint.* For any pair V, W of objects of $\mathcal{C}$, there is a natural map
$$c_{V,W} \colon V \otimes W \longrightarrow W \otimes V,$$
which is required to satisfy
$$c_{U \otimes V, W} = (c_{U,W} \otimes id_V)(id_U \otimes c_{V,W}),$$
$$c_{U, V \otimes W} = (id_V \otimes c_{U,W})(c_{U,V} \otimes id_W).$$

[1] Let us point out that the very general result to be described deals in fact with *framed* links (of which we say a word in the text), so it is a slight abuse of language to speak of Markov functions and so on. It is not our concern to discuss the details of this.

2. *Duality.* For each object V in $\mathcal{C}$, there is an associated object V^* and maps

$$b_V : 1 \longrightarrow V \otimes V^*, \qquad d_V : V^* \otimes V \longrightarrow 1,$$

such that

$$(id_V \otimes d_V)(b_V \otimes id_V) = id_V,$$
$$(d_V \otimes id_{V^*})(id_{V^*} \otimes b_V) = id_{V^*}.$$

(Here for simplicity we have suppressed from the first equation the associativity isomorphism between $(V \otimes V^*) \otimes V$ and $V \otimes (V^* \otimes V)$. It holds as stated when $\mathcal{C}$ is strict.)

3. *Twisting.* For any object V of $\mathcal{C}$, we have a natural morphism

$$\theta_V : V \longrightarrow V,$$

such that

$$\theta_{V \otimes W} = c_{W,V} c_{V,W} (\theta_V \otimes \theta_W).$$

Moreover, we require the following compatibility condition: for any object V of $\mathcal{C}$, one must have

$$(\theta_V \otimes id_{V^*}) b_V = (id_V \otimes \theta_{V^*}) b_V.$$

■

Notice how the "twisting" axiom says that the composition $c_{W,V} \circ c_{V,W}$, while not equal to the identity, is a sort of coboundary.

Example B.10 – Let $\mathcal{C}$ denote the category of finite-dimensional vector spaces over the field k, equipped with the usual tensor product. Define the commutativity constraint to be the usual flip $v \otimes w \to w \otimes v$. The dual of V is its dual in the elementary sense. There are canonical identifications of $V \otimes V^*$ and $V^* \otimes V$ with $Hom(V,V)$; under these, the map b_V is $\lambda \mapsto \lambda id_V$ and d_V is the trace. Finally, take the twisting map θ_V to be the identity. Then $\mathcal{C}$ is a ribbon category.

Example B.11 – Let A be a Hopf algebra with R-matrix R, and let $\mathcal{C}$ be the category of finite-dimensional A-modules. Define the tensor product and duality in the traditional sense for Hopf algebras, with b_V and d_V as in the previous example. Define the commutativity constraint using the R-matrix, as we did just before Theorem B.6.

In this situation, one can show that $\mathcal{C}$ can be turned into a ribbon category provided that A satisfy the following simple extra assumption: there exists $\theta \in A$ which is central and verifies

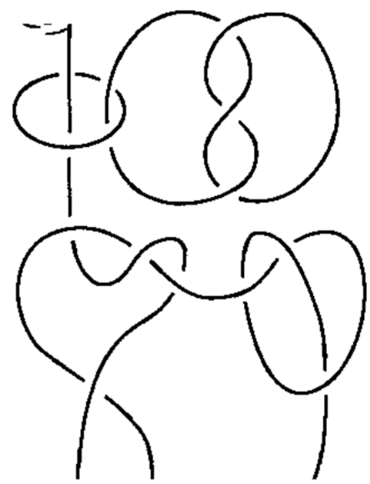
$$\Delta(\theta) = (\tau_{A,A}(R)R)^{-1}(\theta \otimes \theta), \quad \varepsilon(\theta) = 1, \quad \text{and } S(\theta) = \theta.$$

(Here ε is the augmentation of A, while S is the antipode.) The map θ_V is then multiplication by θ^{-1}. The existence of such an element θ is even necessary in the case when A is finite-dimensional.

In the very simple case envisaged in example B.7, that is when $\tau_{A,A}(R) = R^{-1}$ and the actions of B_n factor through S_n, one may take $\theta = 1 \otimes 1$.

