ACTA ARITHMETICA
XCIX.3 (2001)

A generalization of a theorem of Minkowski

by

Marcin Mazur (Urbana, IL)

1. Introduction. Let S be a ring. For an ideal I of S, we denote by R_I the natural map $\mathrm{GL}_n(S) \to \mathrm{GL}_n(S/I)$ and by $\mathrm{GL}_n(S, I)$ its kernel. For any subgroup G of $\mathrm{GL}_n(S)$ we denote by $G(I)$ the kernel of R_I restricted to G. The theorem of Minkowski mentioned in the title says that if S is the ring of integers or the ring of 2-adic integers then any finite subgroup of $\mathrm{GL}_n(S, 2S)$ is conjugated in $\mathrm{GL}_n(S)$ to diagonal matrices. For a local field or a number field K we denote by O_K the ring of integers of K. By μ_{p^∞} we denote the group of roots of unity of p-power order. In the present note we prove the following generalization of Minkowski's result:

Theorem 1. *Suppose that either K is a finite Galois extension of $\mathbb{Q}$ which is unramified at all finite primes except p and such that there is a unique prime ideal γ in K over p or K is a finite Galois extension of $\mathbb{Q}_p$ contained in $\mathbb{Q}_p(\mu_{p^\infty})$ and γ is the maximal ideal of O_K. Let $G \subseteq \mathrm{GL}_n(O_K)$ be a finite Γ-stable subgroup, where Γ is the Galois group of K. Then $G(\gamma)$ can be conjugated to diagonal matrices by a matrix in $\mathrm{GL}_n(\mathbb{Z})$ (in $\mathrm{GL}_n(\mathbb{Z}_p)$ in the local case).*

The motivation behind this result came from our work on the following conjecture of Y. Kitaoka:

Conjecture 1. *Any finite subgroup G of $\mathrm{GL}_n(\overline{\mathbb{Z}})$ stable under the action of $\Gamma = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is pointwise fixed by the commutator of Γ.*

Here $\overline{\mathbb{Z}}$ denotes the ring of all algebraic integers. Nevertheless, we think that Theorem 1 is of independent interest.

The innocent looking conjecture of Kitaoka has rather deep consequences in the theories of quadratic lattices, arithmetic groups and finite group schemes. For more information about this intriguing conjecture we refer the reader to [1], [3], [4], and [6].

2000 *Mathematics Subject Classification*: 20G30, 20G25, 11R33.

Theorem 1 in the global case can be derived from the results of Kitaoka and Suzuki [2]. Their approach is quite different from ours and is based on the theory of quadratic lattices. In particular, it does not extend in any obvious way to the local situation. The present note provides in particular a new, more direct proof of the results of [2].

As explained in [4] and [5], Theorem 1 is in fact a statement about finite flat group schemes over $\mathbb{Z}$ (or $\mathbb{Z}_p$). Our technique can be interpreted as an alternative way of studying such group schemes.

2. Fundamental construction. In this section we recall the technical core of our approach, explained more carefully in [3].

Let S be a commutative domain and suppose that P is a finite abelian group sitting in $\mathrm{GL}_n(S)$ as a subgroup of diagonal matrices. In other words, there are abelian characters $\chi_1, \ldots, \chi_n$ of P with values in the multiplicative group of S such that $g = \mathrm{diag}(\chi_1(g), \ldots, \chi_n(g))$ for all $g \in P$. After conjugating by a permutation matrix (which has entries in the prime subring of S) we can and will assume that there are integers $k_0 = 0 < k_1 < \ldots < k_s < k_{s+1} = n$ such that $\chi_i = \chi_j$ iff $k_t < i, j \leq k_{t+1}$ for some $0 \leq t \leq s$. We say in this case that P is in a *strongly diagonal* form. Set $N(P)$ for the normalizer of P in $\mathrm{GL}_n(S)$ and $C(P)$ for its centralizer.

Lemma 1. *The centralizer $C(P)$ of P in $\mathrm{GL}_n(S)$ equals $\mathrm{GL}_{k_1-k_0}(S) \times \ldots \times \mathrm{GL}_{k_{s+1}-k_s}(S)$. The group $W(P) = N(P)/C(P)$ is finite.*

The first part of the lemma is pretty obvious and we omit the proof. The second part follows from the discussion below.

