Can. J. Math.Vol. **43** (3), 1991 pp. 540–558

SCHUR AND PROJECTIVE SCHUR GROUPS OF NUMBER RINGS

PETER NELIS

Introduction. The Schur or projective Schur group of a field consists of the classes of central simple algebras which occur in the decomposition of a group algebra or a twisted group algebra. For number fields, the projective Schur group has been determined in [8], whereas the Schur group is extensively studied in [25]. Recently, some authors have generalized these concepts to commutative rings. One then studies the classes of Azumaya algebras which are epimorphic images of a group ring or a twisted group ring. Though several properties of the Schur or projective Schur group defined in this way have been obtained, they remain rather obscure objects. Apart from some examples in [3] and [4] and the determination of the Schur group for the $\mathbb{S}$ integers of a cyclotomic number field in [16], no concrete calculations have been carried through. Since a complete classification of the finite subgroups of the multiplicative group of the quaternions is known, we use this to describe all Schur algebras embeddable in a quaternion algebra over a number field. This classification also allows us to describe number rings having a non-trivial projective Schur algebra embeddable in a quaternion field, though one has to apply some techniques of projective representation theory in order to reduce information of the twisted case to the untwisted one. It turns out that many projective Schur algebras may be obtained by a small deformation of a Schur algebra, but a set of examples is given to show that this is not true in general. All this is being dealt with in § 2. In § 3, we show that the groups which span a Schur algebra are always subgroups of the automorphism groups of a modular quadratic or hermitian form. In case the number ring is $\mathbb{Z}$, these quadratic forms are moreover even and positive definite. As a consequence, $M_n(\mathbb{Z})$ is not a Schur algebra if $8 \not| n$ and $n \neq 1$, whereas for fields, $M_n(k)$ is always a Schur algebra. One may now wonder whether it is possible to represent Schur algebras by means of easy groups. We finally prove that nilpotent groups are not apt to fulfill this task, but an example shows that solvable groups may span a Schur algebra.

1. **The Schur- and projective Schur group of number rings.** Throughout, K is a number field, R its ring of integers, G a finite group, $c \in Z^2(G, R^*)$, i.e. c is a 2-cocycle on G with values in the units of R, ϵ_n is an n-th root of unity, $\theta_n = \epsilon_n + \bar{\epsilon}_n$ an unadorned tensor product is over R.

Research assistant of the N.F.S.R.

Received by the editors February 5, 1990; revised: January 2, 1991 .

DEFINITION 1.1. A Schur algebra A over R is an Azumaya algebra which is an epimorphic image of some group ring RG. We call A a projective Schur algebra if A is the epimorphic image of a twisted group ring RG^c.

DEFINITION 1.2. The Schur group $S(R)$ of R is the group consisting of the Brauer classes of Schur algebras. A similar definition holds for the projective Schur group $PS(R)$.

Clearly, R itself is always a Schur algebra and a fortiori a projective Schur algebra. We will call it the trivial Schur or projective Schur algebra and it will be excluded in most of our considerations. If A is a Schur algebra, then $K \otimes A$ is epimorphic image of $K \otimes RG$, hence $[K \otimes A]$, its class in $\mathrm{Br}(K)$, is an element of $S(K)$. Since the natural map $\mathrm{Br}(R) \longrightarrow \mathrm{Br}(K)$ is injective, (cf. [12], p. 57 Theorem 6.19) this proves that $S(R) \subseteq \mathrm{Br}(R) \cap S(K)$. Similarly $PS(R) \subseteq \mathrm{Br}(R) \cap PS(K)$. By a theorem of Lorenz and Opolka (cf. [8]), $PS(K) = \mathrm{Br}(K)$. If K' is the maximal subcyclotomic number field contained in K and $R' = R \cap K'$, then it has been proved in [15] that $S(R) = \{[R \otimes_{R'} A'], A'$ is a Schur algebra over $R'\}$, in analogy with a similar theorem for fields. This reduces the calculation of $S(R)$ to the subcyclotomic case, for which there is the following more general conjecture:

CONJECTURE 1.3. *If T is the ring of $\mathbb{S}$ integers of a subcyclotomic number field K, where $\mathbb{S}$ is any finite set of places, then $S(T) = \mathrm{Br}(T) \cap S(K)$ and $PS(T) = \mathrm{Br}(T)$*

