SMOOTH SYMMETRIES OF MANIFOLDS AND ARITHMETIC OF THE SPHERE SPECTRUM

John Rognes

These are notes for a colloquium talk in Bonn, November 18th 2005. We make no claim to originality in this exposition, perhaps apart from the last half-page.

1. Algebraic number theory. In classical algebraic number theory one considers the number systems given by the ring of integers in a number field.

A number field F is a finite field extension of the rational numbers $\mathbb{Q}$, and its ring of integers $\mathcal{O}_F$ consists of the roots in F of monic polynomial equations

$$x^n + a_1 x_{n-1} + \cdots + a_{n-1} x + a_n = 0$$

where the a_i are integers. We also call $\mathcal{O}_F$ a number ring.

Here are some examples. (1) When $F = \mathbb{Q}$, this recovers the usual ring of integers $\mathcal{O}_\mathbb{Q} = \mathbb{Z}$. (2) When $F = \mathbb{Q}(i)$, with $i^2 = -1$, we obtain the ring of Gaussian integers $\mathcal{O}_{\mathbb{Q}(i)} = \mathbb{Z}[i]$. (3) The formulas are not always so simple, since when $F = \mathbb{Q}(\sqrt{5})$ we have $\mathcal{O}_F = \mathbb{Z}[\varphi]$ where $\varphi = (1 + \sqrt{5})/2$ is the golden ratio, and this ring properly contains $\mathbb{Z}[\sqrt{5}]$. (4) For each natural number n let $\zeta_n = \exp(2\pi i/n)$ be a primitive n-th root of unity. The n-th cyclotomic field (meaning circle-dividing) is $F = \mathbb{Q}(\zeta_n)$, and its ring of integers is $\mathcal{O}_F = \mathbb{Z}[\zeta_n]$.

It can be fruitful to study the problem of prime factorization in a number ring. In the case of the Gaussian integers, this leads to Fermat's 17th century result that each prime $p \equiv 1 \mod 4$ can be written as a sum of two squares $p = a^2 + b^2$. In the case of the p-th cyclotomic field $\mathbb{Q}(\zeta_p)$, for p an odd prime, one obtains the factorization

$$x^p + y^p = \prod_{i=1}^{p} (x + \zeta_p^i y)$$

over $\mathbb{Z}[\zeta_p]$ of one side of the integral equation $x^p + y^p = z^p$, also considered by Fermat.

In general, the issue of existence and uniqueness of prime factorization in a number ring is complicated. In 1844, Kummer published examples of non-uniqueness of such factorizations in cyclotomic number rings, and was led to extend the set of elements in a number ring by adjoining ideal numbers. In 1876, Dedekind reinterpreted these in terms of the modern notion of ideals in the number ring. For ideals, the familiar existence and uniqueness of prime factorizations of natural numbers is restored: each non-zero ideal $\mathfrak{a}$ in a number ring $\mathcal{O}_F$ can be written as a finite product of prime ideals

$$\mathfrak{a} = \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_n ,$$

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

uniquely up to reordering. In other words, the multiplicative monoid of non-zero ideals $\mathfrak{a}$ in $\mathcal{O}_F$ is isomorphic, via prime factorization, to the free abelian monoid on the set of non-zero prime ideals. The rule that to a nonzero element a associates the exponents $(e_\mathfrak{p})_\mathfrak{p}$ of the prime factorization $(a) = \prod_\mathfrak{p} \mathfrak{p}^{e_\mathfrak{p}}$ of the principal ideal $(a) = a\mathcal{O}_F$ defines a homomorphism

$$\mathcal{O}_F \setminus \{0\} \to \bigoplus_\mathfrak{p} \mathbb{N}_0$$

of abelian monoids.

Two classical arithmetic invariants of the number field F measure the difference between the original problem of prime factorization in $\mathcal{O}_F$ and the solved problem of prime ideal factorization, after passing to the abelian groups generated by the abelian monoids above. (1) The ideal class group $\mathrm{Cl}(F)$ is the free abelian group generated by the non-zero prime ideals $\mathfrak{p}$ of $\mathcal{O}_F$, modulo the subgroup generated by the principal ideals (a) for nonzero a in $\mathcal{O}_F$. It measures the obstruction for an ideal number to be an actual number. (2) The group of units $\mathcal{O}_F^\times$ measures what is lost when passing from numbers to ideals. There is an exact sequence

$$1 \to \mathcal{O}_F^\times \to F^\times \to \bigoplus_\mathfrak{p} \mathbb{Z} \to \mathrm{Cl}(F) \to 0\,.$$

Here $F^\times$ is the group completion of $\mathcal{O}_F \setminus \{0\}$, and $\bigoplus_\mathfrak{p} \mathbb{Z}$ is the group completion of $\bigoplus_\mathfrak{p} \mathbb{N}_0$.

