Indian Institute of Technology, Kanpur

MTH724A
An introduction to Algebraic K-theory

Milnor K-theory and its applications

Submitted by

Ajay Prajapati

Roll No- 17817063

Dept. of Mathematics and Statistics

Indian Institute of Technology, Kanpur

Course Instructor

Dr. Amit Shekhar Kuber

Dept. of Mathematics and Statistics

Indian Institute of Technology, Kanpur

April 2021

Contents

1 Introduction

In Shashwat's report, we have seen the definition of the K_2 of a ring in terms of quotient of Steinberg group. We have also seen how to add three more terms to the left of the long exact sequence which contained 3 terms from K_0 and K_1 each. In general, it is difficult to compute K_2 of rings. Even proving it is non-trivial is a difficult task. In this report, we will see the notion of Steinberg symbols which can be used to prove that K_2 of a particular ring is non-trivial. K_2 of fields has applications in various fields. We will see its application number theory. Finally, we will see Milnor's definition of higher K-groups of a field.

2 Preliminaries

We recall some of the important results and notions from Shashwat's report.

Definition 2.1. For $n \geq 3$, the *Steinberg group* $St_n(R)$ of a ring R is the group defined by the generators $x_{ij}(r)$, with $1 \leq i, j \leq n$, $i \neq j$ and $r \in R$ with the following relations:

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

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

Since 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 surjective homomorphism $\varphi : St(R) \longrightarrow E(R)$.

Definition 2.2. The group $K_2(R)$ is defined to be kernel of $\varphi : St(R) \longrightarrow E(R)$.

We have the following important theorem regarding $K_2(R)$.

Theorem 2.3. ***(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, one can prove that it is the universal central extension. Combining this result with a theorem of Hopf, we have natural isomorphism $K_2(R) \cong H_2(E(R), \mathbb{Z})$.

3 Steinberg Symbols

Suppose $x, y \in E(R)$ are s.t. $xy = yx$, then $[\varphi^{-1}(x), \varphi^{-1}(y)]$ is a well-defined element of $St(R)$ 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 (see theorem 4.1).

Let R be a commutative ring.

Definition 3.1. Let $u, v \in R^\times$. The *Steinberg Symbol* $\{u, v\}$ is defined as

$$\{u, v\} := [\varphi^{-1}(d_{12}(u)), \varphi^{-1}(d_{13}(v))] \quad \text{where } d_{12}(u) = \begin{pmatrix} u & 0 & 0 \\ 0 & u^{-1} & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad d_{13}(v) = \begin{pmatrix} v & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & v^{-1} \end{pmatrix}$$

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
- $d_{13}(u) = (e_{13}(u)e_{31}(-u^{-1})e_{13}(u))(e_{13}(1)e_{31}(-1)e_{13}(1))$

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 $\{u, v\} = [h_{12}(u), h_{13}(v)]$.

Now we see some properties of Steinberg symbols. But first we state some properties of commutator operator (which are trivial to prove).

Lemma 3.2. *Let G be a group and $u, v, w \in G$. Then*

(a) $[u, v] = [v, u]^{-1}$

(b) $[u, v][u, w] = [u, vw][v, [w, u]]$

(c) Jacobi Identity If $[G, G]$ is commutative, then $[u, [v, w]][v, [w, u]][w, [u, w]] = 1$.

Lemma 3.3. *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.

$$\varphi(w_{23}(1))d_{12}(u)\varphi(w_{23}(1))^{-1} = d_{13}(u) \quad \text{since } \varphi(w_{23}(1)) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix}$$

First we prove the skew-symmetric property

$$\begin{aligned} \{u, v\} &= [\varphi^{-1}(d_{12}(u)), \varphi^{-1}(d_{13}(v))] \\ &= [w_{23}(1)\varphi^{-1}(d_{13}(u))w_{23}(1)^{-1}, w_{23}(1)\varphi^{-1}(d_{12}(v))w_{23}(1)^{-1}] \\ &= w_{23}(1)[\varphi^{-1}(d_{13}(u)), \varphi^{-1}(d_{12}(v))]w_{23}(1)^{-1} \\ &= w_{23}(1)\{u, v\}^{-1}w_{23}(1)^{-1} = \{u, v\}^{-1} \quad \text{(since } K_2(R) \text{ is central)} \end{aligned}$$

