united nations
educational, scientific
and cultural
organization

international atomic
energy agency

the
abdus salam
international centre for theoretical physics

SMR1233/3

School on Automorphic Forms on GL(n)

(31 July - 18 August 2000)

Minkovski reduction

M.S. Raghunathan
School of Mathematics
Tata Institute of Fundamental Research
Homi Bhabha Road
Mumbai 400 005
India

Minkowski reduction

1. ~~[illegible]~~

1.1. We denote as usual by $\mathbb{Z}$ (resp. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$) the ring of integers (resp. the field of rational, real, complex numbers). $\mathbb{N}$ will be the natural numbers. ~~[illegible]~~ For a prime $p \in \mathbb{N}$, $\mathbb{Q}_p$ will denote the field of p-adic numbers, $\mathbb{Z}_p$ the ring of p-adic integers and $|\ |_p$ the p-adic ~~valuation~~ (absolute value) on $\mathbb{Q}_p$: For $x \in \mathbb{Q}$ with $x = p^r a/b$ with $r, a, b \in \mathbb{Z}$ ~~[illegible]~~ with p, a and b mutually coprime, $|x|_p = p^{-r}$. Let k be a number field i.e., a finite extension of $\mathbb{Q}$. An absolute value $|\ |_v : k \longrightarrow \mathbb{R}^+ \ (= \{x \in \mathbb{R} \mid x \geq 0)$ on k is canonical iff the following holds: let k_v be the completion of k w.r.t $|\ |_v$ and $\mathbb{Q}_v$ the closure of $\mathbb{Q}$ in k_v so that $\mathbb{Q}_v \simeq \mathbb{R}$ or $\mathbb{Q}_{p_v}$ for some prime $p_v \in \mathbb{N}$ (In the sequel we sometimes $\mathbb{R}$ by $\mathbb{Q}_\infty$); then for $x \in k_v$, $|x|_v = |N_{k_v/\mathbb{Q}_v}(x)|$ where $N_{k_v/\mathbb{Q}_v} : k_v \longrightarrow \mathbb{Q}_v$ is the norm map. We denote by $M = M_k$ the set of all canonical valuations on k. The subset of all archimedean (resp. nonarchimedean) valuations in M

For $v \in M$, k_v is a locally compact field

is denoted ∞ (resp. M_f). For $v \in M_f$, O_v will denote the ring of integers in k_v, $\mathfrak{P}_v$ the unique non-zero prime ideal in O_v and F_v the residue field $O_v/\mathfrak{P}_v$. We denote by p_v the characteristic of the residue field. – one then has $Q_v \cong Q_{p_v}$. Let $M' \subset M$ be any subset and set $_{M'}\mathbb{A}_k = \{ \underline{x} = (x_v)_{v \in M'} \in \prod_{v \in M'} k_v \mid x_v \in O_v$ for all but finitely many v in $M' \}$. Under coordinate wise addition and multiplication $_{M'}\mathbb{A}_k$ is a ring and contains k as a subring through the diagonal inclusion so that it is in fact a k-algebra. $_M\mathbb{A}_k$ carries a natural topology under which it is a locally compact ring. A base for open sets for this topology is given by the following collection $\mathcal{B}$ of subsets. A set in $\mathcal{B}$ is of the form $\Omega \times \prod_{v \in M' \setminus S} O_v$ where S is a finite subset of M' containing $M' \cap \infty$, Ω is an open subset of $\prod_{v \in S} k_v$ for the product topology and $\prod_{v \in S'} k_v \times \prod_{v \in M' \setminus S} O_v$ is identified

with a subset of ${}_{M'}\mathbb{A}_k$ in the natural fashion. (and call it the ring of adeles)
When $M' = M$ we denote ${}_{M'}\mathbb{A}$ by $\mathbb{A}$ and when $M' = M \setminus \infty$, ${}_{M'}\mathbb{A}$ is also denoted $\mathbb{A}_{k,f}$ (and is called the ring of finite adeles. If S is a finite subset of M, (containing ∞) we denote by $\mathbb{A}_{k,S}$ the ring $\{ \underline{x} = (x_v)_{v \in M} \in \mathbb{A}_k \mid x_v \in O_v \text{ for } v \notin S \}$.
Evidently $\mathbb{A}_S$ has a natural identification with

$$\prod_{v \notin S} O_v \times \prod_{v \in S} k_v .$$

It is an algebra over the ring $O_S = \{ x \in k \mid x \in O_v \text{ for } v \notin S \}$ of S-integers in k. In the sequel when the context makes clear what field k we are working with we denote ${}_{M'}\mathbb{A}_k$ by ${}_{M'}\mathbb{A}$.