By Minkowski's geometry of numbers, one finds that $\mathrm{Cl}(F)$ is a finite group, which sometimes can be computed explicitly (its order is the class number of F), and $\mathcal{O}_F^\times$ is a finitely generated abelian group. A third classical arithmetic invariant is the Brauer group $\mathrm{Br}(F)$ of Morita equivalence classes of central simple algebras over F, and its variant $\mathrm{Br}(\mathcal{O}_F[1/p])$ for the ring of p-integers, defined in terms of Azumaya algebras. We shall mention it only in passing.

2. Classifying spaces. One motivation for the definition of algebraic K-theory is that these arithmetic invariants, $\mathrm{Cl}(F)$, $\mathcal{O}_F^\times$ and $\mathrm{Br}(\mathcal{O}_F[1/p])$, naturally can be derived from the category of finitely generated projective modules over the ring $\mathcal{O}_F$.

Modules M over a ring R generalize the ideals in the ring, and form an abelian category, which is a convenient place to do algebra. In particular we can talk about the sum $M_1 \oplus M_2$ of two modules, and about the kernel and cokernel of a module homomorphism $f\colon M_1 \to M_2$. A finitely generated projective R-module P is a direct summand of a finitely generated free R-module, i.e., of the sum of a finite number of copies of R considered as an R-module. In the case of a number ring $R = \mathcal{O}_F$, there is the relation

$$\mathfrak{a} \oplus \mathfrak{b} = \mathfrak{ab} \oplus \mathcal{O}_F$$

between the direct sum of two ideals and their product. It is analogous to the relation

$$L_1 \oplus L_2 \cong L_1 \otimes L_2 \oplus \mathbb{C}_X$$

for complex line bundles L_1, L_2 over an algebraic curve or topological surface X. It follows that each nonzero ideal is a finitely generated projective $\mathcal{O}_F$-module, of constant rank one. The relation also connects the multiplicative study of ideals discussed above to the additive study of modules that follows.

Let $\mathcal{C}$ be a small category, i.e., a set $\mathrm{ob}\,\mathcal{C}$ of objects, a set $\mathcal{C}(a,b)$ of morphisms $f\colon a \to b$ for each pair of objects a and b, and a unital and associative composition law

$$\circ\colon \mathcal{C}(b,c) \times \mathcal{C}(a,b) \to \mathcal{C}(a,c)$$

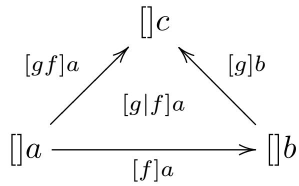
for each triple of objects a, b and c. For brevity, we mostly suppress mention of identity objects and unitality hereafter.

(0) Given a group G, there is a category $\mathcal{G}$ with only one object $*$, and morphism set $\mathcal{G}(*,*) = G$, with composition given by the group multiplication. In fact, it suffices to assume that G is a monoid.

(1) Given a ring R, there is a category $\mathcal{P}_R$ of finitely generated projective R-modules and their homomorphisms, and the subcategory $i\mathcal{P}_R$ of such R-modules and their isomorphisms.

(2) Given a space X, let $R(X)$ be the category of finite retractive spaces over X, meanings spaces Y built from X by attaching finitely many cells, together with a choice of retraction $r\colon Y \to X$. In particular, (Y, X) is a finite relative CW complex. When $X = *$, this is the same as a finite based CW complex Y, and there is only one choice for the retraction. A morphism from Y' to Y in the category $R(X)$ is a continuous map $f\colon Y' \to Y$ that is the identity on X and commutes with the retractions to X. By restricting the morphisms f to be homotopy equivalences, we obtain the subcategory $hR(X)$.

To each small category $\mathcal{C}$ we can associate a topological space $B\mathcal{C}$, called the classifying space of the category. In rough terms, it is a geometric picture of the objects, the morphisms and the composition law of the category. We begin by drawing one separate point $[]a$ for each object of the category. Next, for each morphism $f\colon a \to b$ in the category, we draw a separate edge $[f]a$ from the point $[]a$ to the point $[]b$. Then, for each pair (g, f) of composable morphisms $f\colon a \to b$ and $g\colon b \to c$ in the category, with composite $gf\colon a \to c$, we fill in a separate triangle $[g|f]a$ with vertices $[]a$, $[]b$ and $[]c$ and edges $[f]a$, $[g]b$ and $[gf]a$.