Now we prove bilinearity. Let $x_{ij}(u) = \varphi^{-1}(d_{ij}(u))$. Then

$$\begin{aligned} \{u, v_1v_2\} &= [x_{12}(u), x_{13}(v_1v_2)] \\ &= [x_{12}(u), x_{13}(v_1)x_{13}(v_2)] \\ &= [x_{12}(u), x_{13}(v_1)][x_{12}(u), x_{13}(v_2)][x_{13}(v_1), [x_{13}(v_2), x_{12}(u)]] \\ &= \{u, v_1\}\{u, v_2\}[x_{13}(v_1), \{u, v_2\}]^{-1} \\ &= \{u, v_1\}\{u, v_2\} \quad \text{(since } K_2(R) \text{ is central)} \end{aligned}$$

Bilinearity in other variable follows from skew-symmetry. □

Now we see two results which help us to prove theorem 3.6. Proofs of the next lemma and its corollary are routine exercises and are left to the reader.

Lemma 3.4. *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*

$$(w_{ij}(u))^{-1} = w_{ij}(-u), \quad w_{ij}(u) = w_{ji}(-u^{-1}), \quad h_{ij}(1) = 1$$

$$w_{kl}(u)w_{ij}(v)(w_{kl}(u))^{-1} = \begin{cases} w_{ij}(v), & i, j, k, l \text{ all distinct}, \\ w_{lj}(-u^{-1}v), & k = i, \quad i, j, l \text{ all distinct}, \\ w_{il}(-vu), & k = j, \quad i, j, k \text{ all distinct}, \\ w_{ji}(-u^{-1}vu^{-1}), & k = i, j = l \end{cases}$$

Corollary 3.5. *Let $u, v \in R^\times$, then $h_{12}(uv) = h_{12}(u)h_{12}(v)\{u,v\}^{-1}$.*

Theorem 3.6. *The Steinberg symbol map $R^\times \times R^\times \longrightarrow K_2(R)$ also satisfies*

(a) $\{u, -u\} = 1$ *for* $u \in R^\times$,

(b) $\{u, 1-u\} = 1$ *for* $u \in R^\times$, $1-u \in R^\times$.

Proof. (a) By corollary 3.5, we need to show that $h_{12}(-u^2) = h_{12}(u)h_{12}(-u)$. Using last identities of lemma 3.4, we have

$$\begin{aligned} h_{12}(u)h_{12}(-u) &= w_{12}(u)w_{12}(1)w_{12}(-u)w_{12}(1) \\ &= w_{21}(u^{-2})w_{12}(1) \\ &= w_{12}(-u^2)w_{12}(1) = h_{12}(u^2) \end{aligned}$$

(b) Since $-r = (1-r)/(1-r^{-1})$, the first part implies

$$\{r, -r\} = \{r, 1-r\}\{r, 1-r^{-1}\}^{-1} = \{r^{-1}, 1-r^{-1}\} = 1$$

□

Corollary 3.7. *If R is a finite field, then all Steinberg symbols vanish in $K_2(R)$.*

Proof. Let $R = F_q$. Then $\mathbb{F}_q^\times$ is cyclic say generated by u. By bilinearity of symbol, it suffices to prove that $\{u, u\} = 1$. If $char(R) = 2$, then $1 = -1$ and by (a) of theorem 3.6, 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. 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 $\mathbb{F}_q^\times$, by theorem 3.6(b), it suffices to find a non-square x s.t. $1-x$ is also a non-square. But such an x exists because the map $x \longrightarrow 1-x$ is an involution on the set $\mathbb{F}_q - \{0, 1\}$ and this set consists of $(q-1)/2$ non-squares but only $(q-3)/2$ squares. □

4 K_2 of fields

We state the following important theorem (without proof). It's proof is very long and makes extensive use of group homology and cohomology. Interested reader is referred to section 4.3, [Rosenberg, 1994] or chapter 12, [Milnor, 1971].