1.2. Suppose now that X is an affine variety defined over k and $k[X]$ its coordinate ring (over k). — this means that $k[X]$ is a finitely generated k-algebra such that $k[X] \otimes_k \bar{k}$ has no nilpotent elements. As usual we denote by $X({}_{M'}\mathbb{A})$ the ${}_{M'}\mathbb{A}$ points of X: $X({}_{M'}\mathbb{A}) = \mathrm{Hom}_{k\text{-alg}}(k[X], {}_{M'}\mathbb{A})$. This set has a natural locally compact topology deduced from that on $\mathbb{A}$.

This topology can be described as follows. Let

$$\varphi : k[T_1, \ldots, T_r] \longrightarrow k[X]$$

be a surjective homomorphism of a polynomial algebra over k on $k[X]$. Composition with φ gives an injective map

$$X({}_{M'}\mathbb{A}) \longrightarrow \mathrm{Hom}_{k\text{-alg}}(k[T_1, \ldots, T_r], {}_{M'}\mathbb{A}) = ({}_{M'}\mathbb{A})^r$$

The topology on $X_{M'}(\mathbb{A})$ is that induced from this inclusion by the (locally compact) product topology on $({}_{M'}\mathbb{A})^r$ – the topology is independent of the choice of φ. Of particular interest to us are varieties G which are algebraic groups over k. The corresponding adelic groups $G({}_{M'}\mathbb{A})$ are then locally compact groups. The algebraic group of the greatest importance to us is the group $GL(n)$ over k: its coordinate ring is the (quotient of) k-algebra $k[T_{ij}, 1 \le i, j \le n, T]$ (polynomial algebra in (n^2+1) variables (T_{ij} $1 \le i, j \le n$ and T) by the ideal generated by the element $(\det(T_{ij})T-1)$.

Clearly then $GL(n)(_{M'}\mathbb{A}) = GL(n, _{M'}\mathbb{A})$ the group of $(n\times n)$-invertible matrices over $_{M'}\mathbb{A}$ (or equivalently $\{g \in M(n, _{M'}\mathbb{A}) \mid \det g$ is a unit in $_{M'}\mathbb{A}\}$. Note that the (locally compact) topology on $GL(n, _{M'}\mathbb{A}) = GL(n)(_{M'}\mathbb{A})$ is not that induced from $M(n, _{M'}\mathbb{A})$. ~~The topology ...~~ From the definitions one sees easily the following: the underlying set of $GL(n, _{M'}\mathbb{A})$ is

$$\{\underline{x} = (x_v)_{v\in M'} \in \prod_{v\in M'} GL(n, k_v) \mid x_v \in GL(n, O_v) \text{ for all but finitely many } v\}.$$

The topology on $GL(n, _{M'}\mathbb{A})$ is that for which a base for open sets is given by

$$\Omega \times \prod_{v\notin S} GL(n, O_v) = \mathcal{U}, \text{ say}$$

as S varies over finite subsets of M' containing $M'\cap\infty$ and Ω varies over open subsets of $\prod_{v\in S} GL(n, k_v)$ (with the product topology) with $\mathcal{U}$ identified with a subset of $GL(n, _{M'}\mathbb{A})$ in the obvious fashion. Note that as a set $\mathbb{I} = \{\underline{x} = (x_v)_{v\in M} \in \prod_{v\in M} k_v^* \mid x_v \in O_v^*$ for all but finitely many $v\in M\}$ (Here O_v^* = invertible elements in O_v).

1.3 The locally compact group $GL(1, {}_{M'}\mathbb{A})$ will also be denoted ${}_{M'}\mathbb{I}$ in the sequel and ${}_{M}\mathbb{I}$ simply $\mathbb{I}$. It is also called the group of ideles and ${}_{M \setminus \infty}\mathbb{I}$ called the "finite" ideles is also denoted $\mathbb{I}_f$. As already remarked (in case of general n), the inclusion of $\mathbb{I}$ in $\mathbb{A}$ is continuous but the topology induced from $\mathbb{A}$ on $\mathbb{I}$ under this inclusion is weaker than the topology on ideles (described above) that will be used. For a general affine variety ~~the~~ one has a natural inclusion

$$\operatorname{Hom}_{k\text{-alg}}(k[X], {}_{M'}\mathbb{A}) = X(k) \hookrightarrow X({}_{M'}\mathbb{A})$$

hence in particular

$$X(k) \hookrightarrow X(\mathbb{A}).$$

In this last inclusion, $X(k)$ is a closed subset and the induced topology is discrete. Since the topology on $X(\mathbb{A})$ is induced from that on $\mathbb{A}^r$ for a suitable inclusion and $X(k)$ is the inverse image of k^r ($\subset \mathbb{A}^r$) for this inclusion, one is reduced to showing that ~~[illegible]~~ k is a closed subset of $\mathbb{A}$ and the topology induced on k is discrete. Let Ω be an open neighbourhood of 0 in $\prod_{v \in \infty} k_v$ ~~and~~

Consider the open set $\Omega \times \prod_{v \notin \infty} \mathcal{O}_v$ in $\mathbb{A}$. If $x \in k$ belongs to this open set, then x is an integer in O_v for all $v \in M_f$. ie $x \in O$ = ring of integers in the number field. Now $\prod_{v \in \infty} k_v$ is isomorphic (as a locally compact group) to the (finite dimensional) real vector space $k \otimes_{\mathbb{Q}} \mathbb{R}$ and O imbeds in this vector space as the $\mathbb{Z}$-span of a suitable basis of $k \otimes_{\mathbb{Q}} \mathbb{R}$ over $\mathbb{R}$. One sees immediately from this that k is a discrete closed subgroup of $\mathbb{A}$ and in fact more: that $\mathbb{A}/k$ is compact.

