Milnor K Theory

Ajay Prajapati 17817063

Dept. of Mathematics and Statistics Indian Institute of Technology, Kanpur

End-Semester Exam presentation

Steinberg group of a ring R, $St_n(R)$ (For $n \ge 3$)

It is the group defined by the generators $x_{ij}(r)$, with $1 \le i, j \le n$, $i \ne j$ and $r \in R$ with the following relations:

$$x_{ij}(r)x_{ij}(s) = x_{ij}(r+s)$$

$$[x_{ij}(r), x_{kl}(s)] = \begin{cases} 1 & \text{if } j \neq k \text{ and } i \neq l \\ x_{il}(rs) & \text{if } j = k \text{ and } i \neq l \\ x_{kj}(-sr) & \text{if } j \neq k \text{ and } i = l \end{cases}$$

The above relations are also satisfied by elementary matrices $e_{ij}(r)$ which generate the subgroup E(R) of GL(R), we have surjective group homomorphism $\varphi_n : St_n(R) \longrightarrow E_n(R), x_{ij}(r) \longmapsto e_{ij}(r)$. Taking direct limit, we get a map $\varphi : St(R) \longrightarrow E(R)$.

K_2 of R

The group $K_2(R)$ is defined to be kernel of $\varphi : St(R) \longrightarrow E(R)$.

Theorem

(Steinberg) $K_2(R) = Z(St(R))$. In particular, $K_2(R)$ is abelian.

Thus St(R) is a central extension of E(R). Infact, we have

Theorem (Kervaire, Steinberg)

St(R) is the universal central extension of E(R).

イロト イヨト イヨト イヨト

- Steinberg Symbols
- **2** K_2 of fields
- **③** Some applications of K_2 in number theory
 - Hilbert Symbols and Quadratic Reciprocity
 - Brauer Groups
 - Norm residue symbols
- Higher Milnor K groups

- Suppose x, y ∈ E(R) are s.t. xy = yx, then [φ⁻¹(x), φ⁻¹(y)] is a well-defined element of St(R)
- 3 which maps to [x, y] = 1 under φ . i.e. $[\varphi^{-1}(x), \varphi^{-1}(y)] \in K_2(R)$.
- Infact, this is the most useful way of constructing elements of $K_2(R)$ and in case of fields, $K_2(R)$ is generated by such elements.

Let R be a commutative ring.

Definition

et
$$u, v \in R^{\times}$$
. The Steinberg Symbol $\{u, v\}$ is defined as
 $\{u, v\} := [\varphi^{-1}(d_{12}(u)), \varphi^{-1}(d_{13}(v))]$ where
 $d_{12}(u) = \begin{pmatrix} u & 0 & 0 \\ 0 & u^{-1} & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad d_{13}(v) = \begin{pmatrix} v & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & v^{-1} \end{pmatrix}$

Note that we have

•
$$d_{12}(u) = (e_{12}(u)e_{21}(-u^{-1})e_{12}(u))(e_{12}(1)e_{21}(-1)e_{12}(1))$$
 and
• $d_{13}(u) = (e_{13}(u)e_{31}(-u^{-1})e_{13}(u))(e_{13}(1)e_{31}(-1)e_{13}(1))$

< ∃ ►

Notation

Define
$$w_{ij}(u) := x_{ij}(u)x_{ji}(-u^{-1})x_{ij}(u) \in St(R)$$
 and
 $h_{ij}(u) := w_{ij}(u)w_{ij}(-1) \in St(R)$. It is clear that $\{u, v\} = [h_{12}(u), h_{13}(v)]$.

Lemma

The Steinberg symbol map $R^{\times} \times R^{\times} \longrightarrow K_2(R)$ is skew-symmetric and bilinear. i.e. $\{u, v\} = \{v, u\}^{-1}$ and $\{u_1u_2, v\} = \{u_1, v\}\{u_2, v\}$.

