Here is one easy method for constructing Steinberg symbols. Recall that a *discrete valuation* v on a field F is a homomorphism from the multiplicative group $F^\bullet$ onto the additive group of integers, satisfying $v(x+y) \geq \mathrm{Min}(v(x), v(y))$. The associated *valuation ring* $\Lambda \subset F$ consists of all x with $v(x) \geq 0$, together with the zero element of F. There is a unique maximal ideal $\mathfrak{P} \subset \Lambda$; and the quotient $\Lambda/\mathfrak{P}$ is called the *residue class field* $\bar{F}$.

LEMMA 11.5. *The formula* $d_v(x, y) = (-1)^{v(x)v(y)} x^{v(y)}/y^{v(x)} \bmod \mathfrak{P}$ *defines a continuous Steinberg symbol* d_v *on* F *with values in the discrete group* $\bar{F}^\bullet = (\Lambda/\mathfrak{P})^\bullet$.

(Compare Serre, *Corps locaux*, p. 217.) This d_v is called the *tame symbol* associated with the valuation v. Evidently d_v gives rise to a homomorphism from K_2F onto the group $\bar{F}^\bullet = K_1(\bar{F})$.

Proof of 11.5. The element $\pm x^{v(y)}/y^{v(x)}$ is a unit of Λ, since both $x^{v(y)}$ and $y^{v(x)}$ have the same image (namely $v(x)v(y)$) under v. It is clear that d_v is bimultiplicative, and continuous in the v-topology. The proof that $d_v(1-x, x) = 1$ will be divided into several cases. If $v(x) > 0$, then $x \in \mathfrak{P}$, hence $1-x \equiv 1 \bmod \mathfrak{P}$ and $v(1-x) = 0$, so that

$$(-1)^{v(1-x)v(x)}(1-x)^{v(x)}/x^{v(1-x)} = (1-x)^{v(x)} \equiv 1 \bmod \mathfrak{P}.$$

The proof when $v(1-x) > 0$ is similar. Now suppose that $v(x) < 0$. Then $x^{-1} \in \mathfrak{P}$, hence the quotient

$$(1-x)/x = -1 + x^{-1} \equiv -1 \bmod \mathfrak{P}$$

is a unit. Therefore $v(1-x) = v(x)$, and

$$(1-x)^{v(x)}/x^{v(1-x)} = ((1-x)/x)^{v(x)} \equiv (-1)^{v(x)} \bmod \mathfrak{P}.$$

Multiplying by the sign $(-1)^{v(1-x)v(x)} = (-1)^{v(x)}$, we obtain $1 \bmod \mathfrak{P}$, as required. The case $v(1-x) < 0$ is similar. Since the remaining case $v(x) = v(1-x) = 0$ is trivial, this proves 11.5. ∎

Gauss and Quadratic Reciprocity

To illustrate these concepts let us look at the field Q of rational numbers. What Steinberg symbols c(x,y) can be defined on the field Q?

For any prime p, the p-adic valuation v_p on Q gives rise to a Steinberg symbol $d_{v_p}(x,y)$ with values in the cyclic group $(Z/pZ)^\bullet$ of order p−1. If p is odd we will denote this symbol briefly by $(x,y)_p$, and its target group $(Z/pZ)^\bullet$ by A_p.

For $p = 2$ this construction is useless. However a 2-adic symbol $(x,y)_2$ can be defined as follows. Any non-zero rational can be written uniquely as a product of the form $\pm 2^j 5^k u$, where k equals 0 or 1, and where u is a quotient of integers congruent to 1 modulo 8. Now if

$$x = (-1)^i 2^j 5^k u, \quad y = (-1)^I 2^J 5^K u',$$

then set

$$(x,y)_2 = (-1)^{iI+jK+kJ}.$$

Thus the target group A_2 is the cyclic group $\{\pm 1\}$. The verification that this is a well defined Steinberg symbol will be left as an exercise.

REMARK. The following assertion may help to motivate the definition of $(x,y)_p$.