This conjecture has been proven when T is the ring of integers of K in [11]. If K has no real embeddings and R is the ring of integers of K, then $\mathrm{Br}(R) = 0$. In what follows, we will therefore assume that K has at least one real embedding. This certainly implies that $t(R^*) = \{\pm 1\}$, where t denotes the torsion group of R^*. Note that $\mathrm{Br}(R) \cap S(K) \subseteq C_2$, the cyclic group of order 2. Indeed, any element $[A] \in \mathrm{Br}(R) \cap S(K)$ vanishes at the finite places of R, since A is Azumaya. (cf. [12], p. 76 Proposition 6.34). Also $\mathrm{Inv}[A] = 0$ or $\mathrm{Inv}[A] = 1/2$ at the infinite places. Moreover, the invariants of A at the infinite places are all equal, by a theorem of Benard and Schacher. (cf. [25], p. 89 Theorem 6.1.). This proves our assertion. If K is a subcyclotomic extension of $\mathbb{Q}$, then equality holds if and only if K has an even number of real places. This condition is clearly necessary, by the above discussion on the Hasse invariants of $[A]$ and by Hasse's sum Theorem. If K has an even number of real places and K is subcyclotomic, then K contains a quadratic extension L. Let p be a prime of $\mathbb{Z}$ which ramifies in L or with even residue degree. Then $K \otimes \left(\frac{\mathbb{Q}(\epsilon_p), -1}{\mathbb{Q}}\right)$ is a central simple, cyclic K algebra and its class is a non-trivial element of $\mathrm{Br}(R) \cap S(K)$. This proves the equality $\mathrm{Br}(R) \cap S(K) = C_2$ in this case. In order to prove the equality $S(R) = \mathrm{Br}(R) \cap S(K)$, it is therefore sufficient to find one Schur algebra over R with a non-trivial class. These can often be found using the following theorem.

THEOREM 1.4 (AUSLANDER GOLDMAN). *Let L be a Galois extension of K, with Galois group $\mathcal{G}$ and ring of integers S, let $d \in Z^2(\mathcal{G}, S^*)$ and $A = \oplus_{\sigma \in \mathcal{G}} S u_\sigma$, the R order such that $u_\sigma s = \sigma(s) u_\sigma$, $u_\sigma u_\tau = d(\sigma, \tau) u_{\sigma\tau}$. Then A is Azumaya if and only if S is unramified over R.*

PROOF. Cf. [13], p. 374, Theorem 40.14. The same proof holds, showing that the difference of A is equal to 1 if and only if S is unramified over R. But then A only ramifies at the infinite places, i.e., A is Azumaya. ∎

NOTATION 1.5. *With notations as in Theorem 1.4, let L be a quadratic extension of K and let T be an R algebra such that $R \subseteq T \subseteq S$ and T is stable under the unique non-trivial K automorphism σ of L. Furthermore, let d be the normalized 2-cocycle such that $d(\sigma,\sigma) = \beta$ for some $\beta \in R^*$. Then we write $\binom{T\beta}{R}$ for $\oplus_{\sigma\in\mathcal{G}} Tu_\sigma$.*

Most examples of Schur algebras were constructed using Theorem 1.4. However, for $R = \mathbb{Z}[\sqrt{2}]$, there does not exist any unramified extension, but there exists a non-trivial Schur algebra over R, which is embeddable in a quaternion algebra over K. In the next paragraph, we investigate which Schur or projective Schur algebras can be constructed in this way.

Let $\mathbb{S}$ be any finite set of places of K and let $R_{\mathbb{S}}$ be the ring of $\mathbb{S}$ integers of K. The equality $S(R_{\mathbb{S}}) = \mathrm{Br}(R_{\mathbb{S}}) \cap S(K)$ has recently been proved for $R = \mathbb{Z}[\epsilon_n]$ by C. R. Riehm in [16]. However, in the cases we are interested in, $\mathbb{S}$ is the set of all Archimedian primes and the theorem then becomes trivial.

2. **Schur and projective Schur algebras embeddable in quaternion skew fields.** In this paragraph, we give necessary and sufficient conditions on R for the existence of non-trivial Schur or projective Schur algebras that are embeddable as subalgebras of a quaternion skew field over K. If $[B]$ is a Schur algebra or a projective Schur algebra such that $[B] \neq 0$ in $\mathrm{Br}(R)$, then $\mathrm{Index}(K \otimes B) = 2$, so $K \otimes B \cong M_n(D)$ for some $n \in \mathbb{N}$ and some quaternion skewfield D over K. Here we investigate the case $n = 1$.

