

FINITE GROUPS OVER ARITHMETICAL RINGS AND GLOBALLY IRREDUCIBLE REPRESENTATIONS

F. Van Oystaeyen

*Department of Mathematics
University of Antwerp, U.I.A.
2610 Antwerp, Belgium*

A. E. Zalesskii

*School of Mathematics
University of East Anglia
Norwich NR4 7TJ, United Kingdom*

Abstract

Given the ring of integers R of an algebraic number field K , for which natural number n is there a finite group $G \subset GL(n, R)$ such that RG , the R -span of G , coincides with $M(n, R)$, the ring of $(n \times n)$ -matrices over R ? Given $G \subset GL(n, R)$ we show that $RG = M(n, R)$ if and only if the Brauer reduction of G modulo every prime is absolutely irreducible. Besides, the question above is fully answered if n is an odd prime.

§1. Introduction

In the study of the Schur subgroup of the Brauer group of a commutative ring R one is interested in finding the Azumaya algebras over R that are epimorphic images of a group ring $R[G]$ for some finite group G . Azumaya algebras are the central separable algebras, they can also be viewed as the algebras A with center R such that A is a progenerator as an $A^e = A \otimes_R A^o$ -module where A^o is the opposite R -algebra. In this context one is actually interested in such algebras up to Brauer equivalence, but the more precise

⁰This work is performed as a part of the INTAS project ‘Noncommutative algebra and geometry with focus to representation theory’. It was started when the second named author visited the University of Antwerp.

question which Azumaya algebras over R are obtainable as an epimorphic image of $R[G]$ for some finite group G is interesting in its own right. That it is a non-trivial problem may be appreciated from the fact that $M(n, \mathbf{Z})$ is an epimorphic image of some $\mathbf{Z}[G]$ if and only if $n = 1$ or n is divisible by 8, cf. [Ne, Ne2]. In this paper we study this problem for arithmetical rings R by which we mean the ring of integers of an algebraic number field. The results here emanate from the symbiosis of the Schur subgroup approach of Nelis, Van Oystaeyen, cf. [NO], and a recent work of Dixon-Zaleski, cf. [DZ].

For a commutative ring R the matrix ring $M(n, R)$ is called a Schur ring if there exist a finite group $G \subset GL(n, R)$ such that the R -span of G is just $M(n, R)$. We mainly study the following problem:

1.1. Problem Let R be an arithmetical ring and $M(n, R)$ the matrix ring over R . For which n is $M(n, R)$ a Schur ring?

For $G \subset GL(n, R)$ we denote by RG the R -span of G in $M(n, R)$. Another problem of particular interest is:

1.2. Problem Let $G \subset GL(n, R)$ be a finite subgroup. When do we have $RG = M(n, R)$?

Our first main result (Theorem 1.4) solves Problem 1.2 in terms of the representation theory of finite groups. To state it we need the following

1.3. Definition Let \mathbf{C} denote the field of complex numbers and $G \subset GL(n, \mathbf{C})$. We call G globally irreducible if for every prime p a reduction of G modulo p is absolutely irreducible.

The term "globally irreducible" was introduced by Gross [Gr], however, the content of this notion in [Gr] differs from the one here. Analysis of global irreducibility in the sense of Gross was continued by Tiep [T1, T2, T3, T4]. Observe that global irreducibility of certain representations can be deduced from results of [Gr, T1, T2, T3, T4].

1.4. Theorem Let $G \subset GL(n, R)$. Then $RG = M(n, R)$ if and only if G is globally irreducible.

Theorem 1.4 allows us to restate Problem 1.1 in terms of representation theory:

1.5. Problem For which n does there exist a globally irreducible finite subgroup $G \subset GL(n, R)$?

Recall that we assume R to be the ring of integers of an algebraic number field K . It is well known (see [CR], Theorem 75.4) that for any finite group $G \subset GL(n, K)$ there exists a finite extension L of K such that G is conjugate to a subgroup of $GL(n, R_L)$ where R_L is the ring of integers of L . This shows that one of the main ingredients of 1.5 is the following problem:

1.6. Problem Determine globally irreducible finite subgroups of $GL(n, \mathbf{C})$.

One can expect no easy solution of 1.6. Only fragmentary results are known at the moment.

By using [DZ], we describe primitive globally irreducible linear groups of odd prime degrees:

1.7. Proposition Let $p > 2$ be a prime and let $G \subset GL(p, \mathbf{C})$ a primitive subgroup. Then G is globally irreducible if and only if $G = H \cdot Z(G)$ where H is globally irreducible and one of the following holds:

- (1) $p = 3$, $H \cong 3 \cdot Alt(6)$, the 3-fold cover of the alternating group;
- (2) $H \cong PSL(2, q)$, $p = (q - 1)/2$ where q is an odd prime;
- (3) $H \cong PSp(2l, 3)$, $p = (3^l - 1)/2$ where $l > 1$ is an odd prime.

It is not difficult to consider the case where G is imprimitive because in this case $G(\text{mod } r)$ is induced from a 1-dimensional representation of a certain subgroup. One can use a well-known irreducibility condition for such a representation to obtain a description of G .

One may expect that the existence of a globally irreducible subgroup $G \subset GL(n, K)$ does imply that $M(n, R)$ is a Schur ring. For this it suffices to show that G is conjugate to a subgroup of $GL(n, R)$. However, there is no reason for this to hold. Moreover, the argument in [CRW] hints that this is not true.

Our second main result solves the problems 1.1 and 1.5 if n is an odd prime. The case of prime n is of particular importance in view of the following fact: $M(kn, R)$ is a Schur ring for any $k \in \mathbf{N}$ whenever $M(n, R)$ is a Schur ring (see Lemma 3.5). For a field L we denote by L_π the subgroup of elements of finite order in L^* , the multiplicative group of L .

1.8. Theorem Let $p > 2$ be an odd prime. Then $M(p, R)$ is a Schur ring if and only if one of the following holds:

- (i) K contains an odd root of 1;
- (ii) there exists a field extension L of K such that $L : K = p$ and L_π/K_π contains a cyclic group of order st where s, t are distinct primes;
- (iii) $q = 2p + 1$ is a prime and K contains $\sqrt{-q}$.

Notation Throughout the paper R is the ring of integers of an algebraic number field K , R^* denotes the unit group of R , and R_π is the torsion subgroup of R^* . Let $M(n, R)$ stand for the ring of $(n \times n)$ -matrices over R . For an ideal I of R we denote by ϕ_I the canonical epimorphism $M(n, R) \rightarrow M(n, R/I)$. We write $GL(n, R)$ for the multiplicative group of the invertible elements of $M(n, R)$. For a subgroup G of $GL(n, R)$ we let RG be the R -span of G in $M(n, R)$. The group ring $R[G]$ maps canonically onto RG , hence RG is a Clifford system for G in sense of [FVO]. Let π be the set of all natural primes. If $\sigma \subseteq \pi$ and A is an abelian group, then A_σ stands for the Sylow σ -subgroup of A . In particular, A_π is the torsion subgroup of A . We denote by \mathbf{Q}, \mathbf{C} the fields of rational and complex numbers, respectively, and by \mathbf{Z}, \mathbf{N} the set of integers and positive integers.

§2. Connection with globally irreducible representations

In this section we discuss the notion of global irreducibility and prove Theorem 1.4.

