Carbondale, April 1980.
Lecture Notes 848 (1981),
in Math 110-124

SIMPLE LIE GROUPS AND THE LEGENDRE SYMBOL

V.G. Kac
Math. Dept. MIT, Cambridge MA 02139

§0. In [6] Serre asks the following question. Let C be a subgroup of $E_8(\mathbb{Q})$ of order 31. Is it true that C acts on each fundamental module of E_8 by a multiple of the regular representation? Same question with $(E_8,31)$ replaced by $(E_7,19)$ and $(F_4,13)$.

In these notes I show that the answer is "yes" for $(E_8,31)$, $(F_4,13)$ and $(G_2,7)$, and "almost yes" for $(E_7,19)$ and $(E_6,13)$ (the answer is "no" only for the fundamental representations of E_6 and E_7 of minimal dimension).

The proof is very simple and goes as follows. Let G be a complex simple connected simply connected Lie group, and let h be the Coxeter number of G (recall that h = 6,12,12,18 and 30 for G_2,F_4,E_6,E_7 and E_8, respectively). Then G has a unique,up to conjugation,regular element of order h+1, which we denote by σ_M. It is easy to see that in the case when h+1 is a prime number, Serre's question is equivalent to whether it is true that $\mathrm{tr}_F(\sigma_M) = 0$ in any fundamental module F of G. We write down a product formula for $\mathrm{tr}_F(\sigma_M)$ in any irreducible G-module F and show that

(1) $$\mathrm{tr}_F(\sigma_M) = 0 \text{ or } \pm 1.$$

This together with the remark that

(2) $$\mathrm{tr}_F(\sigma_M) \equiv \dim F \bmod (h+1),$$

whenever h+1 is a prime number, gives an effective way of computing the $\mathrm{tr}_F(\sigma_M)$.

Remark that by the way we obtain the following curious statement:

(3) $\dim F \equiv 0 \text{ or } \pm 1 \bmod (h+1)$ for any irreducible module F, provided that h+1 is a prime number.

A statement similar to (1) has been proved by Kostant [4] for the "principal" element and the "principal element of type ρ", which we denote by σ_K and σ'_K, respectively (see subsection 3 for their definition). Our method gives a simpler proof of these statements as well.

Let F be an irreducible G-module. Denote

$$\left(\frac{F}{G}\right) := \mathrm{tr}_F\, \sigma_M. \tag{4}$$

We call the number $\left(\frac{F}{G}\right)$ the Legendre symbol of the G-module F. The name is justified by the following formula which easily follows from (2):

$$\left(\frac{F_{(a-1)\rho}}{SL_{p-1}}\right) = \left(\frac{a}{p}\right). \tag{5}$$

Here p is an odd prime, F_λ denotes the irreducible SL_{p-1}-module with highest weight λ, ρ is the half-sum of positive roots, and $\left(\frac{a}{p}\right)$ denotes the ordinary Legendre symbol ($\left(\frac{a}{p}\right) = 0$, 1 or -1 according as $p|a$, $p\nmid a$ and a is or is not a square mod p, respectively; e.g., see [7]).

We shall see that the numbers $\mathrm{tr}_F\sigma_K$, $\mathrm{tr}_F\sigma'_K$ and also $\mathrm{tr}_F\nu$ (see §5) are also related to the Legendre symbol, and that Eisenstein's proof of the quadratic reciprocity law is nothing else but an exercise in the Weyl character formula.

§1. In this section we expose the classification of the elements of finite order of the adjoint group $\bar{G}$ of the group G and discuss some important examples.

