TWO-REGULAR NUMBER FIELDS AND ALGEBRAIC K-THEORY

John Rognes

March 25th 1999

In this talk I will discuss some number theory, algebraic K-theory and the Lichtenbaum–Quillen conjectures. These were proved at the prime 2 in 1996 by combining results of Suslin, Voevodsky, Bloch, Lichtenbaum, Rognes and Weibel. This gives a calculation of all higher 2-primary algebraic K-groups of rings of integers in number fields, in terms of the étale cohomology groups of the associated rings of 2-integers. In a joint paper with Østvær we make these calculations fully explicit for the class of 2-regular number fields, which include the rationals together with infinitely many quadratic and cyclotomic number fields. It is our aim to review these results today.

1. Number theory.

Let F be a number field, i.e., a finite extension of the field $\mathbb{Q}$ of rational numbers. A field homomorphism $F \to \mathbb{R}$ is called a real embedding of F, while a field homomorphism $F \to \mathbb{C}$ that does not factor through $\mathbb{R}$ is called a complex embedding of F. The latter always occur in pairs of two distinct complex embeddings, related by complex conjugation. Let r_1 be the number of distinct real embeddings of F, and let r_2 be the number of complex conjugate pairs of distinct complex embeddings. Then $n = r_1 + 2r_2$ where n is the dimension of F as a rational vector space. We say that F is real if $r_1 > 0$ (so F has at least one real embedding), while F is imaginary if $r_2 > 0$. Also if $r_2 = 0$ then F is totally real, while if $r_1 = 0$ then F is totally imaginary.

Let O_F be the ring of algebraic integers in F. These are the roots in F of monic polynomials with integer coefficients, i.e., the solutions to equations

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

where $n \geq 1$ and all the a_i are integers. Algebraic number theory is largely concerned with the (always nonzero) prime ideals $\mathcal{P} \subset O_F$ in such number rings. When $\mathcal{P} \subset O_F$ is a prime ideal in O_F, its intersection with $\mathbb{Z} \subseteq O_F$ is a prime ideal in $\mathbb{Z}$, hence has the form $\mathcal{P} \cap \mathbb{Z} = (p)$ for some prime number p. We say that the prime ideal $\mathcal{P}$ lies over the rational prime (p), and write $\mathcal{P} \mid (p)$.

Here are some examples:

(1) $F = \mathbb{Q}$, the rational numbers themselves, have $r_1 = 1$ and $r_2 = 0$. The ring of integers is $O_{\mathbb{Q}} = \mathbb{Z}$, whose prime ideals are the principal ideals $(p) = p \cdot \mathbb{Z}$ for all prime numbers p.

Typeset by $\mathcal{A}_\mathcal{M}\mathcal{S}$-TeX

(2) $F = \mathbb{Q}(\sqrt{d})$ with d a square-free integer. When $d > 0$ this is a real quadratic number field with $r_1 = 2$ and $r_2 = 0$. When $d < 0$ this is an imaginary quadratic number field with $r_1 = 0$ and $r_2 = 1$. The ring of integers O_F is $\mathbb{Z}[\sqrt{d}]$ or $\mathbb{Z}[(1+\sqrt{d})/2]$, depending on the congruence class of d mod 4. There are either one or two prime ideals in O_F over each rational prime (p), as determined by quadratic reciprocity. Not all of these will generally be principal.

(3) $F = \mathbb{Q}(\zeta_q)$ with $\zeta_q = \exp(2\pi\sqrt{-1}/q)$ and $q \geq 3$. This is the q'th cyclotomic field. It is totally imaginary with $r_2 = \varphi(q)/2$ where φ is the Euler phi-function. The ring of integers is $\mathbb{Z}[\zeta_q]$, and over each rational prime (p) there may be a number of prime ideals, this time counted by the cyclotomic reciprocity law. Again these will generally not be principal.