Recall that the Brauer reduction of a representation modulo a natural prime p is defined as follows. Let $\phi : H \rightarrow GL(n, \mathbf{C})$ be a representation of a finite group H . Then there exists a finite extension F of \mathbf{Q} such that ϕ is equivalent to a representation into $GL(n, F)$. Let L be the subring of p -integers of F . Then L is a principal ideal domain, and ϕ is equivalent to a representation $\tau : G \rightarrow GL(n, L)$. If I is a unique maximal ideal of L , set $P = L/I$. Then the homomorphism $h : G \rightarrow GL(n, P)$ induced by the natural projection $GL(n, L) \rightarrow GL(n, P)$ is called a reduction of ϕ modulo p . The group $h(G)$ is usually regarded as a subgroup of $GL(n, \bar{P})$ where \bar{P} stands for the algebraic closure of P . The reduction homomorphism h depends on τ which is not unique; however, by the Brauer-Nesbitt theorem (see [CR, Theorem 82.1]) the irreducible constituents of $h(G)$ do not depend on the choice of h . Therefore, the notion of a globally irreducible representation is well defined.

2.1. Lemma Let $G \subset GL(n, F)$ and $h : G \rightarrow GL(n, P)$ be as above. Set $\bar{G} = h(G)$. Then $\dim_P(P\bar{G}) \leq \dim_F(FG)$.

Proof. Set $k = \dim_P(P\bar{G})$, and $\bar{g} = h(g)$ for $g \in G$. Let $\bar{g}_1, \dots, \bar{g}_k$ be a P -basis of $P\bar{G}$. Then g_1, \dots, g_k are linearly independent over F (otherwise, there exist elements $\alpha_1, \dots, \alpha_k \in L$ not all in I , such that $\sum_i \alpha_i g_i \in M(n, I)$, and then $\sum_i \bar{\alpha}_i \bar{g}_i = 0$, where $\bar{\alpha}_i = \alpha_i \pmod{I}$, which is a contradiction).

2.2. Corollary Let $G \subset GL(n, F)$ be a globally irreducible representation. Then G is absolutely irreducible.

Proof. By the Burnside theorem $\dim_P(P\bar{G}) = n^2$ so $\dim_F(FG) = n^2$ (notation of 2.1).

2.3. Lemma Let $G \subset GL(n, R)$ be a subgroup such that $RG = M(n, R)$. Let I be a maximal ideal of R and $P = R/I$. Set $\bar{G} = \phi_I(G)$. Then $P\bar{G} = M(n, P)$, so \bar{G} is an absolutely irreducible subgroup of $M(n, P)$.

Proof: obvious.

2.4. Lemma Let $G \subset GL(n, \mathbf{C})$ and p be a prime. If G has a normal p -subgroup S such that G/S is abelian, or $|G/S| < n^2$, then G is not globally irreducible.

Proof. Let L, h be as above and let I be a maximal ideal of L containing p . Consider the mapping $G \rightarrow \bar{G} = h(G)$. If \bar{G} is irreducible then $\bar{S} = \text{Id}$. If G/S is abelian then \bar{G} is abelian, so \bar{G} is not absolutely irreducible. If $|G/S| < n^2$ then $|\bar{G}| < n^2$ so again \bar{G} is not absolutely irreducible in view of Burnside's theorem.

2.5. Proposition Let Λ be a subring of $M(n, R)$ containing $R \cdot \text{Id}$ and such that $\phi_I(\Lambda) = M(n, R/I)$ for every maximal ideal I of R . Then $\Lambda = M(n, R)$.

Proof. It is convenient to identify R and $R \cdot \text{Id} \subset M(n, R)$. As R is Noetherian and $M(n, R)$ is a finitely generated R -module, it is Noetherian (see, for instance [L1], Ch. VI, §1, Prop. 3). Hence Λ is finitely generated as an R -module, consequently, it is a Noetherian PI -algebra and it is central over R . (All necessary facts about PI -algebras, i.e. algebras with a polynomial identities can be found in [Ro]). The primitive ideals of Λ are maximal. If $\omega \subset \Lambda$ is such a maximal ideal then Λ/ω is a simple Artinian ring containing $R/(\omega \cap R)$ in its center. Hence $R/(\omega \cap R)$ is a field. Now let us first consider the local case, that is, assume that R is a local ring (hence a discrete valuation ring, in view of the above hypothesis on R), with a unique maximal ideal $I \subset R$. By assumption, $\phi_I(\Lambda) = M(n, R/I)$, hence

$\phi_I(\Lambda) = \phi_I(M(n, R))$ or $M(n, R) = \Lambda + IM(n, R)$. As R is local, I is the Jacobson radical of R , so $M(n, I)$ is the Jacobson radical of $M(n, R)$. Since $M(n, R)$ is finitely generated as a Λ -module, Nakayama's lemma (see [L1], Ch. IX, §1)) implies that $\Lambda = M(n, R)$. If R is not local, let R_I denote the localization of R at I , and $\Lambda_I = \Lambda \otimes_R R_I$. Then $\Lambda_I \subset M(n, R_I)$, and $\phi_I^e : M(n, R_I) \rightarrow M(n, R/I)$ is the canonical localized map extending ϕ_I , so $\phi_I^e(\Lambda_I) \cong M(n, R/I)$. The local case then tells us that $\Lambda_I = M(n, R_I)$, hence Λ_I is an R_I -separable algebra central over R_I , see [MI, p.41, Example II]. The local-global property for separability (see [MI, Theorem 7.2, p.72]) yields that Λ is a separable R -algebra (with center exactly R). The commutator theorem for separable algebras ([MI, Theorem 4.3]) then implies that $M(n, R) = \Lambda \otimes C$, where $C = C_{M(n, R)}(\Lambda) = \{A \in M(n, R) : A\lambda = \lambda A \text{ for all } \lambda \in \Lambda\}$. If $C \neq R$ then the p.i. degree of the Azumaya algebra Λ is strictly less than the p.i. degree of $M(n, R)$ which is of course n . In this case no image of Λ can have p.i. degree equal to n , contradicting $\phi_I(\Lambda) \cong M(n, R/I)$. Therefore, we must have $C = R$ and $\Lambda = M(n, R)$. (Recall that p.i. degree means the least degree of a polynomial identity of Λ .)

Proof of Theorem 1.4 The "only if" part follows from 2.3 and the Brauer-Nesbitt theorem as every natural prime belongs to a proper ideal of R . Let us prove the converse. Obviously, RG contains $R \cdot \text{Id}$ (the ring of scalar matrices). Next, let I be a maximal ideal of R . Then $F = R/I$ is a finite field of characteristic p , say, so the homomorphism $G \rightarrow \bar{G} = \phi_I(G)$ is a p -modular representation of G . As G is globally irreducible, \bar{G} is absolutely irreducible by the Brauer-Nesbitt theorem. Then \bar{G} contains n^2 linearly independent matrices by the classical Burnside theorem, so $F\bar{G} = M(n, F)$. Set $\Lambda = RG$. Hence the assumption of Proposition 2.5 holds, and we conclude that $RG = M(n, R)$.

Remark. From the above argument one can deduce a 'Hasse principle' for RG to coincide with $M(n, R)$: this is the case if and only if $R_I G = M(n, R_I)$ for every prime ideal I of R . We use Nakayama's lemma to show that $R_I G = M(n, R_I)$ is equivalent to $(R/R_I)\bar{G} = M(n, R/R_I)$.

