MILNOR K-THEORY, SYMBOLS, AND HILBERT RECIPROCITY

KYLE ORMSBY

Our story begins with a field F. We may form the *free associative algebra* $\mathrm{FreeAlg}(F^\times)$ generated by the nonzero elements $F^\times = F \smallsetminus \{0\}$ of F. This is the algebra whose underlying $\mathbb{Z}$-module is free on (possibly empty) words in the alphabet $\{[a] \mid a \in F^\times\}$.[1] Multiplication of words is given by concatenation, and the rest of the algebra structure is as it must be for associativity and distributivity to hold. Note that the empty word plays the role of the multiplicative identity, thus we denote it by 1.

Example 1. If $F = \mathbb{F}_2$, the field with 2 elements, then $F^\times = \{1\}$ and every word in $\{[1]\}$ is of the form $[1]^n$ for some $n \in \mathbb{N}$. Thus $\mathrm{FreeAlg}(F^\times)$ is isomorphic to the polynomial algebra $\mathbb{Z}[x]$ via the unique ring homomorphism taking $x \mapsto [1]$.

Remark 2. In general, free associative algebras are not polynomial algebras. When manually manipulating them, it is probably best to think of their elements as "non-commutative polynomials."[2]

There is a natural grading on $\mathrm{FreeAlg}(F^\times)$ given by word length so that, for instance, the degree (*i.e.* grading) of $2[a][b][c] - 5[d]$ is 3 and the degree of $-17[e]^6[f] + 3[g][h]$ is 7. Let $\mathrm{FreeAlg}_n(F^\times)$ denote elements of $\mathrm{FreeAlg}(F^\times)$ which are homogeneous of degree n and note that

$$\mathrm{FreeAlg}(F^\times) \cong \bigoplus_{n\in\mathbb{N}} \mathrm{FreeAlg}_n(F^\times)$$

as a $\mathbb{Z}$-module. In order to remind us that $\mathrm{FreeAlg}(F^\times)$ is graded, we will denote it

$$\mathrm{FreeAlg}_*(F^\times).$$

Here the $*$ is a wildcard which takes values in $\mathbb{N}$.

Having formed $\mathrm{FreeAlg}_*(F^\times)$, it is only natural to reincorporate some of the arithmetic structure of the field F by declaring that

$$[ab] = [a] + [b].$$

What may initially seem less natural is the *Steinberg relation*

$$[a][1-a] = 0 \text{ for } a \in F^\times \smallsetminus \{1\}.$$

Temporarily postponing a justification of this relation, let us rush ahead and give one of our primary definitions.

Date: July 6, 2015.

[1] We could also take words in $F^\times$ without the decorating square brackets, but this would make it hard to distinguish between multiplication in $F^\times$ and multiplication in the algebra.

[2] Note, though, that there is more structure lurking in the background. The assignment if a set S to $\mathrm{FreeAlg}(S)$ is in fact a functor which is left adjoint to the forgetful functor taking a ring (associative and unital) to its underlying set of elements. The reader should check that there is a (natural) bijection between ring homomorphisms $\mathrm{FreeAlg}(S) \to R$ and functions $S \to R$.

Definition 3. Let F be a field and define

$$I := ([ab] - [a] - [b] \mid a, b \in F^\times),$$
$$J := ([a][1-a] \mid a \in F^\times \smallsetminus \{1\})$$

to be (homogeneous) ideals in $\mathrm{FreeAlg}_*(F^\times)$. The *Milnor K-theory* of a field F is the graded ring

$$K_*^M(F) := \mathrm{FreeAlg}_*(F^\times)/(I + J)$$

Abuse of notation 4. We will drop the coset notation $+(I + J)$ from our notation for elements of $K_*^M(F)$. Henceforward, $[a]$ (with $a \in F$) will refer to the image of $[a]$ in $K_*^M(F)$. Furthermore, products $[a_1][a_2]\cdots[a_n]$ will be denoted $[a_1, a_2, \ldots, a_n]$.

Remark 5. The quotient

$$\mathrm{FreeAlg}(F^\times)/I$$

is also known as the *tensor algebra* on the abelian group $F^\times$. Milnor's original definition of Milnor K-theory treats $K_*^M(F)$ as a quotient of the tensor algebra on $F^\times$. Since Milnor-Witt K-theory appears as the quotient of a free algebra, we have chosen this as our starting place for Milnor K-theory as well.

Remark 6. Since I and J are homogeneous, $K_*^M(F)$ inherits its grading from $\mathrm{FreeAlg}_*(F^\times)$. For $n \in \mathbb{N}$, $K_n^M(F)$ denotes the abelian group of homogeneous elements of degree n.