For any prime p *suppose that a Steinberg symbol* $c: Q^\bullet \times Q^\bullet \to A$, *with values in a Hausdorff topological group* A, *is continuous with respect to the* p*-adic topology on* $Q^\bullet$. *Then there is one and only one homomorphism from* A_p *to* A *which carries the symbol* $(x,y)_p$ *to* c(x,y) *for every* x *and* y.

Briefly speaking, $(x,y)_p$ is the "universal continuous Steinberg symbol" for the p-adic topology on $Q^\bullet$. This statement is a special case of a much more general theorem, due to Calvin Moore, which is proved in the Appendix.

Here is an outline of the proof. Let p^n be any prime power which is greater than 2. Then the congruence

$$(4)\qquad (1-rp^n)^p \equiv 1-rp^{n+1} \pmod{p^{n+2}}$$

follows easily from the binomial theorem. Now suppose that p is odd, and that r is prime to p. Let u_1 denote any quotient of the form s/t with $s \equiv t \equiv 1 \pmod p$. Using (4), we note that u_1 can be approximated arbitrarily closely, in the p-adic topology, by a power of 1-rp. In fact we can first choose i so that

$$(1-rp)^i t \equiv s \pmod{p^2},$$

then choose j so that

$$(1-rp)^{i+jp} t \equiv s \pmod{p^3},$$

and so on.

Since $c(rp, (1-rp)^i) = 1$ for every exponent i, it follows by continuity that $c(rp, u_1) = 1$ for every such $u_1 = s/t$. But the entire multiplicative group $Q^\bullet$ is generated by such products rp, with r relatively prime to the fixed prime p. Thus we have proved that

$$(5)\qquad c(x,u_1) = 1 \quad \text{for all } x \text{ in } Q^\bullet.$$

If r and r' denote integers prime to p, then it follows immediately from (5) that $c(r,r')$ depends only on the residue classes of r and r' modulo p. But, applying Steinberg's theorem that every symbol on a finite field must be trivial (§9.9), this proves that

$$(6)\qquad c(r,r') = 1.$$

Let λ denote a primitive root modulo p. Then any x and y in $Q^\bullet$ can be written more or less uniquely in the form

$$x = p^i\lambda^j u_1, \quad y = p^I\lambda^J u_1';$$

and it follows that

$$c(x,y) = c(p,p)^{iI} c(\lambda,p)^{jI-iJ}.$$

Since the equalities

$$c(\lambda,p)^{p-1} = c(\lambda^{p-1},p) = 1$$

and

$$c(p,p) = c(-1,p) = c(\lambda,p)^{(p-1)/2}$$

follow from (5), the proof for p odd can now easily be completed.

For $p = 2$ a similar argument shows that every number u which can be expressed as a quotient s/t with $s \equiv t \equiv 1 \pmod 8$ can be approximated arbitrarily closely, in the 2-adic topology, by a power of 9. Using the equalities

$$c(9,-1) = c(3,-1)^2 = c(3,(-1)^2) = 1,$$
$$c(9,-2) = c(3,-2)^2 = 1, \text{ and}$$
$$c(9,3) \;= c(-3,3)^2 = 1,$$

it follows by continuity that

$$c(u,-1) = c(u,-2) = c(u,3) = 1$$

for every such u. Since -1, -2, and 3 generate a subgroup of $Q^\bullet$ which is everywhere dense, this proves that

$$(7)\qquad c(u,x) = 1 \quad \text{for all } x.$$

As an example, taking $u = -5/3$, it follows that

$$c(5,x) = c(-3,x).$$

Taking $x = 4$, we see that $c(5,4) = 1$, hence $c(5,-1) = c(5,-4) = 1$, and therefore

$$(8)\qquad c(5,5) = c(5,-1) = 1.$$

Similarly the equation $c(-5,-1) = c(3,x)$ for $x = -2$ implies that $c(-5,-2) = 1$, and hence

$$(9)\qquad c(5,2) = c(-1,-1).$$

Now combining (7), (8), and (9) with the evident equation $c(2,2) = c(2,-1) = 1$, we see that

$$c((-1)^i 2^j 5^k u, (-1)^I 2^J 5^K u') = c(-1,-1)^{iI+jK+kJ};$$

which clearly completes the proof. ∎

Using these Steinberg symbols $(x,y)_p$, we are now ready to compute the group K_2Q.