(4) $F = \mathbb{Q}(\zeta_q + \bar{\zeta}_q)$ with $\bar{\zeta}_q$ the complex conjugate of ζ_q. This is the maximal real subfield of $\mathbb{Q}(\zeta_q)$. It is totally real with $r_1 = \varphi(q)/2$. The ring of integers is $\mathbb{Z}[\zeta_q + \bar{\zeta}_q]$.

The number rings O_F are Dedekind domains, meaning that they have unique factorization of ideals. Thus every nonzero ideal $\mathfrak{a} \subseteq O_F$ admits a unique factorization as products of prime ideals

$$\mathfrak{a} = \prod_{\mathcal{P}} \mathcal{P}^{e_{\mathcal{P}}}$$

where $\mathcal{P}$ ranges over the prime ideals in O_F and the exponents $e_{\mathcal{P}}$ are non-negative integers. The factorization is finite, i.e., only finitely many of the $e_{\mathcal{P}}$ are nonzero. Given a nonzero element $a \in O_F$, its principal ideal $(a) = a \cdot O_F$ can be factorized in this way. We write

$$(a) = \prod_{\mathcal{P}} \mathcal{P}^{e_{\mathcal{P}}(a)}$$

defining the integers $e_{\mathcal{P}}(a)$. Clearly $e_{\mathcal{P}}(ab) = e_{\mathcal{P}}(a) + e_P(b)$, so there are monoid homomorphisms $e_{\mathcal{P}} \colon O_F \setminus \{0\} \to \mathbb{N}_0 = \mathbb{N} \cup \{0\}$. They assemble to a monoid homomorphism

$$e \colon O_F \setminus \{0\} \to \bigoplus_{\mathcal{P}} \mathbb{N}_0 \,.$$

It is generally more convenient to work with groups than with monoids. We extend the map above as follows: For a fraction $a/b \in F$ with $a, b \in O_F \setminus \{0\}$ let $e_{\mathcal{P}}(a/b) = e_{\mathcal{P}}(a) - e_{\mathcal{P}}(b) \in \mathbb{Z}$. This defines a group homomorphism

$$e \colon F^{\times} \to \bigoplus_{\mathcal{P}} \mathbb{Z}$$

which fully describes the prime ideal factorization of principal ideals in O_F. How far is e from being an isomorphism ?

Lemma. *The kernel* $\ker(e) = O_F^{\times}$ *is the group of units (invertible elements) in the ring of integers* O_F.

Definition. The ideal class group of F is the cokernel $\mathrm{Cl}(F) = \mathrm{cok}(e)$.

Theorem. *Let F be a number field. Its ideal class group* $\mathrm{Cl}(F)$ *is a finite abelian group.*

If all prime ideals in O_F are principal then $\mathrm{Cl}(F)$ is the trivial group, so nontrivial elements in the ideal class group detect non-principal ideals in O_F. The order of $\mathrm{Cl}(F)$ is called the class number of F, denoted h_F.

2. ℓ-regular number fields.

It will be convenient to be able to disregard a set S of prime ideals of O_F, i.e., to neglect the factors in a prime ideal factorization that involve elements in the set S. Fix a prime number ℓ. We shall only be concerned with the case when S is the set of prime ideals in O_F that lie over the rational prime (ℓ). We define the ring R_F of ℓ-integers in F as the subring $R_F = O_F[1/\ell]$ of F.

Consider the modified group homomorphism

$$\bar{e}\colon F^\times \to \bigoplus_{\mathcal{P}\nmid(\ell)} \mathbb{Z}$$

where $\mathcal{P}$ ranges over the prime ideals in O_F that do not lie over (ℓ). For these $\mathcal{P}$, the $\mathcal{P}$'th component of $\bar{e}(a/b)$ is still $e_{\mathcal{P}}(a) - e_{\mathcal{P}}(b)$.

Lemma. *The kernel* $\ker(\bar{e}) = R_F^\times$ *is the group of units in the ring of ℓ-integers* $R_F = O_F[1/\ell]$.

Definition. The Picard group of R_F is the cokernel $\mathrm{Pic}(R_F) = \mathrm{cok}(\bar{e})$.

