A VARIANT OF MOORE'S UNIQUENESS OF RECIPROCITY LAWS

B. SURY

Abstract. In the case of F-isotropic groups for a global field F, Moore [Mo] computed the metaplectic kernel using crucially his theorem of uniqueness of reciprocity laws. For F-anisotropic G, a variant of Moore's theorem is, therefore, needed to compute the metaplectic kernel. Such a variant was announced by G. Prasad [GP1] (in 1986) and here we give the details.

Introduction. Let G be an absolutely simple, simply-connected algebraic group over a global field F. For any finite set S of places of F, it is of interest to compute the relative fundamental group of the S-adele group of G with respect to $G(F)$. Indeed, if S contains all the archimedean places of F and if

$$S\text{-rank of }(G) = \sum_{v \in S} F_v\text{-rank }(G) \geqslant 2,$$

this computation along with the normal subgroup structure of $G(F)$ gives the computation of the congruence subgroup kernel ([P-R]). In the case of F-isotropic groups, Moore [Mo] computed this relative fundamental group (or, equivalently, its Pontryagin dual 'the metaplectic kernel') using crucially his theorem of uniqueness of reciprocity laws. For F-anisotropic G, a variant of Moore's theorem is, therefore, needed to compute the metaplectic kernel. In fact, this variant enables us to compute the metaplectic kernel for anisotropic groups of type A_n, which is used, in turn, to compute the metaplectic kernel for any F-anisotropic G. The details of the computation of the metaplectic kernel will be published elsewhere. The appropriate variant of Moore's Theorem was announced in [GP1]. Here, we give the details of that announcement. We adopt the same method adopted by Chase and Waterhouse in [C-W], where they gave an elegant proof of Moore's theorem. In [R], A. S. Rapinchuk has computed the metaplectic kernel for anisotropic G for some S though not quite singling out a result like this variant of Moore's uniqueness theorem. Our format is as follows. We formulate the variant of the uniqueness theorem as the exactness of a particular sequence involving the elements of norm 1 from a cyclic extension of global fields. The formulations also vary according to the parity of the extension degree. In Section 2, we give the proof when the cyclic extension is of odd degree. Sections 3 and 4 contain the formulations and the proofs for extensions of even degree which are nonquadratic and quadratic, respectively. The proofs will be first given for number fields and in the last section, the modifications necessary for the same proofs to work in positive characteristics, will be pointed out.

Notations. F is a Global field, $\mathscr{F}/F$ is a cyclic extension of degree n, $\Gamma = \mathrm{Gal}\,(\mathscr{F}/F)$, σ is a generator of Γ, N is the Norm map from $\mathscr{F}$ to F, p is a rational prime fixed once for all, $\mathscr{F}^1 = \{x \in \mathscr{F} : N(X) = 1\}$, $\mu(\mathscr{F})_p$, is the p-primary part of the group of roots of unity in $\mathscr{F}$. For a non-archimedean place v of $\mathscr{F}$, let p_v denote the residue field characteristic of $\mathscr{F}_v$ and $\mathcal{O}_v$ denote the ring of integers in $\mathscr{F}_v$.

Further let $\mu = \text{Card. } \mu(\mathscr{F})_p$ and $\mu_v = \text{Card. } \mu(\mathscr{F}_v)_p$ for all places v of $\mathscr{F}$. The μ_v-th power norm residue symbol is denoted by $(\ ,\ )_v$. The symbol is called wild or tame according as $p_v = p$ or not. Finally, we let $\tilde{\Sigma}$ denote the set of all places of $\mathscr{F}$, Σ denote the subset of noncomplex ones, and Σ_f the subset of nonarchimedean places.

§1. *Remarks on symbols.*

1. For each place v of $\mathscr{F}$, the field automorphism $\sigma : (\mathscr{F}, |\ \ |_v) \to (\mathscr{F}, |\ \ |_{\sigma, v})$ is continuous, and hence extends to a topological field isomorphism from $\mathscr{F}_v$ to $\mathscr{F}_{\sigma \cdot v}$; we denote this again by σ. Moreover,

$$\mathrm{Ord}_{\sigma \cdot v}\,(\sigma x) = \mathrm{Ord}_v\,(x) \qquad \text{for all} \qquad x \in \mathscr{F}_v.$$

2. For any finite set S of places of $\mathscr{F}$, the diagonal embedding

$$\mathscr{F} \xrightarrow{\text{diag.}} \bigoplus_{v \in S} \mathscr{F}_v$$

has dense image. In particular, if v is a place of $\mathscr{F}$ and

$$\Gamma \cdot v = \{v, \sigma \cdot v, \ldots, \sigma^{d-1} \cdot v\}$$

then the composite embedding

$$\alpha_v : \mathscr{F} \longrightarrow \bigoplus \mathscr{F}_{\sigma^i \cdot v} \longrightarrow \bigoplus_{d \text{ copies}} \mathscr{F}_v$$

$$x \longmapsto \text{diag. } (x) \longmapsto (x, \sigma^{-1} x, \sigma^{-2} x, \ldots, \sigma^{-(d-1)} x)$$

has dense image. We note that d divides n; indeed the decomposition group at v is the cyclic group $\langle \sigma^d \rangle$ generated by σ^d.

3. By Hilbert's Theorem 90, we have $\mathscr{F}^1 = \{x\sigma(x)^{-1} : x \in \mathscr{F}^*\}$. If v is an inert place *i.e.* $\Gamma \cdot v = v$, then $\mathscr{F}^1$ is dense in $\mathscr{F}_v^1$. If v is such that $\Gamma \cdot v \neq v$, then there exists d dividing n such that $\Gamma \cdot v = \{v, \sigma \cdot v, \ldots, \sigma^{d-1} \cdot v\}$ and $d \geqslant 2$.