It is now clear that for any integer $n > 0$, $GL(n,k)$ is a closed discrete subgroup $GL(n,\mathbb{A})$. The Theory of automorphic forms (seeks to) explore profound connections between (finite dimensional) representation ~~between~~ of the Galois group $Gal(\bar{k}/k)$ ($\bar{k}$ an algebraic closure of k) and harmonic analysis on the homogeneous space $GL(n,\mathbb{A})/GL(n,k)$; and in the case $n=1$, Abelian Class Field Theory is the result.

On the group $\mathbb{I} = GL(1,\mathbb{A})$ there is a natural continuous homomorphism (called the norm) $|\ |: \mathbb{I} \to \mathbb{R}^{\times}$ (into positive real numbers in fact) given by

$$|\underline{x}| = \prod_{v \in M} |x_v|_v \quad \text{where } \underline{x} = (x_v)_{v \in M}.$$

This is well defined since $|x_v|_v = 1$ for all but finitely many $v \in M$ and is easily seen to be continuous. The kernel of this map is denoted $\mathbb{I}^0$. From our definitions of ideles and canonical absolute values, it is easy to prove the

Exercise (Product formula) If $x \in k^*$ (imbedded diagonally in $\mathbb{I}$), $|x| = 1$.

Less obvious is the well known and important ~~lemma~~

Theorem $\mathbb{I}^0/k^*$ is compact.

Exercise Prove the theorem in the case $k = \mathbb{Q}$. We will ~~not~~ prove the general case later ~~but take it as known~~ using the "Minkowski reduction" (See 1.4 below) for the case $k = \mathbb{Q}$

1.4. Our aim in this paragraph is to give a description of a nice "fundamental domain" for $GL(n, k)$ acting on $GL(n, \mathbb{A})$. Towards this end we need to introduce certain subgroups and subsets of $GL(n, A)$ which we will denote simply G. The group $GL(n, k)$ is denoted Γ. Let D be the group of diagonal matrices in $GL(n, A)$. If $\underline{\underline{d}} \in D$, $\underline{d}_i$ will denote its i^{th} diagonal entry which is necessarily an idele. We denote by D^0 the subgroup $\{\underline{d} \in D \mid \underline{d}_i$ is an idele of norm 1 for $1 \le i \le n\}$. Let N be the subgroup of G consisting of upper triangular unipotent matrices in G. For $v \in M_f$, we denote by H_v the compact open subgroup $GL(n, O_v)$: it is a maximal compact subgroup of $GL(n, k_v)$ and every maximal compact subgroup in $GL(n, k_v)$ is conjugate to H_v. If $v \in \infty$, $GL(n, k_v) \simeq GL(n, \mathbb{C})$ or $GL(n, \mathbb{R})$ according as $k_v = \mathbb{C}$ or $\mathbb{R}$, and we take H_v to be the compact subgroup that under this isomorphism maps onto $U(n)$ or $O(n)$ according as $k_v \simeq \mathbb{C}$ or $\mathbb{R}$. The group D normalises N and $D.V$ is the group of all upper triangular matrices which we denote B. We also set $B^0 = D^0.V$. Finally we denote by A the subgroup of D consisting of all diagonal matrices $\underline{\underline{d}} = \text{diagonal}(\underline{d}_1, \underline{d}_2 \cdots \underline{d}_n)$ where each d_i is an idele whose components $\underline{d}_{iv} = 1$ for $v \in M_f$ and $\underline{d}_{iv} \in \mathbb{R} = \bar{Q}_v$ for all $v \in \infty$: this group A is isomorphic to a product of n copies of the multiplicative group of positive real numbers. For a real number $c > 0$, let

$$A_c = \{ \underline{\underline{d}} = \text{diagonal}(\underline{d}_1, \cdots \underline{d}_n) \mid d_i / d_{i+1} < c \text{ for } 1 \leq i < n \}$$

$\bar{A}_c$ is the closure of A_c in A. With this notation the main result is

<u>Theorem</u> (Minkowski reduction). $B^0/B^0 \cap \Gamma$ is compact. There is a constant $c_0 > 0$ with the following property. Let ω be any compact subset of B^0 with $\omega(\Gamma \cap B^0) = B^0$. Then for all $c \geq c_0$, $H \cdot A_c \cdot \omega \cdot \Gamma = G$ where H is the subgroup $\prod_{v \in M} H_v$.
Moreover the set $\{ \gamma \in \Gamma \mid HA_c\omega\gamma \cap HA_c\omega \neq \phi \}$ is finite.