Proof

Note that $\varphi(w_{23}(1))$ conjugates $d_{12}(u)$ to $d_{13}(u)$ and vice-versa. i.e. $\varphi(w_{23}(1))d_{12}(u)\varphi(w_{23}(1))^{-1} = d_{13}(u)$ since $\varphi(w_{23}(1)) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix}$

イロト 不得 トイラト イラト 一日

proof continued

Skew-symmetry is proved as $\{u, v\} = [\varphi^{-1}(d_{12}(u)), \varphi^{-1}(d_{13}(v))]$ $= [w_{23}(1)\varphi^{-1}(d_{13}(u))w_{23}(1)^{-1}, w_{23}(1)\varphi^{-1}(d_{12}(v))w_{23}(1)^{-1}]$ $= w_{23}(1)[\varphi^{-1}(d_{13}(u)),\varphi^{-1}(d_{12}(v))]w_{23}(1)^{-1}$ $= w_{23}(1)\{v, u\}^{-1}w_{23}(1)^{-1} = \{v, u\}^{-1}$ (since $K_2(R)$ is central) Let $x_{ii}(u) = \varphi^{-1}(d_{ii}(u))$. Then $\{u, v_1 v_2\} = [x_{12}(u), x_{13}(v_1 v_2)]$ $= [x_{12}(u), x_{13}(v_1)x_{13}(v_2)]$ $= [x_{12}(u), x_{13}(v_1)][x_{12}(u), x_{13}(v_2)][x_{13}(v_1), [x_{13}(v_2), x_{12}(u)]]$ $= \{u, v_1\}\{u, v_2\}[x_{13}(v_1), \{u, v_2\}]^{-1}$ $= \{u, v_1\}\{u, v_2\}$ (since $K_2(R)$ is central)

< □ > < □ > < □ > < □ > < □ > < □ >

Lemma

Let R be any ring and $u, v \in R^{\times}$ and $i \neq j, k \neq l$, then the elements w_{ij} and h_{ij} of St(R) defined above satisfy $(w_{ij}(u))^{-1} = w_{ij}(-u), \quad w_{ij}(u) = w_{ji}(-u^{-1}), \quad h_{ij}(1) = 1$ $w_{ij}(v), \quad i, j, k, l \text{ all distinct}, \quad w_{ij}(-u^{-1}v), \quad k = i, \quad i, j, l \text{ all distinct}, \quad w_{il}(-vu), \quad k = j, \quad i, j, k \text{ all distinct}, \quad w_{il}(-vu), \quad k = j, \quad i, j, k \text{ all distinct}, \quad w_{ji}(-u^{-1}vu^{-1}), \quad k = i, j = l \quad w_{ji}(-uvu), \quad k = j, i = l$

Corollary

Let $u, v \in R^{\times}$, then $h_{12}(uv) = h_{12}(u)h_{12}(v)\{u, v\}^{-1}$.

Theorem

The Steinberg symbol map $R^{\times} \times R^{\times} \longrightarrow K_2(R)$ also satisfies

•
$$\{u,-u\}=1$$
 for $u\in R^{ imes}$,

2
$$\{u, 1-u\} = 1$$
 for $u \in R^{ imes}$, $1-u \in R^{ imes}$.

Proof

(a) By above corollary, we need to show h₁₂(-u²) = h₁₂(u)h₁₂(-u).
Using last identities of the lemma, we have h₁₂(u)h₁₂(-u) = w₁₂(u)w₁₂(-1)w₁₂(-u)w₁₂(-1) = w₂₁(u⁻²)w₁₂(-1) = w₁₂(-u²)w₁₂(-1) = h₁₂(-u²)
(b) Since -r = (1 - r)/(1 - r⁻¹), the first part implies 1 = {r, -r} = {r, 1-r}{r, 1-r⁻¹}⁻¹ = {r, 1-r}{r⁻¹} = {r, 1-r⁻¹}

Properties of Steinberg symbols

Corollary

If R is a finite field, then all Steinberg symbols vanish in $K_2(R)$.