We turn to the definition of the "free" ribbon categories. Fix n points in the plane $P_1 = \{z = 1\}$ in $\mathbb{R}^3$, and m points in the plane $P_0 = \{z = 0\}$. An (n,m)-*tangle* is a 1-manifold with boundary, embedded in $\mathbb{R}^3$ between P_0 and P_1, and whose boundary is made of (all of) our selected points. Tangles here are also assumed to be oriented, and to have a normal vector field; one may speak of framed tangles for emphasis, or indeed, of ribbons. So braids in B_n are special (n,n)-tangles, while links are $(0,0)$-tangles.[2] More possibilities are now allowed, as on the picture of a $(1,3)$-tangle below.

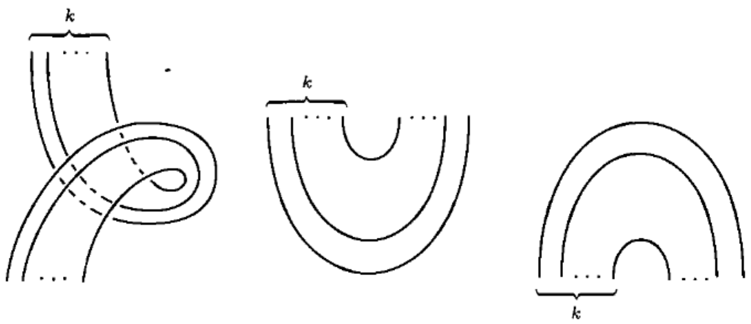
[2] this holds provided you endow them with a framing, which can be done canonically for braids and non-canonically in general; we will mostly ignore these technicalities in what follows. See previous footnote.



The isotopy classes of (n,m)-tangles can be seen as the morphisms between n and m in the category $\mathcal{T}$, whose objects are the natural numbers. Composition is defined by stacking and rescaling, as for braids.

Finally, given any category $\mathcal{C}$, we define $\mathcal{T}_{\mathcal{C}}$ to be the category whose objects are finite sequences $(V_1, \varepsilon_1, \ldots, V_n, \varepsilon_n)$ of objects of $\mathcal{C}$ and signs $\varepsilon_i = \pm 1$, and whose morphisms are isotopy classes of *$\mathcal{C}$-coloured tangles*. The latter are tangles with an object of $\mathcal{C}$ decorating each connected component. (We need a compatibility between the signs and the orientations, for example we may agree that near a boundary point corresponding to a -1 sign the orientation is going up.) The composition law should be obvious.

We are going to state shortly that $\mathcal{T}_{\mathcal{C}}$ is ribbon. Let us briefly indicate that the duality on objects reverses the order and the signs. The picture below shows the twist, as a morphism $k \to k$ in $\mathcal{T}$, as well as the maps $b\colon 0 \to 2k$ and $d\colon 2k \to 0$.



Here is finally the Reshetikhin-Turaev Theorem, whose proof can be found in [Tur10].

Theorem B.12 – *The category $\mathcal{T}_{\mathcal{C}}$ is the free ribbon category on the objects of $\mathcal{C}$, for any category $\mathcal{C}$.*

More precisely, $\mathcal{T}_{\mathcal{C}}$ is ribbon, and if $\mathcal{C}$ is itself ribbon, then there exists a unique functor

$$F\colon \mathcal{T}_{\mathcal{C}} \longrightarrow \mathcal{C}$$

compatible with the ribbon structures.

Let us indicate at once the following consequences. Assume that $\mathcal{C}$ is the category of A-modules for a Hopf algebra A over a field k as in example B.11; such a $\mathcal{C}$ is ribbon. Pick any (framed) link L, and decorate all its connected components with an arbitrary object V of $\mathcal{C}$. Then L can be seen as a morphism in $\mathcal{T}_{\mathcal{C}}$ between the empty sequence and itself, so $F(L)$ is a morphism $k \to k$ (in $\mathcal{C}$ the "unit" for the tensor product is the object k). As a result $F(L)$ defines an element of k which is a (framed) link invariant. (Framed links may be replaced by plain links when the element θ in example B.11 is 1.)

The famous examples of *quantum groups* are Hopf algebras over $k = \mathbb{C}(q)$ satisfying the above conditions. The celebrated *Jones polynomial* of a link L is an element of $\mathbb{C}(q)$ which may be constructed in this fashion (for the reader familiar with the notation, for the Jones polynomial one takes $A = U_q(\mathfrak{sl}_2)$ and V is the unique 2-dimensional irreducible module).