That $B^0/B^0 \cap \Gamma$ is compact follows from §1.3: a simple induction starting with the fact that A/k is compact shows that $N/N \cap \Gamma$ is compact. Combining this with the theorem stated in §1.3, one sees that $B^0/B^0 \cap \Gamma$ is compact. In the sequel we will give a proof of the theorem for $k = Q$.

1.5. We assume now that $k = \mathbb{Q}$. This means that ∞ consists of only one valuation which also we denote by ∞. We will in fact show that in the statement of the theorem (in §1.4) we can take $c_0 = 2/\sqrt{3}$. For the proof we need to introduce the notion of primitive elements in $\mathbb{A}^n$ and their height. We set $V = \mathbb{Q}^n$ and $V(\mathbb{A}) = \mathbb{A}^n$. An element $e \in \mathbb{A}^n$, $e = \sum_{1 \le i \le n} \underline{x}_i e_i$, $\underline{x}_i \in \mathbb{A}$ is primitive if $e = g e'$ $(g \in GL(n, \mathbb{A}))$ with $e' \in V \setminus \{0\}$. If $e_1, \ldots, e_n$ is the standard basis of $\mathbb{A}^n$ (over $\mathbb{A}$), $e \in \mathbb{A}^n$ is primitive iff $e \in GL(n, \mathbb{A}) \cdot e_1$. We denote by $\mathcal{P}$ the set of primitive elements. The following characterisation of primitive elements is easy to prove: $\underline{x} = \sum_{1 \le i \le n} \underline{x}_i e_i$, $\underbrace{\underline{x}_i}_{= (x_{iv})_{v \in M}} \in \mathbb{A}$ is primitive iff the following (two conditions) hold: (i) for any $v \in M$, there is an i with $1 \le i \le n$ such that, $x_{iv} \neq 0$. (ii) there is a finite set S containing ∞ such that for all $v \in S$, $\underline{x}_{iv} \in \mathcal{O}_v$ (for all i) and x_{iv} is a unit in $\mathcal{O}_v$ for some i. We can define the height $h : \mathcal{P} \longrightarrow \mathbb{R}^\times$ as follows: For $e \in k_v^n$, $e = \sum x_i e_i$ $(x_i \in k_v)$, $|e|_v = \max_i |x_i|_v$ if $v \in M_f$

and $= \left(\sum_{1\le i\le n} |x_i|_\infty^2\right)^{1/2}$ if $v = \infty$. If $e \in P$, $e = \sum_{1\le i\le n} x_i e_i$ with $\underline{x}_i \in \mathbb{A}$, let $e_v = \sum_{1\le i\le n} x_{iv} e_i$ and set

$$h(e) = \prod_{v\in M} |e_v|$$

This makes sense since $|e_v| = 1$ for almost all v. The following properties of the height function are left as an exercise to the reader:

(i) If $g \in H$ and $e \in P$, $h(ge) = h(e)$

(ii) If $\underline{x} \in V$, $h(\underline{x}) \geq 1$

(iii) If $\underline{e} \in P$ and $\lambda \in \mathbb{Q}^*$, $h(\lambda \underline{x}) = h(e)$

(iv) If $g \in GL(n, \mathbb{A})$ and $\alpha > 0$, the set ~~[illegible]~~ $\{g\underline{e} \mid e \in V \setminus \{0\}, h(g\underline{e}) \leq \alpha\}$ is finite modulo (multiplication by elements of) k^*

(v) If $x_n \in P$ is sequence then $h(x_n)$ tends to zero if and only if there is a sequence $\lambda_n \in \mathbb{Q}^*$ such that $\lambda_n x_n$ tends to zero in $\mathbb{A}^n$.

With this notion of height, one has the following

~~[illegible]~~ If $g \in GL(n, \mathbb{A})$, one sees from (iv) above that there is an element $e' \neq 0$ in V such that $h(ge') \leq h(ge'')$ for all $e'' \neq 0$ in V. Since $GL(n, \mathbb{Q})$

acts transitively on V, we see that if we set

$$\mathcal{R}_n = \{ g \in GL(n, \mathbb{A}) \mid h(g\gamma e_1) \geq h(ge_1) \text{ for } \gamma \in GL(n,k)\}$$

then $\mathcal{R}_n\, GL(n, \mathbb{Q}) = GL(n, \mathbb{A})$. Suppose now that $g \in \mathcal{R}_n$; then $g = u \cdot a \cdot b$ with $u \in H$, $a \in A$ and $b \in B^0$. Let $g'' = a \cdot b$; then g'' is of the form