Weaker versions of the notion of global irreducibility may be of interest. For instance, one can omit the word "absolute" from Definition 1.3 and obtain a much weaker notion (closer to Gross' one). We introduce the following:

2.6. Definition Let $\phi : G \rightarrow GL(n, R)$ be a representation of a finite

group G . (i) ϕ is called an Azumaya representation if for every maximal ideal I of R the ring $\phi_I(RG)$ is simple. (ii) An Azumaya representation ϕ is called a strong Azumaya representation if G is absolutely irreducible.

The notion of an Azumaya representation is fairly close to the one introduced by Nelis [Ne] (see Def. 2.2.6 and Theorem 2.2.8 in [Ne]). Examples of Azumaya representations that are not strong Azumaya can be found in [Ne]. The gap between the content of Definitions 1.3 and 2.6(ii) seems to be quite small, however, these are different notions. We give an example of a strong Azumaya representation of a finite group $G \subset GL(2^k, \mathbf{Z}[i])$ that is not globally irreducible. Set $R = \mathbf{Z}[i]$ and $n = 2^k$, $k > 2$. Define a group $\mathcal{E}_k \subset GL(n, R)$ to be the Kronecker product of k copies of \mathcal{E}_1 where $\mathcal{E}_1 \subset GL(2, R)$ is generated by the matrices $\text{diag}(\pm i, i)$ and $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Observe that \mathcal{E}_k is absolutely irreducible. Let H be the normalizer of \mathcal{E}_k in $GL(n, R)$. Then $H/Z(H) \cdot \mathcal{E}_k \cong Sp(2k, 2)$, see [Ward] or [Sup, §20]. In particular, the quotient group is finite and coincides with its commutator subgroup (as $k > 2$). It follows that H' , the commutator subgroup of H , is finite. Since $R = \mathbf{Z}[i]$ is a principal ideal domain, H' is conjugate with a subgroup of $GL(n, R)$, see [CR]. So we assume that $H' \subset GL(n, R)$. Let U be a 2-dimensional non-degenerate subspace of the underlying space of $Sp(2k, 2)$, and $X = \{x \in Sp(2k, 2) : xu = u \text{ for all } u \in U\}$. Then $X \cong Sp(2k - 2, 2)$. We define G to be the pullback of X in H' .

Observe first that G is a strong Azumaya representation of itself. Indeed, let I be a maximal ideal of R , and $F = R/I$. Then F is a field. Set $p = \text{char}(F)$. If $2 \notin I$ then $(|\mathcal{E}_k|, p) = 1$ so $\mathcal{E}_k \pmod{p}$ is absolutely irreducible. Therefore, $\phi_I(RG) \cong M(n, F)$. If $2 \in I$ then $\phi_I(RG) \cong M(n/2, F)$. To see this, observe that $\phi_I(H')$ is irreducible and is conjugate to the image of $Sp(2k, 2)$ under the so called spinor representation, see [Za, Theorem 3.10]. (The spinor representation can be described as the restriction to $Sp(2k, 2)$ of the irreducible representation of the algebraic group $Sp(2k, \overline{\mathbf{F}}_2)$ with highest weight ω_k .) Of course, \mathcal{E}_k belongs to the kernel of the projection $H' \rightarrow \phi_I(H')$ as \mathcal{E}_k is a normal 2-subgroup of H' , and $\phi_I(H')$ is irreducible. Thus, H' is globally irreducible (see [Go]). Next, for $1 \leq l < k$ the restriction of the spinor representation σ of $Sp(2k, 2)$ to the naturally embedded subgroup $Sp(2l, 2)$ is homogenous (in fact, this follows from the irreducibility of the restriction of σ to the subgroup $Sp(2l, 2) \times Sp(2(k-l), 2)$, the stabilizer of

a non-degenerate $2l$ -dimensional subspace; this is fairly well-known). This means that the F -span of $\sigma(Sp(2l, 2))$ is a simple F -algebra. As $\phi_I(G) = \sigma(Sp(2l, 2))$, we conclude that $F\phi_I(G)$ is a simple F -algebra.

Recall that a subgroup $G \subset GL(n, K)$ is called quasi-primitive if for every normal subgroup N of G the ring KN is simple.

2.7. Lemma Let $G \subset GL(n, K)$ be a quasi-primitive globally irreducible subgroup. Suppose that A is an abelian normal subgroup of G , and $C = C_G(A)$. Let $M = C_{M(n, K)}(A)$. Then M is isomorphic to a matrix ring $M(n/l, L)$ where $L = KA$, $(L : K) = l$, and C is a globally irreducible subgroup of $GL(n/l, L)$.

Proof. It is convenient to prove a more general fact:

(*) Let $G \subset GL(n, K)$ be a quasi-primitive globally irreducible subgroup. Suppose that $L \subset M(n, K)$ is an abelian Galois extension of K , and L contains the identity of $M(n, K)$. Set $C = C_G(L)$, $M = C_{M(n, K)}(L)$, $l = L : K$. Then M is isomorphic to a matrix ring $M(n/l, L)$ and C is globally irreducible as a subgroup of $M(n/l, L)$.

As A is a finite abelian group, $L = KA$ is a field, so L satisfies the assumption of (*), and the lemma follows from (*).

Proof of (*). By Galois theory $G : C = l$. Suppose first that l is a prime.

Let r be a prime, and let K_r be any maximal subring of K not containing r^{-1} . Then K_r is a local ring. Let I be a unique maximal ideal of K_r , $P = K_r/I$ (so P is a field of characteristic r) and $h : GL(n, K_r) \rightarrow GL(n, P)$ the natural projection. As K_r is a principal ideal domain, G is conjugate to a subgroup of $GL(n, K_r)$. So we may assume that $G \subset GL(n, K_r)$.

Let L_r be the ring of r -integers of L so $K_r \subset L_r$. As L_r is a torsion free K_r -module, and K_r is a principal ideal domain, L_r is a free K_r -module. It follows that the action of L_r on L_r by multiplication represents L_r by $(l \times l)$ -matrices over K_r . Then $M(n/l, L_r)$ represents by $(n \times n)$ -matrices over K_r , so we have the natural injective homomorphism $M(n/l, L_r) \rightarrow M(n, K_r)$ such that $M(n, K_r) \cap M \cong M(n/l, L_r)$. Set $N = M \cap M(n, K_r)$, so $C \subseteq N$. Let ν be a maximal ideal of L_r containing I . Then $N/N\nu \cong M(n/l, L_r/\nu)$ is a simple quotient of N/NI , and we have a natural homomorphism $\varepsilon : N/NI \rightarrow N/N\nu$. Observe that $\dim_P(N/NI) = n^2/l$. The projection α of C into $M/M\nu$ is just a reduction homomorphism of C modulo r as a subgroup of M . This shows that $\alpha = \varepsilon(h|C)$. We have to prove that $\alpha(C)$ is absolutely irreducible.

Let \bar{C}, \bar{G} stand for the images of C, G , respectively, under h . As G is globally irreducible, \bar{G} is absolutely irreducible. By Clifford's theorem $P\bar{C}$ is a semisimple P -algebra and the simple components of $P\bar{C}$ are transitively permuted by G under the conjugation action.