It is also important to realize that Theorem B.12 implies Theorem B.6 for the corresponding Hopf algebras. Indeed, pick a braid β in B_n, decorate all its connected components with the object V, and view the result as a morphism between the object $(V, +1, \ldots, V, +1)$ (appearing n times) and itself, in $\mathcal{T}_\mathcal{C}$. Now apply F, and get a morphism $V^{\otimes n} \to V^{\otimes n}$ which is that of Theorem B.6.

Finally, from this Theorem we get a new, more satisfying outlook on the operation of closure. Indeed, a braid β and its closure $\hat{\beta}$, appropriately decorated, are both morphisms in $\mathcal{T}_\mathcal{C}$, and there *does* exist a general ribbon-theoretic construction that specializes to the operation $\beta \mapsto \hat{\beta}$ (no matter how geometric the latter seems). This is the *quantum trace* (so nominated in order to distinguish it from the usual trace, which in many examples of ribbon categories is also available; in the case considered in example B.10, the quantum trace is just the trace, but the two are distinct already in example B.11). In a general ribbon category for which the unit object for the monoidal structure is written 1, the quantum trace of $f\colon V \to V$ is

$$Tr_q(f) = d_V c_{V,V^*}((\theta_V f) \otimes id_{V^*})\, b_V \colon 1 \longrightarrow 1\,.$$

It is amusing to check that the quantum trace of a braid β is indeed $\hat{\beta}$.

In a category of modules $\mathcal{C}$ over a Hopf algebra as above, the quantum trace of the morphism $F(\beta)\colon V^{\otimes n} \to V^{\otimes n}$ defines an element of k, and it is a consequence of the Theorem that the functions $f_n\colon B_n \to k$ mapping β to $Tr_q(F(\beta))$ form a Markov function. We conclude by adding that in the case of quantum groups, the quantum trace is well-understood: there is a distinguished element $K \in A$ such that the quantum trace of any morphism $f\colon V \to V$ in $\mathcal{C}$ is the usual trace of Kf.

Appendix C

Algebraic cycles and classifying spaces

In this appendix we collect some of my early results on Chow rings of classifying spaces. In contrast with the other chapters of this document, we give little background information.

Very briefly, the situation is as follows. One considers an algebraic group G over $\mathbb{C}$, for example a finite group. The object is to study the cycle map

$$CH^*BG \longrightarrow H^*(BG, \mathbb{Z})$$

or the variant

$$CH^*BG \otimes_{\mathbb{Z}} \mathbb{F}_p \longrightarrow H^*(BG, \mathbb{F}_p).$$

(See appendix A on how BG can be considered as an algebraic variety.) Sometimes one is able to compute CH^*BG, sometimes only the image $\mathfrak{Ch}^*BG$ of the cycle map is described.

Recall also Totaro's factorization of the cycle map as follows:

$$CH^*BG \longrightarrow MU^*(BG) \otimes_{MU^*} \mathbb{Z} \longrightarrow H^*(BG, \mathbb{Z}).$$

Here MU is the complex cobordism spectrum.

§1. Symmetric groups & Chevalley groups

The results in this section complete those of §2, of which we use the notation.

$\longrightarrow$ Theorem C.1 – *Let S_n denote the symmetric group on n letters, and let p be a prime number. There are isomorphisms*

$$CH^*BS_n \otimes_{\mathbb{Z}} \mathbb{F}_p \cong MU^*(BS_n) \otimes_{MU^*} \mathbb{Z} \cong \tilde{O}H^*(BS_n, \mathbb{F}_p).$$

Moreover

$$CH^*BS_n \otimes_{\mathbb{Z}} \mathbb{F}_p \cong \lim_{E} CH^*BE \otimes_{\mathbb{Z}} \mathbb{F}_p$$

where E runs through the elementary abelian p-groups of S_n.

See [Gui05].

$\longrightarrow$ Theorem C.2 – *Let G be a Chevalley group, let p be a prime number such that $H^*(G(\mathbb{C}), \mathbb{Z})$ does not have p-torsion, and let k be a finite field of characteristic $\neq p$ containing the p-th roots of unity. Then there is an isomorphism*

$$MU^*(BG(k)) \otimes_{MU^*} \mathbb{Z} \cong H^*(BG(\mathbb{C}), \mathbb{F}_p),$$

and this ring injects into $H^*(BG(k), \mathbb{F}_p)$.