Let $\mathfrak{g}$ be the Lie algebra of the group G, $(\ ,\ )$ the Killing form, $\mathfrak{h}$ a Cartan subalgebra, $\Delta \subset \mathfrak{h}^*$ the root system, W the Weyl group, $\Delta_+ \subset \Delta$ a subsystem of positive roots, $\Pi = \{\alpha_1,\dots,\alpha_\ell\}$ the system of simple roots. For $\alpha \in \Delta$ we denote by $\alpha^\vee \in \mathfrak{h}^*$ the dual root, i.e., $\alpha^\vee = \frac{2\alpha}{(\alpha,\alpha)}$. We denote by $\Delta_+^\vee$ the set of positive dual roots. Let $\alpha_0 = -\sum_{i=1}^{\ell} a_i\alpha_i$ be the lowest root, so that setting $a_0 = 1$, we have:

$$\sum_{i=0}^{\ell} a_i\alpha_i = 0, \tag{6}$$

where a_i's are positive integers. One also has:

$$\sum_{i=0}^{\ell} a_i^\vee\alpha_i^\vee = 0, \tag{7}$$

where $a_i^\vee$ are positive integers and $a_0^\vee = 1$.

We fix some non-zero root vectors $E_0,\dots,E_\ell$, corresponding to the roots $\alpha_0,\alpha_1,\dots,\alpha_\ell$. Consider a sequence of non-negative, relatively prime integers $\bar{s} = (s_0,s_1,\dots,s_\ell)$. Set $m = \sum_{i=0}^{\ell} s_i a_i$. Then there exists a unique element $\sigma[\bar{s}] \in \bar{G}$, of order m defined by:

$$\sigma[\bar{s}]E_k = (\exp 2\pi i s_k/m)E_k\ , \quad k = 0,1,\dots,\ell. \tag{8}$$

Proposition 1.[1] Any element $\sigma \in \bar{G}$ of finite order m is a conjugate of an element $\sigma[\bar{s}]$. Two elements $\sigma[\bar{s}_1]$ and $\sigma[\bar{s}_2]$ are conjugate in $\bar{G}$ if and only if $\bar{s}_1$ can be transformed to $\bar{s}_2$ by an automorphism of the extended Dynkin diagram preserving the orientation.[1)]

For the element $\sigma \in \bar{G}$ of finite order its conjugate element of the form $\sigma[\bar{s}]$ is called a canonical form of the element σ.

---

1) In [1] this is stated in a slightly different form (up to conjugation in Aut $\mathfrak{g}$).

Examples. 1) Let $\bar{s} = (1,1,\ldots,1)$; we denote $\sigma[\bar{s}]$ by $\bar{\sigma}_K$. This is Kostant's principal element [4] of $\bar{G}_1$. Its order is the Coxeter number h.

2) Let $\mathcal{J}$ be one of the Lie algebras B_ℓ, C_ℓ, F_4 and G_2 and set d = 2,2,2 and 3, respectively. Set $\bar{s} = (s_0,\ldots,s_\ell)$, where $s_k = 1$ if α_k is a short root and $s_k = d$ if α_k is a long root. We denote $\sigma[\bar{s}]$ by $\bar{\sigma}'_K$. This is Kostant's principal element of type ρ [4] of $\bar{G}$. Its order is dg, where

$$g := (\alpha_0,\alpha_0)^{-1} = 1 + \sum_{i=1}^{\ell} a_i^\vee. \tag{9}$$

3) Let $\bar{s} = (2,1,\ldots,1)$; we denote $\sigma[\bar{s}]$ by $\bar{\sigma}_M$. The order of this element is h+1. This element appears in the paper by Macdonald [5].

From Proposition 1 and the fact that $\sigma(\bar{s})$ is regular if and only if all $s_i > 0$ we obtain:

Corollary. a) [2] The conjugacy class of $\bar{\sigma}_K$ contains all regular elements of order h in $\bar{G}$. All elements of order < h are not regular.

b) [2] The conjugacy class of $\bar{\sigma}_M$ contains all regular elements of order h+1 in $\bar{G}$.

c) The conjugacy class of $\bar{\sigma}'_K$ contains all regular elements σ of order dg in $\bar{G}$ such that σ^g centralizes the connected simple subgroup of $\bar{G}$, whose root system is the system of long roots in Δ.

§2. In this section we define the action of the affine Weyl group in terms convenient for us and prove the first lemma.