$$g'' = \begin{pmatrix} a_1 & * \\ 0 & g' \end{pmatrix}$$

where $g' \in G' = SL(n-1, \mathbb{A})$. Now by induction hypothesis there is a $\gamma' \in SL(n-1, \mathbb{Q})$ such that

$$g'\gamma' = u'\, a'\, b'$$

where $u' \in H \cap GL(n-1, \mathbb{A})$ ($GL(n-1, \mathbb{A})$ is identified with the subgroup $\left\{\begin{pmatrix} 1 & 0 \\ 0 & g' \end{pmatrix} \mid g' \in GL(n-1, \mathbb{A})\right\}$ of $GL(n, \mathbb{A})$), $b' \in B'^0 = B' \cap GL(n-1, \mathbb{A})$ and

$$a' \in A'_c = \{ \operatorname{diag}(a_2 \cdots a_n) \mid a_i \in \mathbb{R}, a_i > 0, a_i/a_{i+1} \leq c\}$$

with $c \geq 2/\sqrt{3}$. Let

$$g_1 = \begin{pmatrix} a_1 & * \\ 0 & g' \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & \gamma' \end{pmatrix} = \begin{pmatrix} a_1 & * \\ 0 & u'a'b' \end{pmatrix}.$$

Since $\begin{pmatrix} 1 & 0 \\ 0 & \gamma' \end{pmatrix}$ leaves e_1 invariant it is clear that $g_1 \in \mathcal{R}_n$. Thus we find that:

$$|a_1| = h(g_1 e_1) \leq h(g_1(e_2 + \lambda e_1)) \text{ for all } \lambda \in k^*$$

Now $g_1 e_2 = a_2 e_2 + \beta e_1$ for some $\beta \in \mathbb{A}$ so that we have

$$|a_1| \leq |a_2 e_2 + a_1(\beta+\lambda)e_1| \qquad *$$

for all $\lambda \in k^*$. We now choose $\lambda \in k$ such that $|\beta+\lambda|_v \leq 1$ for $v \in M_f$ and $|\beta+\lambda|_\infty \leq 1/2$: such a choice is possible as is seen by using the Chinese remainder theorem. ~~but~~ We need to show that $a_1/a_2 = |a_1|/|a_2| \leq 2/\sqrt{3}$. We may assume that $a_1/a_2 \geq 1$; in this case one has for all $v \in M_f$,

$$|a_2 e_2 + a_1(\beta+\lambda)e_1|_v = \max(1, |(\beta+\lambda)_v|_v) = 1$$

so that $*$ implies that (since $|\beta+\lambda|_\infty \leq 1/2$),

$$a_1 = |a_1|_\infty \leq (a_2^2 + 1/4\, a_1^2)^{1/2}$$

leading to $a_1 \leq 2/\sqrt{3} \cdot a_2$. This establishes the theorem in 1.4.

1.6 <u>Theorem</u> (Mahler's criterion). Let g_n be a sequence in $GL(n, \mathbb{A})$ such that there are constants $a', a'' > 0$ such that $a' \leq |\det g_n| \leq a''$. Then $\{g_n\}$ admits no subsequence that converges modulo $GL(n,k)$ if and only if there exists a sequence $\alpha_r \in k^n \setminus \{0\}$ such that $h(g_r(\alpha_r))$ converges to zero.

Proof. Suppose g_r has a subsequence that converges modulo $GL(n,k)$. Replacing the sequence by the subsequence, we assume that there exist $\gamma_r \in GL(n,k)$ such that $g_r\gamma_r$ converges to a limit g in $GL(n,\mathbb{A})$. It follows that $h(g_r(\alpha_r)) = h(g_r\gamma_r(\alpha_r))$ converges to zero. Now if $\Omega \subset GL(n,\mathbb{A})$ is a compact set, one sees easily that there is a constant $c > 0$ such ~~and this~~ that $h(\omega e) \geq c$ for all $e \in k^n \setminus \{0\}$, ~~a contradict~~ contradicting this. Thus g_r cannot ~~be~~ converge modulo $GL(n,k)$. Conversely suppose g_r has no convergent subsequence modulo $GL(n,k)$. Let γ_r in $GL(n,k)$ be so chosen that $g_r\gamma_r \in H\,A_c\,\omega$ ($\omega \subset B^0$ a relatively compact set and $c > 0$ chosen suitably). Let $g_r\gamma_r = u_r \cdot a_r \cdot \omega_r$ with $u_r \in H$, $a_r \in A_c$, $\omega_r \in B^0$. It is easy to see that ~~[illegible]~~ the set $\{a x a^{-1} \mid a \in A_c,\ x \in \omega_r\}$ is relatively compact. Then

$$g_r\gamma_r = \xi_r \cdot a_r$$

with $\xi_r \in \Omega'$ a compact subset of $GL(n,\mathbb{A})$

It follows that a_r must tend to infinity in A.