Lemma. *There is an exact sequence*

$$0 \to O_F^\times \to R_F^\times \to \bigoplus_{\mathcal{P}\mid(\ell)} \to \mathrm{Cl}(F) \to \mathrm{Pic}(R_F) \to 0\,.$$

The surjection $\mathrm{Cl}(F) \to \mathrm{Pic}(R_F)$ *annihilates the classes of prime ideals lying over (ℓ). In particular* $\mathrm{Pic}(R_F)$ *is a finite abelian group, of order dividing the class number of F.*

In the case of real number fields, it will also be necessary to restrict attention to the principal ideals generated by elements in $F^\times$ which map to positive real numbers under all real embeddings $F \to \mathbb{R}$.

Let $F_+^\times \subseteq F^\times$ be the subgroup of totally positive fractions, i.e., the elements $x \in F^\times$ such that $\rho(x) > 0$ for each real embedding $\rho\colon F \to \mathbb{R}$. When F is totally imaginary $F_+^\times = F^\times$, but for real F the group $F_+^\times$ is a proper subgroup of $F^\times$.

Also let $R_{F+}^\times \subseteq R_F^\times$ be the subgroup of totally positive units in the ring of ℓ-integers, given by $R_{F+}^\times = R_F^\times \cap F_+^\times$.

There is then a restricted group homomorphism

$$\bar{e}_+\colon F_+^\times \to \bigoplus_{\mathcal{P}\nmid(\ell)} \mathbb{Z}\,.$$

Lemma. *The kernel* $\ker(\bar{e}_+) = R_{F_+}^\times$ *is the group of totally positive units in the ring of ℓ-integers* $R_F = O_F[1/\ell]$.

Definition. The narrow Picard group of R_F is the cokernel $\mathrm{Pic}_+(R_F) = \mathrm{cok}(\bar{e}_+)$.

Lemma. *Let F be a number field with r_1 real embeddings. There is an exact sequence*

$$0 \to R_{F+}^\times \to R_F^\times \xrightarrow{\sigma} (\mathbb{Z}/2)^{r_1} \to \mathrm{Pic}_+(R_F) \to \mathrm{Pic}(R_F) \to 0\,.$$

The signature map $\sigma\colon R_F^\times \to (\mathbb{Z}/2)^{r_1}$ *takes a unit* $x \in R_F^\times$ *to its images under the* r_1 *real embeddings* $R_F^\times \to \mathbb{R}^\times$ *followed by the homomorphism* $\mathbb{R}^\times \to \mathbb{R}^\times/(\mathbb{R}^\times)^2 \cong \mathbb{Z}/2$.

Hence also the narrow Picard group $\mathrm{Pic}_+(R_F)$ is a finite group. For F totally imaginary it equals the Picard group, while for F real it has order at most 2^{r_1-1} times that of the Picard group. (Exercise: Why not 2^{r_1} ?)

The ℓ-rank $\mathrm{rk}_\ell(A)$ of an abelian group A is the dimension of the kernel ${}_\ell A$ of the multiplication by ℓ map $A \to A$, as a vector space over $\mathbb{F}_\ell$. Let t be the ℓ-rank of the Picard group $\mathrm{Pic}(R_F)$, and let u be the ℓ-rank of the narrow Picard group $\mathrm{Pic}_+(R_F)$. So $u = t$ for ℓ odd, and $t \le u < t + r_1$ for $\ell = 2$. Let s be the number of prime ideals in O_F that lie over (ℓ).

Definition. A number field F is ℓ-regular if there is only one prime ideal in O_F above the rational prime (ℓ), and the narrow Picard group $\mathrm{Pic}_+(R_F)$ has order prime to ℓ, i.e., $s = 1$ and $t = u = 0$.

So ℓ-regular number fields have relatively simple number-theoretic behavior at the prime ℓ.