We consider, as before, the embedding

$$\alpha_v : \mathscr{F} \longrightarrow \bigoplus \mathscr{F}_v,$$

$$x \longmapsto (x, \sigma^{-1} x, \ldots, \sigma^{-(d-1)} x).$$

Here, and henceforth, we write $\bigoplus \mathscr{F}_v$ for $\bigoplus_{d \text{ copies}} \mathscr{F}_v$. Since the image is dense, for arbitrary $x_0, x_1, \ldots, x_{d-1} \in \mathscr{F}_v$ we can find $x \in \mathscr{F}$ such that $\sigma^{-i} x \sim x_i$ for $0 \leqslant i \leqslant d-1$ in $\mathscr{F}_v$. We have written $\sim$ to mean that the elements are as near as we want them to be with respect to the topology of $\mathscr{F}_v$. Therefore, $\alpha_v(\sigma x)=(\sigma x, x, \ldots, \sigma^{-(d-2)}x)\sim(\sigma^d x_{d-1}, x_0, \ldots, x_{d-2})$ in $\bigoplus_{d \text{ copies}} \mathscr{F}_v$. Hence, we note

$$\alpha_v(x\sigma(x)^{-1})\sim(x_0\sigma^d(x_{d-1}^{-1}), x_1x_0^{-1}, \ldots, x_{d-1}x_{d-2}^{-1}).$$

It is trivial to check that

$$N_v(x_0\sigma^d(x_{d-1}^{-1})x_1x_0^{-1}\ldots x_{d-1}x_{d-2}^{-1})=1.$$

Here, N_v stands for the norm on $\mathscr{F}_v$. Conversely, it is easy to see that any $(y_0, \ldots, y_{d-1})$ in $\bigoplus \mathscr{F}_v$ satisfying $N_v(y_0\ldots y_{d-1})=1$, is of the form

$$(x_0\sigma^d(x_{d-1}^{-1}), \ldots, x_{d-1}x_{d-2}^{-1}).$$

Thus $\alpha_v(\mathscr{F}^1)$ is dense in

$$\{(y_0, \ldots, y_{d-1}): N_v(y_0\ldots y_{d-1})=1\}.$$

This can be thought of as the weak approximation property for the anisotropic F-torus $\mathscr{F}^1$.

4. For a place of $\mathscr{F}$, we denote by $\mu(\mathscr{F}_v)_p^1$ the subgroup of $\mu(\mathscr{F}_v)_p$ generated by $\{(x, y)_v : x, y\in\mathscr{F}^1\}$.

(a) If $\Gamma\cdot v\neq v$ (which is so for infinitely many v by Cebotarev density theorem), then by Remark 3, $\mathscr{F}^1$ is dense $\mathscr{F}_v$ and so $\mu(\mathscr{F}_v)_p^1=\mu(\mathscr{F}_v)_p$.

(b) If $\Gamma\cdot v=v$ and v is non-archimedean and $p_v=p$, it follows from the main theorem in [GP 2] and from the density of $\mathscr{F}^1$ in $\mathscr{F}_v^1$ that, if $\mu(\mathscr{F}_v)_p\neq\{1\}$ and either p or n is different from 2, then again $\mu(\mathscr{F}_v)_p^1=\mu(\mathscr{F}_v)_p$.

(c) If $\Gamma\cdot v=v$, v is non-archimedean and $p_v\neq p$, then $(\ ,\ )_v$ is tame, and since $\mathscr{F}^1\subset\mathscr{O}_v^*$, the symbol is trivial on $\mathscr{F}^1\times\mathscr{F}^1$ and hence $\mu(\mathscr{F}_v)_p^1=\{1\}$.

5. If $(\ ,\ )_v$ is tame, then $(a, b)_v$ is the unique element of $\mathscr{F}_v$ which is congruent, modulo the maximal ideal to

$$(-1)^{\mathrm{Ord}_v a\, \mathrm{Ord}_v b}a^{\mathrm{Ord}_v b}b^{-\mathrm{Ord}_v a}.$$

Thus, if $\mathrm{Ord}_v a=0$ and $\mathrm{Ord}_v b=\mathrm{Ord}_v c$, then $(a, b)_v=(a, c)_v$.

6. Given $x, y\in\mathscr{F}^1$, for almost all v, $(x, y)_v=1$. Thus, we have a homomorphism

$$\phi: \mathscr{F}^1\otimes_{\mathbf{Z}}\mathscr{F}^1\longrightarrow\bigoplus_{v\in\Sigma}\mu(\mathscr{F}_v)_p^1.$$

On the other hand, if $\rho_v\in\mu(\mathscr{F}_v)$, then $\rho_v^{\mu_v/\mu}\in\mu(\mathscr{F})$. So, we have a homomorphism

$$\psi: \bigoplus_{v\in\Sigma}\mu(\mathscr{F}_v)_p^1\longrightarrow\mu(\mathscr{F})_p$$

which is surjective, since, for some (in fact, infinitely many) v, $\mu(\mathscr{F}_v)_p^1=\mu(\mathscr{F}_v)_p$.

With these remarks we can state the main results. We first consider odd degree extensions in the next section.

§2. *Odd degree extensions.*

THEOREM 1. *If $n=|\mathscr{F}:F|$ is odd, then*

$$\mathscr{F}^1 \underset{Z}{\otimes} \mathscr{F}^1 \xrightarrow{\phi} \bigoplus_{v\in\Sigma} \mu(\mathscr{F}_v)_p^1 \xrightarrow{\psi} \mu(\mathscr{F})_p \to 1$$

is exact.

Proof. We shall give the proof when Char $(F)=0$ and in the last section give the necessary modifications for positive characteristic. We have already remarked that ψ is surjective, and since Artin's reciprocity law implies that $\psi \circ \phi$ is trivial, we have to prove only the assertion Ker $(\psi) \subset$ Im (ϕ). We first observe that for any finite set S of noncomplex places of $\mathscr{F}$, the homomorphism $\mathscr{F}^1 \otimes_Z \mathscr{F}^1 \to \bigoplus_{v\in S} \mu(F_v)_p^1$ is surjective. For this, it is enough to show that for any v in S and any ρ_v in $\mu(\mathscr{F}_v)_p^1$, there exists $x_v, y_v \in \mathscr{F}^1$ such that $(x_v, y_v)_v = \rho_v$ and $(x_v, y_v)_w = 1$ for w in S, $w \neq v$. Consider any v in S. We may assume that $\rho_v \neq 1$.