Proof

- Let $R = \mathbb{F}_q$. Then \mathbb{F}_q^{\times} is cyclic say generated by u.
- **2** By bilinearity of symbol, it suffices to prove that $\{u, u\} = 1$.
- If char(R) = 2, then 1 = -1 and we have $\{u, u\} = \{u, -u\} = 1$.
- Otherwise q is odd. By skew-symmetry, we have {u, u} = {u, u}⁻¹.
 i.e. {u, u} has order atmost 2.
- So For any odd $m, n \in \mathbb{Z}$, we have $\{u, u\} = \{u, u\}^{mn} = \{u^m, u^n\}$.
- Since odd powers of *u* are same as non-squares in F[×]_q, it suffices to find a non-square *x* s.t. 1 − *x* is also a non-square.
- Such an x exists because the map x → 1 x is an involution on the set F_q {0,1} and this set consists of (q 1)/2 non-squares but only (q 3)/2 squares.

Theorem

If F is a field, then $K_2(F)$ is generated by Steinberg symbols.

Matsumoto's Theorem

If F is any (commutative) field, then $K_2(F)$ is the free abelian group on generators $\{u, v\}$, $u, v \in F^{\times}$, subject only to the relations of bilinearity in both variables and the relation $\{u, 1 - u\} = 1$.

- 4 回 ト 4 ヨ ト 4 ヨ ト

Some applications of K_2 in number theory

- We have seen K₂(F_q) = 1 for any finite field F_q while it is a classical fact that there are no non-commutative finite division algebras (Wedderburn Theorem).
- Some close relationship between K₂(F) for a field F and the existence of non-commutative finite dimensional division algebras over F. This is measured by Brauer Group Br(F) and is an important invariant of the arithmetic of a field.

Hilbert symbol

Let *F* be a field of characteristic $\neq 2$. The *Hilbert symbol of F* is the map $(,)_F : F^{\times} \times F^{\times} \longrightarrow \{\pm 1\}$ defined as: for $a, b \in F^{\times}$, (a, b) = 1 if there exists $x, y, z \in F$, not all zero s.t. $z^2 - ax^2 - by^2 = 0$, and (a, b) = -1 otherwise.

Why Hilbert Symbol?

Quadratic residue

Let $a \in \mathbb{Z} - \{0\}$ and p be an odd prime. If the equation $x^2 \equiv a \mod p$ has solution in F_p^{\times} , then a is said to be *quadratic residue* mod p.

Legendre Symbol

$$\left(rac{a}{p}
ight)=1$$
 if a is a quadratic residue mod p and -1 o.w.

Quadratic reciprocity law (Theorema "aureum")

Let p and q be odd primes. Then

p is quadratic residue mod $q \iff q$ is quadratic residue mod p (if $p, q \not\equiv 3 \mod 4$)

p is quadratic residue mod $q \iff q$ is quadratic non-residue mod p

More compactly,
$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\epsilon(p)\epsilon(q)}$$
 where $\epsilon(n) = (n-1)/2$.

Proposition

Let *F* be a field of characteristic $\neq 2$ and suppose for any quadratic extension $F(\sqrt{q})$ of *F*, $N(F((\sqrt{q}))^{\times})$ has index atmost 2 in F^{\times} . Then the Hilbert symbol $(a, b)_F$ depends only on the Steinberg symbol $\{a, b\} \in K_2(F)$, and defines a homomorphism $K_2(F) \longrightarrow \{\pm 1\}$.

Lemma

The Hilbert symbol $(a, b)_F = 1 \iff a$ lies in the image of the norm map $N: F(\sqrt{b})^{\times} \longrightarrow F^{\times}$.

Proof

 (\implies) Let $z^2 = ax^2 + by^2$ where not all x, y, z are 0. If x = 0 then b is perfect square and $F(\sqrt{b}) = F$. If not then $N(z/x + \sqrt{b}y/x) = a$. (\Leftarrow) If $b = c^2$ then (0, 1, c) is the solution of $z^2 = ax^2 + by^2$. If not then $a = N(\alpha + \sqrt{b}\beta) = \alpha^2 - b\beta^2 \implies (1, \beta, \alpha)$ is a solution.