By Lemma 2.1 $\dim_P(\bar{P}C) \leq \dim_K(KC)$. Recall that \bar{G} is absolutely irreducible due to global irreducibility of G . It follows that $n^2 = \dim_P(P\bar{G}) \leq \dim_P(P\bar{C}) \cdot (\bar{G} : \bar{C}) \leq \dim_K(KC) \cdot (G : C) = n^2$. Therefore, $\dim_P(P\bar{C}) = n^2 / (G : C) = n^2 / l$. It follows that $\bar{P}C = N/IN$. Then $\varepsilon(P\bar{C}) = N/N\nu \cong M(n/l, L_r/\nu)$. It follows that $\varepsilon(P\bar{C})$ is absolutely irreducible subgroup of $M(n/l, L_r/\nu)$, as desired.

Let now l be arbitrary. As L is an abelian Galois extension of $K \cdot \text{Id}$, there is a series $K \cdot \text{Id} = L_0 \subset L_1 \subset \dots \subset L_t = L$ of subfields of L such that $L_i : L_{i-1}$ is prime, $i = 1, \dots, t$. So induction on t completes the proof.

2.8. Theorem Let $G \subset GL(n, K)$ be a quasi-primitive globally irreducible subgroup and $p > 2$. Then every normal p -subgroup of G is abelian.

Proof. Let P be a normal p -subgroup of G . As G is quasi-primitive, every characteristic subgroup of P is cyclic; if P is not abelian, this implies $P = \mathcal{E} \cdot Z(P)$ where \mathcal{E} is an extraspecial p -subgroup, see [Dix], Theorem 4.4. Set $C = C_G(Z(P))$. By 2.7 C is globally irreducible as a subgroup of $GL(l, L)$ where $L = KZ(P)$, and $l = n / (L : K)$. We need fairly precise information about the structure of C . Set $H = C/P$. As $LP = KP$ is a simple ring, the action of C on LP by conjugation can be realized via inner automorphisms of LP . It follows that there exists a projective representation $\tau : C \rightarrow GL(l, L)$ such that $\tau|_P = \eta|_P$. It can be deduced from this that $\tau = \eta \otimes \lambda$ where λ is an irreducible projective representation of $H = C/P$, and $\eta(\mathcal{E}) \cong \mathcal{E}$ is irreducible. This is essentially Clifford's theorem. As τ is globally irreducible, η is too. Let $SL^\pm(l, L)$ stand for the group of all matrices of $GL(l, L)$ with determinant ± 1 , and set $N = N_{SL^\pm(l, L)}(P)$. It is known that N is finite. Let $k = \dim(\eta)$, and S the group of all scalar matrices in $SL^\pm(k, L)$. As $\eta(\mathcal{E})$ is irreducible in $GL(k, L)$, and $\mathcal{E} \cong \eta(\mathcal{E})$, we have $k > 1$. Then $N/PS \cong Sp(2k, p)$, see [Sup, §20]. Moreover, N is a semi-direct product of PS and of a subgroup T of N such that $T \cong Sp(2k, p)$, see [Ward]. Let t be a unique central involution in T . Then $t \notin S$. Show first that N is not globally irreducible. Indeed, if $h : N \rightarrow GL(k, F)$ is a reduction homomorphism then $h(P) = 1$ (otherwise, $h(N)$ is reducible as $p = \text{char}(F)$) and $h(P)$ is a normal subgroup of $h(N)$. Hence $h(N) = h(S) \cdot h(T)$. As

$(|t|, p) = 1$, $h(t)$ is non-scalar central element of $h(N)$, which is impossible. Therefore, $\eta(C)$ is not globally irreducible. This is a contradiction.

Remark. The assertion of Theorem 2.8 fails for $p = 2$. An example is given by the group H' in the argument prior Lemma 2.7.

§3. $M(n, R)$ as a Schur ring: general approach

3.1. Definition $M(n, R)$ is called a Schur ring if $M(n, R) = RG$ for some finite group $G \subset GL(n, R)$.

3.2. Lemma Let $L \subset R$ be a subring and $G \subset GL(n, L)$. If $LG = M(n, L)$ then $RG = M(n, R)$.

Proof: obvious.

The following lemma shows that the case of prime n is of particular importance for Problem 1.

3.3. Lemma Let $G \subset GL(k, R)$ with $k > 1$ and $RG = M(k, R)$. Then there exists $H_m \subset GL(km, R)$ such that $RH_m = M(km, R)$.

Proof (cf. [Ne, Theorem 2.5.7]). Take for H_m the matrix wreath product of G and S_m .

3.4. Theorem (see [Ne, Corollary 2.5.8]) $M(n, \mathbf{Z})$ is a Schur ring if and only if n is a multiple of 8 or $n = 1$.

3.5. Corollary If n is a multiple of 8 then $M(n, R)$ is a Schur ring for every R .

Proof. For $R = \mathbf{Z}$ this is proved in [Ne, Corollary 2.5.8] so 3.5 follows from 3.2.

Observe that it suffices to examine maximal finite subgroups of $GL(n, R)$ in order to check whether $M(n, R)$ is a Schur ring.

3.6. Lemma Suppose that n is relatively prime to the ideal class number of K . (i) ([CR1], Theorem 23.17) Every finite subgroup of $GL(n, K)$ is conjugate to a subgroup of $GL(n, R)$. (ii) If $GL(n, K)$ contains a globally irreducible subgroup then $M(n, R)$ is a Schur ring.

The second assertion follows from (i) and Theorem 1.4.

3.7. Proposition Let $n > 1$. Then $M(n, \mathbf{Z}[i])$ is a Schur ring if and only if n is even.

Proof. The "if" part. In view of Lemma 3.3 it suffices to prove the proposition for $n = 2$. Set $R = \mathbf{Z}[i]$, where $i^2 = -1$. Let $G \subset GL(2, \mathbf{C})$ be a nonsplit extension of an irreducible group of order 16 with the center of order 4 by $S_3 \cong Sp(2, 2) \cong SL(2, 2)$. It is well known that G is conjugate with a subgroup of $GL(2, \mathbf{Q}[i])$. The class ideal number of $\mathbf{Q}[i]$ is equal to 1, and $\mathbf{Z}[i]$ is the ring of integers of $\mathbf{Q}[i]$. It follows from 3.6 that G is conjugate with a subgroup of $GL(2, R)$. It is easy to verify that G remains irreducible under reduction at any prime p (for $p > 2$ the reduction mapping is an isomorphism, and for $p = 2$ the image of this mapping is $SL(2, 2)$: the argument is similar to that prior Lemma 2.7). By Theorem 1.4 $RG = M(2, R)$. By Lemma 3.3 $M(2k, R)$ is a Schur ring for any $k \in \mathbf{N}$.

The "only if" part follows from the following lemma (with $K = \mathbf{Q}[i]$) which is essentially contained in [Gr]. The symbol \mathbf{F}_2 denotes the field of 2 elements.

3.8. Lemma Let σ denote the complex conjugation. Let $K \subset \mathbf{C}$ be a σ -stable algebraic number field and R the ring of integers of K . Let I be an ideal of R containing 2 and $F = R/I$. Let $G \subset GL(n, R)$ and \bar{G} be the image of G under the projection $M(n, R) \rightarrow M(n, R/I)$. Suppose that \bar{G} is absolutely irreducible and K/K^σ is ramified over 2 (K^σ denotes the subfield of σ -fixed elements of K .) Then $n(F : \mathbf{F}_2)$ is even. In particular, if n is odd then $F \neq \mathbf{F}_2$.