THEOREM 2.1. *Let $\mathbb{H} = \mathbb{R} \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$. Any finite subgroup of $\mathbb{H}$ is conjugate to one of the following*

i A cyclic group of order n, $C_n = \langle \epsilon_n \rangle = \langle cos(2\pi/n) + sin(2\pi/n)i \rangle$
ii The quaternion group of order $4n$, $H_n = \langle \epsilon_{2n}, j \rangle$
iii The binary tetraedral group of 24 elements,

$$E_{24} = \{\pm 1, \pm i, \pm j, \pm k, (\pm 1 + \pm i + \pm j + \pm k)/2\}$$

iv The binary octaedral group of 48 elements,

$$E_{48} = E_{24} \cup \{(\pm\alpha \pm \beta)/\sqrt{2}; \{\alpha,\beta\} \in \mathcal{P}_2(\{1,i,j,k\})\}$$

v The binary icosaedral group of 120 elements

$$E_{120} = E_{24} \cup \{x/2; x = yz, y \in E_{24}, z = i + \big((1+\sqrt{5})/2\big)j + \big((-1+\sqrt{5})/2\big)k\}$$

PROOF. Cf. [24], p. 17, Theorem 3.7. ∎

The names of the E_i have been chosen so that they are isomorphic to the group of isometries under which the corresponding geometrical object is stable. In particular, E_{48}

is isomorphic to the group of isometries of an octaeder. Now take three vertices of one face of the octaeder and call them 1, 2, 3 respectively. The opposite vertices will then be called $-1, -2, -3$ respectively. In this way, E_{48} may be viewed as the group of signed permutations on 3 elements, $C_2^3 \rtimes S_3$. This description will reappear later on. Other noteworthy isometries are $E_{24} \cong \mathrm{Sl}_2(\mathbb{F}_3)$ and $E_{120} \cong \mathrm{Sl}_2(\mathbb{F}_5)$, cf. [24], p. 17.

DEFINITION 2.2. $n \in \mathbb{N}$ is truly composite if and only if either n is divisible by at least two odd primes or $4|n$ and n is divisible by at least one odd prime.

LEMMA 2.3. *The field $\mathbb{Q}(\epsilon_n)$ is unramified over $\mathbb{Q}(\theta_n)$ if and only if n is truly composite.*

PROOF. The discriminant of $\mathbb{Q}(\epsilon_n)$ over $\mathbb{Q}(\theta_n)$ is $(\epsilon_n - \bar{\epsilon}_n)^2$. Now $(\epsilon_n - \bar{\epsilon}_n)^2 \in \mathbb{Z}[\theta_n]^*$ if and only if $(1-\epsilon_n^2) \in \mathbb{Z}[\epsilon_n]^*$. Let Φ_n denote the n-th cyclotomic polynomial.

CASE 1. n odd. If $n = p^r$, then $\mathbb{Q}(\epsilon_{p^r})/\mathbb{Q}$ is totally ramified and the Lemma is true. Otherwise, $\Phi_n(1) = \prod_{d=1,(d,n)=1}^{n}(1-\epsilon_n^d) = (1-\epsilon_n^2)\cdot x$, for some $x \in S$. By differentiating the equality $\prod_{d|n}\Phi_d = X^n - 1$, evaluating it for $X = 1$ and using induction, one easily proves that $\Phi_{p^r}(1) = p$ for p prime and $\Phi_n(1) = 1$ if n is divisible by two primes. Since $\Phi_n(1) = \mathbb{N}(1-\epsilon_n) = \mathbb{N}(1-\epsilon_n^2)$, where $\mathbb{N}$ denotes the norm for the extension $\mathbb{Q}(\epsilon_n)/\mathbb{Q}$, this proves the Lemma for this case.