Proof

- By Matsumoto's theorem, it is sufficient to prove that (a, b)_F bilinear in both variables and (a, 1 − a)_F = 1 for all a ∈ F − {0,1} (which is obvious since a1² + (1 − a)1² = 1).
- Hilbert symbol is symmetric as it takes values {±1} hence sufficient to prove bilinearity in first variable.
- If $(a_1, b)_F = (a_2, b)_F = 1$, then $a_1, a_2 \in Im(N) \implies a_1a_2 \in Im(N)$ hence $(a_1a_2, b)_F = 1$.
- Similarly, if $(a_1, b)_F = 1$ and $(a_2, b)_F = -1$ then also result is clear.
- Lastly, if (a₁, b)_F = (a₂, b)_F = −1, then both a₁, a₂ represent non-trivial element of the quotient F[×]/N(F((√q))[×]) which has cardinality atmost 2. Hence a₁a₂ ∈ Im(N).

< □ > < 同 > < 回 > < 回 > < 回 >

Definition

A field which is locally compact w.r.t. a non-discrete topology is called a *local field*.

Theorem

Any local field is isomorphic to either \mathbb{R} or \mathbb{C} , or a finite extension of \mathbb{Q}_p or $\mathbb{F}_p((t))$, the field of formal Laurent power series over the finite field \mathbb{F}_p .

Theorem

Let F be a local field of characteristic $\neq 2$. Then for any non-trivial quadratic extension $F(\sqrt{b})$ of F, $N(F(\sqrt{q})^{\times})$ has index exactly 2 in F^{\times} .

p-adic fields

Fix a positive prime $p \in \mathbb{Z}$.

p-adic metric

For $x \in \mathbb{Z}$, write $x = p^n y$ where $p \nmid y$. Define $|x|_p := p^{-n}$ is called p-adic norm on \mathbb{Z} . This can be extended to \mathbb{Q} by $\left|\frac{a}{b}\right|_p = \frac{|a|_p}{|b|_p}$ and will induce a metric $d(x, y) = |x - y|_p$ for $x, y \in \mathbb{Q}$.

It satisfies Strong triangle inequality: $|x - y|_p \le max\{|x|_p, |y|_p\}$.

p-adic numbers

The completion of \mathbb{Q} w.r.t. $|.|_p$ is called p-adic numbers denoted by \mathbb{Q}_p .

Ostrowski's Theorem

Every non-trivial absolute value on \mathbb{Q} is either equivalent to ususal absolute value or p-adic absolute value for some prime p.

Ajay Prajapati

イロン イヨン イヨン

Theorem

- K₂(Q) is a direct limit of finite abelian groups, and K₂(Q) ⊗_Z Z/2Z is an infinite direct sum of Z/2Z, one for each prime number p.
- O The Hilbert symbol (,)_{Q_p} when restricted to Q, kills the summands of K₂(Q) corresponding to primes other than p, and maps the summand corresponding to p onto {±1}.
- **(Hilbert Reciprocity law)** For $a, b \in \mathbb{Q}^{\times}$, we have

$$(a,b)_{\mathbb{R}} = \prod_{p \text{ prime}} (a,b)_{\mathbb{Q}_p}$$

Quadratic reciprocity law

Quadratic reciprocity

$$\left(rac{p}{q}
ight)\left(rac{q}{p}
ight)=(-1)^{\epsilon(p)\epsilon(q)}$$
 where $\epsilon(n)=(n-1)/2$.

Proof

Suppose r is a prime $\neq p, q$, then $(p, q)_{\mathbb{Q}_r} = 1$ (Chevalley's Theorem) If $a, b, c \in \mathbb{Z}$, then $aX^2 + bY^2 + cZ^2 = 0$ has a non-trivial solution in \mathbb{F}_p for every prime p and it lifts to \mathbb{Q}_p if $p \nmid 2abc$.