Theorem 4.1. *If F is a field, then $K_2(F)$ is generated by Steinberg symbols.*

Corollary 4.2. *If F is a finite field, then $K_2(F)$ is trivial.*

With somewhat more work, one can strengthen the above result and prove the following (famous and difficult) theorem which was proven by Matsumoto in 1969.

Theorem 4.3. ***(Matsumoto)*** *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 $\{u, 1-u\} = 1$.*

5 Applications in Number Theory

We have seen that $K_2(\mathbb{F}_q) = 1$ for any finite field $\mathbb{F}_q$ while it is a classical fact that there are no non-commutative finite division algebras (Wedderburn Theorem). This might suggest a close relationship between $K_2(F)$ 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. But we start with Hilbert symbols and we will encounter Brauer group during its generalization.

5.1 Hilbert Symbol

Definition 5.1. 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.

Clearly, (a, b) depends only on the images of a and b in $F^\times/(F^\times)^2$. Thus $(a, b) = 1$ for all $a, b \in F^\times$ if $F = F^2$. E.g. algebraically closed fields.

Definition 5.2. Let $a \in \mathbb{Z} - 0$ and p be an odd prime. If the equation $x^2 \equiv a \bmod p$ has solution in $F_p^\times$, then a is said to be *quadratic residue* mod p.

Legendre Symbol: $\left(\frac{a}{p}\right) = 1$ if a is a quadratic residue mod p and -1 o.w.

Theorem 5.3. ***(Quadratic Reciprocity law)*** *Let p and q be odd primes. Then*

$$p \text{ is quadratic residue mod } q \iff q \text{ is quadratic residue mod } p \text{ (if } p, q \not\equiv 3 \bmod 4)$$
$$p \text{ is quadratic residue mod } q \iff q \text{ is quadratic non-residue mod } p \text{ (otherwise)}$$

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

The above theorem was conjectured by Euler and proven by Gauss. Gauss called it Theorema "aureum"(Golden theorem). This theorem can be said to be the starting point of Algebraic Number Theory.

We will see later(theorem 5.9) that there is an reciprocity law related to Hilbert symbols which is equivalent to the Quadratic reciprocity law. Legendre symbol helps us understand quadratic extensions of $\mathbb{Q}$. Hilbert symbol can be thought as a generalisation of Legendre symbol as it is defined for arbitrary fields of characteristic $\neq 2$ and helps us understand their quadratic extensions.

Lemma 5.4. *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. ($\Longrightarrow$) 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 $N(z/x + \sqrt{b}y/x) = a$.

($\Longleftarrow$) 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 the solution of $z^2 = ax^2 + by^2$. □

Next proposition connects Hilbert symbol to K-theory.

Proposition 5.5. *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 $K_2(F) \longrightarrow \{\pm 1\}$.*

Proof. By Matsumoto's theorem, it is sufficient to prove that $(a,b)_F$ bilinear in both variables and $(a,1-a)=1$ for all $a \in F-\{0,1\}$ (which is obvious since $a1^2+(1-a)1^2=1$). Clearly Hilbert symbol is symmetric as it takes values $\{\pm 1\}$ hence sufficient to prove bilinearity in first variable. If $(a_1,b)_F=(a_2,b)_F=1$, then $a_1,a_2 \in Im(N)$ by lemma 5.4 $\implies a_1a_2 \in Im(N)$ hence $(a_1a_2,b)=1$. Similarly, if $(a_1,b)_F=1$ and $(a_2,b)_F=-1$ then also result is clear. Lastly, if $(a_1,b)_F=(a_2,b)_F=-1$, then both a_1,a_2 represent non-trivial element of the quotient $F^\times/F((\sqrt{q}))^\times$ which has cardinality atmost 2. Hence $a_1a_2 \in Im(N)$. □

The hypothesis of proposition 5.5 may appear somewhat special but it is satisfied in a non-trivial case of great interest.