CASE 2. $4|n$. Then $\epsilon_n^2 = \epsilon_{n/2}$. As above, one proves that $1-\epsilon_{n/2}$ is a unit if and only if n is divisible by an odd prime. ∎

LEMMA 2.4. *Let $K \subseteq L$ be an extension of number fields, with rings of integers R and S respectively. Then an algebra A is Azumaya over R if and only if $S \otimes A$ is Azumaya over S.*

PROOF. If A is Azumaya over R, then $S \otimes A$ is Azumaya over S, by a classical theorem on Azumaya algebras. Conversely, if A is not Azumaya, then $\mathrm{disc}(A/R) \neq R$, $\mathrm{disc}(S \otimes A/S) = \mathrm{disc}(A/R)S \neq S$ and $S \otimes A$ is not Azumaya over S. ∎

THEOREM 2.5. *Let K be a number field having a real embedding. Then a non-trivial Schur algebra over R is embeddable in a quaternion skew field over K if and only if K satisfies one or more of the following:*

i $\mathbb{Q}(\theta_n) \subseteq K$, *n truly composite.*
ii $\mathbb{Q}(\sqrt{2}) \subseteq K$
iii $\mathbb{Q}(\sqrt{5}) \subseteq K$

The corresponding Azumaya algebras A are:

i $\left(\frac{R[\epsilon_n]\ -1}{R}\right)$
ii $A \cong R\langle 1, (1+i)/\sqrt{2}, (1+j)/\sqrt{2}, (1+i+j+k)/2\rangle$
iii $A \cong R\langle 1, \left(-1+\sqrt{5}+2i+(1+\sqrt{5})j\right)/4, j, \left(-1-\sqrt{5}+(-1+\sqrt{5})j+2k\right)/4\rangle$

PROOF. If A is such a Schur algebra and $\pi: RG \twoheadrightarrow A$ is a representation, then, up to replacing G by $\pi(G)$ if necessary, we may assume that $\pi|G$ is faithful. Hence G is a finite subgroup of $\mathbb{R} \otimes_R A = \mathbb{H}$. The R order generated by G will be denoted by $R\langle G\rangle$. There are now five cases to consider, corresponding to the five types of finite subgroups of $\mathbb{H}$.

CASE 1. G is conjugate to C_n.
If $n \leq 2$, then $R\langle G\rangle$ is Azumaya over R, but it is trivial. If $n > 2$, then $R\langle G\rangle \neq R$ and $R\langle G\rangle$ is a commutative R algebra, hence it is not Azumaya over R.

CASE 2. G is conjugate to H_n.
Then $(\epsilon_n + \bar{\epsilon}_n) = \theta_n$ commutes with every element of H_n in A, hence with every element of $K \otimes A$. But $K \otimes A$ is central simple, so $\theta_n \in K$. Clearly, θ_n is integral over $\mathbb{Z}$, which shows that $\theta_n \in R$. Then $R\langle G\rangle \cong R \otimes_{\mathbb{Z}[\theta_n]} \left(\frac{\mathbb{Z}[\epsilon_n]-1}{\mathbb{Z}[\theta_n]}\right)$. According to Theorem 1.4 and Lemma 2.3 ,$\left(\frac{\mathbb{Z}[\epsilon_n]-1}{\mathbb{Z}[\theta_n]}\right)$ is Azumaya if and only if n is truly composite. Also, $R\langle G\rangle$ and $\left(\frac{\mathbb{Z}[\epsilon_n]-1}{\mathbb{Z}[\theta_n]}\right)$ are both Azumaya or not by Lemma 2.4, which proves the theorem in this case.

CASE 3. G is conjugate to E_{24}.
Since Azumaya algebras over $\mathbb{Z}$ are trivial, $\mathbb{Z}\langle E_{24}\rangle$ is not Azumaya. By Lemma 2.4, $R\langle E_{24}\rangle$ is not Azumaya.

CASE 4. G is conjugate to E_{48}.
Let $x = \frac{1+i}{\sqrt{2}} \in E_{48}$. A little calculation then shows that $x - x^3 = \sqrt{2}$, so $\sqrt{2} \in R$. Now $\operatorname{disc}(R\langle G\rangle / R) = \operatorname{disc}\langle 1, \frac{1+i}{\sqrt{2}}, \frac{1+j}{\sqrt{2}}, \frac{1+i+j+k}{2}\rangle = -1$. So $\mathbb{Z}[\sqrt{2}]\langle E_{48}\rangle$ is Azumaya and by Lemma 2.4, $R\langle E_{48}\rangle$ is Azumaya too.