Note that P is stable under the action of the automorphism group Γ of S. Thus both $N(P)$ and $C(P)$ are Γ-stable. We denote by Π_n the group of permutation matrices in $\mathrm{GL}_n(S)$. If $N \in N(P)$ and ϕ is the automorphism of P induced by conjugation with N then clearly the map $\chi \mapsto \chi \circ \phi$ permutes the characters $\chi_1, \ldots, \chi_n$. Let Σ_n be the symmetric group of degree n. It is fairly obvious that we can choose a permutation $\pi \in \Sigma_n$ such that $\chi_i \circ \phi = \chi_{\pi(i)}$ and whenever $i < j$ and $\chi_{\pi(i)} = \chi_{\pi(j)}$ then $\pi(i) < \pi(j)$. Moreover, such a permutation is unique and if we denote by T_N the corresponding permutation matrix then $NT_N^{-1} \in C(P)$ and $N \mapsto T_N$ is a group homomorphism $\sigma : N(P) \to \Pi_n \cap N(P)$. We denote by Π_P the image of σ. Thus we get the following

Lemma 2. *The group $N(P)$ is a semidirect product of $C(P)$ and Π_P. In particular, the induced action of Γ on $W(P)$ is trivial.*

Note that $N(P)$ acts by conjugation on $M_{k_1-k_0}(S) \times \ldots \times M_{k_{s+1}-k_s}(S)$, which has a basis consisting of matrices with one entry equal to 1 and all others being 0. With respect to this basis the action of $N(P)$ defines a

representation ϱ of $N(P)$ in $\mathrm{GL}_{m_1^2+\ldots+m_{s+1}^2}(S)$, where $m_i = k_i - k_{i-1}$. It is clear that this representation respects the action of Γ. The kernel of ϱ is equal to the product of the centers of $M_{k_i-k_{i-1}}(S)$. In particular, we get the following

LEMMA 3. *Suppose that G is a finite, Γ-invariant subgroup of $N(P)$. Then $\varrho(G)$ is a finite, Γ-invariant subgroup of $\mathrm{GL}_{m_1^2+\ldots+m_{s+1}^2}(S)$ and the map $\varrho : G \to \varrho(G)$ commutes with the action of Γ. For any ideal I of S the map ϱ takes $G(I)$ into $\varrho(G)(I)$.*

We will use the above observations when S is the ring of integers in a finite Galois extension of $\mathbb{Q}$ or $\mathbb{Q}_p$ and Γ is the Galois group.

3. Main result. Let K be an algebraic number field or a local field. Let β be a prime ideal of the ring of integers O_K of K lying over a rational prime p. By f we denote the ramification index of β.

The following is a variant of a well known Minkowski's lemma:

MINKOWSKI'S LEMMA. *Any torsion element of $\mathrm{GL}_n(O_K, \beta)$ has p-power order. If $\mathrm{GL}_n(O_K, \beta^k)$ contains an element of order p^s then $k \leq fp^{1-s}/(p-1)$.*

For a proof see [3], Proposition 1.

LEMMA 4. *Let p be a prime. Suppose that $L \subseteq K$ are finite extensions of $\mathbb{Q}_p$ such that K/L is Galois and the residue field of K has p elements. Denote by γ the maximal ideal of O_K. Let $G \subseteq \mathrm{GL}_n(O_K)$ be a finite group stable under the action of the Galois group Γ of K/L. Then for each $m \geq 1$ and any $\tau \in \Gamma$, τ acts on $G(\gamma^m)/G(\gamma^{m+1})$ by raising to the kth power, where k is an integer such that $k \equiv (\pi^m)^\tau/\pi^m \pmod{\gamma}$ and π is a generator of γ.*