Definition 5.6. A field which is locally compact w.r.t. a non-discrete topology is called a *local field*.

We recall some standard theorems from algebraic number theory.

Theorem 5.7. *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 5.8. *Let F be a local field of characteristic $\neq 2$. Then for any non-trivial quadratic extension $F(\sqrt{b})$ of F, $N((\sqrt{q})^\times)$ has index exactly 2 in $F^\times$.*

We now see how Hilbert symbol helps us compute K_2 of rational numbers.

Theorem 5.9. *(a) $K_2(\mathbb{Q})$ is a direct limit of finite abelian groups, and $K_2(\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$ is an infinite direct sum of $\mathbb{Z}/2\mathbb{Z}$, one for each prime number p.*

(b) The Hilbert symbol $(\ ,\ )_{\mathbb{Q}_p}$ when restricted to $\mathbb{Q}$, kills the summands of $K_2(\mathbb{Q})$ corresponding to primes other than p, and maps the summand corresponding to p onto $\{\pm 1\}$.

*(c) **(Hilbert Reciprocity law)** For $a,b \in \mathbb{Q}^\times$, we have $(a,b)_{\mathbb{R}} = \prod_{p\ prime}(a,b)_{\mathbb{Q}_p}$.*

Proof. **(a) and (b)(Outline)** By Matsumoto's theorem, $K_2(\mathbb{Q})$ is generated by Steinberg symbols and by Fundamental theorem of Arithmetic, $Q^\times$ is generated by -1 and by the prime numbers p (linearly independent and each of infinite order).

For each positive integer m, let $A_m=\{(u,v) : u,v \in \mathbb{Z} \text{ and } |u|,|v| \leq m\}$. Then $K_2(\mathbb{Q}) = \varinjlim A_m$. By prime factorization property of integers, $A_{m-1}=A_m$ if m is not a prime. Then we construct a surjective homomorphism $\mathbb{F}_p^\times \longrightarrow A_p/A_{p-1}$, given by $x \longmapsto \{x,p\}$. This shows that A_p/A_{p-1} is finite cyclic of order atmost $p-1$. One can prove the *(b)* part by doing various computations with the Hilbert symbol. Now A_p/A_{p-1} is cyclic and various $(\ ,\ )_{\mathbb{Q}_p}$ are linearly independent homomorphisms to $\{\pm 1\}$, so it follows by induction on p that A_p is a direct sum of cyclic groups, each of even order, one for each prime $p' \leq p$. Passing to the limit, we get desired sturcture for $K_2(\mathbb{Q})$.

(c) The proof of this is very long and uses a lot of number theoretic results. So we refer the reader to [Serre, 1996], chapter 3. □

We now give the proof of Quadratic reciprocity law using Hilbert reciprocity law. But first we state two theorems from algebraic number theory which will be used.

Theorem 5.10. ***(Chevalley)*** *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 $p \nmid 2abc$.*

Theorem 5.11. ***(Hensel's Lemma):*** *Let $f(X) \in \mathbb{Z}[X]$ be a polynomial and $f(X) \equiv 0 \ mod\ p$ has a solution $y \in \mathbb{F}_p$ s.t. $f'(y) \not\equiv 0 \ mod\ p$. Then $\exists b \in \mathbb{Z}_p$ s.t. $y \equiv b \ mod\ p$ and $f(b)=0$.*

Corollary 5.12. ***(Quadratic Reciprocity law)*** *Let p and q be different odd primes. Then $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\epsilon(p)\epsilon(q)}$ where $\epsilon(n)=(n-1)/2$.*

Proof.