Case I. $\Gamma v = v$. Then, by Remark 4, the symbol $(x, y)_v$ is necessarily wild. By weak approximation for $\mathscr{F}^1$, we can choose $x, y \in \mathscr{F}^1$ such that $x \sim x_v$, $y \sim y_v$ in $\mathscr{F}_v$ and $x, y \sim 1$ in $\mathscr{F}_w$ for all $w \in S \setminus \{v\}$.

Case II. $\Gamma \cdot v = \{v, \sigma\cdot v, \ldots, \sigma^{d-1}\cdot v\} \neq v$. We note that d divides n and is, therefore, odd. We choose $x_v, y_v \in \mathscr{F}_v$ such that $(x_v, y_v)_v = \rho_v$. Let $x \in \mathscr{F}^1$ be so chosen that

$$\alpha_v(x) \sim (x_v, 1, 1, \ldots, x_x^{-1}) \in \bigoplus \mathscr{F}_v.$$

Choose $y \in \mathscr{F}$ be such that $\alpha_v(y) \sim (y_v, 1, \ldots, 1)$. Then, $\alpha_v(y\cdot\sigma(y)^{-1}) \sim (y_v, y_v^{-1}, 1, \ldots, 1)$. Thus, $(x, y\cdot\sigma(y)^{-1})_v = \rho_v$ and $(x, y\cdot\sigma(y)^{-1})_{\sigma^i\cdot v} = 1$ for $i = 1, \ldots, d-1$. In fact, by weak approximation, we can get $x \in \mathscr{F}^1$, $y \in \mathscr{F}$ such that additionally $x, y \sim 1$ in $\mathscr{F}_w$ for all $w \in S \setminus \Gamma\cdot v$. Thus, $x, y\sigma(y)^{-1}$ are elements of $\mathscr{F}^1$ satisfying $(x, y\sigma(v)^{-1})_v = \rho_v$ and $(x, y\sigma(y)^{-1})_w = 1$ for all $w \in S$, $w \neq v$. To continue with the proof of the theorem, consider any $(\rho_v) \in$ Ker (ϕ). We will exhibit a place u and an element (η_v) of $\bigoplus \mu(\mathscr{F}_v)_p^1$ such that

(i) $\eta_v = 1$ for $v \neq u$,
(ii) $(\rho_v) = (\eta_v)$ modulo Im (ϕ);
(iii) $\mu_v = \mu$.

This would prove the theorem since, we would have that $(\eta_v) \in$ Ker (ϕ) and so $\eta_u = 1$ so that $(\rho_v) \in$ Im (ϕ). Consider the field extension $\mathscr{F}(\zeta)$ where ζ is a primitive p^{r+1}-th root of unity where ζ does not belong to $\mathscr{F}$ but $\zeta^p \in \mathscr{F}$. Let $T = \{v: \rho_v \neq 1\}$. We consider the finite set

$$S = \{\text{set of archimedean places}\} \cup \{\text{Primes in } \mathscr{F} \text{ which ramify in } \mathscr{F}(\zeta)\}$$
$$\cup \{\text{Primes in } \mathscr{F} \text{ which divide } p\} \cup \{\text{places } v: (\quad,\quad)_v \text{ is wild}\}.$$

By our observation in the beginning of the proof, if necessary, we change (ρ_v) by an element in Im (ϕ) and assume that $\rho_v = 1$ for v in S. Thus, with this notation, $T \cap S = F$. We will show now that, we can change (ρ_v) by an element of Im (ϕ) and assume that T is equal either to φ or to $\{u, \sigma \cdot u\}$ for some place u of $\mathscr{F}$ such that $\mu_u = \mu$. To do this, we show that any three elements in T can be replaced by two elements of the form $\{v, \sigma \cdot v\}$. Consider any three places $\{v_1, v_2, v_3\} \in T$. We will have three cases to consider according to the way Γ acts on v_1, v_2, v_3.

Case I. $\Gamma v_1, \Gamma v_2, \Gamma v_3$ *are disjoint.* Since v_i are tame, we can choose $x_{v_i}, y_{v_i} \in \mathscr{F}_{v_i}$ of orders 0 and 1, respectively, such that $(x_{v_i}, y_{v_i})_{v_i} = \rho_{v_i}$ for $i = 1, 2, 3$. Writing $\Gamma v_i = \{v_i, \sigma v_i, \dots \sigma^{d_i - 1} v_i\}$ for $i = 1, 2, 3$, we note that d_i are odd integers dividing n. We choose $x \in \mathscr{F}^1$ with $\alpha_{v_i}(x) \sim (x_{v_i}, 1, \dots, x_{v_i}^{-1})$ in $\bigoplus \mathscr{F}_{v_i}$. By Dirichlet's theorem on arithmetic progressions ([B–M–S]), there exists a place u outside $\Gamma \cdot S \cup \Gamma \cdot v_i$ such that if P_v denotes the prime ideal corresponding to a place v, then

$$P_u P_{v_1} P_{v_2} P_{v_3} = (y)$$

with y close to 1 at all those places where x is not a unit as well as at the places in $\Gamma \cdot S$. Then, it can be seen that multiplying (ρ_v) by $\varphi(x \otimes y\sigma(y)^{-1})^{-1}$ replaces v_1, v_2, v_3 in T by $u, \sigma \cdot u$.

Case II. $\Gamma v_1 = \Gamma v_2 \neq \Gamma v_3$, *so that* $v_2 = \sigma^i v_1$ *for some* $1 \leqslant i \leqslant d-1$ *where* $\Gamma \cdot v_1 = \{v_1, \sigma \cdot v_1, \dots \sigma^{d-1} \cdot v_1\}$. We choose $x_{v_i}, y_{v_i} \in \mathscr{F}_{v_i}$ such that $(x_{v_i}, y_{v_i})_{v_i} = \rho_{v_i}$ for $i = 1, 2, 3$ and where the x's have order 0 and y_{v_1}, y_{v_3} have order 1, whereas y_{v_2} is chosen to have order -1. Choose $x \in \mathscr{F}^1$ so that

$$\alpha_{v_1}(x) \sim (x_{v_1}, 1, \dots, \sigma^{-i}(x_{v_2}), 1, \dots, x_{v_1}^{-1}\sigma^{-i}(x_{v_2}^{-1}), 1, \dots, 1)$$

$$\alpha_{v_3}(x) \sim (x_{v_3}, 1, \dots, x_{v_3}^{-1})$$

Again, by Dirichlet's theorem, there exists a prime $u \notin \Gamma \cdot S \cup \Gamma \cdot v_i$ such that

$$P_u P_{v_3} \prod_{0 \leqslant j < i} P_{\sigma^j \cdot v_1} = (y)$$

where $y \sim 1$ at all places in $\Gamma \cdot S$ as well as wherever x is not a unit. Then, once again we can replace v_1, v_2, v_3 in T by $u, \sigma \cdot u$ by changing (ρ_v) by $\varphi(x \otimes y \cdot \sigma(y)^{-1})$.