Let $\omega_0,\dots,\omega_\ell$ be the standard basis of the lattice $\Gamma := \mathbb{Z}^{\ell+1}$. Define $\bar{\alpha}_0^\vee,\dots,\bar{\alpha}_\ell^\vee \in \Gamma$ by

$$\bar{\alpha}_j^\vee = ((\alpha_0,\alpha_j^\vee),\dots,(\alpha_\ell,\alpha_j^\vee)).$$

Define <u>fundamental reflections</u> r_i, $i = 0,\dots,\ell$, by:

$$r_i(\omega_j) = \omega_j - \delta_{ij}\bar{\alpha}_i^\vee, \quad j = 0,\dots,\ell.$$

The group of automorphisms of Γ generated by all fundamental reflections is denoted by $\hat{W}$. Clearly, the subgroup W of $\hat{W}$ generated by $r_1,\dots,r_\ell$ is isomorphic to the Weyl group of G. For an integer m set: $\Gamma_m := \{\bar{s} \in \Gamma \mid \sum_{i=0} a_i s_i = m\}$. Introduce also translations t_i, $i = 1,\dots,\ell$, by

$$t_i(\bar{s}) := \bar{s} + m\bar{\alpha}_i^\vee, \quad \bar{s} \in \bar{\Gamma}_m.$$

<u>Proposition</u> 2. a) Γ_m <u>is</u> $\hat{W}$<u>-invariant.</u>

b) <u>Any</u> $\hat{W}$<u>-orbit in</u> Γ_m <u>for</u> $m > 0$ <u>contains a unique element</u> $\bar{s}$ <u>with non-negative coordinates.</u>

c) <u>The group</u> $\hat{W}$ <u>is a semidirect product of the subgroup</u> W <u>and the normal free abelian subgroup</u> T <u>of rank</u> ℓ <u>generated by</u> t_i, $i = 1,\dots,\ell$.

<u>Proof</u> is left to the reader (cf. e.g. [3]).

<u>Corollary.</u> <u>Let</u> $\bar{s} \in \Gamma_m$ <u>be a sequence of relatively prime integers, and let</u> σ <u>denote the corresponding element of</u> $\bar{G}$ <u>defined by</u> (8). <u>Let</u> $\bar{s}_1$ <u>be the element in</u> $\hat{W}_a(\bar{s})$ <u>with non-negative coordinates. Then</u> $\sigma[\bar{s}_1]$ <u>is a canonical form of</u> σ.

<u>Let</u> $\rho \in \mathfrak{f}^*$ <u>(respectively,</u> ρ'<u>) denote the half sum of the roots</u> $\alpha \in \Delta_+$ <u>(respectively dual roots</u> $\alpha^\vee \in \Delta_+$.)

<u>Lemma</u> 1. a) <u>Let</u> $r = 0$ <u>or</u> 1 <u>and let</u> h <u>be the Coxeter number of</u> G. <u>Let</u> $\lambda \in \mathfrak{f}^*$

be such that $(\lambda,\alpha^\vee) \in \mathbb{Z}$ and $(\lambda,\alpha) \not\equiv 0 \bmod (h+r)$ for all $\alpha \in \Delta$. Then the set

$$S_\lambda := \{(\lambda,\alpha) \bmod (h+r),\ \alpha \in \Delta\}$$

coincides with the set $S_{\rho'}$.

b) Let $\lambda \in \mathfrak{f}^*$ be such that $(\lambda,\alpha) \in dg(\alpha,\alpha)\mathbb{Z}$ and $(\lambda,\alpha) \not\equiv 0 \bmod dg$ for all $\alpha \in \Delta$. Then the set

$$S'_\lambda := \{(\lambda,\alpha) \bmod dg,\ \alpha \in \Delta\}$$

coincides with the set $S'_{2dg\rho}$.