- Suppose r is a prime $\neq 2, p, q$, then $(p,q)_{\mathbb{Q}_r} = 1$ by Chevalley's theorem.
- $(p,q)_{\mathbb{R}} = 1$
- $(p,q)_{\mathbb{Q}_q} = \left(\frac{p}{q}\right)$. Suppose $\left(\frac{p}{q}\right) = 1$, then $X^2 = q$ has solution in $\mathbb{F}_p$. Using Hensel's lemma this can be lifted to a solution in $\mathbb{Q}_p$. Hence $z^2 - px^2 - qy^2$ has a solution. Conversely, suppose that $z^2 - px^2 - qy^2 = 0$ has a non-zero solution in $\mathbb{Q}_p$. WLOG we can assume it is primitive. i.e. $gcd(x,y,z) = 1$.
  Note that $y \neq 0$ otherwise $p = z^2/x^2$ would be a square in $\mathbb{Q}_p$. But if $(a_0 + a_1 p + \ldots)^2 = p$ then taking mod p yields that $a_0 = 0$ and taking mod p^2 yields a contradiction.
  So $y \neq 0$ in $\mathbb{Q}_p$ and we have $z^2 = qy^2 \bmod p$. Note that $y, z \neq 0$ in $\mathbb{F}_p$ otherwise solution would not be primitive. So $q = (z/x)^2$ in $\mathbb{F}_p$.
- $(p,q)_{\mathbb{Q}_p} = \left(\frac{q}{p}\right)$. This is clear by symmetry of Hilbert symbol.
- $(p,q)_{\mathbb{Q}_2} = (-1)^{(p-1)(q-1)/4}$
  We need to prove that $(p,q)_{\mathbb{Q}_2} = -1$ if $p, q \equiv 3 \bmod 4$ and is 1 o.w. Suppose $p \equiv 1 \bmod 4$ then either $p \equiv 1 \bmod 8$ or $p \equiv 5 \bmod 8$. Now we use the following fact: **If $n \in \mathbb{Z}$ is s.t. $n \equiv 1$ mod 8, then n is a square in $\mathbb{Q}_2$.**
  Then either p or $p + 4q = p.1^2 + q.2^2$ is square in $\mathbb{Q}_2$.
  If $p, q \equiv 3 \bmod 4$ and let (x,y,z) be primitive solution of $z^2 - px^2 - qy^2 = 0$. Taking mod 4, we get that $x^2 + y^2 + z^2 \equiv 0 \bmod 4$. But $x^2, y^2, z^2 \equiv 0$ or $1 \bmod 4$. Only possible solution is $x, y, z \equiv 0 \bmod 4$ contradicting primitivity of solution (x,y,z).

□

5.2 Brauer Groups

As we have seen that Hilbert symbol helped us understand quadratic extensions of arbitrary fields of characteristic $\neq 2$. We would hope to define a similar notion which helps us understand degree n extensions. This is clearly very ambitious as a degree n extension could be anything. But we can define a notion which helps us understand simple radical extensions. This comes from the theory of Brauer groups.

Let F be a field of characteristic $\neq 2$ and $a, b \in F^\times$.

Definition 5.13. The *quaternion algebra* $A_F(a,b)$ is the associative algebra over F generated by two elements x, y subject to the relations $x^2 = a$, $y^2 = b$ and $xy = -yx$.

Example 5.14. The Hamilton quaternion is $A_{\mathbb{R}}(-1,-1)$.

Lemma 5.15. *If $(a,b)_F = 1$, then $A_F(a,b) \cong M_2(F)$, whereas if $(a,b)_F = -1$, then $A_F(a,b)$ is non-commutative division algebra.*

Proof. If $(a,b)_F = 1$ then either both a and b are perfect squares or $a \in N(F(\sqrt{b})^\times)$. In first case, suppose $a = a_0^2$ and $b = b_0^2$. Then the map $A_F(a,b) \longrightarrow M_2(F)$, $x \mapsto X$ and $y \mapsto Y$ is an isomorphism where X and Y are matrices

$$X = \begin{pmatrix} a_0 & 0 \\ 0 & -a_0 \end{pmatrix} \quad Y = \begin{pmatrix} 0 & b_0 \\ b_0 & 0 \end{pmatrix}$$

In the second case, suppose $a = u^2 - bv^2$ then the following matrices X and Y give an isomorphism of $M_2(F)$ and $A_F(a,b)$

$$X = \begin{pmatrix} -u & -bv \\ v & u \end{pmatrix} \quad Y = \begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix}$$