THEOREM 11.6 (Tate). *The group* K_2Q *is canonically isomorphic to the direct sum* $A_2 \oplus A_3 \oplus A_5 \oplus \ldots$, *where* A_2 *is the cyclic group* $\{\pm 1\}$, *and where* $A_p = (Z/pZ)^\bullet$ *for* p *odd.*

In fact the isomorphism will be given by the correspondence

$$\{x,y\} \mapsto (x,y)_2 \oplus (x,y)_3 \oplus (x,y)_5 \oplus \ldots$$

for all x and y in $Q^\bullet$.

Tate remarks that his proof of this theorem is lifted directly from the argument which was used by Gauss in his first proof of the quadratic reciprocity law. (Compare Gauss, *Disquisitiones Arithmeticae*, Yale Univ. Press 1966, pp. 84-98.)

To start the proof, for each positive integer m let L_m denote the subgroup of K_2Q generated by all symbols $\{x,y\}$ where x and y are integers of absolute value $\leq m$. Then clearly

$$L_1 \subset L_2 \subset L_3 \subset \ldots$$

with union K_2Q. Note that $L_m = L_{m-1}$ if m is not a prime number.

LEMMA 11.7. *For each prime* p *the quotient group* L_p/L_{p-1} *is cyclic of order* $p-1$.

In particular the quotient L_2/L_1 is trivial. Assuming this lemma for the moment, the proof proceeds easily as follows.

For each prime p the correspondence $\{x,y\} \mapsto (x,y)_p$ defines a homomorphism from K_2Q to A_p. If p is odd, it is clear that this homomorphism annihilates L_{p-1}, but maps L_p onto the cyclic group $A_p = (Z/pZ)^\bullet$. Hence it induces an isomorphism $L_p/L_{p-1} \cong A_p$. On the other hand, for $p = 2$, this homomorphism maps the generator $\{-1,-1\}$ of L_1 onto the element $(-1,-1)_2 = -1$, and hence induces an isomorphism from $L_1 = L_2$ to A_2. An easy induction now shows that, for each prime p, the correspondence

$$\{x,y\} \mapsto (x,y)_2 \oplus (x,y)_3 \oplus \ldots \oplus (x,y)_p$$

maps the group L_p isomorphically onto the direct sum $A_2 \oplus A_3 \oplus \ldots \oplus A_p$. Taking the direct limit as $p \to \infty$, the Theorem follows.

To prove Lemma 11.7, consider the correspondence

$$\phi : (Z/pZ) \to L_p/L_{p-1}$$

defined by the formula

$$x \mapsto \{x,p\} \text{ modulo } L_{p-1} .$$

Here x is to vary over all non-zero integers of absolute value less than p. To show that ϕ is well defined, and a homomorphism, we suppose that

$$xy \equiv z \mod p,$$

where x, y and z are all non-zero integers of absolute value less than p. Then $xy = z+pr$ with $|pr| \leq |xy| + |z| \leq (p-1)^2 + p-1$, hence $|r| < p$. Now

$$1 = z/xy + pr/xy$$

so

$$1 = \{z/xy, pr/xy\} \equiv \{z/xy, p\} \mod L_{p-1}.$$

Therefore

$$\{z,p\} \equiv \{xy,p\} \mod L_{p-1},$$

so that ϕ is a homomorphism, and (taking $y = 1$) ϕ is well defined.

To prove that ϕ is surjective, note that L_p is generated by the symbols $\{x,\pm p\}$, $\{\pm p,x\}$, and $\{\pm p,\pm p\}$, together with L_{p-1}. Hence the identities

$$\{-p,-p\} = \{p,p\} \equiv \phi(-1) \mod L_{p-1},$$
$$\{\pm p,x\}^{-1} = \{x,\pm p\} \equiv \phi(x) \mod L_{p-1},$$

and

$$\{-p,p\} = \{p,-p\} = 1,$$

show that ϕ is indeed surjective. This proves that L_p/L_{p-1} has at most $p-1$ elements. Since we already know, using the symbol $(x,y)_p$, that L_p/L_{p-1} has at least $p-1$ elements, this completes the proof. ∎

Another way of stating our conclusion is the following.