At this point, all of the defining data of the category have been used, but not the associativity axiom for the composition. So we continue, inserting a separate pyramid, or tetrahedron, $[h|g|f]a$ for each triple (h, g, f) of composable morphisms

$$d \xleftarrow{h} c \xleftarrow{g} b \xleftarrow{f} a$$

in $\mathcal{C}$. This also accounts for associativity, but we do not stop here. Instead we keep going indefinitely, inserting a convex q-simplex

$$\Delta^q = \{(t_0, \dots, t_q) \mid \sum_{i=0}^{q} t_i = 1, t_i \geq 0\}$$

(labeled $[f_1|f_2|\dots|f_{q-1}|f_q]a_q$) for each composable chain of q morphisms

$$a_0 \xleftarrow{f_1} a_1 \xleftarrow{f_2} \dots \xleftarrow{f_{q-1}} a_{q-1} \xleftarrow{f_q} a_q$$

in the category $\mathcal{C}$. It is attached along its $(q+1)$ boundary faces to the convex $(q-1)$-simplices that correspond to omitting one of the objects in this chain (composing the two morphisms that meet there, if necessary).

More precisely, to the small category $\mathcal{C}$ we associate the simplicial set $N\mathcal{C}$, its nerve, with q-simplices $N_q\mathcal{C}$ the set of functors $F\colon [q] \to \mathcal{C}$, where

$$[q] = \{0 < 1 < \cdots < q-1 < q\}$$

is the linearly ordered set considered as a category. The classifying space of the category is the geometric realization $B\mathcal{C} = |N\mathcal{C}|$ of this simplicial set. This is obtained from the disjoint union of convex simplices

$$\coprod_{q \geq 0} N_q\mathcal{C} \times \Delta^q$$

by gluing each face in the boundary of a simplex $\{F\} \times \Delta^q$ to the appropriate lower-dimensional simplex.

(0) In the example of a category $\mathcal{G}$ with only one object and a group G of morphisms, the classifying space $B\mathcal{G}$ of the category equals the bar construction BG of a classifying space for the group G, i.e., a space that classifies principal G-bundles, or fiber bundles with structure group G. The name bar construction refers to the vertical bars used in the notation above.

When G has a topology, $\mathcal{G}$ is a topological category and $BG = B\mathcal{G}$ takes this topology into account. Then there is an equivalence $G \simeq \Omega BG$ and an isomorphism of homotopy groups $\pi_{i+1}BG \cong \pi_i G$. We say that the classifying space BG is a delooping of G.

For example, with $G = U(n) \simeq GL_n(\mathbb{C})$ the space $BU(n)$ classifies rank n complex vector bundles, in the sense that for each topological space X there is a natural bijection

$$[X, BU(n)] \cong \mathrm{Vect}_n^{\mathbb{C}}(X)$$

between homotopy classes of maps $g\colon X \to BU(n)$ and the isomorphism classes of (numerable) rank n complex vector bundles over X. The infinite Grassmannian $\mathrm{Gr}_n(\mathbb{C}^\infty)$ of complex n-planes in $\mathbb{C}^\infty$ has the same universal property, so there is a homotopy equivalence $BU(n) \simeq \mathrm{Gr}_n(\mathbb{C}^\infty)$.

(1) The category $i\mathcal{P}_R$ of finitely generated projective R-modules and isomorphisms is equivalent to a small subcategory with exactly one object P from each isomorphism class of such modules. The only morphisms are the automorphisms $i\mathcal{P}_R(P,P) = \mathrm{Aut}_R(P)$, which in the case of a finitely generated free module $P = R^n$ specializes to $\mathrm{Aut}_R(R^n) = GL_n(R)$. It follows that the classifying space of $i\mathcal{P}_R$ decomposes as the disjoint union of classifying spaces

$$Bi\mathcal{P}_R \simeq \coprod_{[P]} B\,\mathrm{Aut}_R(P)$$

of these automorphism groups.

(2) There is a similar decomposition

$$BhR(*) \simeq \coprod_{[Y]} BF(Y)$$

for the classifying space of finite based CW complexes and homotopy equivalences, with one representative Y for each homotopy type of such spaces. By $F(Y)$ we mean the grouplike monoid of based homotopy equivalences $f\colon Y \to Y$, under composition. It is not usually a group, but the bar construction of its classifying space still makes sense. There is a more complicated description for $BhR(X)$.

3. Algebraic K-theory. One point of algebraic K-theory is that it is usually more realistic to replace these classifying spaces $Bw\mathcal{C}$, which carry some symmetric monoidal or similar structure, with an infinite loop space $K(\mathcal{C}, w)$, which acts as a kind of abelian group completion of the classifying space, in a homotopy-theoretic sense.