Proposition 7. *For any field F, $K_0^M(F) = \mathbb{Z}$ and the assignment $a \mapsto [a]$ is an isomorphism of abelian groups $F^\times \to K_1^M(F)$. In particular, $[1] = 0$.*

Proof. The statement about $K_0^M(F)$ is obvious. In $K_1^M(F)$, we have that $[ab] = [a] + [b]$, so the assignment is a homomorphism. Bijectivity is clear.

To see that $[1] = 0$ completely explicitly, note that

$$[1] = [1 \cdot 1] = [1] + [1]$$

and subtract $[1]$ from both sides. □

Example 8. We have $K_*^M(\mathbb{F}_2) \cong \mathbb{Z}$, concentrated in degree 0.

Example 9. In fact, for any finite field $\mathbb{F}_q$ of order q, $K_*^M(\mathbb{F}_q)$ is concentrated in degrees 0 and 1 with $K_1^M(\mathbb{F}_q)$ cyclic of order $q - 1$. See [2, Example V.6.14] for details (but be wary that the group law in his K_2F is written multiplicatively).

We now consider the job of Milnor K-theory, or more precisely the universal property of $K_2^M(F)$. Recall that $K_2^M(F)$ is the quotient of $F^\times \otimes_{\mathbb{Z}} F^\times$ by the Steinberg relation $(a \otimes (1-a) \mid a \in F^\times \smallsetminus \{1\})$. Since the job of the tensor product of R-modules $M \otimes_R N$ is to to turn bilinear forms $M \times N \to L$ into module homomorphisms $M \otimes_R N \to L$, we see that $K_2^M(F)$ similarly encodes a certain type of form on $F^\times \times F^\times$.

Definition 10. A *symbol* (or *Steinberg symbol*) on a field F with values in an abelian group G (say with group law written multiplicatively) is a function $(\ ,\ ) : F^\times \times F^\times \to G$ such that for all $a, b, c \in F^\times$,

(i) $(ab, c) = (a, c)(b, c)$ and $(a, bc) = (a, b)(a, c)$, and
(ii) if $a + b = 1$, then $(a, b) = 1$.

Remark 11. Condition (i) says that $(\ ,\ )$ is bimultiplicative (in analogy with bilinearity), and condition (ii) is exactly the Steinberg relation. As such, we immediately have the following proposition.

Proposition 12. *Given any symbol* $(\ ,\ ) : F^\times \times F^\times \to G$*, there exists a unique homomorphism* $K_2^M(F) \to G$ *such that*

$$\begin{array}{ccc} F^\times \times F^\times & & \\ \downarrow & \searrow^{(\ ,\ )} & \\ K_2^M(F) & \longrightarrow & G \end{array}$$

where the vertical map takes (a, b) *to* $[a, b]$.

Symbols arise naturally in several number theoretic contexts. The simplest one to define is the *tame symbol* $(\ ,\ )_v$ of a field F with discrete valuation v. A *discrete valuation* is a homomorphism $v : F^\times \to \mathbb{Z}$ satisfying $v(a+b) \geq \min\{v(a), v(b)\}$ for all $a, b \in F^\times$. The ring $\mathcal{O} = \{a \in F \mid v(a) \geq 0\} \cup \{0\}$ is called the *valuation ring* of (F, v); it contains a maximal ideal $\mathfrak{m}$ consisting of 0 and all elements with positive valuation. The quotient $\overline{F} := \mathcal{O}/\mathfrak{m}$ is called the *residue field* of (F, v).[3]

Given a discretely valued field (F, v) we define

$$(a, b)_v := (-1)^{v(a)v(b)} \frac{a^{v(b)}}{b^{v(a)}} \mod \mathfrak{m},$$

a well-defined element of $\overline{F}^\times$ since $\pm\frac{a^{v(b)}}{b^{v(a)}}$ is clearly a unit in $\mathcal{O}$.

Lemma 13. *For any discretely valued field* (F, v)*, the tame symbol* $(\ ,\ )_v$ *is a Steinberg symbol.*

Before proving the lemma, let us consider the example of the rational numbers equipped with the p-adic valuation v_p. Writing $\alpha \in \mathbb{Q}$ in the form $p^r \frac{a}{b}$ where $r \in \mathbb{Z}$ and $p \nmid a, b$, we have

$$v_p(\alpha) := r.$$

In this case, $\mathcal{O} = \mathbb{Z}_{(p)}$, the ring of *$p$-local integers*, *i.e.*, rational numbers for which the denominator is not divisible by p. Moreover, $\mathfrak{m} = p\mathbb{Z}_{(p)}$, so $\overline{\mathbb{Q}} = \mathbb{F}_p$. Write $(\ ,\ )_p$ for $(\ ,\ )_{v_p}$. A simple computation gives that

$$\left(p^r \frac{a}{b}, p^s \frac{c}{d}\right)_p = (-1)^{rs} \frac{a^s d^r}{b^s c^r} \mod p\mathbb{Z}_{(p)}$$

where $p \nmid a, b, c, d$. It is then easy to check manually that $(\ ,\ )_p$ is bimultiplicative and satisfies the Steinberg relation.