COROLLARY 11.8. *Given any Steinberg symbol* $c(x,y)$ *on the rational numbers, with values in an abelian group* A, *there exist unique homomorphisms*

$$\phi_p : A_p \to A$$

so that

$$c(x,y) = \prod \phi_p((x,y)_p),$$

the product being taken over all prime numbers p.

In this formulation, the result could have been proved directly, without ever mentioning K_2.

To illustrate this corollary, consider the local symbol $(x,y)_\infty$, defined by

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

which is associated with the embedding of the rational numbers in the real numbers. (Compare §8.4.) This is the "universal continuous Steinberg symbol" for the archimedean topology of Q. According to 11.8 there must be a relation of the form

$$(x,y)_\infty = \prod \phi_p((x,y)_p).$$

In fact one has the following.

QUADRATIC RECIPROCITY LAW. *The symbol* $(x,y)_\infty$ *is equal to the product, over all primes* p, *of* $((x,y))_p$, *where the Hilbert symbol* $((x,y))_p = \pm 1$ *is defined to be* $(x,y)_2$ *if* $p = 2$ *and is defined by the condition*

$$((x,y))_p \equiv (x,y)_p{}^{(p-1)/2} \mod p$$

if p *is odd.*

Proof. It is clear from the Corollary that there exists some relation of the form

$$(x,y)_\infty = \prod ((x,y))_p{}^{\varepsilon_p},$$

where the exponents $\varepsilon_2, \varepsilon_3, \varepsilon_5, \ldots$ must be either 0 or 1. Taking $x = y = -1$ we see that the exponent ε_2 must be 1. If p is a prime of the form $8k\pm3$, then since

$$(2,p)_\infty = 1, \quad (2,p)_2 = -1,$$

we must have

$$(2,p))_p{}^{\varepsilon_p} = -1,$$

so that ε_p cannot be zero. Similarly, if p is a prime of the form $8k+7$ (or $8k+3$), then the equations

$$(-1,p)_\infty = 1 \qquad (-1,p)_2 = -1$$

imply that ε_p cannot be zero.

There remains only the case of a prime of the form $8k+1$. Following Gauss we prove the following.

LEMMA 11.9. *If* p *is a prime of the form* $8k+1$, *then there exists a prime* $q < \sqrt{p}$ *so that* p *is not a quadratic residue modulo* q.

(Examples such as $109 \equiv 2^2 \mod 3{\cdot}5{\cdot}7$ show that the hypothesis $p \equiv 1 \mod 8$ is essential, at least for small values of p.)

Proof (following Tate). Consider the product

$$N = \frac{p-1^2}{4} \cdot \frac{p-3^2}{4} \cdot \frac{p-5^2}{4} \cdot \ldots \cdot \frac{p-m^2}{4}.$$

Here m should be the largest odd number less than $\sqrt{p}$, so that $m^2 < p < (m+2)^2$. Then for each factor $(p-i^2)/4$ of the product N we have

$$0 < \frac{p-i^2}{4} < \frac{(m+2)^2-i^2}{4} = \frac{m+2+i}{2} \cdot \frac{m+2-i}{2}.$$

Taking the product, for $i = 1,3,5,\ldots,m$, this yields

$$0 < N < (m+1)!\ .$$

Now suppose that p is a quadratic residue modulo every prime less than $\sqrt{p}$. Then we will prove that

$$N \equiv 0 \mod (m+1)!\ ,$$

thus yielding a contradiction. We will use the notation $[\xi]$ for the largest integer $\leq \xi$.

First note, following Gauss, that in order to prove a congruence of the form $a_1 a_2 \ldots a_k \equiv 0 \mod n!$ it suffices to prove, for each prime power $q^s \leq n$, that at least $[n/q^s]$ of the factors a_j are divisible by q^s. The congruence then follows easily, using the identity $n! = \prod_{q^s \leq n} q^{[n/q^s]}$.