Proof. (cf. [4]). We shall prove a); the proof of b) is the same. To any $\lambda \in \mathfrak{f}^*$ such that $(\lambda,\alpha) \in \mathbb{Z}$, $\alpha \in \Delta$, we associate $\overline{\lambda} = (s_0,s_1,\ldots,s_\ell) \in \Gamma_{h+r}$ setting $s_i = (\lambda,\alpha_i)$ for $i = 1,\ldots,\ell$, and $s_0 = (h+r) - \sum_{i=1}^{\ell} a_i s_i$. By Proposition 2c) it is clear that $S_\lambda = S_{w(\lambda)}$ for w from the affine Weyl group. By Proposition 2c) and a), $w_0(\overline{\lambda})$ has positive coordinates for some $w_0 \in \hat{W}$ and lie in Γ_{h+r}. But $\sum_{i=0}^{\ell} a_i = h$, hence, if $r = 0$, the only possibility is that $w_0(\overline{\lambda}) = \overline{\rho}'$, which proves the lemma in this case. If $r = 1$, there are several possibilities for $w_0(\overline{\lambda})$, but all of them are equivalent by an automorphism of the extended Dynkin diagram (since all α_i for which $a_i = 1$, are equivalent to α_0). Hence again we obtain that $S_\lambda = S_{\rho'}$.

§3. In this section we consider the notion of a rational element of the group G and discuss some important examples.

We will view G as the group of complex points of the connected simply connected algebraic group $\underline{G}$ defined over $\mathbb{Q}$. An element $x \in \underline{G}(\mathbb{Q}) \subset G$ is called rational. An element $x \in \underline{G}$ is called conjugate-rational if its orbit is defined over $\mathbb{Q}$.

From the results of [8] one deduces:

Proposition 3. An orbit of a conjugate-rational regular element $x \in G$ contains a rational element.

Identifying $\mathfrak{g}$ with $\mathfrak{g}^*$ by the Killing form, we have: $\rho, \rho' \in \mathfrak{g}$. We introduce the following elements in the group G:

$$\sigma_K = \exp \frac{2\pi i}{h} \rho' \quad [4];$$

$$\sigma_K' = \exp 4\pi i \rho \quad [4];$$

$$\sigma_M = \exp \frac{2\pi i}{h+1} \rho' .$$

One has the following characterisation of their conjugacy classes.

Proposition 4. a) The conjugacy class of σ_K (resp. $\sigma_{K'}$) is precisely the pre-image of the conjugacy class $\bar{\sigma}_K \in \bar{G}$ (resp. $\bar{\sigma}_K'$).

b) The conjugacy class of σ_M is precisely the set of all regular elements in G of order h+1.

Proof. For a) see [4]. To prove b) recall that all regular elements in $\bar{G}$ of order h+1 are conjugate (Corollary b) of Proposition 1). But since the order of the centre of G and h+1 are relatively prime, each such element of $\bar{G}$ has a unique pre-image in G of order h+1, which proves b).

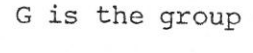
Proposition 4 together with Proposition 3 imply:

Lemma 2. There exists a rational element in G, which is a conjugate of σ_K (σ'_K, σ_M, respectively).

Proof. The orbit of σ_K (or σ'_K or σ_M) is invariant with respect to the action of the Galois group, since these orbits are defined in group-theoretical terms (by Proposition 4). Hence this orbit is defined over $\mathbb{Q}$ and we apply Proposition 3.

An element $x \in G$ is called quasirational[2] if the characteristic polynomial of Adx has rational coefficients. It is clear that a conjugate rational element is quasirational.

The following example has been computed together with B.G. Katz.

Example. G is the group of type G_2. Its extended Dynkin diagram is 

, where the labels are a_0, a_1, a_2. This group has 12 conjugacy classes of conjugate-rational elements $\sigma[\bar{s}_1], \ldots, \sigma[\bar{s}_{12}]$ and 10 conjugacy classes of quasirational elements, which are not conjugate-rational $\sigma[\bar{s}_{13}], \ldots, \sigma[\bar{s}_{22}]$ and form 5 conjugate by the Galois group pairs. Here is the complete list of all 22 quasirational elements of G_2.