In particular, $K(\mathcal{C}, w)$ can be constructed as a particular (based) loop space ΩZ, and there is a canonical map

$$\iota\colon Bw\mathcal{C} \to K(\mathcal{C}, w)$$

that takes suitable extensions in $\mathcal{C}$ to loop sums in this loop space. So if $a \to b \to c$ is such an extension in $\mathcal{C}$, then the loop $\iota(b)$ in Z is coherently homotopic to the composite of the loops $\iota(a)$ and $\iota(c)$ in Z. By coherence, we mean that for longer extensions in $\mathcal{C}$, the various homotopies that arise are suitable compatible. The reversal of loops provides the algebraic K-theory space $K(\mathcal{C}, w)$ with an inverse, which effects the group completion. Note also that for another extension $a \to b' \to c$ in $\mathcal{C}$, the loops $\iota(b)$ and $\iota(b')$ become homotopic, so the K-theory construction forces all extensions to be the same. We shall omit the precise, slightly lengthy, construction of $K(\mathcal{C}, w)$.

(1) When $\mathcal{C} = \mathcal{P}_R$ is the category of finitely generated projective R-modules, the extensions are the short exact sequences

$$0 \to P' \to P \to P'' \to 0\,,$$

which split because P'' is projective, so $P \cong P' \oplus P''$ and the continuous pairing on $Bi\mathcal{P}_R$ induced by direct sum of modules acquires an additive inverse in $K(\mathcal{P}_R, i)$. We write

$$\iota\colon Bi\mathcal{P}_R \to K(R) := K(\mathcal{P}_R, i)$$

and define Quillen's algebraic K-groups of R as the homotopy groups $K_i(R) = \pi_i K(R)$ of this infinite loop space.

In the special case $R = \mathcal{O}_F$, each nonzero finitely generated projective $\mathcal{O}_F$-module P has the form

$$P \cong \mathfrak{a} \oplus \mathcal{O}_F^n$$

for some $n \geq 0$, from which it follows that there is split short exact sequence

$$0 \to \mathrm{Cl}(F) \to K_0(\mathcal{O}_F) \to \mathbb{Z} \to 0\,.$$

The first map takes the ideal class $[\mathfrak{a}]$ to the difference of projective classes $[\mathfrak{a}]-[\mathcal{O}_F]$, and is a group homomorphism by the relation $\mathfrak{a} \oplus \mathfrak{b} \cong \mathfrak{ab} \oplus \mathcal{O}_F$. The second map records the (constant) rank of a finitely generated projective module.

Furthermore, there is an isomorphism

$$K_1(\mathcal{O}_F) \cong \mathcal{O}_F^\times .$$

As a consequence of the proven Bloch–Kato and Lichtenbaum–Quillen conjectures, the Brauer group $\mathrm{Br}(\mathcal{O}_F[1/p])$ also appears in $K(\mathcal{O}_F)$, but spread out in many degrees. For example, its p^ν-torsion appears as a subgroup of $K_i(\mathcal{O}_F; \mathbb{Z}/p^\nu)$ whenever i is a positive multiple of $2p^{\nu-1}(p-1)$. Conversely, all of the algebraic K-groups $K_i(\mathcal{O}_F)$ can be recovered from these three classical arithmetic invariants, for various finite extensions of F, as we shall illustrate later.

There are also many classical conjectures in number theory that can be expressed only in terms of the algebraic K-theory (infinite loop) space $K(\mathcal{O}_F)$. For example, the Kummer–Vandiver conjecture for a prime p asserts that p does not divide the class number of the maximal real subfield $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ of the p-th cyclotomic field. It is equivalent to the assertion that $K_i(\mathbb{Z}) = 0$ for all $i = 4k$, $1 \le k \le (p-3)/2$. For another example, the Leopoldt conjecture for F asserts that the inclusion

$$\mathcal{O}_F[1/p] \to \prod_{v|p} F_v ,$$

into the product of completions at the primes dividing p, induces an injection of p-adically completed unit groups. It is equivalent to the finiteness of $\pi_{-2} L_{K(1)} K(\mathcal{O}_F)$, where $L_{K(1)}(-)$ denotes Bousfield localization with respect to Morava $K(1)$-theory.

We therefore take the point of view that the algebraic K-theory of a ring encodes its arithmetic properties, making this the definition of arithmetic properties when no other characterization is available.