3. Quadratic and cyclotomic examples.

We now restrict attention to the case $\ell = 2$ and consider 2-regular number fields. We have the following examples:

(1) $F = \mathbb{Q}$ is 2-regular, since (2) cannot split and the narrow Picard group $\mathrm{Pic}_+(\mathbb{Z}[1/2])$ is trivial.
(2) The 2-regular quadratic number fields $F = \mathbb{Q}(\sqrt{d})$ with d assumed square free were classified by Browkin and Schinzel: F is 2-regular precisely for $d = -2, -1, 2, \pm p$ or $\pm 2p$, with $p \equiv \pm 3 \bmod 8$ a prime.
(3) The 2-cyclotomic number fields $E = \mathbb{Q}(\zeta_q)$ with $q = 2^m$ are all 2-regular. Here (2) is totally ramified in E, and the Picard group $\mathrm{Pic}(\mathbb{Z}[\zeta_q, 1/2])$ is trivial since the class number of E is odd (by Iwasawa).
(4) For q an odd prime power, the q'th cyclotomic number field $E = \mathbb{Q}(\zeta_q)$ is sometimes 2-regular. The rational prime (2) is inert in E precisely when 2 is a primitive root mod q, i.e., when 2 generates the group of units in $\mathbb{Z}/q$. When additionally the Picard group $\mathrm{Pic}(\mathbb{Z}[\zeta_q, 1/2])$ has odd order, E is 2-regular.
(5) The maximal real subfields $F = \mathbb{Q}(\zeta_q + \bar{\zeta}_q)$ with $q = 2^m$ of 2-cyclotomic number fields are all 2-regular. For the norm homomorphism $\mathrm{Pic}_+(R_E) \to \mathrm{Pic}_+(R_F)$ with $E = \mathbb{Q}(\zeta_q)$ is surjective (by an argument using class field theory).
(6) For q an odd prime power such that 2 is a primitive root mod q, the maximal real subfield $F = \mathbb{Q}(\zeta_q + \bar{\zeta}_q)$ of the q'th cyclotomic field $E = \mathbb{Q}(\zeta_q)$ is 2-regular when $\mathrm{Pic}(R_E)$ has odd order, or more generally when $\mathrm{Pic}_+(R_F)$ has odd order.

These examples account for all quadratic and cyclotomic 2-regular number fields, since (2) is always split in the q'th cyclotomic field $E = \mathbb{Q}(\zeta_q)$ when q is not a prime power. The Picard group $\mathrm{Pic}(R_E)$ certainly has odd order when the class number h_E is odd, which is the case for all prime powers q with $\varphi(q) \le 66$, except $q = 29$. For more examples, recall that a Sophie Germain prime is a prime p such that also $(p-1)/2$ is a prime. By a theorem of Estes, the class number of $E = \mathbb{Q}(\zeta_p)$ is odd for Sophie Germain primes p such that 2 is a primitive root mod p. Hence the

q'th cyclotomic field is 2-regular for odd prime powers $q \neq 29$ such that $\varphi(q) \leq 66$, or $q = p$ a Sophie Germain prime, such that 2 is a primitive root mod q. Some examples are the primes $q = 83, 107$ and 179.

4. Étale cohomology.

Consider an extension E/F of number fields. Let $\mathfrak{p} \subseteq O_F$ be a prime ideal. Then $\mathfrak{p} \cdot O_E \subset O_E$ is a nonzero ideal in O_E and admits a unique factorization in prime ideals:

$$\mathfrak{p} \cdot O_E = \prod_{\mathcal{P}} \mathcal{P}^{e_{\mathcal{P}}}$$

where the $\mathcal{P}$ range over prime ideals in O_E. If some $e_{\mathcal{P}} > 1$ we say that $\mathfrak{p}$ is ramified in the extension. Otherwise, if all $e_{\mathcal{P}} \leq 1$ we say that $\mathfrak{p}$ is unramified. If all prime ideals $\mathfrak{p}$ in O_F are unramified, we say that the extension E/F is (finitely) unramified.

By Minkowski's theorem, no nontrivial finite extensions of $\mathbb{Q}$ are unramified.