Case III. $\Gamma v_1 = \Gamma v_2 = \Gamma v_3$. We first consider the case $d \neq 3$ *i.e.* $\Gamma v_1 \neq \{v_1, v_2, v_3\}$. We write $\Gamma v_1 = \{v_1, \sigma v_1, \dots, \sigma^{d-1} v_1\}$, $v_2 = \sigma^i v_1$, $v_3 = \sigma^j v_1$ with $1 \leqslant i < j \leqslant d-1$. Choose x_{v_i}, y_{v_i} in $\mathscr{F}_{v_i}$ of orders 0 and 1 respectively such that $(x_{v_i}, y_{v_i})_{v_i} = \rho_{v_i}$. We take $x \in \mathscr{F}^1$ such that

$$\alpha_{v_1}(x) \sim (x_{v_1}, 1, \dots, \sigma^{-i}(x_{v_2}), 1, \dots, \sigma^{-j}(x_{v_3}),$$
$$1, \dots, x_{v_1}^{-1}\sigma^{-i}(x_{v_2}^{-1})\sigma^{-j}(x_{v_3}^{-1}), 1, \dots, 1).$$

Here the term $x_{v_1}^{-1}\sigma^{-i}(x_{v_2}^{-1})\sigma^{-j}(x_{v_3}^{-1})$ is at the t-th place where t depends only on i and j. We will choose y as before using Dirichlet's theorem. In each case, we just write down the choices and it is straightforward to verify that they satisfy the properties

$$(x, y\sigma(y)^{-1})_{v_i} = \rho_{v_i} \qquad \text{for} \qquad i = 1, 2, 3,$$

$$(x, y\sigma(y)^{-1})_v = 1 \qquad \text{for} \qquad v \neq u, \sigma u, v_1, v_2, v_3.$$

We write down the choice of u and y when $i>1$ (the case $i=1$ is easier). By Dirichlet's theorem, we choose $u\notin\Gamma S\cup\Gamma v_1$ satisfying

$$P_uP_{v_1}^4P_{\sigma^{i-1}\cdot v_1}P_{\sigma^i\cdot v_1}^2P_{\sigma^{i+1}\cdot v_1}^2\dots P_{\sigma^j\cdot v_1}^3\dots P_{\sigma^{d-1}\cdot v_1}^3=(y),$$

unless we have $i+1=j=d-1$, in which case, we choose u such that

$$P_uP_{v_1}^4P_{\sigma^{d-3}\cdot v_1}P_{\sigma^{d-2}\cdot v_1}^2P_{\sigma^{d-1}\cdot v_1}^3=(y),$$

where $y\sim 1$ at the places where x is not a unit as well as at the places in $\Gamma\cdot S$.

Finally, when $d=3$ in Case III, we can just ignore v_3 and replace v_1, v_2 in T by w, σw on choosing a prime w not in $\Gamma\cdot S\cup\Gamma\cdot v_1$ with $P_wP_{v_1}=(y)$ *etc.* Then, as in Case II we can replace, w, $\sigma\cdot w$, v_3 by u, $\sigma\cdot u$ for some u.

Thus, we have shown now that any three elements in T can be replaced by two elements of the form u, $\sigma\cdot u$ for some u. If we had at the most 2 places in T to start with, then again, it is easy to see as before that this 'reduction' can be done. We claim we can assume without loss of generality that $\mu_u=\mu$. For this, we choose $x_u, y_u\in\mathcal{F}_u$ and $x_{\sigma\cdot u}, y_{\sigma\cdot u}\in\mathcal{F}_{\sigma\cdot u}$ with $(x_{\sigma^i\cdot u}, y_{\sigma^i\cdot u})_{\sigma^i\cdot u}=\rho_{\sigma^i\cdot u}$ for $i=0$, 1, and the x's have order 0, y_u has order 1 and $y_{\sigma\cdot u}$ has order -1. Also, by Chebotarev's density theorem, we can choose a place v such that $(P_vP_u,\mathcal{F}(\zeta)/\mathcal{F})\neq 1$. We can get $x\in\mathcal{F}^1$ such that $\alpha_u(x)\sim(x_u,\sigma^{-1}(x_{\sigma\cdot u}), x_u^{-1}\sigma^{-1}(x_{\sigma\cdot u}^{-1}), 1,\dots, 1)$ and $x\sim 1$ in $\mathcal{F}_{\gamma\cdot v}$ for all γ in Γ. Again, by Dirichlet's theorem, there exists w not in $\Gamma\cdot S\cup\Gamma\cdot u\cup\Gamma\cdot v$ satisfying $P_wp_uP_v=(y)$ with $y\sim 1$ at all places where x is not a unit. For these last-mentioned places v_0, since $y\sim 1$, therefore $(x, y\sigma(y)^{-1})_{v_0}=1$. Clearly, $(x, y\sigma(y)^{-1})_{\sigma^i\cdot u}=1$ when $i\neq 0$, 1 and equals $\rho_{\sigma^i\cdot u}$ for $i=0$, 1. At any other place v_0 excepting w, $\sigma\cdot w$, the symbol $(x, y\sigma(y)^{-1})_{v_0}=1$. We have hence changed u, $\sigma\cdot u$ to w, $\sigma\cdot w$ where, moreover, we have $\mu_w=\mu$ since $(P_w,\mathcal{F}(\zeta)/\mathcal{F})\neq 1$. Thus, we could have assumed that $T=\{u, \sigma\cdot u\}$ with $\mu_u=\mu$.