(2) When $w\mathcal{C} = hR(X)$ we obtain Waldhausen's algebraic K-theory

$$\iota \colon BhR(X) \to A(X) := K(R(X), h)$$

of the space X. When $X = *$ and $R(*)$ is the category of finite based CW complexes, the extensions are the cofiber sequences

$$Y' \rightarrowtail Y \to Y''$$

with Y' a subcomplex of Y and $Y'' \cong Y/Y'$. Then Y is represented in $A(*)$ by the loop sum of the representatives for Y' and Y'', up to coherent homotopy. In the special case of the cone-suspension cofiber sequence

$$Y \rightarrowtail CY \to \Sigma Y$$

we find that the loop sum of the representatives of Y and ΣY is that of CY, which is contractible and therefore represents zero, so ΣY represents the additive inverse of Y. Repeating the argument, we see that the double suspension $\Sigma^2 \colon R(*) \to R(*)$ induces the identity on $A(*)$, up to homotopy. Again, there is a similar statement for $A(X)$ in general.

It follows that $A(*)$ is equivalent to the algebraic K-theory of the colimit of the direct system

$$R(*) \xrightarrow{\Sigma} R(*) \to \cdots \to R(*) \xrightarrow{\Sigma} R(*) \to \cdots \to$$

which is the category of finite CW spectra, in the sense of algebraic topology. The passage to this colimit extends the trivial pairing $S^0 \wedge Y_0 \cong Y_0$ of a zero-sphere with a space at the zero-th stage of the system, to a collection of pairings $S^k \wedge Y_\ell \to Y_{k+\ell}$ between spaces at the ℓ-th and $(k+\ell)$-th stages of the system, somewhat like how an abelian group A is a module over the ring of integers $\mathbb{Z}$, with a bilinear pairing $\mathbb{Z} \times A \to A$.

In modern terms, spectra are the modules over the structured sphere spectrum $\mathbb{S}$, so the algebraic K-theory of the colimit above is the algebraic K-theory $K(\mathbb{S}) = K(\mathcal{C}_{\mathbb{S}}, h)$ of the category $\mathcal{C}_{\mathbb{S}}$ of finite cell $\mathbb{S}$-modules, up to stable homotopy equivalence. Thus

$$A(*) = K(\mathbb{S})\,.$$

In particular, we will interpret the arithmetic of the sphere spectrum to mean the algebraic K-theory $A(*)$.

More generally, for a connected space $X = BG$ we have an equivalence $R(X) \simeq R(*, G)$ to the category of finite based free G-CW complexes. A retractive space Y over X goes first to the fiber product $EG \times_{BG} Y$, which contains EG as a retract. Collapsing EG yields a based free G-space. The finiteness conditions carry over. The suspension $\Sigma\colon R(*, G) \to R(*, G)$ still induces an equivalence in algebraic K-theory, so $A(X)$ is the algebraic K-theory of finite free G-CW spectra. Free G-spectra are modules over the spherical group ring spectrum $\mathbb{S}[G] = \Sigma^\infty G_+$, so this is the algebraic K-theory of the category $\mathcal{C}_{\mathbb{S}[G]}$ of finite cell $\mathbb{S}[G]$-modules. We allow ourselves to write ΩX for G, so $A(X) = K(\mathbb{S}[\Omega X])$.

4. Smooth symmetries of manifolds. In the case when X is a compact smooth manifold, Waldhausen's stable parametrized h-cobordism theorem establishes a relation between the algebraic K-theory space $A(X)$ and the space of smooth symmetries of X, i.e., the infinite dimensional Lie group $\mathrm{Diff}(X \operatorname{rel} \partial)$ of diffeomorphisms $f\colon X \cong X$ fixing the boundary ∂X.

More precisely, for closed X let

$$H(X) := \{(W, X, X') \mid \partial W = X \sqcup X', X \simeq W \simeq X'\}$$

be the space of smooth h-cobordism on the fixed base X, equipped with such a topology that a map to $H(X)$ classifies a locally trivial bundle of such h-cobordisms. There is a similar definition when X has a boundary. Then

$$H(X) \simeq \coprod_{[W]} B\,\mathrm{Diff}(W \operatorname{rel} X)$$

where W ranges over the isomorphism classes of these h-cobordisms. The classical h-cobordism theorem of Smale (as extended by Barden, Mazur and Stallings, independently) identifies the set of path components $\pi_0 H(X)$ with the Whitehead group

$$\mathrm{Wh}_1(\pi) = K_1(\mathbb{Z}[\pi])/(\pm\pi)$$

of the fundamental group $\pi = \pi_1(X)$, when X is connected and of dimension ≥ 5. The correspondence takes the h-cobordism to the Whitehead torsion of the pair (W, X).