Proof. As K is ramified over K^σ , one has $\sigma(I) = I$. Set $d = F : \mathbf{F}_2$. Suppose that nd is odd. The standard 'average argument' yields a matrix $M \in M(n, R)$ such that $\sigma(M^t) = M$ and $gM\sigma(g^t) = M$ (M^t stands for the transpose of M). Let $N = M(\text{mod } I)$. The complex conjugate induces a field automorphism of F which must be trivial as d is odd. It follows that $N^t = N$ and $hNh^t = N$ for all $h \in \bar{G}$. As \bar{G} is absolutely irreducible, N is nondegenerate. Let τ be the involution of $M(n, F)$ defined by $x \rightarrow Nx^tN^{-1}$. Then \bar{G} is contained in the group $U = \{x \in GL(n, F) : x\tau(x) = \text{Id}\}$. It is known that U is reducible for n odd (a proof may be found in [DTZ], Proposition 1).

3.9. Lemma Let $g \in GL(n, R)$ be an element of finite order, and let ε be an eigenvalue of g . Suppose that $\varepsilon \in K$. Then $\varepsilon \in R$.

Proof. Obvious, as ε is an integer in K .

Let $H(n, R) \subset GL(n, R)$ be the group of the monomial matrices in $GL(n, R)$ whose matrix entries belong to R_π . In particular, $H(n, R)$ contains the group Π_n of permutation matrices.

The proof of the following proposition is similar to that of Theorem 1.8 in [NO].

3.10. Proposition Suppose that K contains an odd root of 1. Then the R -span of $H(n, R)$ is $M(n, R)$. In particular, $M(n, R)$ is a Schur ring, and $H(n, R)$ is globally irreducible.

Proof. Let $G = H(n, R)$ and let $D = RG$. Let $\varepsilon \in K$ be a primitive k -root of 1 with k to be an odd prime. By 3.9 $\varepsilon \in R$. Then the matrices $d^i = \text{diag}(\varepsilon^i, 1, \dots, 1)$ belong to G . Hence $d^i - \text{Id} = \text{diag}(\varepsilon^i - 1, 0, \dots, 0) \in D$. Then $d = \sum_{i=1}^{k-1} (d^i - \text{Id}) = \text{diag}(-k, 0, \dots, 0) \in D$. Similarly, $\text{diag}(-1, 1, \dots, 1) \in G$ and $\text{diag}(-2, 0, \dots, 0) \in D$. As 2 and k are relatively prime, $\text{diag}(1, 0, \dots, 0) \in D$. Since all permutation matrices are in G , all the matrix unities e_{ij} are in D , so $D = M(n, R)$.

3.11. Lemma Suppose that K contains no odd roots of 1. Then $H(n, R)$ is not globally irreducible and the R -span of $H(n, R)$ does not coincide with $M(n, R)$.

Proof. Let I be a maximal ideal of R such that $2 \in I$, and let $F = R/I$. Let X be the projection of $H(n, R)$ in $M(n, F)$. Then X consists of all permutation matrices. It is clear that X is not irreducible. By Lemma 2.3 the R -span of $H(n, R)$ is not $M(n, R)$.

3.12. Proposition Suppose that K contains no odd roots of 1. Let $G \subset GL(n, K)$ be conjugate (in $GL(n, K)$) to a subgroup of $H(n, K)$. Then G is not globally irreducible.

Proof. Let $\phi : G \rightarrow GL(n, K)$ be the identical representation of G . Then ϕ is induced from a one-dimensional representation τ of a subgroup H of G . Set $X = \tau(H)$. Then X is cyclic; let x be a generator of X , and let h be an element of H such that $\tau(h) = x$. Then $x \in K$ is an eigenvalue of h ; by Lemma 3.9 $x \in R$. The standard construction of an induced representation shows that G can be realized over R , i.e. G is conjugate in $GL(n, K)$ with a subgroup of $H(n, R)$. By Lemma 3.11 G is not globally irreducible.

3.13. Lemma (see [Fr], Theorem 4.3). Let L be a Galois extension of a field K , and $l = L : K$. Let R, T be the rings of integers in K, L , respectively. Suppose that l is odd and L is non-ramified over K for every prime. Then T is a free R -module.

3.14. Proposition Let L be a field extension of K and let $l = L : K$. Suppose that l is odd and for every $p \in \pi$ we have $KL_{\pi \setminus p}^* = L$ (i.e. $L_{\pi \setminus p}^*$ spans L over K). Then $M(n, R)$ is a Schur ring for every n that is a multiple of l .

Proof. Let p be a prime. As L can be obtained from K by adding certain p' -roots of 1, L is non-ramified over p . Also, L is cyclotomic, so L/K is an abelian Galois extension. Set $\Gamma = \text{Gal}(L/K)$.

Let T be the ring of integers of L . By Lemma 3.13 T is a free R -module. Observe that T is Γ -stable so one can consider the cross product $V = T * \Gamma$ of T and Γ with trivial set of factors, i.e. V is a free left T -module formed by the set of all expressions $\sum_{\gamma \in \Gamma} t_\gamma \gamma$ where $t_\gamma \in T$, with multiplication determined by $\gamma t = \gamma(t)\gamma$ for $t \in T$. We can turn T to a V -module by defining an action of an element $v = \sum t_i \gamma_i$ (where $t_i \in T, \gamma_i \in \Gamma$) on T as follows: $v \circ t = \sum t_i \gamma_i(t)$ where $t \in T$ and $t \rightarrow \gamma_i(t)$ is the Galois action. Obviously, T is a faithful V -module, so we can view V as a subring of $GL(l, R)$. The subring R of T acts on T by scalar multiplication, so $R \cdot \text{Id} \subset V$. To show that $M(l, R)$ is a Schur ring, by Proposition 2.5 it suffices to prove that V/VI is isomorphic to $M(l, R/I)$ for every maximal ideal I of R . As L/K is non-ramified, $\bar{T} = T/IT$ is semisimple of dimension l over $F = R/I$ and Γ acts faithfully on \bar{T} (see, for instance [L], §5, Proposition 11). By Galois theory, Γ acts transitively on maximal ideals of T containing I so Γ acts transitively on maximal ideals of \bar{T} . Let J_1, \dots, J_m be minimal ideals of \bar{T} , and e_i the idempotent of J_i for $i = 1, \dots, m$. Then $\bar{V} = \bar{T} * \Gamma$. It is well known that \bar{V} is a simple ring. This can be seen as follows.

By the above, Γ acts transitively on J_1, \dots, J_m . Suppose that U is a non-zero ideal of \bar{V} , and let $0 \neq u = \sum_{\gamma \in \Gamma} t_\gamma \gamma \in U$ with $t_\gamma \in \bar{T}$ be an element with minimum number of non-zero summands. By replacing u by $u\gamma$ with some $\gamma \in \Gamma$ one can assume that $t_1 \neq 0$. One can assume that $0 \neq e_1 t_1 \in J_1$ by replacing u by $e_1 \gamma u \gamma^{-1}$ with a suitable $\gamma \in \Gamma$. By minimality of u for every $t \in J_1$ we have $tu - ut = 0$, so $t_\gamma(t - \gamma(t)) = 0$ for all $\gamma \in \Gamma$. This implies that $\gamma(t) = t$ for all $t \in J_1$ and $\gamma \in \Gamma$ such that $t_\gamma \neq 0$. It follows that these γ belong to Γ_1 where Γ_1 is the stabilizer of J_1 in Γ . As Γ is abelian and

transitive on J_1, \dots, J_m , we have $\Gamma : \Gamma_1 = m$ so $|\Gamma_1| = l/m$. By a dimension reason $J_1 : F = l/m$. Therefore, Γ_1 is the Galois group of J_1/F . Hence $\gamma(t) = t$ for $t \in J_1$ and $\gamma \in \Gamma_1$ implies $\gamma = 1$ or $t \in F$, i.e. $J_1 \cong F$. The latter implies that $\Gamma_1 = 1$. In both the cases we obtain $u \in J_1$. As J_1 is a field, $J_1 \subset U$. Then $\bar{T} \subset U$. This is impossible as \bar{T} contains the identity of $\bar{T} * \Gamma$.