Fix a rational prime ℓ and let $R_F = O_F[1/\ell]$ and $R_E = O_E[1/\ell]$ be the rings of ℓ-integers. We say that E/F is unramified away from ℓ if all prime ideals $\mathfrak{p} \nmid (\ell)$ in O_F are unramified, i.e., if all prime ideals in O_F that do not lie over the rational prime (ℓ) are unramified in the extension E/F. When this happens, we also say that R_E/R_F is a finite étale covering.

The ℓ-cyclotomic number fields $\mathbb{Q}(\zeta_{\ell^m})$ provide examples of extensions over $\mathbb{Q}$ which are unramified away from ℓ. Thus the $\mathbb{Z}[\zeta_{\ell^m}, 1/\ell]$ give examples of finite étale covers of $\mathbb{Z}[1/\ell]$.

Consider a Galois extension E/F with Galois group $G = \mathrm{Gal}(E/F)$. Let $\mu_{\ell^m}(E) \subset E^\times$ be the subgroup of elements of order dividing ℓ^m, i.e., the ℓ^m'th roots of unity in E. Then G acts on $\mu_{\ell^m}(E)$ by restriction of its action on E. The invariants of this action will be $\mu_{\ell^m}(E)^G = \mu_{\ell^m}(F)$, i.e., the ℓ^m'th root of unity in F. We may consider the right derived functors of taking G-invariants, i.e., the group cohomology of G with coefficients in $\mu_{\ell^m}(E)$:

$$H^n_{\mathrm{gp}}(G; \mu_{\ell^m}(E)) := H^n(\mathrm{Hom}_G(EG_*, \mu_{\ell^m}(E)))$$

where EG_* is a projective resolution of $\mathbb{Z}$ by $\mathbb{Z}[G]$-modules, e.g, the bar resolution. More generally we can form the i-fold tensor product $\mu_{\ell^m}(E)^{\otimes i}$ with the diagonal G-action, and consider $H^n_{\mathrm{gp}}(G; \mu_{\ell^m}(E)^{\otimes i})$.

Now consider only the Galois extensions E/F that are unramified away from ℓ, and form the colimit of cohomology groups:

$$H^n_{\text{ét}}(R_F; \mu_{\ell^m}^{\otimes i}) := \operatorname*{colim}_{E/F} H^n_{\mathrm{gp}}(G; \mu_{\ell^m}(E)^{\otimes i}) \,.$$

This defines the n'th étale cohomology group of R_F with coefficients in the étale sheaf $\mu_{\ell^m}^{\otimes i}$, also written $\mathbb{Z}/\ell^m(i)$.

The ℓ-adic integers $\mathbb{Z}_\ell$ are the limit of the groups $\mathbb{Z}/\ell^m$. There is an extension of the definition above to étale cohomology groups with coefficients in the étale pro-sheaf $\{\mu_{\ell^m}^{\otimes i}\}_m$, also written $\mathbb{Z}_\ell(i)$. Thus we can talk about the ℓ-adic étale cohomology groups $H^n_{\text{ét}}(R_F; \mathbb{Z}_\ell(i))$. By a finiteness result, there are isomorphisms

$$H^n_{\text{ét}}(R_F; \mathbb{Z}_\ell(i)) \cong \lim_m H^n_{\text{ét}}(R_F; \mu_{\ell^m}^{\otimes i}) \,.$$

Theorem. *Let F be a number field with r_1 real embeddings and r_2 pairs of complex embeddings. Then*

$$H^n_{\text{ét}}(R_F;\mathbb{Z}_\ell(i)) \cong \begin{cases} \mathbb{Z}_\ell & \text{for } n=i=0, \\ 0 & \text{for } n=0,\ i>0, \\ \mathbb{Z}_\ell^{r_2} \oplus \mathbb{Z}/w_i^{(\ell)} & \text{for } n=1,\ i\geq 2 \text{ even}, \\ \mathbb{Z}_\ell^{r_1+r_2} \oplus \mathbb{Z}/w_i^{(\ell)} & \text{for } n=1,\ i\geq 3 \text{ odd}, \\ \text{(finite } \ell\text{-group)} & \text{for } n=2,\ i\geq 2, \\ (\mathbb{Z}/(\ell,2))^{r_1} & \text{for } n\geq 3 \text{ and } i-n \text{ even}, \\ 0 & \text{for } n\geq 3 \text{ and } i-n \text{ odd}. \end{cases}$$