Now $\rho_u=\theta\in\mu(\mathcal{F})_p$, $\rho_{\sigma\cdot u}=\theta^{-1}$ and other $\rho_v=1$. We choose a place v outside $\Gamma\cdot S\cup\Gamma\cdot u$ such that $P_vP_u=(y)$ with $y\sim 1$ at all places in S as well as wherever θ is not a unit. Then $(\theta, y)_u=(\theta, y)_v=\theta$ and other $(\theta, y)_w=1$. Thus, by the usual Artin reciprocity (*i.e.* for the field $\mathcal{F}$), we have $\theta\theta^{\mu_v/\mu}=1$, *i.e.* $\theta^2=1$ as $\mu_v=\mu$. Hence, we have that $\mathrm{Ker}(\psi)/\mathrm{Im}(\phi)$ is 2-torsion. So we assume $p=2$. To conclude the proof, we must show that $\rho\in\mathrm{Im}(\phi)$, where $\rho_u=\rho_{\sigma\cdot u}=-1$ and $\rho_v=1$ for $v\neq u$, where u is any non-inert place not in S such that $\mu_v=\mu$.

If there exists an inert place v not in S with $\mu_v=\mu$, then we will have finished. For, we can choose w_0 not in S such that P_{w_0}, $P_vP_u\mathcal{F}(\zeta)/\mathcal{F})\neq 1$. We can also get $x\in\mathcal{F}^1$ with x, $\sigma x\sim 1$ in $\mathcal{F}_{w_0}$ $\alpha_u(x)\sim(-1,-1,1,\dots,1)$ and x is a unit in $\mathcal{F}_v$ which is congruent to -1 modulo the maximal ideal. By Dirichlet's theorem there is a place $w\notin S\cup\Gamma_u\cup\Gamma_v$ such that $P_wP_uP_v=(y)$, with $y\sim 1$ at all places in S as well as at all those places where x is not a unit. Now, $\varphi(x\otimes y)=\xi$ where $\xi_v=\xi_u=-1$ and $\xi_{v_0}=1$ for $v_0\neq v, u$ by Artin's reciprocity, since $\mu_v=\mu_u=\mu_w=\mu$. Similarly, we get $\varphi(x\otimes y\sigma(y)^{-1})=\rho$.

Another situation when we would have finished is when there is a non-inert place $u\notin S$ with $\mu_u\neq\mu$. Therefore, we may assume that $\mu_u=\mu$ (resp. $\neq\mu$) if u is non-inert (resp. inert) (for places $u\notin S$). Note that $\mathcal{F}(\zeta)/\mathcal{F}$ is a quadratic extension. Let u be non-inert and outside S. Choose x in $\mathcal{F}^1$ satisfying

$\alpha_u(x)\sim(-1,-1,1,\ldots,1)$ and get v outside S with $P_vP_u=(y)$ where $y\sim 1$ at S as well as where x is not a unit. Then $\mu_v=\mu$ and so v is non-inert. Moreover, clearly $\varphi(x\otimes y\sigma(y)^{-1})=\xi$ with $\xi_w=-1$ for $w=u$, v, σu, σv and $\xi_w=1$ for other w. Now, we choose v_0 not in S with $(P_{v_0}P_vP_u, \mathscr{F}(\zeta)/\mathscr{F})\neq 1$. Let x_0 in $\mathscr{F}^1$ be so that $\alpha_u(x_0)\sim(-1,-1,1,\ldots,1)$, $\alpha_v(x_0)\sim(-1,1,\ldots,-1)$ and x, $\sigma x\sim 1$ in $\mathscr{F}_{v_0}$. Get $w\notin S$ such that $P_wP_{v_0}P_uP_v=(y_0)$ with $y_0\sim 1$ at S and those places where x_0 is not a unit. Then $\mu_w=\mu$ so that w is non-inert. Also, it is clear that $\xi^{-1}\varphi(x_0\otimes y_0\sigma(y_0)^{-1})=\eta$ where $\eta_{\sigma\cdot w}=\eta_{\sigma\cdot v}=-1$ and $\eta_{w_0}=1$ at other places. We have $\eta\in\operatorname{Im}(\phi)$. We rename $\sigma\cdot w$ and $\sigma\cdot v$ as v_1 and v_2. Get v_3 not in S with $(\prod_{1\leqslant i\leqslant 3}P_{v_i}, \mathscr{F}(\zeta)/\mathscr{F})\neq 1$. Choose x_1 in $\mathscr{F}^1$ with $\alpha_{v_1}(x_1)\sim(-1,1,\ldots,1,-1)$, $\alpha_{v_2}(x_1)\sim(1,-1,\ldots,1,-1)$ and x_1, $\sigma x_1\sim 1$ in $\mathscr{F}_{v_3}$. There is a place u not in S such that $P_u\prod P_{v_i}=(y_1)$ with $y_1\sim 1$ in S and where x is not a unit. Then $\mu_u=\mu$ and so $\eta^{-1}\varphi(x_1\otimes y_1\sigma(y_1)^{-1})=\rho$, where $\rho_w=-1$ for $w=u$, σu and $=1$ for other w. Hence $\rho\in\operatorname{Im}(\phi)$. Of course, we have already seen how to get from this the fact that for any non-inert w not in S, the element θ defined by $\theta_{w_0}=-1$ if $w_0=w$, σw and $=1$ otherwise, is in $\operatorname{Im}(\phi)$. This completes the proof of the theorem.