3.15. Proposition If $M(n, R)$ is not a Schur ring then there exists a quadratic extension K_1 of K with the ring of integers R_1 such that $M(n, R_1)$ is a Schur ring.

Proof. One can take $K_1 = K(\varepsilon)$ where $\varepsilon^3 = 1$, $\varepsilon \neq 1$. Observe that $\varepsilon \notin K$ by 3.10 as $M(n, K)$ is not a Schur ring. Therefore, $K_1 : K = 2$. By 3.10 $M(n, R_1)$ is a Schur ring.

§4. Globally irreducible representations of prime degrees and Schur rings

In this section p denote a prime integer.

4.1. Lemma Let $G \subset GL(p, K)$ be an irreducible subgroup and N a normal subgroup of G . Then N is either absolutely irreducible or abelian. If N abelian then N is either irreducible or diagonalizable.

Proof. If N is reducible then by Clifford's theorem irreducible constituents of N are of the same dimension $d < p$. This implies $d = 1$, i.e. N is diagonalizable. If N is not abelian then N can not be diagonalized under any field extension, i.e. N remains irreducible and hence is absolutely irreducible.

Recall that $H(p, K)$ denotes the group of monomial $n \times n$ -matrices over K .

4.2. Lemma Let $G \subset GL(p, K)$ be an absolutely irreducible subgroup. Then one of the following holds:

- (A) G is imprimitive and is conjugate to a subgroup of $H(p, K)$;
- (B) G is primitive and contains a non-central abelian normal subgroup A such that $P = KA$ is a field, and then $P : K = p = |G/A|$;
- (C) G contains a non-abelian normal irreducible p -subgroup N , and $|N/Z(N)| = p^2$;
- (D) G contains a quasi-simple normal irreducible subgroup.

Proof. Let V be the underlying space of $GL(n, K)$. Suppose first that G is imprimitive. Then V is a direct sum of subspaces, say, V_1, \dots, V_k , $k > 1$, such that $gV_i = V_{j(g)}$ for $g \in G$, and the action of G on the V_i 's by conjugation is transitive. Hence $k \cdot \dim V_i = p$ so $k = p$ and $\dim V_i = 1$ for $i = 1, \dots, k$. Therefore, G is conjugate to a subgroup of $H(p, K)$.

Next, suppose that G is primitive. Let N be a minimal non-central normal subgroup of G . As G is primitive, KN is a simple K -algebra by Clifford's theorem. Since N is not scalar, N is irreducible by 4.1. Suppose first that N is abelian. Then $L = KN$ is a field, and V is irreducible as an L -module. It follows that $L : K = p$. Set $A = G \cap L$ so $A = C_G(N)$. Then the conjugation action of G on L induces an embedding $G/A \rightarrow \text{Gal}(L/K)$, so $|G/A| = p$ or $G = A$. In the last case G is abelian, and then G fails to be absolutely irreducible. So we arrive at (B).

Now suppose that N is not abelian. If $N/Z(N)$ is abelian then we have (C) by Theorem 4.4 in [Dix]. Assume $N/Z(N)$ is not abelian. Then $N/Z(G)$ is a direct product of simple non-abelian groups. As above, every non-central normal subgroup of N is irreducible. Hence by Schur's lemma $N/Z(G)$ must be simple. Then N' , the commutator subgroup of N , is quasi-simple, and we obtain (D).

4.3. Proposition Let $G \subset GL(p, K)$, $p > 2$, be globally irreducible. Suppose that K contains no odd root of 1. Then one of the following holds:

- (i) G has an abelian normal subgroup A of index p such that $A/Z(G)$ is not of prime power order;
- (ii) G contains a primitive globally irreducible normal simple subgroup.

Proof. Suppose first that G is imprimitive. From 4.2(A) we deduce that G is conjugate to a subgroup of $H(p, K)$. By 3.12 G can not be globally irreducible. This is a contradiction.

Let G be primitive so 4.2(A) does not hold. If 4.2(B) holds then $L = KA$ is a field. If $A/Z(G)$ is of prime power order, say, r^α where r is a prime, then $A = Z(A) \cdot \text{Syl}_r(A)$. It follows that $G/\text{Syl}_r(A)$ is abelian. This is impossible by Lemma 2.4. So we obtain (i).

Assume 4.2(C) holds. Let P be a non-abelian normal irreducible p -subgroup of G . Then $Z(P)$ is scalar, so G contains a scalar matrix of order p . Hence K contains a primitive p -root of 1, which contradicts the assumption.

Assume 4.2(D) holds. Let N be an irreducible normal quasi-simple subgroup of G . By 4.1 N is absolutely irreducible so $Z(N)$ is scalar by Schur's lemma. As N is quasi-simple, $N \subset SL(p, K)$. Then $|Z(N)|$ divides p , hence either $Z(N) = 1$ or K contains an odd root of 1. The second case does not hold by assumption. We are left to prove that N is globally irreducible. Let r be a prime such that $N(\text{mod } r)$ is reducible. Set $\bar{G} = G(\text{mod } r)$ and $\bar{N} = N(\text{mod } r)$. Then \bar{G} is irreducible so \bar{N} is completely reducible by Clifford's theorem. As the dimensions of the irreducible constituents of \bar{N} divide p , these are equal to 1. Then \bar{N} is abelian. As the kernel of the reduction modulo r is an r -group, N is solvable, which is a contradiction. So we have (ii).

4.4. Corollary Suppose that K contains no odd root of 1, $p > 2$ and $M(p, R)$ is a Schur ring. Then either $M(p, R) = RG$ where G is simple and primitive or there exists a Galois extension L of K such that $L : K = p$ and L_π/K_π contains elements of relatively prime orders.

Remark The group $A/Z(G)$ in 4.3 and L_π/K_π in 4.4 contains no element of order p , as K has no p -root of 1. (Indeed, if $x \in A \setminus Z(G)$ and $y \in G \setminus A$ then $xyx^{-1}y^{-1}$ is an element of order p in K . Similarly for 4.4.)

4.5. Proposition Suppose that there exists an extension L of K such that $L : K = p > 2$ and L_π/K_π contains elements of relatively prime finite orders. Then $M(p, R)$ is a Schur ring.

Proof. As $L : K = p$ is prime, $KS = L$ for any subgroup $S \subseteq L^*$ such that $S \not\subseteq K$. Since L_π/K_π contains elements of relatively prime finite orders, the hypothesis of Lemma 3.14 holds, so claim follows from 3.14.