If $(a,b)_F = -1$, then b is not a perfect square. Define an F-linear automorphism σ of $A_F(a,b)$ by $\bar{1} = -1$, $\bar{x} = -x$, $\bar{y} = -y$, $\bar{xy} = -xy = yx$. Then σ is an algebra anti-automorphism and if $u_0, u_1, u_2, u_3 \in F$ then

$$(u_0 + u_1x + u_2y + u_3xy)\overline{(u_0 + u_1x + u_2y + u_3xy)} = u_0^2 - u_1^2a - u_2^2b + u_3^2ab$$

Prove that $u_0^2 - u_1^2a - u_2^2b + u_3^2ab$ is definite quadratic form by contradiction. Suppose $u_0^2 - u_1^2a - u_2^2b + u_3^2ab = 0 \implies aN(u_1 + u_3\sqrt{b}) = N(u_2 + u_4\sqrt{b})$. If some $u_i \neq 0$, then $(a,b)_F = 1$. □

The above has natural generalisation, which is the theory of Brauer group of F.

Definition 5.16. 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 $n \geq 1$ and some f.d. division algebra D with center F.

Definition 5.17. We call two central simple algebras A and B *stably isomorphic* if for some r, s, $M_r(A) \cong M_s(B)$.

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.

Definition 5.18. 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 $(a \otimes b^{op})(c) = acb$.

It is clear from remark before above definition that $Br(F)$ is actually the set of isomorphism classes of central division algebras over F.

Example 5.19. It is a classical theorem of Frobenius that every finite dimensional division algebra over $\mathbb{R}$ is either isomorphic to $\mathbb{R}$, $\mathbb{C}$ or $\mathbb{H}$. Hence $Br(\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$ because $\mathbb{C}$ is not central over $\mathbb{R}$. ($\mathbb{H} \otimes_{\mathbb{R}} \mathbb{H} \cong M_4(\mathbb{R})$)

Definition 5.20. K/F is a field extension and A a central simple F-algebra, then A is said to be *split by* K if $K \otimes_F A \cong M_n(K)$ as K-vector spaces.

Fact: Every central simple F-algebra is split by some Galois extension of F.

Definition 5.21. *Relative Brauer group* $Br(F;K)$ is the stable isomorphism classes of K-split central simple F-algebras.

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

Theorem 5.22. *Let K/F be a finite Galois extension, then there is an isomorphism*

$$H^2(Gal(K/F), K^\times) \longrightarrow Br(F;K)$$

which sends class of cocycle ω to $[A_F(\omega)]$, where $A_F(\omega)$ is a K-vector space $KGal(K/F)$ with "twisted multiplication": $u_\sigma x = \sigma(x)u_\sigma$, $u_\sigma u_\tau = \omega(\sigma,\tau)u_{\sigma\tau}$.(Here u_σ is the basis element of $A_F(\omega)$ corresponding to $\sigma \in Gal(K/F)$)

Remark 5.23. Above theorem is also true for infinite Galois extensions by passing to the limit. In particular, fix an algebraic closure $\bar{F}$ of F and let F_{sep} denote the seperable closure of F in $\bar{F}$ then $Br(F) = H^2(Gal(F_{sep}/F); F_{sep}^\times)$. (the inductive limit of maximal chain of finite Galois extensions which exists by Zorn's lemma)

Using theorem 5.22, we can generalize proposition 5.5. We begin with the generalised Hilbert theorem 90 and a theorem of Kummer.