Proof. Let π be a generator of γ. Fix $m > 0$ and let $g, h \in G(\gamma^m)$. We can write $g = 1 + \pi^m a$, $h = 1 + \pi^m b$ for some $a, b \in M_n(O_K)$. Note that $gh \equiv 1 + \pi^m(a+b) \pmod{\pi^{m+1}}$. This shows that the map R which assigns to each $g \in G(\gamma^m)$ the reduction mod γ of $(g-I)/\pi^m$ is a group homomorphism $R : G(\gamma^m) \to M_n(O_K/\gamma)$. The kernel of this homomorphism equals $G(\gamma^{m+1})$. Let $\tau \in \Gamma$. By our assumption O_K/γ has p elements. In particular, there is an integer k such that $k \equiv (\pi^m)^\tau/\pi^m \pmod{\gamma}$. Thus $R(g^\tau) = kR(g)$ for all $g \in G(\gamma^m)$. Consequently, $g^\tau g^{-k} \in G(\gamma^{m+1})$. It follows that τ acts on $G(\gamma^m)/G(\gamma^{m+1})$ by raising to the kth power. ∎

Suppose now that K is a finite Galois extension of $\mathbb{Q}$ or $\mathbb{Q}_p$ with Galois group Γ. Let $G \subseteq \mathrm{GL}_n(O_K)$ be a finite Γ-stable group. Recall that for a prime β of O_K we defined $G(\beta)$ as the kernel of R_β (reduction mod β) restricted to G. Let p be the rational prime in β. Thus $G(\beta)$ is a normal

p-subgroup of G by Minkowski's Lemma. In the global case, define $G(p)$ to be the subgroup of G generated by the elements of all the groups $G(\beta)$ with β containing p. Clearly $G(p)$ is a normal p-subgroup of G stable under the action of Γ. By $D(\beta)$, $I(\beta)$ we denote the decomposition and inertia subgroups of β respectively.

LEMMA 5. *Let $K/\mathbb{Q}$ be a finite Galois extension with Galois group Γ and let G be a finite Γ-stable subgroup of $\mathrm{GL}_n(O_K)$. If β, β' are primes of O_K lying over distinct rational primes p, p' then $I(\beta')$ acts trivially on $G(\beta)$.*

Proof. Since $G(p)$ is a p-group and $G(\beta')$ is a p'-group, it follows that $G(p)\cap G(\beta') = 1$. In particular, $R_{\beta'}$ is injective on $G(p)$ so the action of $I(\beta')$ on $G(p)$ is trivial. Since $G(\beta)$ is contained in $G(p)$, the lemma follows. ∎

Proof of Theorem 1. Suppose that the theorem is false. Let b be the order of a counterexample of minimal possible order (when both n and K vary) and let n be minimal such that there is a counterexample G of order b in $\mathrm{GL}_n(O_K)$ for some K. We can assume that Γ acts faithfully on G. Since γ is the unique prime over p, we deduce that $G(\gamma)$ is Γ-stable. Thus $G = G(\gamma)$ by minimality of G. By Minkowski's Lemma the group G is a p-group. Let F be the Frattini subgroup of G. Then F is a proper characteristic subgroup of G, so it is Γ-stable. Let H be a maximal proper Γ-stable subgroup of G containing F. By minimality of G we can assume that H consists of diagonal matrices and is in a strongly diagonal form (after conjugation by an element in $\mathrm{GL}_n(\mathbb{Z})$ (or $\mathrm{GL}_n(\mathbb{Z}_p)$) if necessary).

LEMMA 6. *The group H is central in $\mathrm{GL}_n(K)$, i.e. consists of scalar matrices.*

Proof. The group G is a subgroup of the normalizer of H in GL_n. Thus we can use the results of Section 2. In particular, any $g \in G$ can be written as cw, where w is a permutation matrix in the subgroup Π_H of the normalizer of H and c centralizes H, i.e. $cw = g \in \mathrm{GL}_n(O_K)$. By reducing mod γ we find that $R_\gamma(c) = R_\gamma(w)^{-1}$ in $\mathrm{GL}_n(O_K/\gamma)$. Recall that the centralizer of H consists of block-diagonal matrices. Thus $R_\gamma(w) = R_\gamma(c)^{-1}$ is block-diagonal. Since w is a permutation matrix, it is block-diagonal and therefore centralizes H. Consequently, $w = I$ by the very definition of Π_H. The upshot is that G centralizes H.