§3. *Even degree nonquadratic extensions.* When n is even, the image of the map φ (introduced in remark 6 of §) is slightly smaller than in the odd degree case; in fact as we will see, it injects into the following subset Δ of $\bigoplus\mu(\mathscr{F}_v)_p^1$

For a non-complex place v such that $\Gamma\cdot v=\{v, \sigma\cdot v\}$, let μ_v^1 denote the subgroup spanned by $(x, u)_v$ for $x\in\mathscr{F}_v^*$ and $u\in\mathscr{F}_v^1$. Let

$$\Delta=\{(\rho_v)\in\bigoplus\mu(\mathscr{F}_v)_p^1 : \rho_v^{-1}\cdot\sigma^{-1}(\rho_{\sigma\cdot v})\in\mu_v^1 \qquad \text{if} \qquad \Gamma v=\{v, \sigma v\}\}.$$

We note that $\mu_v^1=\mathscr{F}_v^1\cap\mu(\mathscr{F}_v)$, if $p_v\neq p$. To see that $\operatorname{Im}(\phi)\subset\Delta$, consider any $x, y\in\mathscr{F}^1$, and any v with $\Gamma\cdot v=\{v, \sigma\cdot v\}$. Now

$$\sigma^{-1}((x, y)_{\sigma\cdot v})=(\sigma^{-1}x, \sigma^{-1}y)_v=(x^{-1}x\sigma^{-1}x, y^{-1}y\sigma^{-1}y)_v\in(x, y)_v\cdot\mu_v^1$$

by the bimultiplicativity of $(\quad,\quad)_v$ and by the fact that $x\sigma^{-1}x$, $y\sigma^{-1}y\in\mathscr{F}_v^1$ (if we write $x=t/\sigma^{-1}\cdot t$, then $x\cdot\sigma^{-1}x=t/\sigma^{-2}\cdot t\in\mathscr{F}_v^1=\{s/\sigma^{-2}s : s\in\mathscr{F}_v^*\}$) whence

$$(x, y)_v^{-1}\cdot\sigma^{-1}((x, y)_{\sigma\cdot v})\in\mu_v^1.$$

We also notice that in case $n=2$, we have $\mu_v^1=\{1\}$. With this notation, the next result is the following.

THEOREM 2. *If* $|\mathscr{F}:F|=2m>2$, *then we have the exact sequence.*

$$\mathscr{F}^1\otimes_Z\mathscr{F}^1\xrightarrow{\ \phi\ }\Delta\xrightarrow{\ \psi\ }\mu(\mathscr{F})_p\to 1$$

Proof. Once again, we give the proof for number fields and the positive characteristic case is discussed in Section 5. As before $\psi\circ\phi$ is trivial by Artin's reciprocity law. Also, ψ is surjective, since, for some (in fact, infinitely many) v, we have $\Gamma\cdot v\neq\{v, \sigma\cdot v\}$ and $\Gamma\cdot v\neq v$ so that $\mu(\mathscr{F}_v)_p^1=\mu(\mathscr{F}_v)_p$. So, we have to prove only that $\operatorname{Ker}(\psi)\subset\operatorname{Im}(\phi)$. As in the case of odd degree extensions, we first show that for any finite set $S\subset\Sigma$, and $(\rho_v)_{v\in S}$, we can get

$\eta \in \operatorname{Im}(\varphi)$ so that $\eta_v = \rho_v$ for all v in S. If $\Gamma v = v$, or, if $\Gamma v = \{v, \sigma \cdot v, \ldots, \sigma^{d-1} \cdot v\} \neq \{v, \sigma \cdot v\}$, the proof of this fact is exactly the same as the one we gave for odd degree. We have only to consider the case $\Gamma v = \{v, \sigma v\} \neq \{v\}$. Since we have $\rho_v^{-1}\sigma^{-1}(\rho_{\sigma v}) \in \mu_v^1$, we have $\rho_{\sigma \cdot v} = \sigma(\rho_v \eta_v)$ for some η_v in μ_v^1. So there are $a_i \in \mathscr{F}_v^*$ and $b_i \in \mathscr{F}_v^1$ with $\eta_v = \prod_{1 \leqslant i \leqslant r} (a_i, b_i)_v$. We first choose $x_v, y_v \in \mathscr{F}_v^*$ such that $(x_v, y_v)_v = \rho_v$. Let $x_0 \in \mathscr{F}^1$ be so that $\alpha_v(x_0) \sim (x_v, x_v^{-1})$ and $y_0 \in \mathscr{F}$ so that $\alpha_v(y_0) \sim (y_0, 1)$ and also such that $x_0, y_0 \sim 1$ in $\mathscr{F}_w$ for w in $S \backslash \{v, \sigma v\}$. Then, $\alpha_v(y_0 \sigma(y_0)^{-1}) \sim (y_v, y_v^{-1})$. Moreover,

$$(x_0, y_0\sigma(y_0)^{-1})_v = \rho_v,\ (x_0, y_0\sigma(y_0)^{-1})_{\sigma \cdot v} = (\sigma(x_v^{-1}), \sigma(y_v^{-1}))_{\sigma \cdot v}$$
$$= \sigma((x_v^{-1}, y_v^{-1})_v) = \sigma(\rho_v).$$

Now, we choose $x_i, y_i \in \mathscr{F}^1$ such that $\alpha_v(x_i) \sim (a_i^{-1}, a_i)$ and $\alpha_v(y_i) \sim (1, b_i)$. Then, $(x_i, y_i)_v = 1$ and $(x_i, y_i)_{\sigma \cdot v} = \sigma((a_i, b_i)_v)$. Our choice is also so that $x_i, y_i \sim 1$ in $\mathscr{F}_w$ for w in S, $w \neq v, \sigma v$. Hence

$$\phi((x_0 \otimes y_0 \sigma(y_0)^{-1}) . \textstyle\prod_{1 \leqslant i \leqslant r} (x_i \otimes y_i) = \xi$$

satisfies $\xi_v = \rho_v$ and $\xi_{\sigma \cdot w} = \sigma(\rho_v \eta_v) = \rho_{\sigma \cdot v}$, and $\xi_w = 1$ *for all* $w \in \bar{S} \backslash \{v, \sigma \cdot v\}$.