No.	Order	$\bar{s}=(s_0,s_1,s_2)$	No.	Order	$\bar{s}=(s_0,s_1,s_2)$	
1	1	1,0,0	13	8	5,0,1	$\sigma[\bar{s}_{13}]^{-1} \sim \sigma[\bar{s}_{14}]$
2	2	0,1,0	14	8	0,1,2	
3	3	1,1,0	15	8	3,1,1	$\sigma[\bar{s}_{15}]^{5} \sim \sigma[\bar{s}_{16}]$
4	3	0,0,1	16	8	1,2,1	
5	4	2,1,0	17	13	1,3,2	$\sigma[\bar{s}_{18}]^{2} \sim \sigma[\bar{s}_{17}]$
6	4	1,0,1	18	13	6,2,1	
7	6	1,1,1	19	24	4,1,6	$\sigma[\bar{s}_{20}]^{7} \sim \sigma[\bar{s}_{19}]$
8	6	4,1,0	20	24	13,4,1	
9	6	3,0,1	21	24	7,1,5	$\sigma[\bar{s}_{21}]^{5} \sim \sigma[\bar{s}_{22}]$
10	7	2,1,1	22	24	11,5,1	
11	12	1,4,1				
12	12	3,3,1				

Note that $\sigma_K = \sigma[\bar{s}_7]$, $\sigma'_K = \sigma[\bar{s}_{12}]$, $\sigma_M = \sigma[\bar{s}_{10}]$.

---

[2] In [2] these elements are called rational.

In general, there is only a finite number of conjugacy classes of quasirational elements in G. Indeed, if $\bar{\sigma} \in \bar{G}$ is a quasirational element of order $m = p_1^{\alpha_1} \ldots p_n^{\alpha_n}$, then, clearly, $p_i^{\alpha_i} - p_i^{\alpha_i - 1} \leq \dim G - \ell$. Together with B. Katz we have found canonical forms of all of them in F_4 and E_6.

§4. In this subsection we prove product formulae for the traces of some elements of the group G.

For a non-negative integer r set

$$\theta_r = \exp \frac{2\pi i}{h+r} \rho'.$$

Recall that $\theta_0 = \sigma_K$, $\theta_1 = \sigma_M$. Remark also that θ_r is a regular element.

Lemma 3. Let F_λ denote an irreducible finite-dimensional G-module with highest weight λ. Then one has:

$$\text{(10)} \qquad \operatorname{tr}_{F_\lambda} \theta_r = \prod_{\alpha \in \Delta_+^\vee} \frac{\sin \pi(\lambda+\rho,\alpha)/h+r}{\sin \pi(\rho,\alpha)/h+r}$$

$$\text{(11)} \qquad \operatorname{tr}_{F_\lambda} \sigma_K' = \prod_{\alpha \in \Delta_+} \frac{\sin 2\pi(\lambda+\rho,\alpha)}{\sin 2\pi(\rho,\alpha)}$$

Proof. We shall prove (10); the proof of (11) is similar. Recall the Weyl character formula. For $\mu, \mu' \in \mathfrak{f} = \mathfrak{f}^*$ set

$$A_\mu(\mu') = \sum_{w \in W} (\det w) \exp 2\pi i(w(\mu),\mu').$$

Then clearly:

$$\text{(12)} \qquad A_\mu(\mu') = A_{\mu'}(\mu) \quad .$$

The Weyl character formula is:

$$\operatorname{tr}_{F_\lambda} \exp 2\pi i\mu = A_{\lambda+\rho}(\mu)/A_\rho(\mu).$$

If $\exp 2\pi i\mu$ is regular, then $A_\rho(\mu) \neq 0$, which is clear from the Weyl denominator identity:

$$\text{(13)} \qquad A_\rho(\mu) = \prod_{\alpha \in \Delta_+} (2i) \sin \pi(\mu,\alpha).$$

For the dual root system identity (13) is:

$$A_{\rho'}(\mu) = \prod_{\alpha\in\Delta_+^\vee} 2i \sin \pi(\mu,\alpha) \tag{14}$$

Now we have:

$$A_\mu(\frac{\rho'}{h+r}) = A_{\frac{\mu}{h+r}}(\rho') = (\text{by (12)}) = A_{\rho'}(\frac{\mu}{h+r}) = (\text{by (14)})$$

$$= \prod_{\alpha\in\Delta_+^\vee} (2i) \sin \frac{\pi(\mu,\alpha)}{h+r},$$

which by the Weyl character formula gives (10).