Theorem 5.24. *Let K/F be finite Galois extension. Then $H^1(Gal(K/F), K^\times) = 1$.*

Proof. Suppose $u \in H^1(Gal(K/F), K^\times)$ be a 1-cocycle. Since the elements of $Gal(K/F)$ are linearly independent over K (Dedekind's Theorem),

$$\sum_{\sigma \in Gal(K/F)} u(\sigma)\sigma \neq 0 \quad \text{as a function in } Hom_{Ab}(K, K)$$

so there is some $x \in K^\times$ s.t. $y = \sum_\sigma u(\sigma)\sigma(x) \neq 0$. Now, for any $\tau \in Gal(K/F)$

$$\begin{aligned}
\tau(y) &= \sum_\sigma \tau(u(\sigma))\tau(\sigma(x)) \\
&= \sum_\sigma u(\tau)^{-1}(u(\tau\sigma))\tau\sigma(x) \quad \text{(1-cocycle condition: } u(\tau\sigma) = \tau(u(\sigma))u(\tau)) \\
&= u(\tau)^{-1} \sum_{\sigma'} u(\sigma')\sigma'(x) = u(\tau)^{-1} y
\end{aligned}$$

Hence $u(\tau) = \tau(y^{-1})y = d^0(y^{-1})(\tau)$. i.e. u is a 1-coboundary. □

Theorem 5.25. ***(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

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

Now, take free resolution of $Gal(K/F)$-module $\mathbb{Z}$ having trivial action and apply $Hom(-, \mu_n)$ and $Hom(-, K^\times)$ to get a short exact sequence of cochain complexes which gives a long exact sequence in cohomology. (Take $G = Gal(K/F)$)

$$H^0(G, \mu_n) = \mu_n \longrightarrow H^0(G, F^\times) = F^\times \xrightarrow{x \longmapsto x^n} F^\times$$

$$\xrightarrow{\delta} H^1(G, \mu_n) = Hom(G, \mu_n) \longrightarrow H^1(G, F^\times)$$

By theorem 5.24, the result is clear. □

5.3 Norm residue symbol or Galois symbol

We are now ready to define a generalisation of Hilbert symbol for arbitrary simple radical extensions. It is called norm residue symbol.

Definition 5.26. Let n be a positive integer and F be a field with $char(F) = 0$ or $char(F) \nmid n$ 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*, $K_2(F) \longrightarrow \{n\text{-torsion of } Br(F)\}$ defined as:
Identify $Br(F)$ with $H^2(G; F_{sep}^\times)$ by theorem 5.22 and view Kummer isomorphism φ in theorem 5.25 as taking values in

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

and let $\beta : H^1(G, \mathbb{Z}/n\mathbb{Z}) \longrightarrow H^2(G, \mathbb{Z})$ 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 $\mathbb{Z} \longrightarrow F_{sep}^{\times}$, $1 \longmapsto v$.

Now we show how a norm residue symbol generalizes the Hilbert symbol. Note the similarity between the next theorem and the lemma 5.4.

Theorem 5.27. *The above 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")*

Proof. First we show $(u, v) = 1 \iff v \in Im(N)$. If $u \in (F^{\times})^n$ then any $v \in F^{\times}$ is a norm. So suppose $F(u^{\frac{1}{n}})$ is a proper Galois extension say of degree d, where $d|n$, and conjugates of $u^{\frac{1}{n}}$ are $u\zeta^j$ where $j = 0, \frac{n}{d}, ..., \frac{(d-1)n}{d}$ (ζ is a primitive n^{th} root of unity). Let $H = Gal(F(u^{\frac{1}{n}})/F) \cong Gal(F_{sep}/F)/Gal(F_{sep}/F(u^{\frac{1}{n}}))$ is a cyclic group with generator σ which maps $u^{\frac{1}{n}}$ to $u^{\frac{1}{n}}\zeta^{\frac{n}{d}}$. Then $\varphi(u)$ factors through H and $\varphi(u)(\sigma) = \zeta^{\frac{n}{d}}$. So the cohomology class (u, v) factors through $H^2(H, F(u^{\frac{1}{n}}))$ which is just $F^{\times}/N(F(u^{\frac{1}{n}})^{\times})$ by proof of theorem 5.8 given in [Rosenberg, 1994], section 4.4. Under this isomorphism, (u, v) maps to class of v in $F^{\times}/N(F(u^{\frac{1}{n}})^{\times})$.