Now $a_{ir}/a_{i+1,r} \le c$ so that $a_1 \le c^{i-1} a_i$ for $1 \le i \le n$ leading to $a_{1r}^n \le c^{n(n-1)/2} \cdot a_{1r} \cdots a_{nr} \le m$ (a constant depending on a', a'' and Ω). Thus a_r will ~~converge~~ have a convergent subsequence unless a_{1r} tends to zero. But in this case $h(g_r \gamma_r)(e_1) = h(\xi_r a_r e_1)$ $= a_{1r} h(\xi_r e_r)$ tends to zero since ξ_r is in a compact set.

Corollary 1 If k is a number field I^0/k^* is compact.

Proof Consider the isomorphism $k \simeq \mathbb{Q}^n$ $(n=[k:\mathbb{Q}])$ obtained by choosing a basis of k over $\mathbb{Q}$. This induces an isomorphism $\mathbb{A}_k \simeq \mathbb{A}_{\mathbb{Q}}^n$. Left multiplication by elements $\mathbb{I}_k$ are evidently $\mathbb{A}_{\mathbb{Q}}$-linear automorphisms of $\mathbb{A}_k$ (treated as a $\mathbb{A}_{\mathbb{Q}}$-module). We thus obtain an inclusion $\mathbb{I}_k$ in $GL(n, \mathbb{A}_{\mathbb{Q}})$ One checks easily that this is a homeomorphism of $\mathbb{I}_k$ onto the image, a closed subgroup of $GL(n, \mathbb{A}_{\mathbb{Q}})$. The closed subgroup $\mathbb{I}_k^0$ maps into a closed subgroup $GL(n, \mathbb{A}_{\mathbb{Q}})$ all of whose elements have determinants which

are ideles of norm 1 in $\mathbb{I}_Q$. ~~[illegible]~~
We will show that $\mathbb{I}_k$ is relatively compact modulo $GL(n,Q)$ and that on the other hand $\overset{\circ}{\mathbb{I}}_k GL(n,Q)$ is closed in $GL(n,\mathbb{A})$. This will prove that $\overset{\circ}{\mathbb{I}}_k / \overset{\circ}{\mathbb{I}}_k \cap GL(n,Q) = \mathbb{I}_k / k^*$ is compact.
To show that $\overset{\circ}{\mathbb{I}}_k \cdot GL(n,Q)$ is closed in $GL(n,\mathbb{A})$, let $g_\gamma \in \overset{\circ}{\mathbb{I}}_k$ be any sequence such that $g_\gamma \delta_\gamma$ converges in $GL(n,\mathbb{A})$ (to a limit g, say) for some sequence $\delta_\gamma \in GL(n,Q)$.
Now let $\rho \in k^* (\subset GL(n,\mathbb{A}))$. Then one has

$$\delta_\gamma^{-1} g_\gamma^{-1} \rho\, g_\gamma \delta_\gamma = \delta_\gamma^{-1} \rho\, \delta_\gamma ;$$

while the left hand side converges to $g^{-1}\rho g$, the right hand side stays in the discrete group $GL(n,Q)$. Thus for ~~[illegible]~~ some r_0, $\delta_r^{-1} \rho\, \delta_r = \delta_{r_0}^{-1} \rho\, \delta_{r_0}$ so that $g_r \delta_r \delta_{r_0}^{-1}$ converges and $\delta_r \delta_{r_0}^{-1} \in GL(n,Q) \cap (\text{Centraliser } k^*) = k^*$. Now if g_r is any sequence in $\overset{\circ}{\mathbb{I}}_k$ such that g_r tends to ∞ modulo $GL(n,Q)$ we can by Mahler's criterion find ~~[illegible]~~ $e_r \in Q^n \setminus \{0\}$ such that $h(g_r(e_r))$ ~~[illegible]~~ tends to zero. ~~[illegible]~~

Now we assume the identification of k with $\mathbb{Q}^n$ made with the aid of a $\mathbb{Z}$-basis of the ring of integers in k. The determinant on $M(n, \mathbb{Q})$ restricted to $k \simeq \mathbb{Q}^n$ is then the norm on k and is a polynomial of degree n with integral coefficients. It follows from this that for any primitive element $e \in \mathbb{A}^n_{\mathbb{Q}}$, $|\det e| \leq C\,h(e)$. Thus $|\det(g_r e_r)| \leq C\,h(g_r e_r)$ tends to zero. On the other hand $|\det g_r e_r| = |\det g_r||\det e_r|$ and $|\det g_r| = |\det e_r| = 1$, a contradiction.

<u>Corollary 2</u>. Let $\mathfrak{a}$ be an ideal in O. Let $\mathfrak{I}(\mathfrak{a})$ be the group of fractional ideals in k coprime to $\mathfrak{a}$. Let $\mathfrak{P}(\mathfrak{a})$ the subgroup of $\mathfrak{I}(\mathfrak{a})$ generated by principal ideals of the form uO, $u \in k^*$, u an integer in k_v for all $v \in M_f$ such that the prime ideal $(\mathfrak{P}_v)$ corresponding to v divides $\mathfrak{a}$ and $u \equiv 1 \bmod \mathfrak{a}$. Then $\mathfrak{I}(\mathfrak{a})/\mathfrak{P}(\mathfrak{a})$ is finite.