If H is not central in GL_n then the centralizer of H is a product of GL_m's of dimensions smaller than n. Clearly, the image of G in at least one of these GL_m's is a counterexample to Theorem 1, which contradicts the minimality of n. Thus H is central in GL_n. ∎

If the field K contains pth roots of unity then for any $\gamma \in \Gamma$ we denote by $i(\gamma)$ the smallest positive integer such that γ acts on the pth roots of 1 by raising to the power $i(\gamma)$. We call i the *cyclotomic character* of Γ.

LEMMA 7. *The group H is trivial.*

Proof. Suppose that H is not trivial. Then K contains pth roots of 1. Associated with H is the representation ϱ discussed in Section 2. The image $\varrho(G) \in \mathrm{GL}_{n^2}(O_K)$ is isomorphic to G/H. By Lemma 3 we know that $\varrho(G)$ is a finite Γ-stable subgroup of $\mathrm{GL}_{n^2}(O_K, \gamma)$. Moreover, the action of Γ on $\varrho(G) = G/H$ is the same as the induced action from G. By minimality of our counterexample we conclude that $\varrho(G)$ can be conjugated to diagonal matrices by an element of $\mathrm{GL}_{n^2}(\mathbb{Z})$ (or $\mathrm{GL}_{n^2}(\mathbb{Z}_p)$). In particular, Γ acts on G/H via the cyclotomic character i (i.e. the action of τ on G/H is by raising to a power $i(\tau)$) and therefore every subgroup of G/H is Γ-stable. Consequently, G/H is cyclic of order p (recall that H is maximal among proper Γ-stable subgroups of G containing the Frattini subgroup). Since H is central, G is abelian. Let $g \in G$ be such that its image in G/H is a generator (i.e. $g \notin H$). For $\tau \in \Gamma$ there is an integer i such that $k^\tau = k^i$ for any $k \in H$. Clearly $p \,|\, i(\tau) - i$. Thus $g^\tau = g^i h$ for some $h \in H$ (note that the action of τ on G/H is by raising to power i). By raising both sides of the last equality to pth power and using the fact that $g^p \in H$ we conclude that $h^p = 1$.

Suppose that $g^p \neq 1$. Then g^p generates a nontrivial subgroup C of H and therefore $h \in C$ (recall that H is cyclic and $h^p = 1$). Thus the subgroup generated by g is Γ-stable and therefore equals G by minimality of our counterexample. Let $g^p = \xi I$ for some root of unity ξ. Pick $u \in L = K(\xi^{1/p})$ such that $u^p = \xi^{-1}$. Note that the field L satisfies all assumptions of Theorem 1. In the local case this is obvious. In the global case, the inertia I of any prime of L over p surjects onto the Galois group of $K/\mathbb{Q}$ (which coincides with the inertia subgroup of the unique prime of K over p), i.e. $\mathrm{Gal}(L/K)I = \mathrm{Gal}(L/\mathbb{Q})$. Since $\mathrm{Gal}(\mathbb{Q}(u)/\mathbb{Q})$ is abelian, elements of $\mathrm{Gal}(L/K)$ are central in $\mathrm{Gal}(L/\mathbb{Q})$ and therefore I is normal in $\mathrm{Gal}(L/\mathbb{Q})$. Since $\mathbb{Q}$ has no unramified extensions, it follows that $I = \mathrm{Gal}(L/\mathbb{Q})$ and there is a unique prime over p in L.

Let τ be an automorphism of L. There is an integer t such that $g^\tau = g^t$. Also, $u^\tau = u^s$ for some integer s. Clearly we have $u^{ps} = u^{pt}$ so that u^{t-s} is a pth root of 1. Now consider the element $q = ug$. Plainly, $q^p = 1$. Also, $q^\tau = u^s g^t = w q^t$ for some pth root of unity w. Thus, the subgroup generated by q and elements wI, w a pth root of 1, is Γ-stable and it is an elementary abelian p-group of order p^2. Note that g is conjugated to diagonal matrices by an element of $\mathrm{GL}_n(\mathbb{Z})$ (or $\mathrm{GL}_n(\mathbb{Z}_p)$) iff q is such. Thus we can assume that G is elementary abelian of order p^2 and H is cyclic of order p.

Suppose now that $g^p = 1$. Then elements of order p in H and g generate an elementary abelian p-group of order p^2 which is Γ-stable and it has to equal G by minimality of our counterexample.