In the case of the trivial h-cobordism, $W = X \times I$ with $I = [0, 1]$, based on $X \cong X \times \{0\}$ there is a fiber sequence

$$\mathrm{Diff}(X \times I \,\mathrm{rel}\, \partial) \to \mathrm{Diff}(X \times I \,\mathrm{rel}\, X) \to \mathrm{Diff}(X \,\mathrm{rel}\, \partial)$$

where the right hand map restricts a diffeomorphism of $X \times I$ to the free end $X \cong X \times \{1\}$. There is a canonical involution on this fiber sequence, essentially flipping the I-coordinate, which determines how homotopy information about the middle space is divided between the left hand and the right hand spaces (at least, away from 2). This is one way how the smooth symmetries of X are related to the space of h-cobordisms on X.

The achievement of the stable parametrized h-cobordism theorem is to identify the homotopy type of $H(X)$ in a stable range that grows to infinity with the dimension of X. Like the Whitehead group is given in terms of $K_1(\mathbb{Z}[\pi])$, the parametrized answers are given in terms of $A(X)$.

One can stabilize $H(X)$, replacing X by $X \times I^n$ for $n \gg 0$ and forming the stable h-cobordism space

$$\mathcal{H}(X) := \operatorname*{colim}_n H(X \times I^n)$$

as an appropriate homotopy colimit. By the stability theorem for smooth pseudoisotopies of Igusa, the connectivity of the map $H(X) \to \mathcal{H}(X)$ grows to infinity with the dimension of X. More precisely, the map is at least k-connected when the dimension of X exceeds $3k$.

Theorem (Waldhausen). *Let X be a compact smooth manifold. There is a homotopy fiber sequence*

$$\mathcal{H}(X) \to Q(X_+) \to A(X)\,.$$

The right hand map admits a preferred retraction up to homotopy, so there is a splitting

$$A(X) \simeq Q(X_+) \times \mathrm{Wh}^{\mathrm{Diff}}(X)\,,$$

where $\mathrm{Wh}^{\mathrm{Diff}}(X) := B\mathcal{H}(X)$.

For connected X with $\pi = \pi_1(X)$, the long exact sequence of homotopy groups associated to this fiber sequence ends

$$\dots \xrightarrow{0} \mathbb{Z}/2 \times \pi_{ab} \to K_1(\mathbb{Z}[\pi]) \to \pi_0\mathcal{H}(X) \xrightarrow{0} \mathbb{Z} \to \mathbb{Z}\,,$$

so $\mathrm{Wh}_1(\pi) = \pi_1 \mathrm{Wh}^{\mathrm{Diff}}(X)$ and one recovers the h-cobordism theorem in a stable range.

In other words, algebraic K-theory of structured ring spectra places the ideal class groups of number fields and diffeomorphism groups of compact manifolds under one roof.

5. Rational calculations. There is a map $\mathbb{S} \to \mathbb{Z}$ of structured ring spectra. It is 1-connected and a rational equivalence, by Serre's theorem that the stable homotopy groups of spheres $\pi_i(\mathbb{S})$ are all finite for $i > 0$, so it induces a rational equivalence $K(\mathbb{S}) \to K(\mathbb{Z})$. From Borel's rational calculation

$$K_i(\mathbb{Z}) \otimes \mathbb{Q} = \begin{cases} \mathbb{Q} & \text{if } i = 0, \text{ or } i = 4k+1 \text{ for } k \geq 1, \\ 0 & \text{otherwise,} \end{cases}$$

which involves symmetric spaces, Lie algebra cohomology and some nontrivial real harmonic analysis, one obtains the same formula for

$$\pi_i A(*) \otimes \mathbb{Q} = \pi_i K(\mathbb{S}) \otimes \mathbb{Q}\,.$$

Applying Waldhausen's theorem in the case $X = *$, one obtains

$$\pi_i H(D^n) \otimes \mathbb{Q} = \begin{cases} \mathbb{Q} & \text{if } i = 4k-1 \text{ for } k \geq 1, \\ 0 & \text{otherwise,} \end{cases}$$

in the stable range where $n \gg i$. By analyzing the fiber sequence and involution mentioned above, Farrell and Hsiang deduce that

$$\pi_i \operatorname{Diff}(D^n \operatorname{rel} \partial) \otimes \mathbb{Q} = \begin{cases} \mathbb{Q} & \text{if } i = 4k-1 \text{ for } n \text{ odd and } k \geq 1, \\ 0 & \text{otherwise,} \end{cases}$$

when $n \gg i$.

This is to be contrasted with the groups of topological- or piecewise-linear self-homeomorphisms of D^n relative to the boundary, both of which are contractible by the Alexander trick.