The numbers $w_i^{(\ell)} = w_i^{(\ell)}(F)$ are easily computed in terms of the number of ℓ-power roots of unity in F and $F(\sqrt{-1})$. Thus the main complexity in the étale cohomology groups of R_F lie in the finite ℓ-groups $H^2_{\text{ét}}(R_F;\mathbb{Z}_\ell(i))$ for $i\geq 2$.

A main result in the paper of Rognes and Østvær is that for ℓ-regular number fields, $H^2_{\text{ét}}(R_F;\mathbb{Z}_\ell(i))$ is as 'simple as possible.' For $\ell=2$ we prove:

Proposition (Rognes–Østvær). *Let F be a number field with r_1 real embeddings. The following are equivalent:*

(1) *F is 2-regular.*

(2) $H^2_{\text{ét}}(R_F;\mathbb{Z}_2(i)) \cong \begin{cases} (\mathbb{Z}/2)^{r_1} & \text{for } i\neq 0 \text{ even}, \\ 0 & \text{for } i\neq 1 \text{ odd}. \end{cases}$

(3) $H^2_{\text{ét}}(R_F:\mathbb{Z}_2(i)) \cong (\mathbb{Z}/2)^{r_1}$.

5. Conjectures of Lichtenbaum and Quillen.

Let R be a ring, always associative with unit. To the category of finitely generated projective R-modules, Quillen associated a loop space $K(R)$ whose homotopy groups are the algebraic K-groups of R:

$$K_i(R) = \pi_i(K(R))$$

for all integers $i\geq 0$. These are related to algebraic number theory by the following results:

Theorem. *Let F be a number field, with ring of integers O_F and ring of ℓ-integers R_F. Then $K_0(F)\cong\mathbb{Z}$, $K_1(F)\cong F^\times$, $K_0(O_F)\cong\mathbb{Z}\oplus\text{Cl}(F)$, $K_1(O_F)\cong O_F^\times$, $K_0(R_F)\cong\mathbb{Z}\oplus\text{Pic}(R_F)$ and $K_1(R_F)\cong R_F^\times$.*

The arithmetic interpretation of the higher algebraic K-groups (the $K_i(R)$ for $i\geq 2$) is more subtle. In the 1970's, Lichtenbaum and Quillen proposed two related conjectures on this topic. We begin with the Lichtenbaum conjecture.

The Dedekind zeta-function $\zeta_F(s)$ of the number fields F is first defined as a complex analytic function in the region $\Re(s)>1$ of the complex plane, by the absolutely convergent infinite series

$$\zeta_F(s) = \sum_{\mathfrak{a}} \frac{1}{N(\mathfrak{a})^s} .$$

Here $\mathfrak{a}\subseteq O_F$ runs over the nonzero ideals in O_F, and the integer $N(\mathfrak{a})$ is the norm of $\mathfrak{a}$, i.e., the order of the quotient ring $O_F/\mathfrak{a}$. Then one proves that $\zeta_F(s)$

admits a unique meromorphic extension to the entire complex plane. Lichtenbaum's conjecture expresses the value of the extended function at negative odd integers $s = 1 - 2j$, for totally real abelian number fields, in terms of orders of the higher algebraic K-groups of O_F. (A number field F is abelian if it is Galois over $\mathbb{Q}$, with abelian Galois group.)

Conjecture (Lichtenbaum). *Let F be a totally real abelian number field with r_1 real embeddings. Then for all even integers $i \geq 2$*

$$2^{r_1} \cdot \frac{\#K_{2i-2}(O_F)}{\#K_{2i-1}(O_F)} = \zeta_F(1-i)$$

up to sign.