Remark. Let ℓ be a positive odd integer, and x a real number. Then from (10) we obtain (cf. [7]):

$$\mathrm{tr}_{F_{(\ell-1)\rho}}(\exp 2\pi i\, x\, \rho') = (-4)^{1/4(\ell-1)\#\Delta_+} \prod_{\alpha\in\Delta_+} \prod_{j=1}^{\frac{1}{2}(\ell-1)} (\sin^2\pi(\rho_1\alpha)x - \sin^2\frac{2\pi j}{\ell})$$

In particular, for $G = SL_m$, m odd, one has:

$$\mathrm{tr}_{F_{(\ell-1)\rho}}(\exp 2\pi i\, x\, \rho') = (-4)^{1/4(\ell-1)(m-1)} \prod_{k=1}^{m-1} \prod_{j=1}^{\frac{1}{2}(\ell-1)} \left(\sin^2\pi kx - \sin^2\frac{2\pi j}{\ell}\right)^{m-k}. \tag{15}$$

§5. Now we can prove the central result of the notes.

Theorem 1. Let G be a complex connected simply connected simple Lie group, and let h be the Coxeter number. Let F_λ be an irreducible finite-dimensional G-module.

a) All regular elements of G of order h+1 form a single non-empty conjugacy class M. For $\sigma \in M$ one has:

$$\mathrm{tr}_{F_\lambda} \sigma = 0 \text{ or } \pm 1 \tag{16}$$

for any irreducible finite-dimensional G-module F_λ.

b) [4] Property (16) holds for the elements

$$\sigma_K = \exp \frac{2\pi i}{h} \rho' \text{ and } \sigma_K' = \exp 4\pi i \rho.$$

c) Suppose that h+1 is a prime number. Then for $\sigma \in M$ one has:

$$\dim F_\lambda \equiv \mathrm{tr}_{F_\lambda} \sigma \bmod (h+1) .$$

d) For the element σ_K of $G = SL_p$, p being a prime, one has:

$$\dim F_\lambda \equiv \mathrm{tr}_{F_\lambda} \sigma_K \bmod p.$$

Proof. To prove (16) we use formula (10) for r = 1. If $(\lambda+\rho,\alpha) \equiv 0 \bmod h+1$, then $\mathrm{tr}_{F_\lambda} \theta_r = 0$. Otherwise we apply Lemma 1a) where r = 1, λ is replaced by $\lambda+\rho$ and Δ is replaced by $\Delta^\vee$. It follows that up to a sign, the numerator of (10) is equal to the denominator, proving (16). This together with Proposition 4b) gives a). The proof of b) is similar.

To prove c) we consider G as the group of complex points in the algebraic group $\underline{G}$ defined over $\mathbb{Q}$. Then, by Lemma 2, there exists a regular element $x \in G(\mathbb{Q})$ of order

h+1. Let C be the cyclic group generated by x. Since, the G-module F_λ is defined over $\mathbb{Q}$, it follows that as a C-module, F_λ is a direct sum of its irreducible representations defined over $\mathbb{Q}$. But a cyclic group C of prime order h+1 has only two irreducible representations over $\mathbb{Q}$ -- the trivial 1-dimensional and the h-dimensional -- and their direct sum is the regular representation of C. Also tr x = 0 in the regular representation for any $x \in C$, $x \neq 1$. c) now follows. The proof of d) is similar.

Corollary 1. Let G be of one of the types G_2, F_4, E_6, E_7 and E_8 and let p = 7,13,13,19 and 31, respectively. Then for any irreducible G-module F_λ one has:

$$\dim F \equiv 0 \text{ or } \pm 1 \bmod p.$$

Corollary 2. If h+1 is a prime number, then for any irreducible G-module, the multiplicities of all eigenvalues $\neq 1$ of the element σ_M are equal, say, to n; the multiplicity of 1 is n or $n \pm 1$.