Thus in our case, for each prime power $q^s \leq m+1$, we must prove that at least $[(m+1)/q^s]$ of the numbers $(p-i^2)/4$ are divisible by q^s. In other words we must show that the congruence

$$p \equiv i^2 \mod 4q^s$$

has at least $[(m+1)/q_s]$ solutions in the interval $0 < i < m+1$.

First we will show that p is indeed a quadratic residue modulo $4q^s$. Since $p \equiv 1 \mod 8$, it is known that p is a quadratic residue modulo any power of 2. So it suffices to consider the case q odd, hence $q^s \neq m+1$.

Then

$$q \leq q^s \leq m < \sqrt{p},$$

so p is a residue modulo q; and it follows easily that p is a residue modulo $4q^s$.

Thus the congruence $p \equiv i^2 \mod 4q^s$ has at least one solution i. Now, changing the sign of i if necessary, and adding a multiple of $2q^s$, we obtain a solution i_0 which lies in the interval $0 < i_0 < q^s$. (This is possible since $(i+2q^s)^2 \equiv i^2 \mod 4q^s$.) Similarly we obtain a solution $2q^s - i_0$ lying between q^s and $2q^s$, a solution $i_0 + 2q^s$ between $2q^s$ and $3q^s$, and so on. Thus, for each positive n, there exist at least $[n/q^s]$ solutions between 0 and n. Taking $n = m+1$, this completes the proof of Lemma 11.9. ■

The proof of the quadratic reciprocity law, following Gauss and Tate, can now be completed as follows. Suppose that p is a non-residue modulo q, where $q < p$ and $p \equiv 1 \mod 8$. We may suppose inductively that the exponent ε_q equals 1. Then $(p,q)_\infty = ((p,q))_2 = 1$ but $((p,q))_q = -1$. So it follows that $((p,q))_p^{\varepsilon_p} = -1$, and hence that $\varepsilon_p \neq 0$. This completes the proof. ■

Remark. Let F(x) denote the field of rational functions

$$f = (a_0x^n + \ldots + a_n)/(b_0x^m + \ldots + b_m)$$

in one variable over F. It will be convenient to set

$$\deg f = n-m, \quad \text{lead coef } f = a_0/b_0.$$

The technique used above to compute K_2Q can also be applied to $K_2F(x)$, and yields a split exact sequence

$$1 \to K_2F \to K_2F(x) \to \bigoplus (F[x]/\mathfrak{p})^\bullet \to 1,$$

where $\mathfrak{p}$ ranges over all non-zero prime ideals in the polynomial ring. (To prove that the sequence splits one uses a symbol such as $c(f,g) = \{\text{lead coef } f, \text{lead coef } g\}$ with values in K_2F.)

Just as in the rational number case, the proof is based on the symbols $(f,g)_\mathfrak{p}$ associated with the various $\mathfrak{p}$-adic valuations on F(x). And just as in the rational case, one valuation is conspicuously absent from the list. In this case it is the valuation

$$v_\infty(f) = -\deg(f)$$

associated with the point at infinity. Hence, just as before, we can derive a formula which expresses the corresponding Steinberg symbol

$$(f,g)_\infty = (-1)^{\deg f \deg g}(\text{lead coef } g)^{\deg f}/(\text{lead coef } f)^{\deg g}$$

in terms of the $(f,g)_\mathfrak{p}$. The appropriate formula, due to Weil, is

$$(f,g)_\infty^{-1} = \prod \text{norm } (f,g)_\mathfrak{p},$$

taking the product over all non-zero prime ideals $\mathfrak{p}$, and using the norm homomorphism from $(F[x]/\mathfrak{p})^\bullet$ to $F^\bullet$. (Compare Bass, *Algebraic K-Theory*, p. 333.) If f and g are relatively prime polynomials, then the right side of this equation can be written as

$$\prod_{g(\xi)=0} f(\xi) / \prod_{f(\eta)=0} g(\eta),$$

where ξ and η range over the algebraic closure of F, and n-fold zeros are to be counted n times.