Assume moreover that G is semi-simple and that $p > 7$. Then the image of the above ring is precisely the image of the cycle map, and

$$\mathfrak{Ch}^*(BG(k)) = \mathfrak{Ch}^*(BT(k))^W$$

where T is a split maximal torus and W is the Weyl group.

Finally when G is one of GL_n, SL_n, Sp_n, $Spin_n$, SL_n for p prime to n, or an exceptional group, or a product of groups in this list, then the cycle map is injective.

See [Gui04] and again [Gui05] (where the relation between this theorem and Steenrod operations is explained).

§2. The group $Spin_7$

The cohomology ring $H^*(BSpin_7, \mathbb{F}_2)$ is polynomial (see the computation by Quillen in [Qui71]). By contrast, the Chow ring of the same group is much more involved. Here is a description of $CH^*BSpin_7 \otimes_{\mathbb{Z}} \mathbb{Z}_{(2)}$.

⟶ Theorem C.3 – *One has*

$$CH^*(BSpin_7)_{(2)} = \frac{\mathbb{Z}_{(2)}[c_2', c_4, c_4', c_6, c_6', c_7, c_8', \zeta]}{I}$$

where I is the ideal generated by the following relations (with $\delta_i = 0$ or 1 ($i = 1, 2$)):

$$\begin{aligned}
2\zeta = 0, \quad 2c_7 &= 0 \\
\zeta_3^2 = 0, \quad \zeta_3 c_7 = 0, \quad \zeta_3 c_4' &= \zeta_3 c_4 \\
\zeta_3 c_6' = \zeta_3 c_6, \quad \zeta_3 c_2' &= 0 \\
c_2' c_6' - c_2' c_6 &= \frac{2}{3} c_4 (c_4' - c_4) + 16 c_8' \\
c_2' c_7 &= \delta_1 c_6 \zeta_3 \\
c_4'(c_4' - c_4) &= c_4(c_4' - c_4) + 36 c_8' \\
c_4'(c_6' - c_6) &= c_4(c_6' - c_6) + 6 c_2' c_8' \\
c_4' c_7 - c_4 c_7 &= \delta_2 c_8 \zeta_3 \\
(c_2')^2 - 4c_4 &= \frac{8}{3}(c_4' - c_4) \\
c_6'(c_6' - c_6) &= c_6(c_6' - c_6) + c_8'\left(\frac{8}{3} c_4' + \frac{4}{3} c_4\right) \\
c_2' c_4' - c_2' c_4 &= 6(c_6' - c_6) \\
c_6' c_7 &= c_6 c_7 .
\end{aligned}$$

Moreover one has an isomorphism

$$CH^*(BSpin_7)_{(2)} \cong MU^*(BSpin_7) \otimes_{MU^*} \mathbb{Z}_{(2)} .$$

See [Gui07a].

⟶ Theorem C.4 – *There is a finite subgroup G of $Spin_7$ such that the ring CH^*BG is not generated by Chern classes and transfers of Chern classes.*

This is a counter-example to a conjecture of Totaro's (formulated in [Tot99]). We prove this theorem in [Gui08].

§3. Cohomological invariants

In appendix A we have introducted CH^*BG, the cycle map to $H^*(BG)$, and $Inv(G)$. These are related to one another via the following spectral sequence.

Theorem C.5 (Rost, Bloch, Ogus) – *Let k be algebraically closed. There exists a spectral sequence*

$$E_2^{r,s} = A^r(BG, H^{s-r}) \Longrightarrow H_{et}^{r+s}(BG).$$

In particular the E_2 page is zero under the first diagonal, and the resulting map

$$A^n(BG, H^0) = CH^n(BG) \otimes_{\mathbb{Z}} \mathbb{F}_p \longrightarrow H_{et}^n(BG)$$

is the cycle map.

A word of explanation is in order. Here we write $A^*(X, H^*)$ for Rost's Chow groups with coefficients in Galois cohomology, at the implicit prime p, see [Ros96]. This is a bigraded ring, and $A^*(X, H^0) = CH^*(X) \otimes \mathbb{F}_p$, while $A^0(BG, H^*) = Inv(G)$. Also, $H_{et}^*(X)$ is the étale cohomology of X with coefficients in $\mathbb{F}_p$ (when $k = \mathbb{C}$ this is the ordinary cohomology of X).