In any case, we can assume that G is elementary abelian of order p^2. For any $\tau \in \Gamma$ we have $g^\tau = g^{i(\tau)}h(\tau)$, where i is the cyclotomic character and $h(\tau) \in H$. An easy calculation shows that $g^{\tau_1\tau_2} = g^{i(\tau_1)i(\tau_2)}h(\tau_1)^{i(\tau_2)}h(\tau_2)^{i(\tau_1)}$. Consequently, $\tau_1\tau_2$ and $\tau_2\tau_1$ act in the same way on G. Thus, we can assume that Γ is abelian.

If p is odd this implies that Γ is cyclic. Let τ be a generator of Γ. Note that $g^\tau = g^{i(\tau)}h$ for some $h \in H$. An easy calculation shows that $g^{\tau^{p-1}} = gh^{(p-1)i(\tau)^{p-2}} = gh_1$. If $h \neq 1$ then τ has order $p(p-1)$ and $h_1 = \xi I$ for a primitive pth root of unity ξ. It follows that K is the cyclotomic extension of $\mathbb{Q}$ of degree $p(p-1)$ (we use Kronecker–Weber theorem in the global case; recall that p is the only ramified prime in K). Thus there is a primitive p^2th root of unity ζ in K such that $\zeta^{\tau^{p-1}} = \zeta\xi^{-1}$. Note that $(g\zeta)^{\tau^{p-1}} = g\zeta$, i.e. $g\zeta$ has entries in $\mathbb{Q}_p(\xi_p)$ (we pass to the completion at p in the global case). Thus $g\zeta$ is an element of order p^2 in the congruence subgroup $\mathrm{GL}_n(\mathbb{Z}_p[\xi_p], (1-\xi_p))$, which contradicts the inequality in Minkowski's Lemma. Thus $h = 1$ and therefore the subgroup generated by g is Γ-stable. This contradicts the fact that G is a minimal counterexample and H is nontrivial.

If $p = 2$ then Γ acts trivially on H, so we can assume that no nontrivial element of Γ fixes g. In other words, Γ is cyclic of order 2 and $g^\tau = -g$ for a generator τ of Γ. Note that in this case K equals $\mathbb{Q}[w]$, where w is one of $i, \sqrt{2}, \sqrt{-2}$. In any case, $w^\tau = -w$ and therefore $wg \in \mathrm{GL}_n(\mathbb{Q}_2)$ (we pass to the completion at 2 in the global case). If $w = i$, we find that $wg \in \mathrm{GL}_n(\mathbb{Z}_2, 2)$ has order 4, which contradicts Minkowski's Lemma. Otherwise, wg has integral entries with nontrivial 2-adic valuation, so $wg = 2A$ where A has integral entries. But then $(wg)^2 = \pm 2I = 4A^2$, which is a contradiction again. All this shows that H has to be trivial. ∎

By Lemma 7, G is elementary abelian with no nontrivial proper Γ-stable subgroups. For every $r \geq 1$ the congruence subgroups $G(\gamma^r)$ are Γ-stable. Thus there is $r > 0$ such that $G = G(\gamma^r)$ and $G(\gamma^{r+1}) = 1$. Observe that the residue field O_K/γ has p elements. In fact, this is clear in the local case. In the global case, since γ is the only prime over p in $K/\mathbb{Q}$, we infer that $\Gamma = D(\gamma)$ is the decomposition group of γ. Thus, the inertia subgroup $I(\gamma)$ is normal in Γ and its fixed field is an extensions of $\mathbb{Q}$ unramified at all finite primes. Consequently, $\Gamma = I(\gamma)$ and O_K/γ has p elements. Note that Γ is the Galois group of the local extension $K_\gamma/\mathbb{Q}_p$. By Lemma 4, Γ preserves all subgroups of G. It follows that G is cyclic of order p. Therefore we can assume that Γ is cyclic of order $p-1$ and $K = \mathbb{Q}(\xi_p)$ ($K = \mathbb{Q}_p(\xi_p)$ in the local case). From the inequality in Minkowski's Lemma we see that $r = 1$.

Note that $\pi = 1 - \xi_p$ is a generator of γ and $\pi^\tau/\pi = i(\tau) \pmod{\pi}$. Thus Γ acts on G via the cyclotomic character by Lemma 4.