In particular the zeta function is takes rational values at odd negative integers. In fact, Lichtenbaum's original conjecture did not include the factor 2^{r_1}, and asserted equality up to powers of 2. I have included it here because of the following theorem, which says that with this extra factor, the 2-components of the two sides agree.

Theorem (Kolster, Rognes, Weibel). *Lichtenbaum's formula is correct up to odd multiples.*

This uses an extension due to Kolster of Wiles' proof of the Main Conjecture in Iwasawa theory to relate the value of the zeta-function to a ratio of orders of two étale cohomology groups. Next it uses Rognes and Weibel's calculation of the 2-primary algebraic K-groups in terms of étale cohomology groups, which uses Voevodsky's proof of the Milnor conjecture on quadratic forms, and related work by Suslin, Bloch and Lichtenbaum.

Quillen's conjecture concerned the algebraic K-groups themselves. He viewed them as arithmetic analogues of the topological K-groups of Atiyah and Hirzebruch, and conjectured that there should be a spectral sequence converging to the algebraic K-groups of a ring, similar to the Atiyah–Hirzebruch spectral sequence from the singular cohomology of a space to its topological K-theory groups. In more detail, he considered the ring R_F of ℓ-integers in a number field F, and replaced singular cohomology with ℓ-adic étale cohomology. Thus there should be a spectral sequence with E^2 term

$$E^2_{s,t} = \begin{cases} H^{-s}_{\text{ét}}(R_F; \mathbb{Z}_\ell(i)) & \text{for } t = 2i \\ 0 & \text{otherwise} \end{cases}$$

converging to $K_{s+t}(R_F) \otimes \mathbb{Z}_\ell$ for $s + t \geq 1$.

6. Two-primary algebraic K-theory.

Using Suslin's motivic cohomology and Voevodsky's proof of the Milnor conjecture, combined with the Bloch–Lichtenbaum spectral sequence, Rognes and Weibel computed the 2-primary algebraic K-groups of the ring R_F of 2-integers in any number field F, in terms of the 2-adic étale cohomology groups of R_F.

Theorem (Rognes–Weibel). *Let E be a totally imaginary number field. Then for all $n \geq 2$*

$$K_n(R_E) \otimes \mathbb{Z}_2 \cong \begin{cases} H^2_{\text{ét}}(R_E; \mathbb{Z}_2(i+1)) & \textit{for } n = 2i, \\ \mathbb{Z}_2^{r_2} \oplus \mathbb{Z}/w_i^{(2)}(E) & \textit{for } n = 2i-1. \end{cases}$$

Theorem (Rognes–Weibel). *Let F be a real number field. Then for all $n \geq 2$*

$$K_n(R_F) \otimes \mathbb{Z}_2 \cong \begin{cases} H^2_{\text{ét}}(R_F; \mathbb{Z}_2(4k+1)) & \text{for } n = 8k, \\ \mathbb{Z}_2^{r_1+r_2} \oplus \mathbb{Z}/2 & \text{for } n = 8k+1, \\ H^2_{\text{ét}}(R_F; \mathbb{Z}_2(4k+2)) & \text{for } n = 8k+2, \\ \mathbb{Z}_2^{r_2} \oplus (\mathbb{Z}/2)^{r_1-1} \oplus \mathbb{Z}/2w^{(2)}_{4k+2}(F) & \text{for } n = 8k+3, \\ (?) & \text{for } n = 8k+4, \\ \mathbb{Z}_2^{r_1+r_2} & \text{for } n = 8k+5, \\ \tilde{H}^2_{\text{ét}}(R_F; \mathbb{Z}_2(4k+2)) & \text{for } n = 8k+6, \\ \mathbb{Z}_2^{r_2} \oplus \mathbb{Z}/w^{(2)}_{4k+4}(F) & \text{for } n = 8k+7. \end{cases}$$

Here $\tilde{H}^2_{\text{ét}}(R_F; \mathbb{Z}_2(4k+2))$ is the kernel of the natural surjective map

$$H^2_{\text{ét}}(R_F; \mathbb{Z}_2(4k+2)) \to \bigoplus^{r_1} H^2_{\text{ét}}(\mathbb{R}; \mathbb{Z}_2(4k+2)) \cong (\mathbb{Z}/2)^{r_1}$$

induced by the r_1 real embeddings of F.