2
$$(p,q)_{\mathbb{R}}=1$$

Solution (p,q)_{Qq} = $\left(\frac{p}{q}\right)$ (Hensel's Lemma): Let f(X) ∈ Z[X] be a polynomial and f(X) ≡ 0 mod p has a solution y ∈ F_p s.t. f'(y) ≠ 0 mod p. Then ∃b ∈ Z_p s.t. y ≡ b mod p and f(b) = 0.

< 4[™] >

proof continued

Central Simple Algebras

Let *F* be a field. A finite dimensional *F*-algebra *A*(associative with unit) is called *central simple* if $Z(A) \cong F$ i.e. center of *A* is precisely *F* and *A* has no non-trivial two sided ideals, i.e. *A* is simple as a ring.

The Wedderburn structure theorem implies that any such algebra A is F-isomorphic to $M_n(D)$ for some $n \ge 1$ and some f.d. division algebra D with center F.

Definition

We call two central simple algebras A and B stably isomorphic if for some $r, s, M_r(A) \cong M_s(B)$.

Brauer Groups

Definition

The Brauer group of F, denoted Br(F), is the set of isomorphism class of central simple F-algebras, with operation \otimes_F , identity [F] and $[A]^{-1} := [A^{op}]$ since $A \otimes_F A^{op} \cong End_F(A)$ via identification $(a \otimes b^{op})(c) = acb$.

Since $A \cong M_{n_1}(D_1)$ and $B \cong M_{n_2}(D_2)$, A is stably isomorphic to $B \iff D_1 \cong D_2$. Thus each stable isomorphism class contains unique central division algebra.

It is clear that Br(F) is actually the set of isomorphism classes of central division algebras over F.

Frobenius Theorem

Every finite dimensional division algebra over $\mathbb R$ is either isomorphic to $\mathbb R,$ $\mathbb C$ or $\mathbb H.$

So $Br(\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$. $(\mathbb{H} \otimes_{\mathbb{R}} \mathbb{H} \cong M_4(\mathbb{R}))$

< □ > < □ > < □ > < □ > < □ > < □ >

Fix an algebraic closure \overline{F} of F and let F_{sep} denote the seperable closure of F in \overline{F} .

Brauer groups are actually cohomology group of the absolute Galois group in disguise.

Theorem

There is an isomorphism

$$H^2(Gal(F_{sep}/F), F_{sep}^{\times}) \longrightarrow Br(F)$$

Theorem (Kummer)

Let *n* be a positive integer and *F* be a field with char(F) = 0 or $char(F) \nmid n$ and containing μ_n , the group of n^{th} roots of unity. Let K/F be a sufficiently large Galois extension, in particular for $K = F_{sep}$ then there is an isomorphism $\varphi : F^{\times}/(F^{\times})^n \longrightarrow Hom(Gal(K/F), \mu_n)$ given by $\varphi(\sigma)(x) = \sigma(y)y^{-1}$ where $y \in K$ s.t. $y^n = x$.

Proof

Consider the short exact sequence of Gal(K/F)-modules

$$1 \longrightarrow \mu_n \longrightarrow K^{\times} \stackrel{x \mapsto x^n}{\longrightarrow} K^{\times} \longrightarrow 1$$

This gives a long exact sequence of cohomology groups

$$H^{0}(G, \mu_{n}) = \mu_{n} \longrightarrow H^{0}(G, F^{\times}) = F^{\times} \xrightarrow{\times \mapsto \times^{n}} F^{\times}$$
$$\stackrel{\delta}{\longrightarrow} H^{1}(G, \mu_{n}) = Hom(G, \mu_{n}) \longrightarrow H^{1}(G, F^{\times}) \longrightarrow \dots$$