This is the classical Bloch & Ogus spectral sequence, as reinterpreted by Rost in terms of his Chow groups. In [Gui07b] (to which we refer for more details and references) we have explained how to apply it to BG instead of a plain algebraic variety. Surprisingly, the spectral sequence had never been explicitly applied to the computations of cohomological invariants. In *loc. cit.* we note the following.

⟶ Proposition C.6 – *There is a map*

$$H_{et}^*(BG) \longrightarrow Inv(G)$$

which vanishes (for $* > 0$) on the image of the cycle map.

In particular there are isomorphisms

$$Inv^1(G) \cong H_{et}^1(BG)$$

and

$$Inv^2(G) \cong \frac{H_{et}^2(BG)}{\mathfrak{Ch}^1(BG)}.$$

For $k = \mathbb{C}$ this yields

$$Inv^1(G) \cong Hom(\pi_0(G), \mathbb{F}_p)$$

and

$$Inv^2(G) = p\text{-torsion in } H^3(BG, \mathbb{Z}).$$

Finally, any non-zero element in the kernel of the cycle map

$$CH^2(BG) \otimes_{\mathbb{Z}} \mathbb{F}_p \longrightarrow H_{et}^4(BG)$$

determines a non-zero cohomological invariant in $Inv^3(G)$.

The main point in [Gui07b] however is to show how the "stratification method", originally introduced by Vezzozi and already employed in my own computation of CH^*BSpin_7, could be put to good use with cohomological invariants. A possible application is as follows.

⟶ Theorem C.7 – *There is an exact sequence*

$$0 \longrightarrow Inv(Spin_{2n}) \longrightarrow Inv(\mathbb{Z}/2 \times Spin_{2n-1}) \xrightarrow{r} Inv(Spin_{2n-2}).$$

Moreover the image of r contains the image of the restriction map $Inv(Spin_{2n}) \to Inv(Spin_{2n-2})$.

The cohomological invariants of $Spin_n$ are only known for small values of n (up to $n = 14$ to the best of my knowledge).

Bibliography

[Ada92] J. Frank Adams, *Two theorems of J. Lannes, the selected works of J. Frank Adams. Vol. II*, Cambridge University Press, Cambridge, 1992. MR 1203313 (94d:01095b)

[AK08] Eli Aljadeff and Christian Kassel, *Polynomial identities and noncommutative versal torsors*, Adv. Math. **218** (2008), no. 5, 1453–1495. MR 2419929 (2009d:16051)

[AKM99] Alejandro Adem, Dikran B. Karagueuzian, and Ján Mináč, *On the cohomology of Galois groups determined by Witt rings*, Adv. Math. **148** (1999), no. 1, 105–160. MR 1736643 (2001b:12010)

[AM04] Alejandro Adem and R. James Milgram, *Cohomology of finite groups*, second ed., Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 309, Springer-Verlag, Berlin, 2004. MR 2035696 (2004k:20109)

[BC06] Julien Bichon and Giovanna Carnovale, *Lazy cohomology: an analogue of the Schur multiplier for arbitrary Hopf algebras*, J. Pure Appl. Algebra **204** (2006), no. 3, 627–665. MR 2185622 (2006i:16052)

[Ben04] Dave Benson, *Dickson invariants, regularity and computation in group cohomology*, Illinois J. Math. **48** (2004), no. 1, 171–197. MR 2048221 (2005c:20089)

[BF91] D. J. Benson and V. Franjou, *Séries de compositions de modules instables et injectivité de la cohomologie du groupe* $\mathbf{Z}/2$, Math. Z. **208** (1991), no. 3, 389–399. MR 1134584 (93b:55022)

[Bre97] Glen E. Bredon, *Topology and geometry*, Graduate Texts in Mathematics, vol. 139, Springer-Verlag, New York, 1997, Corrected third printing of the 1993 original. MR 1700700 (2000b:55001)

[Bro03] Patrick Brosnan, *Steenrod operations in Chow theory*, Trans. Amer. Math. Soc. **355** (2003), no. 5, 1869–1903 (electronic). MR 1953530 (2004f:14008)

[Car99] Jon F. Carlson, *Problems in the calculation of group cohomology*, Computational methods for representations of groups and algebras (Essen, 1997), Progr. Math., vol. 173, Birkhäuser, Basel, 1999, pp. 107–120. MR 1714605 (2001i:20111)

[Car01] ———, *Calculating group cohomology: tests for completion*, J. Symbolic Comput. **31** (2001), no. 1-2, 229–242, Computational algebra and number theory (Milwaukee, WI, 1996). MR 1806218 (2002c:20083)

[CG] Gaël Collinet and Pierre Guillot, *A link invariant with values in the Witt ring*, to appear in Quantum Topology, Arxiv 1106.3598.