Let g be a generator of G. For every pth root of unit ξ (including $\xi = 1$) define $A_\xi = (\sum_{j=0}^{p-1} \xi^j g^j)/p$. Since the action on both ξ and g is via the cyclotomic character, we find that A_ξ is fixed by Γ, i.e. has entries in $\mathbb{Q}$ ($\mathbb{Q}_p$ in the local case). Note that $A_\xi = (\pi/p)\sum_{j=0}^{p-1} \xi^j b_j$, where $\pi = 1 - \xi_p$ and $b_j = (g^j - I)/\pi \in M_n(O_K)$. In particular, each entry of A_ξ has p-adic valuation at least $1/(p-1) - 1 > -1$. But these entries are in $\mathbb{Q}$ ($\mathbb{Q}_p$), so they are in fact in $\mathbb{Z}$ (or $\mathbb{Z}_p$), i.e. $A_\xi \in M_n(\mathbb{Z})$ ($A_\xi \in M_n(\mathbb{Z}_p)$ in the local case). Note now that A_ξ are commuting idempotent matrices and their sum equals the identity matrix. Also, $gA_\xi = \xi A_\xi$. Let e_i be the standard basis of K^n. The elements $A_\xi e_i$ are eigenvectors for g and they generate $\mathbb{Z}^n$ (resp. $\mathbb{Z}_p^n$). We can chose among them a basis of $\mathbb{Z}^n$ (resp. $\mathbb{Z}_p^n$), which shows that g can be conjugated to diagonal matrix by an element of $\mathrm{GL}_n(\mathbb{Z})$ ($\mathrm{GL}_n(\mathbb{Z}_p)$ in the local case). This contradicts our assumption that G is a counterexample. The proof of Theorem 1 is now complete. ∎

Question. Let K be a finite Galois extension of $\mathbb{Q}_p$ which is totally ramified and set γ for the maximal ideal of O_K. Suppose that G is a finite subgroup of $\mathrm{GL}_n(O_K, \gamma)$ stable under the action of the Galois group Γ of $K/\mathbb{Q}_p$. Is it true that G can be conjugated to diagonal matrices by an element of $\mathrm{GL}_n(\mathbb{Z}_p)$?

Most of the proof of Theorem 1 works in the local situation, but the problem is that not all totally ramified extensions of $\mathbb{Q}_p$ are contained in $\mathbb{Q}_p(\mu_{p^\infty})$. An affirmative answer to our question would be very useful for attacking Conjecture 1.

4. Consequences. Let $K/\mathbb{Q}$ be a finite Galois extension and write O_K for the ring of integers in K. Consider a finite subgroup of $\mathrm{GL}_n(O_K)$ stable under the action of $\Gamma = \mathrm{Gal}(K/\mathbb{Q})$. The group G acts in a natural way on $\mathbb{Z}^n \otimes O_K$ ($(a_{i,j})e_i = \sum a_{i,j}e_j$). After Y. Kitaoka, we say that G is of *A-type* if there exists a decomposition $\mathbb{Z}^n = \bigoplus_{i=1}^k M_i$ such that for every $g \in G$ there are a permutation $\pi(g)$ of $\{1, \dots, k\}$ and roots of unity $\varepsilon_i(g)$ such that $\varepsilon_i(g) g M_i = M_{\pi(g)}$ for $i = 1, \dots, k$.

It is clear that groups of A-type are contained in $\mathrm{GL}_n(K^{\mathrm{ab}})$ (recall that K^{ab} is the maximal abelian subextension of $K/\mathbb{Q}$). But being of A-type means much more. It is not hard to see that if G has odd order then it is of A-type iff it is conjugated by an element of $\mathrm{GL}_n(\mathbb{Z})$ to a semidirect product DB where D is normal in G and consists of diagonal matrices and $B \subseteq \mathrm{GL}_n(\mathbb{Z})$. When the order of G is even, the group theoretic properties are a little harder to spell out. In this case, G can be conjugated over $\mathbb{Z}$ to a subgroup of a semidirect product DB as above.