< □ > < □ > < □ > < □ > < □ > < □ >

- Let n be a positive integer and F be a field with char(F) = 0 or char(F) ∤ n and containing μ_n. Let G denote the absolute Galois group of F, Gal(F_{sep}/F).
- Then there is a homomorphism called norm residue symbol, K₂(F) → {n-torsion of Br(F)} defined as:
- 3 Identify Br(F) with $H^2(G; F_{sep}^{\times})$ and view Kummer isomorphism φ as taking values in

 $Hom(G, \mu_n) \cong Hom(G, \mathbb{Z}/n\mathbb{Z}) = H^1(G, \mathbb{Z}/n\mathbb{Z})$

It β : H¹(G, ℤ/nℤ) → H²(G, ℤ) be the connecting map in the long exact cohomology sequence of short exact sequence of G-modules

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \longrightarrow 0$$

• Then for
$$\{u, v\} \in K_2(F)$$
,
 $\{u, v\} \longmapsto (u, v) := v_*(\beta \circ \varphi(u))$
where we think v as giving the map of G -modules $\mathbb{Z} \longrightarrow F_{sep}^{\times}$,
 $1 \longmapsto v$.

Theorem

The map $\{u, v\} \mapsto (u, v)$ is well defined. $(u, v) = 1 \iff v$ lies in the image of the norm map $N : F(u^{\frac{1}{n}}) \longrightarrow F^{\times}$. (This explains the name "norm residue symbol")

Definition

Given $a, b \in F^{\times}$ and ζ primitive n^{th} -root of unity, define $A_{\zeta}(a, b)$ the associative algebra with unit generated by two elements x and y and relations $x^n = a$, $y^n = b$ and $xy = \zeta yx$.

It can be proved that $A_{\zeta}(a, b)$ is central simple and map $F^{\times} \times F^{\times} \longrightarrow Br(F)$ defines a map $K_2(F) \longrightarrow Br(F)$ which is norm residue map defined above.

Higher Milnor K groups

For a field *F*, consider the tensor algebra of the group F^{\times} $T(F^{\times}) = \mathbb{Z} \oplus F^{\times} \oplus (F^{\times} \otimes F^{\times}) \oplus (F^{\times} \otimes F^{\times} \otimes F^{\times}) \oplus \dots$ **Notation:** I(x) for the element of degree 1 in $T(F^{\times})$ for $x \in F^{\times}$.

Definition

The graded ring $K_*^M(F)$ is defined to be the quotient of $T(F^{\times})$ by the ideal generated by the homogenous elements $l(x) \otimes l(1-x)$ with $x \neq 0, 1$. *Milnor K-groups* are defined to be the subgroup of elements of degree *n*.

Notation: The image of $I(x_1) \otimes \ldots \otimes I(x_n)$ in K_n^M will be denoted by $\{x_1, \ldots, x_n\}$.

- We have $K_0^M(F) = \mathbb{Z}$ and $K_1^M(F) = F^{\times}$.
- By Matsumoto's theorem, we also have K₂^M(F) = K₂(F), the elements {x, y} being the usual Steinberg symbols.
- Matsumoto's theorem was original motivation of Milnor to define the K-groups as above and he hoped that his construction will give some insight into the definition of higher K-groups of general rings.

Ajay Prajapati

- $K_n^M(\mathbb{F}_q) = 0$ for all $n \ge 2$ because $K_2^M(\mathbb{F}_q) = 0$.
- Por fields, Milnor K-groups does not agree with Quillen's K-groups beyond K₂. There is a natural map λ_n : K^M_n(F) → K_n(F) which fails to be injective for global fields(i.e. number fields or finite extension of 𝔽_p(t)) and n = 4.
- Milnor K groups plays a fundamental role in higher class field theory.

- Jonathan Rosenberg, Algebraic K-theory and its applications. GTM167, Springer, 1994
- Charles A. Weibel, The K-book: An Introduction to Algebraic K-theory. American Mathematical Society, 2013
- John Milnor, Introduction to Algebraic K-theory. Princeton university press and University of Tokyo press, 1971
- 9 J. P. Serre.A course in arithmetic. Springer, 1996