Remark. Since $h+1 \mid \dim G$, it follows from Theorem 1, that the multiplicities of all eigenvalues of σ_M in the adjoint representation are equal, provided that h+1 is a prime. It is also clear from (10) that always $\operatorname{tr} \mathrm{Ad}\sigma_M = 0$. It happens that the preceding statement holds when h+1 is not a prime as well (see [5]).

Corollary 3. For an odd m and an integer a and $G = SL_m$ one has:

$$\operatorname{tr}_{F_{(a-1)\rho}} \sigma_K = \left(\frac{a}{m}\right) = \prod_{j=1}^{(m-1)/2} \left(\sin \frac{2\pi ja}{m} / \sin \frac{2\pi j}{m}\right) .$$

Proof. By the Weyl formula,

$$\dim F_{n\rho} = (n+1)^{\#\Delta_+} .$$

Hence, for $G = SL_m$,

$$\dim F_{(a-1)\rho} = a^{1/2m(m-1)}$$

and the corollary follows from theorem 1d) and formula (10), provided that m is a prime. The general case is left to the reader.

Remark. Formula (15) together with Corollary 3 give that for odd m and ℓ one has:

$$(17) \qquad \left(\frac{\ell}{m}\right) = (-4)^{1/4(\ell-1)(m-1)} \prod_{j=1}^{\frac{\ell-1}{2}} \prod_{k=1}^{\frac{m-1}{2}} \left(\sin^2 \frac{2\pi k}{m} - \sin^2 \frac{2\pi j}{\ell}\right) ;$$

and we obtain as a consequence the quadratic reciprocity law:

$$\left(\frac{\ell}{m}\right) = \left(\frac{m}{\ell}\right)(-1)^{(\ell-1)(m-1)/4} \quad \text{for any odd integers } m \text{ and } \ell.$$

Formula (17) was found by Eisenstein in 1845 (cf [7]).

Remark. The symbol $\left(\frac{a}{b}\right)$ used above for any pair of odd integers a and b is the so-called quadratic symbol, which is 0 if $(a,b) \neq 1$ and expressed by bimultiplicativity in terms of the Legendre symbol if $(a,b) = 1$. Note that

$$\left(\frac{F_{(a-1)\rho}}{SL_2}\right) = (-1)^{1/2(a-1)} \quad \text{if } a \text{ is odd and } = 0 \text{ otherwise.}$$

Hence, it is natural to define

$$\left(\frac{a}{2}\right) := \begin{cases} (-1)^{1/2(a-1)} & \text{if } a \text{ is odd} \\ 0 & \text{otherwise} \end{cases} .$$

Now we can define $\left(\frac{a}{b}\right)$, for any pair of integers a and b, as = 0 if $(a,b) \neq 1$, and by bimultiplicativity otherwise. One can show that Corollary 2 holds for any pair (a,b).

Remark. It is also easy to show that (see the introduction):

$$\left(\frac{F_{(a-1)\rho}}{A_{n-2}}\right) = \left(\frac{a}{n}\right) ; \qquad \left(\frac{F_{\lambda_n}}{B_n}\right) = \left(\frac{2}{2n+1}\right) .$$

Proposition 5. Let h+1 be a prime number, let λ_i be a fundamental weight of G, and let $a_i^\vee > 1$. Then

$$\mathrm{tr}_{F_{\lambda_i}} \sigma_M = 0.$$

Proof follows easily from (10).

Definition. We call an element $\nu \in G$ fundamental if

$$\mathrm{tr}_F \nu = 0 \text{ in any fundamental module } F.$$

It is clear that all fundamental elements form a unique conjugacy class in G.