Proof of Lemma 13. Bimultiplicativity is clear. To prove that the Steinberg relation $(a, 1-a)_v = 1$ holds, first consider the case that $v(a) > 0$, *i.e.*, $a \in \mathfrak{m}$. Then $1 - a \equiv 1 \mod \mathfrak{m}$ and hence $v(1-a) = 0$. Thus

$$(-1)^{v(a)v(1-a)} \frac{a^{v(1-a)}}{(1-a)^{v(a)}} = \frac{1}{(1-a)^{v(a)}} \equiv 1 \mod \mathfrak{m},$$

as desired. A similar argument works if $v(1-a) > 0$.

Now suppose $v(a) < 0$ so that $1/a \in \mathfrak{m}$. Since $(1-a)/a = -1 + 1/a \equiv -1 \mod \mathfrak{m}$ is a unit in $\overline{F}$, we learn that $v(1-a) = v(a)$. Moreover,

$$\frac{a^{v(1-a)}}{(1-a)^{v(a)}} = \left(\frac{a}{1-a}\right)^{v(a)} \equiv (-1)^{v(a)} \mod \mathfrak{m}.$$

[3] If unfamiliar with discrete valuations, you should check all of these statements or, alternatively, read Cassels's brilliant book [1].

Multiplying by $(-1)^{v(a)v(1-a)} = (-1)^{v(a)}$, we see that $(a, 1-a)_v = 1$ in this case as well. A similar argument works if $v(1-a) < 0$.

There is only one remaining case, $v(a) = v(1-a) = 0$, which is trivial. □

Of course, the tame symbol is fairly bland when $p = 2$. We rectify this by redefining $(\ ,\ )_2$ as follows. Note that any rational number has a unique expression as $\pm 2^j 5^k c/d$ where $j \in \mathbb{Z}$, $k = 0$ or 1, and both c and d are integers congruent to 1 mod 8. If $a = (-1)^i 2^j 5^k c/d$ and $b = (-1)^I 2^J 5^K c'/d'$, define

$$(a, b)_2 := (-1)^{iI+jK+kJ}.$$

The reader may check that this defines a Steinberg symbol on $\mathbb{Q}$ with values in $\{\pm 1\}$.

Theorem 14 (Tate)**.** *The assignment*

$$\begin{aligned} K_2^M(\mathbb{Q}) &\longrightarrow \{\pm 1\} \oplus {\mathbb{F}_3}^\times \oplus {\mathbb{F}_5}^\times \oplus {\mathbb{F}_7}^\times \oplus \cdots \\ [a, b] &\longmapsto ((a, b)_2, (a, b)_3, (a, b)_5, (a, b)_7, \ldots) \end{aligned}$$

is a well-defined isomorphism.

We will not prove this theorem here, but rather refer the reader to Milnor [4, pp.101–103].

Let $A_p = {\mathbb{F}_p}^\times$ if $p > 2$, and let $A_2 = \{\pm 1\}$. Since all symbols on $\mathbb{Q}$ factor through $K_2^M(\mathbb{Q})$, we learn that for any symbol $(\ ,\ )$ on $\mathbb{Q}$ with values in G, there exist unique homomorphisms $\varphi_p : A_p \to G$ such that

$$(a, b) = \prod \varphi_p(a, b)_p.$$

In particular, we may consider the symbol

$$(a, b)_\infty = \begin{cases} 1 & \text{if } a > 0 \text{ or } b > 0, \\ -1 & \text{if } a, b < 0, \end{cases}$$

for which there are unique $\varphi_p : A_p \to \{\pm 1\}$ such that $(a, b)_\infty = \prod \varphi_p(a, b)_p$.

Definition 15. Let p be a rational prime or ∞. The *Hilbert symbol* $(\!(\ ,\ )\!)_p$ is defined to be $(\ ,\ )_p$ if $p = 2$ or ∞; otherwise, $(\!(a, b)\!)_p$ in the unique value in $\{\pm 1\}$ such that

$$(\!(a, b)\!)_p \equiv (a, b)_p^{(p-1)/2} \mod p.$$

The observation $(a, b)_\infty = \prod \varphi_p(a, b)_p$ now clearly implies that there exists $\varepsilon_p \in \{0, 1\}$ such that for all $a, b \in \mathbb{Q}^\times$, $(\!(a, b)\!)_\infty = \prod (\!(a, b)\!)_p^{\varepsilon_p}$. In fact, all of the $\varepsilon_p = 1$, a statement which is known as Hilbert reciprocity.

Theorem 16 (Hilbert reciprocity)**.** *For all $a, b \in \mathbb{Q}^\times$,*

$$1 = \prod (\!(a, b)\!)_p$$

where the product ranges over all rational primes and ∞.