The missing group $K_{8k+4}(R_F) \otimes \mathbb{Z}_2$ is isomorphic to the maximal finite quotient of $K_{8k+5}(R_F; \mathbb{Q}/\mathbb{Z})$. The latter K-group fits into the short exact sequence

$$0 \to (\mathbb{Z}/2)^{r_1-1} \to K_{8k+5}(R_F; \mathbb{Q}/\mathbb{Z}) \to (\mathbb{Q}/\mathbb{Z})^{r_1+r_2} \oplus H^2_{\text{ét}}(R_F; \mathbb{Z}_2(4k+3)) \to 0.$$

For 2-regular number fields we have the following simplifications:

Theorem. *Let E be a 2-regular totally imaginary number field. Then for $n \geq 2$*

$$K_n(R_E) \otimes \mathbb{Z}_2 \cong \begin{cases} 0 & \text{for } n = 2i, \\ \mathbb{Z}_2^{r_2} \oplus \mathbb{Z}/w^{(2)}_i(E) & \text{for } n = 2i-1. \end{cases}$$

Theorem. *Let F be a 2-regular real number field. Then for $n \geq 2$*

$$K_n(R_F) \otimes \mathbb{Z}_2 \cong \begin{cases} 0 & \text{for } n = 8k, \\ \mathbb{Z}_2^{r_1+r_2} \oplus \mathbb{Z}/2 & \text{for } n = 8k+1, \\ (\mathbb{Z}/2)^{r_1} & \text{for } n = 8k+2, \\ \mathbb{Z}_2^{r_2} \oplus (\mathbb{Z}/2)^{r_1-1} \oplus \mathbb{Z}/2w^{(2)}_{4k+2}(F) & \text{for } n = 8k+3, \\ 0 & \text{for } n = 8k+4, \\ \mathbb{Z}_2^{r_1+r_2} & \text{for } n = 8k+5, \\ 0 & \text{for } n = 8k+6, \\ \mathbb{Z}_2^{r_2} \oplus \mathbb{Z}/w^{(2)}_{4k+4}(F) & \text{for } n = 8k+7. \end{cases}$$

This gives explicit calculations of all the 2-primary algebraic K-groups $K_i(R_F) \otimes \mathbb{Z}_2$ and $K_i(O_F) \otimes \mathbb{Z}_2$ for the examples of 2-regular number fields previously given.

From the zeta-function formula in the totally real abelian case, we can deduce the following formulas. Let $v_2(q) = v_2(a) - v_2(b)$ denote the 2-adic valuation of the rational number $q = a/b$.

Proposition. *Let* $F = \mathbb{Q}(\sqrt{d})$*. Then for all even* $i \geq 2$

$$v_2(\zeta_F(1-i)) = -1 - v_2(i)$$

when $d = 2$*, while*

$$v_2(\zeta_F(1-i)) = -v_2(i)$$

when $d = p$ *or* $d = 2p$ *with* $p \equiv \pm 3 \bmod 8$ *prime.*

Proposition. *Let* $F = \mathbb{Q}(\zeta_{2^m} + \bar{\zeta}_{2^m})$ *with* $m \geq 2$*. Then for all even* $i \geq 2$

$$v_2(\zeta_F(1-i)) = 2^{m-2} - (m + v_2(i)).$$

Proposition. *Let* $F = \mathbb{Q}(\zeta_q + \bar{\zeta}_q)$ *with* q *an odd prime power and* 2 *a primitive root mod* q*. Suppose* $\mathrm{Pic}_+(R_F)$ *has odd order. Then for all even* $i \geq 2$

$$v_2(\zeta_F(1-i)) = \varphi(q)/2 - (2 + v_2(i)).$$

Department of Mathematics, University of Oslo, Norway