Proposition 6. a) σ_M is a fundamental element for C_2, F_4 and E_8.

b) σ_K is a fundamental element for A_ℓ and σ_K' for C_ℓ.

c) For the classical simple groups the fundamental element is defined by its characteristic polynomial in the natural representation, which is given by the following

TABLE

G	ℓ	$\det(1 - \lambda\nu)$	G	ℓ	$\det(1 - \lambda\nu)$
A_ℓ	even	$1 - \lambda^{\ell+1}$	D_ℓ	even	$(1 - \lambda^\ell)^2$
A_ℓ	odd	$1 + \lambda^{\ell+1}$	D_ℓ	odd	$(1 + \lambda^\ell)^2$
B_ℓ	even	$(1 - \lambda^\ell)(1 + \lambda^{\ell+1})$	C_ℓ	any	$\dfrac{1 + \lambda^{2\ell+2}}{1 - \lambda^2}$
B_ℓ	odd	$(1 + \lambda^\ell)(1 - \lambda^{\ell+1})$			

Proof. a) follows from Proposition 5. The proof of b) is similar. c) can be checked directly. The answer for B_λ has been given to me by R. Stanley.

Proposition 7. Let C be a subgroup of $G(\phi)$ of order h+1 and let h+1 be a prime number. Then C acts on each irreducible G-module as a multiple of the regular representation plus ε times of the trivial representation, where $\varepsilon = 0$ or ± 1. For each fundamental G-module, where $G = G_2$, F_4 or E_8, $\varepsilon = 0$.

Proof follows from Theorem 1, Proposition 5 and the fact that each $x \in C$, $x \neq 1$, is regular [6].

The following statement and its proof has been communicated to me by R. Stanley.

Proposition 8. Let d be a divisor of n, and let $x \in SL_n$ have the characteristic polynomial $(1 \mp \lambda^n)/(1 \mp \lambda^d)$, where we take - or + according as n is even or odd, respectively. Then $tr_F x = 0$ or ± 1 in any irreducible SL_n-module F.

Proof follows from the Jacobi-Trudi identity (see, for example, [9]) and the following theorem from the matrix theory: If all the entries of a matrix A are 0 or 1 and for any pair of 1's in a row, such that there are no 1's between them, the number of 0's is a fixed number, then det A = 0 or ± 1.

Problem 1. Find all the elements of finite order in G such that their trace is 0 or ± 1 in any irreducible module (such an element is clearly conjugate-rational). Is it true that for $G = SL_n$ the answer is given by Proposition 8?

Problem 2. Find a "reciprocity law" for the Legendre symbol $\left(\frac{F}{G}\right)$, generalizing the classical quadratic reciprocity law.

Problem 3. Find an explicit expression for $tr_F\sigma$ for $\sigma = \sigma_K$, σ_M, σ_K', ν.

Problem 4. Is it true that for a fundamental element ν one has $tr_F\nu = 0$ or ± 1 in any irreducible module F? (By Proposition 6 it is true for G of type A_n, C_n, G_2, F_4 and E_8).

Problem 5. Find the fundamental element for G of type E_6 and E_7.

I would like to thank B. Kostant, G. Lusztig, J.-P. Serre and R. Stanley for stimulating discussions of the questions considered in these notes.

REFERENCES

1. S. Helgason, Differential Geometry, Lie Groups and Symmetric Spaces, Chapter 10, §5, Academic Press, 1978.)
2. V.G. Kac, Infinite-dimensional algebras ... and the very strange formula, Advances in Math., 30(1978), 85-136.
3. V.G. Kac, D.H. Peterson, Infinite-dimensional Lie algebras, classical theta functions and modular forms, to appear.
4. B. Kostant, On Macdonald's η-function formula ..., Advances in Math. 20(1976), 179-212.
5. I.G. Macdonald, Affine root systems and Dedekind's η-function, Invent. Math. 15(1972), 91-143.
6. J.-P. Serre, Arithmetic Groups, in Homological Group Theory, London Math. Soc. 36(1979), Cambridge University Press, Cambridge, England.
7. J.-P. Serre, "Cours d'arithmetique", Paris, 1970.
8. R. Steinberg, Regular elements of semisimple algebraic groups, Publ. Math. IHES No. 25(1965), 281-312.
9. R.P. Stanley, Theory and application of plane partitions I, Stud. in Appl. Math. L,2, 167-188.