The following theorem was proved by Kitaoka and Suzuki [2]:

THEOREM 2. *If $\Gamma = \mathrm{Gal}(K/\mathbb{Q})$ is nilpotent then any finite Γ-stable subgroup of $\mathrm{GL}_n(O_K)$ is of A-type.*

Below we give a new proof of this result, based on Theorem 1 and the methods of Section 2. For this we need a few lemmas.

LEMMA 8. *Let K be a Galois extension of $\mathbb{Q}$. Suppose that $A \in \mathrm{GL}_n(O_K)$ has the property that for any $\tau \in \mathrm{Gal}(K/\mathbb{Q})$ there is a diagonal matrix $D_\tau = \mathrm{diag}(\xi_1(\tau), \dots, \xi_n(\tau))$ such that $\xi_i(\tau)$'s are roots of unity and $A^\tau = D_\tau A$. Then $A = DM$ where D is a diagonal matrix of finite order and $M \in \mathrm{GL}_n(\mathbb{Z})$.*

Proof. Let $A = (a_{i,j})$. For every i there exists k such that $a_i = a_{i,k} \neq 0$. We have $a_{i,j}^\tau = \xi_i(\tau) a_{i,j}$ for all j. In particular, $a_i^{-1} a_{i,j}$ is stable under the action of $\mathrm{Gal}(K/\mathbb{Q})$ for all j. Thus there are rational numbers $q_{i,j}$ such that $a_{i,j} = a_i q_{i,j}$. For a given i there is a rational number q_i such that $m_{i,j} = q_i q_{i,j}$ are integers with no common factor. Set $d_i = q_i^{-1} a_i$ and let D be the diagonal matrix with $d_1, \dots, d_n$ on the diagonal. Clearly $A = DM$, where $M = (m_{i,j})$. Since each row of M consists of integers with no common factor and A has entries in O_K, it follows that d_i is an algebraic integer for all i. Moreover, $\det A = d_1 \dots d_n \det M$ is a unit in O_K, which implies that each d_i is a unit and $M \in \mathrm{GL}_n(\mathbb{Z})$. Let N be a natural number such that $\xi_i(\tau)^N = 1$ for all automorphisms τ and all i. Since $d_i^\tau = \xi_i(\tau) d_i$, we deduce that $(d_i^N)^\tau = d_i^N$ for all $\tau \in \mathrm{Gal}(K/\mathbb{Q})$. Thus $d_i^N \in \mathbb{Q}$. Since the only units in $\mathbb{Q}$ are 1 and -1 we conclude that d_i is a root of unity. ∎

LEMMA 9. *Let K be a number field which has no abelian extensions unramified at all finite primes. Let β be a prime of O_K and L a Galois extension of K with nilpotent Galois group which is unramified at all finite primes different from β. Then there is a unique prime in O_L over β which is totally ramified.*

Proof. We use induction on the order of the Galois group Γ of L/K. Let π be a prime of O_L over β. If Γ is abelian and the inertia group $I(\pi)$ is a proper subgroup of Γ then $L^{I(\pi)}$ is a nontrivial abelian extension of K, unramified at all finite primes, which contradicts our assumption about K. Thus $\Gamma = I(\pi)$ and consequently π is the only prime in O_L over β.

In general, let F be the Frattini subgroup of Γ. In particular, F is a normal subgroup and Γ/F is abelian. Thus L^F is an abelian extension of K so there is a unique prime γ of L^F over β. In other words, $\Gamma/F = I(\gamma)$. Note that under the natural projection $\Gamma \to \Gamma/F$ the inertia group $I(\pi)$ is mapped onto $I(\gamma)$. Thus $\Gamma = I(\pi)F$. Directly from the definition of the Frattini subgroup it follows that $I(\pi) = \Gamma$, which is exactly what we want to show. ∎