The proof is a case-wise analysis which runs through the potential congruence classes of $p \mod 8$. Primes congruent to $1 \mod 8$ are the trickiest, and that argument relies on a theorem of Gauss.[4] Again, see Milnor [4, pp.104–106].

[4] If a prime $p \equiv 1 \mod 8$, then there exists a prime $q < \sqrt{p}$ such that p is not a quadratic residue mod q.

Interpretation of symbols. As presented, the tame and Hilbert symbols discussed here probably seem horribly *ad hoc*. Yet Hilbert reciprocity is much more than a flashy numeroligical trick. In fact, this reciprocity law implies classical quadratic reciprocity and forms the basis for Hilbert's ninth problem, a program of inquiry which eventually led to class field theory [3, Preface].

The Hilbert symbols derive their power from a connection with quadratic forms. The definitions given above are mere formulas which hide conceptual beauty.

Very briefly, given a field F and $a, b \in F^\times$, let $q_{a,b}$ denote the quadratic form

$$q_{a,b}(x, y, z) = ax^2 + by^2 - z^2.$$

We declare

$$(a, b)_F = \begin{cases} 1 & \text{if } q_{a,b} \text{ is isotropic,} \\ -1 & \text{if } q_{a,b} \text{ is anisotropic.} \end{cases}$$

An n-dimensional quadratic form q is *isotropic* if there exists $x \in F^n \smallsetminus \{0\}$ such that $q(x) = 0$; otherwise, q is *anisotropic*.[5] If F is a local field, $(\ ,\ )_F$ is a Steinberg symbol.[6] In fact, if F is the field of p-adic rationals $F = \mathbb{Q}_p$, then $(\ ,\ )_{\mathbb{Q}_p} = (\!|\ ,\ |\!)_p$. If $F = \mathbb{R} = \mathbb{Q}_\infty$, then $(\ ,\ )_{\mathbb{R}} = (\!|\ ,\ |\!)_\infty$.

Now $\mathbb{Q}$ is the prime field (and thus a subfield) of all the $\mathbb{Q}_p$ (including $\mathbb{Q}_\infty$). Thus Hilbert reciprocity relays (at least) two important facts: First, if $a, b \in \mathbb{Q}^\times$, then for almost every p, $q_{a,b}$ is isotropic as a form over $\mathbb{Q}_p$. Second, the (an)isotropicity of $q_{a,b}$ over all but one $\mathbb{Q}_p$ determines the (an)isotropicity of $q_{a,b}$ over the mystery $\mathbb{Q}_p$.

1. Exercises

Exercise 17. Use the identity $-a = (1 - a)/(1 - 1/a)$ to prove that $[a, -a] = 0 \in K_2^M(F)$ for any $a \in F$.

Exercise 18. Show that for every $x \in K_m^M(F)$ and every $y \in K_n^M(F)$,

$$xy = (-1)^{mn} yx.$$

Hint: It suffices to consider the case $x = [a]$, $y = [b]$. Use the previous exercise to add two clever 0's to $[a, b] + [b, a]$.

Exercise 19. Prove that $[a, a] = [a, -1]$ for all $a \in F$.

Exercise 20. Use induction on n to prove that whenever $a_1 + \cdots + a_n = 0$ or 1, $a_i \in F$, then $[a_1, \ldots, a_n] = 0$.

Exercise 21. Prove that $K_2^M(\mathbb{F}_q) = 0$ for any finite field $\mathbb{F}_q$.

Exercise 22. An (additive) abelian group A is called *divisible* if for every positive integer n and every $x \in A$, there exists $y \in A$ such that $ny = x$. Prove (by induction) that for all $n \geq 1$, $K_n^M(\mathbb{R})$ is the direct sum of a $\mathbb{Z}/2\mathbb{Z}$ summand generated by $[-1]^n$ and a divisible group generated by $\{[a_1, \ldots, a_n] \mid a_1, \ldots, a_n > 0\}$. Hence

$$K_*^M(\mathbb{R})/(2) \cong \mathbb{F}_2[\rho]$$

where ρ is a polynomial generator corresponding to $[-1]$.

---

[5] We will say much more about (an)isotropic quadratic forms later.

[6] It is clear that $(\ ,\ )_F$ always satisfies the Steinberg relation; bimultiplicatiivty takes work.

References

[1] J. W. S. Cassels. *Local fields*, volume 3 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1986.
[2] T. Y. Lam. *Introduction to quadratic forms over fields*, volume 67 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2005.
[3] Franz Lemmermeyer. *Reciprocity laws*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2000. From Euler to Eisenstein.
[4] John Milnor. *Introduction to algebraic K-theory*. Princeton University Press, Princeton, N.J.; University of Tokyo Press, Tokyo, 1971. Annals of Mathematics Studies, No. 72.