4.6. Theorem [DZ]. Let $p > 2$ and let G be a primitive quasi-simple finite irreducible subgroup of $GL(p, \mathbf{C})$. Then one of the following holds:

- (1) $G \cong PSL(2, p)$;
- (2) $G \cong PSL(2, q)$, where $q > 3$ is such that $p = (q - 1)/2$ with q prime or 3-power, or $p = (q + 1)/2$;
- (3) $G \cong PSL(2, q)$ where q is such that $p = q - 1$;
- (4) $G \cong PSp(2l, q)$ where q is such that $p = (q^l + 1)/2$, $l > 1$;
- (5) $G \cong PSp(2l, 3)$ where l is such that $p = (3^l - 1)/2$;
- (6) $G \cong PSU(l, q)$ where q, l are such that $p = (q^l + 1)/(q + 1)$;

- (7) $G \cong A_{p+1}$;
- (8) $p = 3$, $G \cong 3 \cdot Alt(6)$, the 3-fold cover of the alternating group;
- (9) $p = 7$, $G \cong PSp(6, 2)$,
- (10) $p = 11$, $G \cong M_{12}$;
- (11) $p = 23$, $G \cong M_{24}, Co_2, Co_3$.

4.7. Lemma [TZ] Every complex irreducible representation of the group $Sp(2n, q)$, $n \geq 1$, q odd, of degree $(q^n \pm 1)/2$, and of the group $SU(n, q)$, n odd, of degree $(q^n + 1)/(q + 1)$ is realized via a Weil representation.

4.8. Proposition Let G be as in Theorem 4.6. Then G is globally irreducible exactly in the following cases:

- (1) $p = 3$, $G \cong 3 \cdot Alt(6)$, the 3-fold cover of the alternating group;
- (2) $G \cong PSL(2, q)$ with $p = (q - 1)/2$ and q being an odd prime;
- (3) $G \cong PSp(2l, 3)$ with $p = (3^l - 1)/2$ where $l > 1$ is an odd prime.

Proof. In view of Lemma 4.7 every irreducible representation of $Sp(2l, q)$ or $SU(l, q)$ in 4.6 is a Weil representation. Let $q = r^\alpha$ where r is a prime. The fact that for r odd the Weil representation of $Sp(2l, r)$ of degree $(r^l - 1)/2$ is irreducible under reduction modulo r is proved in [SZ], for primes other than r this is shown in [Ward]. The Weil representations of $SU(l, q)$, as well as of $Sp(2l, q)$ for $q \neq r$, are reducible modulo r , see [Z] where the composition factors of the Weil representations under reduction modulo r are determined. The Weil representations of $Sp(2l, r)$ of degree $(r^n + 1)/2$ are reducible modulo 2, see [Ward]. For the groups $PSL(2, q)$ the proposition follows by inspection of the decomposition matrices given in [Sr] for the prime r , and in [Burk] for other primes. For $G = A_{p+1}$ it is well known that the irreducible representation of G of degree p is reducible modulo p . For other groups in 4.6 one can inspect [MAT].

Proof of Theorem 1.7 If G is quasi-simple, then the claim follows from 4.8. Suppose that G is not quasi-simple. Let H be a minimal non-central normal subgroup of G . By 4.1 H is irreducible. Hence H is not abelian. Moreover, H is globally irreducible. (Otherwise, there is a prime r such that $\bar{H} = H(\text{mod } r)$ is reducible, while $\bar{G} = G(\text{mod } r)$ remains irreducible. By Clifford's theorem, \bar{H} is completely reducible, so \bar{H} is abelian as p is a prime.

Hence $X = \ker(H \rightarrow \bar{H})$ is non-scalar normal r -subgroup of G . As G is primitive, X is non-abelian and irreducible (see 4.1). Then $r = p > 2$. This contradicts Theorem 2.8.)

Thus, H is globally irreducible. Therefore, H belongs to the list given in 4.8. Suppose that $G \neq HZ(G)$. By [ATL] this is impossible in case (1) of 4.8. In cases (2) and (3) every outer automorphism arrives from an inner automorphism of $PGL(2, q)$ and $PGSp(2l, 3)$, respectively. The latter group is the central quotient of $GSp(2l, 3)$ which is defined as follows. If σ is an automorphism of $GL(2l, 3)$ whose fixed point subgroup is $Sp(2l, 3)$ then $GSp(2l, 3) = \{x \in GL(2l, 3) : \sigma(x) = xs\}$ where s is a scalar matrix depending on x . By [Ward] $PGSp(2l, 3)$ can not be embedded into $GL(p, \mathbf{C})$. The same is true for $PGL(2, q)$ which has no complex representation of degree $(q - 1)/2$.

4.9. Lemma Let $p > 2$ be a prime, $G \subset GL(p, \mathbf{C})$ a primitive quasi-simple globally irreducible subgroup, and let $Tr(G)$ denote the least subfield of \mathbf{C} containing the traces of all matrices of G . Then one of the following holds:

- (i) $G \cong PSL(2, q)$ with q prime, $p = (q - 1)/2$ and $Tr(G) = \mathbf{Q}(\sqrt{-q})$.
- (ii) $G \cong PSp(2l, 3)$, $p = (3^l - 1)/2$ and $Tr(G) = \mathbf{Q}(\sqrt{-3})$;
- (iii) $G \cong 3 \cdot Alt(6)$ and $Tr(G) = \mathbf{Q}(\sqrt{-3})$.

Proof. The claim about G is contained in 4.8. Let χ be the character of G . For $G \cong 3 \cdot Alt(6)$ the values of χ can be found in [ATL]. By 4.7 the groups $PSp(2l, 3)$ and $PSL(2, q) \cong PSp(2, q)$ are realized in 4.6 via a Weil representation. By [Go] $Tr(G) = \mathbf{Q}(\sqrt{-3})$ for $G = PSp(2l, 3)$. It is well known that $Tr(G) = \mathbf{Q}(\sqrt{-q})$ for the representations of $G = PSL(2, q)$ of degree $(q - 1)/2$.

Remark. The ring of integers of $\mathbf{Q}(\sqrt{-3})$ coincides with $\mathbf{Z}[(-1 + \sqrt{-3})/2] = \mathbf{Z}[\omega]$ where ω is a primitive 3-root of 1.

Proof of Theorem 1.8 The "if" part. If (i) or (ii) holds then $M(p, R)$ is a Schur ring by 3.10 and 4.5, respectively. Let (iii) hold. Set $G = PSL(2, q)$ where $q = 2p + 1$. It well known that G has a complex irreducible representation of degree p . As $p > 2$, the \mathbf{Q} -Schur index of G is 1. Hence G can be realized over $K = Tr(G) = \mathbf{Q}(\sqrt{-q})$. Let R be the ring of integers of K . We show that G can be realized over R . Suppose not, then by 3.6 p divides ν , the

class ideal number of $\mathbf{Q}(\sqrt{-q})$. As $p = (q-1)/2$ is prime, $q \equiv 3 \pmod{4}$. Let a (resp., b) be the number of quadratic residues (resp., non-quadratic residues) modulo q between 1 and p . By [BS], see Theorem 4 in §4, Ch. 5, $\nu = a - b$, if $q \equiv 7 \pmod{8}$, and $\nu = (a - b)/3$, if $q \equiv 3 \pmod{8}$. It follows that the condition above implies $\nu = p = (q - 1)/2$, whence $q \equiv 7 \pmod{8}$, $b = 0$, $a = p$. This means that $1, \dots, p = (q - 1)/2$ are quadratic residues modulo q . Then $p+1, \dots, q-1$ are quadratic non-residues modulo q . Therefore, there exists a natural number m such that $m^2 < (q+1)/2$ and $(m+1)^2 > q-1$. This implies that $2m^2 - 1 < q < m^2 + 2m + 2$, whence $m^2 - 2m - 3 = (m - 3)(m + 1) < 0$. Hence $m \leq 2$, so $q < 10$. Then $q = 7$, however, in this case $b = 1$, contrary to the above. It follows that $(\nu, p) = 1$ and G can be realized over the ring of integers of $\mathbf{Q}(\sqrt{-q})$. By 4.8 G is globally irreducible. By 1.7 $RG = M(n, R)$.