Uncountable Fields

To conclude this section we will give one more application of Lemma 11.5.

THEOREM 11.10. *If a field F has uncountably many elements, then K_2F is uncountable also.*

Proof. Let $\Pi \subset F$ be the prime field, and let $X = \{x_\alpha\}$ be a maximal set of algebraically independent elements over Π. Thus F is an algebraic extension of the uncountable function field $\Pi(X)$. Choosing one of the indeterminates $x_0 \in X$ and letting $X' = X - \{x_0\}$, we obtain a discrete valuation on $\Pi(X)$, with residue class field $\Pi(X')$, by considering the place $f(x_0) \mapsto f(0)$. (Here we are thinking of $f(x_0)$ as a polynomial in the indeterminate x_0 with coefficients in $\Pi(X')$.) Extend this place to a place on F with values in the algebraic closure of $\Pi(X')$. (Compare

Lang, *Introduction to Algebraic Geometry*, p. 8.) Then for every finite extension E of $\Pi(X)$ within F we obtain a discrete valuation on E whose residue class field $\bar{E}$ is a finite extension of $\Pi(X')$. Map K_2E to $\bar{E}^{\bullet}$ by 11.5. If E_1 is an extension field of E with ramification index r, then it is easily verified that the following diagram is commutative,

$$\begin{array}{ccc} K_2E & \longrightarrow & K_2E_1 \\ \downarrow & & \downarrow \\ \bar{E}^{\bullet} & \xrightarrow{r} & \bar{E}_1^{\bullet} \end{array}$$

where r denotes the homomorphism $e \mapsto e^r$. In order to make this bottom homomorphism injective, we will divide out by the countable subgroup consisting of all roots of unity in $\bar{E}^{\bullet}$. Thus we obtain

$$\begin{array}{ccc} K_2E & \longrightarrow & K_2E_1 \\ \downarrow & & \downarrow \\ \bar{E}^{\bullet}/(\text{roots of unity}) & \rightarrow & \bar{E}_1^{\bullet}/(\text{roots of unity}), \end{array}$$

where the bottom arrow is now an injection.

Passing to the direct limit as E varies over all finite extensions of $\Pi(X)$ in F, we thus obtain a homomorphism from K_2F onto a direct limit group which contains $\bar{E}^{\bullet}$/(roots of unity) for all such E. This proves that the group K_2F is necessarily uncountable. ∎

§12. Proof of Matsumoto's Theorem

Let c be a Steinberg symbol on the field F with values in a multiplicative abelian group A. (Compare §11.3.) We will use c to construct a central extension

$$1 \to A \to G \to SL(n,F) \to 1.$$

Here n could be any positive integer, but for convenience we assume that $n \geq 3$. The extension will be constructed first over the subgroup D of diagonal matrices, then over the larger group M of monomial matrices, and finally over the entire group $SL(n,F)$.

To construct the preliminary extension

$$1 \to A \to H \to D \to 1,$$

let H be the set $D \times A$ with the following product operation. If $d = \mathrm{diag}(u_1,\ldots,u_n)$ and $d' = \mathrm{diag}(v_1,\ldots,v_n)$ then

$$(d,a)\,(d',a') = (dd', aa' \prod_{i \geq j} c(u_i,v_j)).$$

It is easily verified that this product is associative, and hence makes H into a group. Let

$$\phi : H \to D$$

be the projection to the first factor. Thus ϕ is a homomorphism with kernel $I \times A$ contained in the center of H. We will identify this kernel with A. Commutators in H can be computed just as in §8.3:

Lemma 12.1. *If* $\phi(h) = \mathrm{diag}(u_1,\ldots,u_n)$ *and* $\phi(k) = \mathrm{diag}(v_1,\ldots,v_n)$, *then* $hkh^{-1}k^{-1}$ *is equal to the product*

$$c(u_1,v_1)\, c(u_2,v_2) \ldots c(u_n,v_n).$$

Proof. This follows easily, using the skew-symmetry of c and the equation $u_1 \ldots u_n = v_1 \ldots v_n = 1$. ∎