To continue with the proof, we start with any ρ in $\operatorname{Ker}(\psi)$ and letting $T = \{v \colon \rho_v \neq 1\}$, we can assume without loss of generality that $T \cap S = \varnothing$, where S is taken to include the archimedean places, the wild places, the places which ramify in $\mathscr{F}(\zeta)$ and the placed dividing p. We once again show that by changing ρ by an element of $\operatorname{Im}(\phi)$, any three elements $v_1, v_2, v_3 \in T$ can be replaced either by $\varnothing$ or by u, σu for some place u. As before we make three cases:

Case I. Γv_i are disjoint. Let $\Gamma \cdot v_i = \{v_i, \sigma \cdot v_i, \ldots \sigma^{d_i - 1} \cdot v_i\}$. If all $d_i > 2$, then the proof is just as before as in the odd case. Therefore we assume that some $d_i = 2$. We want to change ρ by some ξ in $\operatorname{Im}(\phi)$ so that v_1, v_2, v_3 are replaced by some $u\sigma u$, or by $\varnothing$. We note that we have only to take care that our choice of ξ must satisfy $\xi_{\sigma \cdot v_i} = 1$ if $\rho_{\sigma \cdot v_i} = 1$. Now, if some v_i, say v_1, is so that $\rho_{\sigma \cdot v_1} = 1$, then we have $\rho_{v_1} \in \mu_v^1$ (since $\rho \in \Delta$ means that $\rho_{v_1}^{-1}\sigma^{-1}(\rho_{\sigma \cdot v_1}) \in \mu_v^1$). We choose $x \in \mathscr{F}^1$ such that $\alpha_{v_1}(x) \sim (\rho_{v_1}, 1)$ (this is possible because $\rho_{v_1} \in \mu_v^1 = \mathscr{F}_{v_1}^1 \cap \mu(\mathscr{F}_{v_1})$). Similarly, the behaviours of $\alpha_{v_2}, \alpha_{v_3}$ are assumed to be either as in the odd case or as for v_1. By Dirichlet's theorem, we can choose u to be a place outside $\Gamma \cdot S \cup \Gamma \cdot v$ such that $P_u P_{v_1} P_{v_2} P_{v_3} = (y)$, with $y \sim 1$ at all places in $\Gamma \cdot S$ as well as at those places where x is not a unit. If we multiply ρ by $\xi = \varphi(x \otimes y\sigma(y)^{-1})$, then v_i get replaced in T by u, σu.

Case II. $\Gamma v_1 = \Gamma v_2 \neq \Gamma v_3$. If $\Gamma \cdot v_1 \neq \{v_1, v_2\}$, then we choose $\alpha_{v_1}(x)$, $\alpha_{v_2}(x)$ as in the odd case and $\alpha_{v_3}(x)$ as in Case I above.

If $\Gamma \cdot v_1 = \{v_1, v_2\}$, then we proceed as follows. Now $\rho_{\sigma \cdot v_1} = \sigma(\sigma_{v_1} \eta_{v_1})$ for some $\eta_{v_1} \in \mu_v^1 \cap \mathscr{F}_{v_1}^1$. Let $x_{v_1}, y_{v_1} \in \mathscr{F}_{v_1}$ so that $\operatorname{Ord}_{v_1}(x_{v_1}) = 0$, $\operatorname{Ord}_{v_1}(y_{v_1}) = 1$ and $(x_{v_1}, y_{v_1})_{v_1} = \rho_{v_1}$. We let $x \in \mathscr{F}^1$ with $\alpha_{v_1}(x) \sim (x_{v_1}, x_{v_1}^{-1} \eta_{v_1}^{-1})$ and appropriate $\alpha_{v_3}(x)$. Again, by Dirichlet's theorem we choose a place $u \notin \Gamma \cdot S \cup \Gamma \cdot v_i$ such that $P_u P_{v_1} P_{v_2} = (y)$ with $y \sim 1$ at all places in $\Gamma \cdot S$ as well as wherever x is not a unit. Clearly $\xi = \varphi(x \otimes y\sigma(y)^{-1})$ satisfies the requirements.

Case III. $\Gamma v_1 \supseteq \{v_1, v_2, v_3\}$. As $d_1 = d_2 = d_3 > 2$, the proof is exactly as in the case of odd degree extensions.

To recapitulate, therefore, T can be assumed to be either $\emptyset$ or to be of the form $\{u, \sigma u\}$ with $\mu_u = \mu$. We have to show that $\rho \in \mathrm{Im}(\phi)$ in the latter case. Write $\Gamma \cdot u = \{u\sigma \cdot u, \ldots, \sigma^{d-1} \cdot u\} \neq U$.

We first consider the case $d > 3$. Choose v not in S such that $(P_v P_u P_{\sigma \cdot u} \mathscr{F}(\zeta)/\mathscr{F}) \neq 1$, and $x \in \mathscr{F}^1$ with $\alpha_v(x) \sim (-1, -1, 1, \ldots, 1)$ and $\gamma x \sim 1$ in $\mathscr{F}_v$ for all $\gamma \in \Gamma$. By Dirichlet's theorem, there is $w \notin S$ so that $P_w P_v P_u P_{\sigma \cdot u} = \{y\}$ with $y \sim 1$ at places in S as well as wherever x is not a unit. It is easy to check that $\phi(x \otimes y\sigma^2(y)^{-1}) = \rho$. This proves our assertion for $d > 3$. (Incidentally, the same proof works in the odd degree case, if $d > 3$.)

The cases $d = 2$ or 3 are similar. This completes the proof of Theorem 2.

§4. *Quadratic extensions.* In the case $|\mathscr{F}:F| = 2$, we make a minor correction in the announcement of theorem 2 (ii) in [GP1], and we will formulate the theorem in the following way. We fix a set V of places with $V \cap \sigma \cdot V = \emptyset$ and $V \cup \sigma \cdot v = \Sigma_f$. Let S, as before, contain the set of archimedean places, wild places, places lying above p as well as those ramifying in $\mathscr{F}(\zeta)$.

Let us define

$$\psi' : \Delta \longrightarrow \mu(\mathscr{F})_p \qquad \text{by} \qquad (\rho_v) \longmapsto \prod_{v \in V} \rho_v^{\mu_v/\mu}.$$

and denote by C the set $\{\rho \in \Delta : \rho_v = 1 \text{ for all } v \in S\}$. Then $C\,\mathrm{Im}(\phi) = \Delta$. (This can be seen as follows. As in the case of Card. $\Gamma = 2m > 2$, if $\delta \in \Delta$, we can get $d \in \mathrm{Im}(\phi)$ such that $d_v = \delta_v$ for $v \in S$. Thus, $(d^{-1}\delta)_v = 1$ for all $v \in S$ so that $d^{-1}\delta \in C$.) So ψ' gives rise to a homomorphism from $\Delta/\mathrm{Im}(\phi)$ to $\mu(\mathscr{F})_p/\psi'(C \cap \mathrm{Im}(\phi))$. If we define $\overline{\mu(\mathscr{F})} = \mu(\mathscr{F})_p/\psi'(C \cap \mathrm{Im}(\phi)$, and ε to be the resulting map from Δ to $\overline{\mu(\mathscr{F})}$, which is trivial on $\mathrm{Im}(\phi)$, then the result is