<u>Proof</u>. Let $S' = \{v \in M_f \mid$ the prime ideal of v divides $\mathfrak{a}\}$. Let $\mathfrak{a} = \prod_{v \in S} \mathfrak{P}_v^{\,\delta_v}$ and for $v \in M_f$

let $E_v = \mathcal{O}_v^*$ if $v \notin S'$ and $E_v = \{x \in \mathcal{O}_v^* \mid x \equiv 1 \bmod \mathfrak{p}_v^{R_v}\}$ if $v \in S'$. Then ~~...~~ the group $\mathbb{I}_k / k^* \cdot \prod_{v \in \infty} k_v^* \cdot \prod_{v \in M_f} E_v$ is finite since $\mathbb{I}_k^0 \prod_{v \in \infty} k_v^* = \mathbb{I}_k$ and $\underbrace{k^* \prod_{v \in \infty} k_v^* \prod_{v \in M_f} E_v}_{= \mathbb{J}, \text{ say}}$ is open in $\mathbb{I}_k$. One then sees that $\mathbb{I}_k / \mathbb{J} \simeq \mathcal{I}(\mathfrak{a}) / P(\mathfrak{a})$.

1.7. We will now establish the theorem of §1.4 for all number fields k. The identification of k with $\mathbb{Q}^m$ ($m = k : \mathbb{Q}$) through a basis of k as a vector space yields an inclusion of $GL(n, k)$ in $GL(mn, \mathbb{Q})$ and leads to a realisation of $GL(n, \mathbb{A}_k)$ as a <u>closed</u> subgroup $GL(mn, \mathbb{A}_\mathbb{Q})$. The subgroup can be seen easily to be the subgroup of elements of $GL(mn, \mathbb{A}_\mathbb{Q})$ that commute with all the endomorphisms of $\mathbb{A}_\mathbb{Q}^{mn}$ induced by (left) multiplication by elements of k (treated as endomorphisms of $\mathbb{A}_\mathbb{Q}^{mn}$). Now $\mathbb{A}_k^n \simeq \mathbb{A}_\mathbb{Q}^{mn}$ and under this isomorphism, we claim that primitive elements of $\mathbb{A}_k^n$ map into primitive elements in $\mathbb{A}_\mathbb{Q}^{mn}$ — we may assume that the first basis element of the standard basis of $\mathbb{A}_\mathbb{Q}^{mn}$ coincides with that of $\mathbb{A}_k^n$ and then this becomes obvious. Next we claim that the ~~height~~ if h_k (resp $h_\mathbb{Q}$) is the height of a primitive element $\mathcal{P}_k$ (resp $\mathcal{P}_\mathbb{Q}$) in $\mathbb{A}_k^n$ (resp $\mathbb{A}_\mathbb{Q}^{mn}$) then there is a constant $\beta \geq 1$ such that for all $e \in P_k$, $\beta^{-1} h_{\mathbb{Q}}(e)^m \leq h_k(e) \leq \beta h_{\mathbb{Q}}(e)^m$. This is deduced easily from the fact that the norm map from $\mathbb{A}_k \to \mathbb{A}_{\mathbb{Q}}$ is a polynomial with rational coefficients of degree m. Once this is admitted we will show that the Mahler criterion yields the desired result. by an induction on n. Assume that there is a $c_0 > 0$ such that (for all $c \geq c_0$) $H' \bar{A}'_c \omega' GL(n-1, k) = GL(n-1, \mathbb{A})$ where

$$H' = \prod_{v \in M_k} H'_v \ , \ H'_v \cong GL(n-1, O_v) \text{ if } v \in \mathbb{A}_f \text{ and}$$

H'_v is a maximal compact subgroup of $GL(n-1, k_v)$ for $v \in \infty$. ω' is a ~~subset~~ compact subset $B'^0 = \{ g \in GL(n-1, \mathbb{A}_k) \mid$ g upper triangular and the diagonal entries of g are in $\mathbb{I}_k^0 \}$ and A'_c is the set of diagonal matrices with (diagonal) entries $a_2, \ldots, a_n \in \mathbb{R}^\times$ with (for all i) $a_i > 0$ and $a_i / a_{i+1} \leq c'$ for $2 \leq i < n$. Let $\mathcal{R}_n \subset GL(n, \mathbb{A}_k)$ be the set

$$\{ g \in GL(n, \mathbb{A}_k) \mid h_k(g e_1) \leq h(g \gamma e_1), \gamma \in GL(n, k) \}$$