Now we are in a position to prove Theorem 2. Let then G be a finite Γ-stable subgroup of $\mathrm{GL}_n(O_K)$, where $K/\mathbb{Q}$ is a finite Galois extension with nilpotent Galois group Γ. Fix a rational prime p. Let I be the subgroup of Γ generated by all the inertia subgroups $I(\beta)$ such that β does not contain p. For any prime γ of K over p the group I acts trivially on $G(\gamma)$ by Lemma 5. Recall that $G(p)$ is the subgroup of G generated by all the $G(\gamma)$ with γ over p. Thus $G(p)$ is a normal Γ-stable p-subgroup of G and I acts trivially on it. The fixed field K^I of I is unramified at all finite primes different from p and $K^I/\mathbb{Q}$ has nilpotent Galois group. By Lemma 9, there is a unique prime in K^I over p. Theorem 1 applied to $G(p) \subseteq \mathrm{GL}_n(K^I)$ implies that $G(p)$ can be conjugated to diagonal matrices by an element in $\mathrm{GL}_n(\mathbb{Z})$. In particular, the group $G(p)$ is a commutative p-group for every prime p. If $p \neq q$ then clearly the groups $G(p)$ and $G(q)$ commute.

An easy inductive argument shows that the whole group D generated by the subgroups $G(q)$ can be conjugated to diagonal matrices by an element of $\mathrm{GL}_n(\mathbb{Z})$. In fact, D is a commutative abelian group with p-Sylow subgroup $G(p)$. Fix a prime p such that $G(p)$ is not trivial and let $D(p)$ be the product of all Sylow subgroups of D different from $G(p)$. Theorem 1 allows us to assume that $G(p)$ is in a strongly diagonal form. Clearly $D(p)$ centralizes $G(p)$ and therefore it is contained in the centralizer of $G(p)$ in GL_n. As noted in Section 2, this centralizer consists of block-diagonal matrices, i.e. it is a product of GL_m's, and in each of these, the elements of $G(p)$ are scalar matrices. Thus we can use induction and conjugate $D(p)$ to diagonal matrices by an element in $\mathrm{GL}_n(\mathbb{Z})$ which centralizes $G(p)$. Hence we can assume that D is in a strongly diagonal form. Clearly D is normal in G. Note that Γ acts trivially on G/D. In fact, for any prime β of K the inertia $I(\beta)$ acts trivially on $G/G(\beta)$ so it acts trivially on G/D. Since all the inertia groups generate Γ (because $\mathbb{Q}$ has no unramified extensions), our claim follows.

By our discussion of the normalizer of D in Section 2 it follows that any element g of G is of the form $g = cw$, where c centralizes D and w is a permutation matrix in Π_D. Plainly $c \in \mathrm{GL}_n(O_K)$. Since Γ acts trivially on G/D, for any $\tau \in \Gamma$ there is $d \in D$ such that $g^\tau g^{-1} = c^\tau c^{-1} = d$. Now the centralizer of D in GL_n is a product of GL_m's and if we take a component C of c in one of these GL_m's then we have $C^\tau = C\xi$ where ξ is a root of unity (corresponding component of d). By Lemma 8 we get $C = \zeta M$, where M is an invertible integral matrix and ζ is a root of 1. Thus $c = bm$ where b is a diagonal matrix of finite order and $m \in \mathrm{GL}_n(\mathbb{Z})$ centralizes D and b. Thus we proved that any element of G is of the form bmw where b is diagonal of finite order, $m \in \mathrm{GL}_n(\mathbb{Z})$ centralizes b and D, and w is a permutation matrix in Π_D. This is exactly what we need in order to say that G is of A-type.

References

[1] Y. Kitaoka, *Arithmetic of Quadratic Forms*, Cambridge Tracts in Math. 106, Cambridge Univ. Press, 1993.
[2] Y. Kitaoka and H. Suzuki, *Finite arithmetic subgroups of GL_n, IV*, Nagoya Math. J. 142 (1996), 183–188.
[3] M. Mazur, *Finite arithmetic subgroups of GL_n*, J. Number Theory 75 (1999), 109–119.
[4] —, *Finite arithmetic subgroups of GL_n*, part 1 of the University of Chicago PhD. thesis, 1999.
[5] —, *Finite flat group schemes and a conjecture of Kitaoka*, in preparation.
[6] V. P. Platonov and A. S. Rapinchuk, *Algebraic Groups and Number Theory*, Pure Appl. Math. 139, Academic Press, Boston, MA, 1994.

Department of Mathematics
University of Illinois at Urbana-Champaign
1409 W. Green Street
Urbana, IL 61801-2975
E-mail: mazur1@math.uiuc.edu

Received on 28.2.2000
and in revised form on 17.11.2000 (3759)