6. Torsion calculations. The torsion in $K_i(\mathbb{Z})$ is controlled by the classical arithmetic invariants of the cyclotomic fields $\mathbb{Q}(\zeta_n)$, including the ideal class group, and the approximate Galois descent property satisfied by algebraic K-theory.

We illustrate by studying the mod p algebraic K-theory $K_*(\mathbb{Z}; \mathbb{Z}/p)$ at an odd prime p. Each free $\mathbb{Z}$-summand in $K_i(\mathbb{Z})$ contributes a $\mathbb{Z}/p$ in $K_i(\mathbb{Z}; \mathbb{Z}/p)$, and each copy of $\mathbb{Z}/p^\nu$ contributes a $\mathbb{Z}/p$ in $K_i(\mathbb{Z}; \mathbb{Z}/p)$ and in $K_{i+1}(\mathbb{Z}; \mathbb{Z}/p)$, connected by the ν-th order Bockstein operation β_ν.

First, we pass from $\mathbb{Z}$ to the ring of p-integers $\mathbb{Z}[1/p]$. By Quillen's localization sequence the map

$$K_i(\mathbb{Z}; \mathbb{Z}/p) \to K_i(\mathbb{Z}[1/p]; \mathbb{Z}/p)$$

is an isomorphism for each $i \neq 1$, so this makes little difference. However, its utility hinges on the fact that $\mathbb{Z}$ is a Dedekind domain of Krull dimension 1.

The field extension $\mathbb{Q} \to \mathbb{Q}(\zeta_p)$ is a Galois extension, with Galois group $\Delta = (\mathbb{Z}/p)^\times \cong \mathbb{Z}/(p-1)$ acting by permutations among the p-th roots of unity $\mu_p = \langle \zeta_p \rangle$. It is ramified only at p, so the extension $\mathbb{Z}[1/p] \to \mathbb{Z}[1/p, \zeta_p]$ of rings of p-integers is a Δ-Galois extension of commutative rings.

$$\begin{array}{ccc} R = \mathbb{Z}[1/p, \zeta_p] & \longrightarrow & \mathbb{Q}(\zeta_p) = F \\ \Delta \uparrow & & \uparrow \Delta \\ \mathbb{Z}[1/p] & \longrightarrow & \mathbb{Q} \end{array}$$

Hereafter, we write $F = \mathbb{Q}(\zeta_p)$ and $R = \mathbb{Z}[1/p, \zeta_p]$. By naturality, the Galois group Δ acts on the algebraic K-theory of R, and there is a natural map

$$K_i(\mathbb{Z}[1/p]; \mathbb{Z}/p) \xrightarrow{\cong} K_i(R; \mathbb{Z}/p)^\Delta$$

to the invariants of this action. The Galois descent property, and the simplifying fact that p does not divide the order of Δ, ensures that this map is an isomorphism for $i \geq 2$.

There is a Bott element $u \in K_2(R;\mathbb{Z}/p)$ with (integral) Bockstein image the p-torsion class ζ_p in $K_1(R) = R^\times$. By naturality, Δ acts on $\mathbb{Z}/p\{u\}$ just like on μ_p. We write $\mathbb{Z}/p\{u^j\} \cong \mu_p^{\otimes j}$ for the Δ-module where a group element acts by the j-th power of its Galois action on the roots of unity. Note that this action only depends on $j \mod p-1$, by Fermat's little theorem.

The proven Lichtenbaum–Quillen conjecture then ensures that the mod p algebraic K-theory $K_*(R;\mathbb{Z}/p)$ is the free $\mathbb{Z}/p[u]$-module on the sum of terms

$$\mathbb{Z}/p \oplus \mathrm{Cl}(F)/p \subset K_0(R;\mathbb{Z}/p)$$
$$R^\times/p \oplus \mathrm{Cl}(F)[p] \subset K_1(R;\mathbb{Z}/p)$$

since $\mathrm{Br}(R) = 0$ in this case. Here Δ acts trivially on $\mathbb{Z}/p$. The Δ-action decomposes the units modulo p-th powers of R into eigenspaces

$$R^\times/p = \mu_p^{\otimes 0} \oplus \mu_p^{\otimes 2} \oplus \cdots \oplus \mu_p^{\otimes p-3} \oplus \mu_p^{\otimes 1}$$

with twists all even $0 \le j \le p-3$, plus $j = 1$. The arithmetically most interesting part is how the Δ-action decomposes the p-torsion in the ideal class group into eigenspaces:

$$\mathrm{Cl}(F)[p] \cong \bigoplus_{j=0}^{p-2} E_j$$

where $E_j = E^{-j}$ is a sum of copies of $\mu_p^{\otimes -j} = \mu_p^{\otimes p-1-j}$, as a Δ-representation. The lower index j should be read periodically $\mod p-1$, and has the opposite sign of the upper index. The quotient group $\mathrm{Cl}(F)/p$ has the same decomposition. To my knowledge, no primes p are known where $\mathrm{Cl}(F)$ contains an element of order p^2.