The “only if” part. Let $M(p, R)$ be a Schur ring. Suppose that (i) does not hold. By 4.4 either (ii) holds, or $M(p, R) = RG$ for a primitive finite simple subgroup $G \subset GL(p, R)$. By Theorem 1.4 G is globally irreducible. By 4.9 either (iii) holds, or R contains a primitive 3-root of 1 which case is involved in (i).

Remark. The class ideal number of $\mathbf{Q}(\sqrt{-3})$ is equal to 1 (see [BS]) so $G \cong PSp(2l, 3)$ can be realized over the ring of integers of $\mathbf{Q}([\sqrt{-3}])$. By 4.8 G is globally irreducible. By Theorem 1.7 $RG = M(n, R)$. Observe that the ring of integers of $\mathbf{Q}([\sqrt{-3}])$ is $\mathbf{Z}[(-1 + \sqrt{-3})/2]$. It follows that the group ring $\mathbf{Z}[(-1 + \sqrt{-3})/2]G$ where $G \cong PSp(2l, 3)$ has $M((3^l - 1)/2, \mathbf{Z}[(-1 + \sqrt{-3})/2])$ as a quotient ring.

REFERENCES

- [BS] Z. Borevich, I. Shafarevich, *Number theory*, Academic Press, Orlando, 1966.
- [Bu] V. Burichenko, Invariant lattices in the Steinberg module and their isometry groups, Russian Acad. Sci. Sb. Math. 80(1995), 519-529.
- [Burk] B. Burkhardt, Die Zerlegungsmatrizen der Gruppen $PSL(2, p^f)$, J. Algebra 40(1976), 75-96.
- [CRW] G. Cliff, J. Ritter, A. Weiss, Group representations and integrality, J. fur die reine und angew. Math. 426(1992), 193-202.

- [ATL] J. Convey, R. Curtis, S. Norton, R. Parker, R. Wilson. *Atlas of Finite Groups*, Clarendon Press, Oxford, 1985.
- [CR] Ch. Curtis, I. Reiner, *Representation Theory of Finite Groups and Associative Algebras*, Interscience publ., N.Y. 1967.
- [CR2] Ch. Curtis, I. Reiner, *Methods of representation theory, vol.1*, Wiley, New York, 1981.
- [MI] F. De Meyer, E. Ingraham, *Separable Algebras over Commutative Rings*, Springer Lecture Notes, vol.181, Berlin, 1971.
- [DTZ] L. Di Martino, C. Tamburini, A. Zalesskiĭ, Carter subgroups in classical groups, *J. London Math. Soc. (2)* 55(1997), 264 - 276.
- [Dix] J. Dixon, *The Structure of Linear Groups*, Van Nostrand Reinhold Company, London-New York-Ottawa, 1971.
- [DZ] J. Dixon, A.E. Zalesskiĭ, Primitive finite linear group of prime degrees, *J. London Math. Soc.* (to appear).
- [DZ2] J. Dixon, A.E. Zalesskiĭ, Monomial complex irreducible finite linear groups of prime degrees (In preparation).
- [Fr] A. Fröhlich, Discriminants of algebraic number fields, *Math. Z.* 74(1960), 18 - 28.
- [Ge] P. Gerardin, Weil representations associated with finite fields, *J. Algebra* 46(1977), 54-101.
- [Go] R. Gow, Even unimodular lattices associated with the Weil representation of the finite symplectic group, *J. Algebra* 122(1989), 510-519.
- [Gr] B.H. Gross, Group representations and lattices, *J. Amer. Math. Soc.* 2(1990), 929 - 960.
- [MAT] J. Jansen, K. Lux, R. Parker, R. Wilson, *An Atlas of Brauer Characters*, Clarendon Press, Oxford, 1995.
- [L] S. Lang, *Algebraic Number Theory*, Springer-Verlag, Berlin, 1986.
- [L1] S. Lang, *Algebra*, Addison-Wesley, Reading, 1965.
- [Ne] P. Nelis, Schur and projective Schur algebras over Dedekind domains, Thesis, Univ of Antwerp, 1991.

- [Ne2] P. Nelis, Schur and projective Schur group of number rings, *Can. J. Math.* 43(3)(1991), 540-558.
- [Ne3] P. Nelis, The Schur group conjecture for the ring of integers of a number field, *Proc. Amer. Math. Soc.* 114(1992), 307-318.
- [NO] P. Nelis, F. van Oystaeyen, The projective Schur subgroup of the Brauer group and root groups of finite groups, *J. Algebra* 137(1991), 501-518.
- [FVO] F. Van Oystaeyen. On Clifford systems and generalized crossed products, *J. Algebra* 87(1984), 396 - 415.
- [Ro] L.H. Rowen, "Polynomial identities in Ring Theory", Academic Press, New York, 1980.
- [Sr] B. Srinivasan, On the modular characters of the special linear group $SL(2, p^n)$, *Proc. London Math. Soc.* (3) 14(1964), 101-114.
- [T1] Pham Huu Tiep, Globally irreducible representations of the finite symplectic group $Sp_4(q)$, *Comm. in Algebra* 22(1994), 6439 - 6457.
- [T2] Pham Huu Tiep, Basic spin representations of $2 \cdot S_n$ and $2 \cdot A_n$ as globally irreducible representations, *Archiv Math.* 64(1995), 103 - 112.
- [T3] Pham Huu Tiep. Globally irreducible representations of $SL_3(q)$ and $SU_3(q)$, *Isr. J. Math.* (submitted).
- [T4] Pham Huu Tiep, Weil representations as globally irreducible representations, *Math. Nachr.* 184(1997), 313 - 327.
- [T5] Pham Huu Tiep, Globally irreducible representations of finite groups and integral lattices, *Geomet. Dedicata* 64(1997), 85 - 123.
- [TZ] Pham Huu Tiep, A.E. Zalesskiĭ, Minimal characters of the finite classical groups, *Comm. in Algebra* 24(1996), 2093 - 2167.
- [Wa] A. Wagner, The faithful linear representation of least degree of S_n and A_n over a field of characteristic 2, *Math. Z.* 151(1976), 127-137.
- [Ward] H. Ward, Representations of symplectic groups, *Trans. Amer. Math. Soc.* 121(1966), 62-89.
- [Za] A.E. Zalesskiĭ, A fragment of the decomposition matrix of the special unitary group over a finite field, *Izv. AN SSSR, Ser. Math.* 54(1990), 26-44.

[SZ] A.E. Zalesskiĭ, I.D. Suprunenko, Representations of degree $(p^n \pm 1)/2$ of the symplectic group of degree $2n$ over a field of characteristic p (in Russian), Vesti Acad. Nav. Belarus. SSR, Ser. fiz.-mat. navuk 1987, no.6, 9-15.