THEOREM 3. *If* $|\mathscr{F}:F| = 2$, then the following sequence is exact.

$$\mathscr{F}^1 \otimes_Z \mathscr{F}^1 \xrightarrow{\varphi} \Delta \xrightarrow{\varepsilon} \overline{\mu(\mathscr{F})} \to 1$$

Proof. We give the proof for number fields. We first note that ε is well defined. From the definition, we have for any $\delta \in \Delta$, $\varepsilon(\delta) = \psi'(c)$ in $\overline{\mu(\mathscr{F})}$ where $\delta = cd$ for some $c \in C$ and $d \in \mathrm{Im}(\phi)$. ε is well defined because if $cd = c_1 d_1$ then $c_1^{-1}c = d_1 d^{-1} \in C \cap \mathrm{Im}(\phi)$. We have, by the definition of ε, that $\varepsilon(\mathrm{Im}(\phi)) = 1$ in $\overline{\mu(\mathscr{F})}$. We hve to show $\mathrm{Ker}(\varepsilon) \subseteq \mathrm{Im}(\phi)$. Just as in the odd degree case, we may assume that, if u is a non-inert tame place, then $\mu_u = \mu$. As before, we see that for any $\rho \in \Delta$ and for any finite set S, there exists $\eta \in \mathrm{Im}(\phi)$ with $\eta_v = \rho_v$ for all $v \in S$. In fact, if $\rho \in C$, then we can choose η to be in C too. We start with any $\rho \in \mathrm{Ker}(\varepsilon)$. Firstly, since $C.\mathrm{Im}(\phi) = \Delta$, we can assume without loss of generality, that $\rho \in \mathrm{Ker}(\varepsilon) \cap C$. Thus, by the above, we have $S \cap T = \varnothing$, where $T = \{v : \rho_v \neq 1\}$. Therefore, by the definition of ε, we have $\psi'(\rho) \in \psi'(C \cap \mathrm{Im}(\phi))$. After changing ρ by an element of $C \cap \mathrm{Im}(\phi)$, we can assume that $\rho \in \mathrm{Ker}(\psi') \cap C$. Denoting again by T the set $\{v : \rho_v \neq 1\}$, we claim that $\rho_v = -1$ for all $v \in T$. Consider any $v \in T$. Now

$\rho_v \in \mu(\mathscr{F})$; let us call it θ for convenience. Choose $w \notin S$ such that $P_w P_v = (y)$ with $y \sim 1$ at all places in S and wherever θ is not a unit. Also $\mu_w = \mu$. Then $\varphi(\theta \otimes y) = \xi$ where $\xi_w = \xi_v = \theta$ and $\xi_u = 1$ at other places. By Artin's reciprocity law, $\theta^2 = 1$ so that $\theta = -1$. Writing $T = \{v_1, v_2, \ldots, v_r, \sigma \cdot v_1 \ldots \sigma \cdot v_r\}$, since $\rho \in \operatorname{Ker} \psi'$, we get $(-1)^r = \psi'(\rho) = 1$, *i.e.* r is even. In this case we have already shown $\rho \in \operatorname{Im}(\phi)$. This completes the proof of the theorem.

§5. *Modifications for positive characteristic.* The proofs of the theorems work also if the characteristic of F is a prime $l > 0$ with minor modifications. The necessary modifications are already given in [C–W]. For the sake of completeness, we just recall them again. In the case when Char $F = l > 0$ all places are tame since clearly $\mu(\mathscr{F}_v)_l = 1$. In this case we take any place v_0 and consider $S = \{v_0\}$. We work inside the ring O_S of S-integers *viz.* $\{x \in \mathscr{F}_{v_0} : \operatorname{Ord}_{v_0}(x) \geqslant 0 \text{ for all } v \neq v_0\}$.

We notice that:

(i) if $\operatorname{Ord}_{v_0}(y)$ is divisible by $|\mathscr{F}(\zeta) : \mathscr{F}|$, then $|y, \mathscr{F}(\zeta)/\mathscr{F}) = 1$; and

(ii) if $\operatorname{Ord}_{v_0}(y)$ is divisible by $\mu_{v_0} . |\mathscr{F}(\zeta) : \mathscr{F}|$, then $(x, y)_{v_0} = 1$.

Every time we apply Dirichlet's theorem, we just make sure that the above two conditions are satisfied by y. We note that y cannot be close to 1 at S and so these modifications are indeed necessary.

Acknowledgements. The results of this paper were announced by G. Prasad in [GP1], whom I thank heartily. Here the details are worked out based on indications of the proofs given by him.

References

B-M-S. H. Bass, J. Milnor and J.-P. Serre. Solution of the congruence subgroup problem for SL(n) and Sp(2n). *Publ. Math. IHES*, (1967), 421–499.

C-W. S. U. Chase and W. Waterhouse: Moore's theorem on uniqueness of reciprocity laws. *Inv. Math.*, 16 (1972), 267–270.

Mo. C. C. Moore. Group extension of p-adic and adelic linear groups. *Publ. Math. IHES*, 35 (1968), 157–222.

GP1. G. Prasad. Une variante du theoreme de Calvin Moore. *C.R. Acad. Sci. Paris*, 302 (1986), 405–408.

GP2. G. Prasad. On the wild norm residue symbol in an abelian extension. *Math. Ann.* 274 (1986), 419–422.

P-R. G. Prasad and M. S. Raghunathan. On the congruence subgroup problem: determination of the 'metaplectic kernel'. *Inv. Math.*, 71 (1983), 21–42.

R. A. S. Rapinchuk. Multiplicative arithmetic of division algebras over number fields and the metaplectic problem. *Math. USSR Izv.*, 31 (1988), 349–379.

Dr. B. Sury,
School of Mathematics,
T.I.F.R.,
HomiBhabha Road,
BOMBAY 400005,
INDIA.

11R99: *NUMBER THEORY; Algebraic number theory, global fields.*

Received on the 21*st of October*, 1992.