[DH01] William G. Dwyer and Hans-Werner Henn, *Homotopy theoretic methods in group cohomology*, Advanced Courses in Mathematics. CRM Barcelona, Birkhäuser Verlag, Basel, 2001. MR 1926776 (2003h:20093)

[Dwy96] W. G. Dwyer, *Transfer maps for fibrations*, Math. Proc. Cambridge Philos. Soc. **120** (1996), no. 2, 221–235. MR 1384465 (97h:55014)

[FL85] William Fulton and Serge Lang, *Riemann-Roch algebra*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 277, Springer-Verlag, New York, 1985. MR 801033 (88h:14011)

[FS89] Walter Feit and Gary M. Seitz, *On finite rational groups and related topics*, Illinois J. Math. **33** (1989), no. 1, 103–131. MR 974014 (90a:20016)

[GG05] Jean-Marc Gambaudo and Étienne Ghys, *Braids and signatures*, Bull. Soc. Math. France **133** (2005), no. 4, 541–579. MR 2233695 (2007d:57014)

[GK10] Pierre Guillot and Christian Kassel, *Cohomology of invariant Drinfeld twists on group algebras*, Int. Math. Res. Not. IMRN (2010), no. 10, 1894–1939. MR 2646345 (2011i:16016)

[GKM12] Pierre Guillot, Christian Kassel, and Akira Masuoka, *Twisting algebras using non-commutative torsors: explicit computations*, Math. Z. **271** (2012), no. 3-4, 789–818. MR 2945585

[GM] Pierre Guillot and Ján Mináč, *Milnor K-theory and the graded representation ring*, Arxiv 1109.0046.

[GMS03] Skip Garibaldi, Alexander Merkurjev, and Jean-Pierre Serre, *Cohomological invariants in Galois cohomology*, University Lecture Series, vol. 28, American Mathematical Society, Providence, RI, 2003. MR 1999383 (2004f:11034)

[Gui04] Pierre Guillot, *Chow rings and cobordism of some Chevalley groups*, Math. Proc. Cambridge Philos. Soc. **136** (2004), no. 3, 625–642. MR 2055051 (2005b:19010)

[Gui05] ______, *Steenrod operations on the Chow ring of a classifying space*, Adv. Math. **196** (2005), no. 2, 276–309. MR 2166309 (2006f:55018)

[Gui07a] ______, *The Chow rings of G_2 and Spin(7)*, J. Reine Angew. Math. **604** (2007), 137–158. MR 2320315 (2008e:14005)

[Gui07b] ______, *Geometric methods for cohomological invariants*, Doc. Math. **12** (2007), 521–545 (electronic). MR 2365912 (2008m:14015)

[Gui07c] ______, *The representation ring of a simply connected Lie group as a λ-ring*, Comm. Algebra **35** (2007), no. 3, 875–883. MR 2305237 (2007k:22010)

[Gui08] ______, *Addendum to the paper: "The Chow rings of G_2 and* Spin(7)*" [J. Reine Angew. Math.* **604** *(2007), 137–158; 2320315]*, J. Reine Angew. Math. **619** (2008), 233–235. MR 2414952 (2009h:14011)

[Gui10] ______, *The computation of Stiefel-Whitney classes*, Ann. Inst. Fourier (Grenoble) **60** (2010), no. 2, 565–606. MR 2667787 (2011f:20119)

[Gui12] ______, *Examples of quantum algebra in positive characteristic*, Arxiv 1202.5951.