Now we prove that the map is well defined. By Matsumoto's theorem, it is sufficient to prove that (u, v) is bilinear in both variables and $(u, 1-u) = 1$ for all $u \in F^{\times}$ s.t. $1-u \in F^{\times}$. Bilinearity is easy to see. To prove $(u, 1-u) = 1$, observe that for $v \in F$,

$$N(v - u^{\frac{1}{n}}\zeta^i) = \prod_{j=0}^{d-1}(v - u^{\frac{1}{n}}\zeta^{i+\frac{jn}{d}})$$

$$v^n - u = \prod_{i=0}^{n-1}(v - u^{\frac{1}{n}}\zeta^i) = \prod_{i=0}^{\frac{n}{d}-1} N(v - u^{\frac{1}{n}}\zeta^i)$$

Take $v = 1$, this shows $1 - u$ is product of norms hence a norm. So $(u, 1-u) = 1$. □

Above definition norm residue symbols is very long, complicated and not very explicit. But it can be defined in other ways which gives a more explicit mapping ([Milnor, 1971], chapter 15). But proving that it is well-defined is long.

Definition 5.28. 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.

6 Higher Milnor K-groups

So far we have just discussed K_2. But Milnor defined all K-groups for fields. In this section, we give his construction and outline some of its properties. These K-groups does not match the K-groups defined by Quillen beyond K_2. More details on this topic can be found in [Weibel, 2013], chapter 3, section 7.

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: We write $l(x)$ for the element of degree 1 in $T(F^{\times})$ for $x \in F^{\times}$.

Definition 6.1. 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 $x \neq 0, 1$. The *Milnor K-groups* are defined to be the subgroup of elements of degree n.

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

Clearly, we have $K_0^M(F) = \mathbb{Z}$ and $K_1^M(F) = F^\times$. By Matsumoto's theorem (4.3), we also have $K_2^M(F) = K_2(F)$, the elements $\{x, y\}$ being the usual Steinberg symbols (note here the group operation is written additively). Infact, Matsumoto's theorem was original motivation of Milnor to define the $K-$groups as above. The following are its properties:

- $K_n^M(\mathbb{F}_q) = 0$ for all $n \geq 2$ because $K_2^M(\mathbb{F}_q) = 0$ by corollary 3.7 and thm 4.1.

  Explaination: $K_2(\mathbb{F}_q) = \frac{\langle l(x) \otimes l(y) : x, y \in \mathbb{F}_q^\times \rangle}{\langle l(x) \otimes l(1-x) : x \in \mathbb{F}_q - \{0,1\} \rangle}$ is trivial. This means that every $l(y) \otimes l(z)$ is in the ideal generated by the homogenous elements $l(x) \otimes l(1-x)$. Hence every simple tensor $l(x_1) \otimes l(x_2) \ldots \otimes l(x_n)$ is in the ideal generated by elements $l(x) \otimes l(1-x)$. To see this, write $l(x_1) \otimes l(x_2) = \sum_i l(y_i) \otimes l(1-y_i)$. Then

$$l(x_1) \otimes l(x_2) \ldots \otimes l(x_n) = \sum_i l(y_i) \otimes l(1-y_i) \otimes l(x_3) \ldots \otimes l(x_n)$$

  Since simple tensors generate $T(F^\times)$, we actually have that every element of $T(F^\times)$ of degree ≥ 2 is in the ideal generated by $l(x) \otimes l(1-x)$. Hence $K_*^M(F^\times)$ contains no homogenous elements of degree $n \geq 2$.

- Bass and Tate proved that if F has transcendence degree 1 over a finite field (a global field of finite characteristics), $K_n^M(F) = 0$ for $n \geq 3$.

- Milnor K groups plays fundamental role in **higher class field theory** replacing $K_1(F) = F^\times$ in the one-dimensional class field theory.

References

J. Milnor. *Introduction to Algebraic K-theory.* Princeton university press, 1971.

J. Rosenberg. *Algebraic K-theory and its applications.* GTM167, Springer, 1994.

J. P. Serre. *A course in arithmetic.* Springer, 1996.

C. A. Weibel. *The K-book: An Introduction to Algebraic K-theory.* American Mathematical Society, 2013.