Let $g \in \mathcal{R}_n$ and $g = u \cdot a \cdot n$ with $u \in H$, $a \in A$ and $n \in \omega$, ω a compact subset of B^0 with $\omega(B^0 \cap \Gamma) = B^0$. Clearly then $a \cdot n \in \mathcal{R}_n$ as well. Now $a \cdot n = \begin{pmatrix} a_1 & * \\ 0 & g''_* \end{pmatrix}$ with $g'' \in GL(n-1, \mathbb{A}_k)$

and we can find θ ~~such that~~ in $GL(n-1, k)$

$$a n \begin{pmatrix} 1 & 0 \\ 0 & \theta \end{pmatrix} = \begin{pmatrix} a_1 & * \\ 0 & g' \end{pmatrix} = g_1, \text{ say with } g' \in H' \bar{A}'_c \omega'$$

for $c \geq c_1$. Evidently $g_1 \in \mathcal{R}_n$. Once again we may write $g_1 = \left(\begin{array}{cc|c} a_1 & * & * \\ 0 & a_2 & \\ \hline & 0 & g_2 \end{array}\right)$ with $g_2 \in GL(n-2, \mathbb{A}_k)$. If we modify g_1 to ρg_1 where ρ is a (positive) scalar matrix (with entries in $\mathbb{R}$). $\rho g_1 \in \mathcal{R}_n$. We chose ρ such that

$$\rho g_1 = \left(\begin{array}{cc|c} a_1 & * & * \\ 0 & a_1^{-1} & \\ \hline & 0 & g_2 \end{array}\right).$$

Note that this does not disturb the ratios of the diagonal entries so that if we set

$$g^* = \rho g_1 = u \cdot a \cdot b$$

with $u \in H$, $a \in A$ and $b \in B^0$, $a_i/a_{i+1} \leq c$ for $2 \leq i < n$. We need only show now that $a_1/a_2 \leq c'$ for a suitable constant $c' > 0$. Since $(g^* =) \rho g_1 \in \mathcal{R}_1$ we have

$$a_1 = h_k(g_1^* e_1) \leq h_k(g^*(e_2 + \lambda e_1)) \text{ for all } \lambda \in k^*$$

Now $g^*(e_2 + \lambda e_2) = a_2 e_2 + a_1(b + \lambda) e_1$ with $b \in \mathbb{A}$.

Let $\rho g_1 = \begin{pmatrix} g^* & * \\ 0 & g_2 \end{pmatrix}$ with $g_2 \in GL(n-2, \mathbb{A})$ and g^* $= \begin{pmatrix} a & * \\ 0 & a^{-1} \end{pmatrix}$. Then $g^* \in \mathcal{R}_2 \overset{\text{ie}}{\iff} h_k(g^* e_1) = \min\limits_{e \in k^2 - \{0\}} h_k(g^* e)$

Since $\mathbb{A}_k / k$ is compact using the Chinese remainder theorem, one sees that there is a constant $L > 0$ such that for any $b \in \mathbb{A}_k$, there is a $\lambda \in k$ such that

$$|b+\lambda|_v \leq 1 \quad \text{for } v \in M_{k,f}$$

and $|b+\lambda|_v \leq L$ for $v \in \infty_k$. Consider now the subset

$$\tilde{E} = \{ g \in \mathcal{R}_2 \mid h_k(g e_1) \geq \frac{1}{2^{|\infty|}} \cdot \frac{1}{L^{|\infty|}} \}$$

This set of relatively compact in $GL(2, \mathbb{A}_k)$ modulo scalar matrices over $\mathbb{R}$ and $GL(2,k)$. In other words we have a compact set $E \subset GL(2, \mathbb{A}_k)$ such that $E \cdot GL(2,k) \cdot \mathbb{R}^\times = \tilde{E}$. Since there is a constant $C_2 > 0$ such that (for $g \in E$) if we write $g = u_1 t_1 b_1$ with $u_1 \in GL(2, \mathbb{A}_k) \cap H$, $t_1 = \begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix}$, $a \in \mathbb{R}, a > 0$ and $b_1 \in GL(2, \mathbb{A}_k) \cap B^0$, then $|t| < C_2$. Thus if $g^* \in \tilde{E}\Gamma$, we conclude that $\rho g_1 \in H \cdot A_C \omega$ for all $C \geq \max(C_1, C_2)$

We may therefore assume that $g^* \notin \widetilde{E}\,GL(n, k)$. But this would mean that $h_k(g^* e_1) = \min\{h_k(g^* e) \mid e \in k^n \setminus \{0\}\} \leq \frac{1}{2^{1001} L^{100}}$

ie $|a| (= a) \leq \frac{1}{2^{1001} L^{1001}}$ and thus we see that if we take

$$c_0 = \max(c_1, c_2, 1/2^{\infty} L^{\infty}),$$

for $c \geq c_0$, $\quad H \cdot \overline{A}_c \cdot GL(n, k) = GL(n, \mathbb{A}_k)$.