[Kas95] Christian Kassel, *Quantum groups*, Graduate Texts in Mathematics, vol. 155, Springer-Verlag, New York, 1995. MR 1321145 (96e:17041)

[Kas04] ______, *Quantum principal bundles up to homotopy equivalence*, The legacy of Niels Henrik Abel, Springer, Berlin, 2004, pp. 737–748. MR 2077593 (2005f:16059)

[KRT97] Christian Kassel, Marc Rosso, and Vladimir Turaev, *Quantum groups and knot invariants*, Panoramas et Synthèses [Panoramas and Syntheses], vol. 5, Société Mathématique de France, Paris, 1997. MR 1470954 (99b:57011)

[KT76] D. M. Kan and W. P. Thurston, *Every connected space has the homology of a $K(\pi,1)$*, Topology **15** (1976), no. 3, 253–258. MR 0413089 (54 #1210)

[KT08] Christian Kassel and Vladimir Turaev, *Braid groups*, Graduate Texts in Mathematics, vol. 247, Springer, New York, 2008, With the graphical assistance of Olivier Dodane. MR 2435235 (2009e:20082)

[MH73] John Milnor and Dale Husemoller, *Symmetric bilinear forms*, Springer-Verlag, New York, 1973, Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 73. MR 0506372 (58 #22129)

[Mil58] John Milnor, *The Steenrod algebra and its dual*, Ann. of Math. (2) **67** (1958), 150–171. MR 0099653 (20 #6092)

[Mil70] ______, *Algebraic K-theory and quadratic forms*, Invent. Math. **9** (1969/1970), 318–344. MR 0260844 (41 #5465)

[MS74] John W. Milnor and James D. Stasheff, *Characteristic classes*, Princeton University Press, Princeton, N. J., 1974, Annals of Mathematics Studies, No. 76. MR 0440554 (55 #13428)

[MS96] Ján Mináč and Michel Spira, *Witt rings and Galois groups*, Ann. of Math. (2) **144** (1996), no. 1, 35–60. MR 1405942 (97i:11038)

[Mum65] David Mumford, *Geometric invariant theory*, Ergebnisse der Mathematik und ihrer Grenzgebiete, Neue Folge, Band 34, Springer-Verlag, Berlin, 1965. MR 0214602 (35 #5451)

[MV99] Fabien Morel and Vladimir Voevodsky, *$\mathbf{A}^1$-homotopy theory of schemes*, Inst. Hautes Études Sci. Publ. Math. (1999), no. 90, 45–143 (2001). MR 1813224 (2002f:14029)

[Qui71] Daniel Quillen, *The* mod 2 *cohomology rings of extra-special* 2*-groups and the spinor groups*, Math. Ann. **194** (1971), 197–212. MR 0290401 (44 #7582)

[Rad93] David E. Radford, *Minimal quasitriangular Hopf algebras*, J. Algebra **157** (1993), no. 2, 285–315. MR 1220770 (94c:16052)

[Ros96] Markus Rost, *Chow groups with coefficients*, Doc. Math. **1** (1996), No. 16, 319–393 (electronic). MR 1418952 (98a:14006)

[Sah68] Chih-han Sah, *Automorphisms of finite groups*, J. Algebra **10** (1968), 47–68. MR 0229713 (37 #5287)

[Ser02] Jean-Pierre Serre, *Galois cohomology*, english ed., Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2002, Translated from the French by Patrick Ion and revised by the author. MR 1867431 (2002i:12004)

[Ste99] Norman Steenrod, *The topology of fibre bundles*, Princeton Landmarks in Mathematics, Princeton University Press, Princeton, NJ, 1999, Reprint of the 1957 edition, Princeton Paperbacks. MR 1688579 (2000a:55001)

[Swe68] Moss Eisenberg Sweedler, *Cohomology of algebras over Hopf algebras*, Trans. Amer. Math. Soc. **133** (1968), 205–239. MR 0224684 (37 #283)

[Tot99] Burt Totaro, *The Chow ring of a classifying space*, Algebraic K-theory (Seattle, WA, 1997), Proc. Sympos. Pure Math., vol. 67, Amer. Math. Soc., Providence, RI, 1999, pp. 249–281. MR 1743244 (2001f:14011)

[Tur10] Vladimir G. Turaev, *Quantum invariants of knots and 3-manifolds*, revised ed., de Gruyter Studies in Mathematics, vol. 18, Walter de Gruyter & Co., Berlin, 2010. MR 2654259 (2011f:57023)

[Voe03] Vladimir Voevodsky, *Motivic cohomology with* $\mathbf{Z}/2$*-coefficients*, Publ. Math. Inst. Hautes Études Sci. (2003), no. 98, 59–104. MR 2031199 (2005b:14038b)

[Voe11] ———, *On motivic cohomology with* $\mathbf{Z}/l$*-coefficients*, Ann. of Math. (2) **174** (2011), no. 1, 401–438. MR 2811603