Tensoring with $\mathbb{Z}/p[u]$ and taking Δ-invariants, we find that

$$K_{2j}(\mathbb{Z};\mathbb{Z}/p) \cong E_j \oplus \begin{cases} \mathbb{Z}/p & \text{for } j \equiv 0 \mod p-1 \\ 0 & \text{otherwise,} \end{cases}$$

and

$$K_{2j+1}(\mathbb{Z};\mathbb{Z}/p) \cong E_j \oplus \begin{cases} \mathbb{Z}/p & \text{for } j \text{ even or } j \equiv -1 \mod p-1 \\ 0 & \text{otherwise,} \end{cases}$$

for $j \ge 0$.

The contributions $\mathbb{Z}/p$ to K_{2j+1} for $j = 2k$ even are from the Borel $\mathbb{Z}$-summands in K_{4k+1}, the contributions $\mathbb{Z}/p$ for $j \equiv 0, -1 \mod p-1$ are from the image of J, and the remaining contributions are from the p-torsion in the p-th cyclotomic ideal class group $\mathrm{Cl}(F)$. When p is a regular prime, the latter contribution is zero.

Following Kummer, the $(n-1)$-st eigenspace E_{n-1} is nonzero if and only if

$$p \mid \mathrm{num}(\frac{B_n}{n})$$

where the B_n are the Bernoulli numbers, in the indexing

$$\frac{z}{e^z - 1} = \sum_{n=0}^{\infty} \frac{B_n}{n!} z^n \,.$$

For example, among the B_n with $1 \leq n \leq 690$ the irregular prime $p = 691$ only divides the numerator of $B_{12} = -691/2730$ and B_{200}, so

$$E_j = \begin{cases} \mathbb{Z}/p & \text{for } j \equiv 11, 199 \mod 690, \\ 0 & \text{otherwise.} \end{cases}$$

From this it follows that there are subgroups

$$\mathbb{Z}/691 \subset K_{2j}(\mathbb{Z})$$

precisely for $j \equiv 11, 199 \mod 690$, starting with $K_{22}(\mathbb{Z})$ and $K_{398}(\mathbb{Z})$. Similarly, the prime $p = 37$ only divides the numerator of B_n/n for $n \equiv 32 \mod 36$, so there are subgroups $\mathbb{Z}/37 \subset K_{2j}(\mathbb{Z})$ precisely when $j \equiv 31 \mod 36$, starting with $K_{62}(\mathbb{Z})$.

7. Galois descent for structured ring spectra. A program is underway to describe the p-torsion in $A(X)$ in similar terms. In the basic case, $A(*) = K(\mathbb{S})$, the short Krull filtration $\mathbb{Z} \subset \mathbb{Z}[1/p]$, or its p-local version $\mathbb{Z}_{(p)} \subset \mathbb{Q}$, gets expanded to an infinite chromatic filtration

$$\mathbb{S}_{(p)} \to \cdots \to L_n\mathbb{S} \to L_{n-1}\mathbb{S} \to \cdots \to L_0\mathbb{S} = \mathbb{Q}\,.$$

The n-th layer of this filtration is controlled by a structured ring spectrum $L_{K(n)}\mathbb{S}$, obtained from the sphere spectrum by applying Bousfield localization with respect to the n-th Morava K-theory spectrum.

The author has developed a theory of Galois extensions for such structured ring spectra, and work of Hopkins et al. exhibits interesting pro-Galois extensions

$$L_{K(n)}\mathbb{S} \to E_n$$

related to the Lubin–Tate deformation theory of formal group laws over fields in characteristic p. One hope is to extract arithmetic information about $K(\mathbb{S})$ from the chromatic filtration and by Galois descent along these extensions. The partial results so far indicate that the Lubin–Tate spectrum E_n plays the role of the valuation ring in a "brave new" higher $(n+1)$-local field $f\!f(E_n)$, with $(n+2)$ different residue characteristics. In particular, its Galois cohomology has been found by Ausoni and the author to satisfy a form of local arithmetic duality, like that found by Tate–Poitou (and Artin–Verdier) for ordinary local fields.

Max Planck Institute for Mathematics, Bonn
E-mail address: `rognes@math.uio.no`