CASE 5. G is conjugate to E_{120}
Let $A = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]\langle 1, \big(-1+\sqrt{5}+2i+(1+\sqrt{5})j\big)/4, j, \big(-1-\sqrt{5}+(-1+\sqrt{5})j+2k\big)/4\rangle$. This case is very similar to the previous one. One first shows that $\sqrt{5} \in R$ and that $A = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]\langle E_{120}\rangle$ is Azumaya over $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$. This may be done by a very cumbersome calculation of $\operatorname{disc}(A/\mathbb{Z}[\frac{1+\sqrt{5}}{2}])$. Alternatively, one may observe that $B = \left(\frac{\mathbb{Z}[\epsilon_5]-1}{\mathbb{Z}[\theta_5]}\right) \cong \mathbb{Z}[\frac{1+\sqrt{5}}{2}]\langle 1, (-1+\sqrt{5}+2i+(1+\sqrt{5})j)/4, k, \big((1+\sqrt{5})i-2j+(-1+\sqrt{5})k\big)/4\rangle \subseteq A$ and $C = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]\langle E_{24}\rangle \subseteq A$. But C is Azumaya at every prime $P \in \operatorname{Spec}(R)$ such that $2 \notin P$. On the other hand, B is Azumaya at every prime $P \in \operatorname{Spec}(R)$ such that $5 \notin P$, since $\mathbb{Z}[\epsilon_5]/\mathbb{Z}[\theta_5]$ is only ramified at the unique prime above 5. Therefore, A is Azumaya at every prime $P \in \operatorname{Spec}(\mathbb{Z}[\frac{1+\sqrt{5}}{2}])$, so $R \otimes_{\mathbb{Z}[\theta_5]} A$ is Azumaya over R.

COROLLARY 2.6. *If K satisfies at least one of the 3 conditions in Theorem 2.5, then the equality $S(R) = \operatorname{Br}(R) \cap S(K)$ holds.*

PROOF. This is an immediate consequence of Theorem 2.5 and the remark after Conjecture 1.3. ∎

This equality was proved for $R = \mathbb{Z}[\sqrt{2}]$ in [3] and in the same article the question has been posed for the case $R = \mathbb{Z}[(1+\sqrt{5})/2]$.

As a by product, Theorem 2.5 yields an infinite sequence of examples of pairs of Azumaya algebras which are not isomorphic but embedded in the same quaternion skew field.

COROLLARY 2.7. *If K satisfies 2 (resp. 3) of the conditions of Theorem 2.5., then there exists a quaternion skew field over K containing a pair (respectively triple) of pairwise non-isomorphic Azumaya algebras.*

PROOF. Let $t(A)$ denote the group of norm 1 units of an Azumaya algebra A in a quaternion skew field. Then $t(A)$ is finite, by a theorem of Eichler (see also Swan, [22], p. 58 Remark 2). If A_i denotes the Azumaya algebra constructed in Theorem 2.5 when K satisfies hypothesis i, then $H_n \subseteq t(A_1)$, $E_{48} \subseteq t(A_2)$, $E_{120} \subseteq t(A_3)$. By the enumeration of all the finite groups of $\mathbb{H}$ (Theorem 2.1), it is now clear that no Azumaya algebra can contain two of these groups. On the other hand, the quaternion skew field in which these Azumaya algebras are embedded are isomorphic. Indeed, their invariants at the finite places are 0 whereas at the infinite places, they are all equal by the theorem of Benard and Schacher (cf. [25], p. 89, Theorem 6.1). ∎

REMARK 2.8. In [3] examples of Azumayas over $\mathbb{Q}(\sqrt{n})$ were constructed if $p|n$, $p \equiv 3 \bmod 4$ using Theorem 1.4. These Azumayas are embeddable in a quaternion algebra over $\mathbb{Q}(\sqrt{n})$. Theorem 2.5. shows that they are not Schur algebras, contrary to the assertion made in [3]. As a consequence, the determination of $S(R)$, where R is the ring of integers of a quadratic number field, remains an open question, except in the special cases when $R = \mathbb{Z}[\sqrt{2}]$ or $R = \mathbb{Z}[(1+\sqrt{5})/2]$.

We now proceed to determine all number fields having a projective Schur algebra embeddable in a quaternion skew field. First, we recall some techniques which are very often used in projective representation theory. If $f : G \longrightarrow H$ is a homomorphism of groups and β is a 2-cocycle on H with values in a $\mathbb{Z}G$ module F, then we define a 2-cocycle α on G by:

$$\forall g, h \in G : \alpha(g, h) = \beta\big(f(g), f(h)\big)$$

In particular, one may apply this when N is a normal subgroup of G, $H = G/N$ and f is the canonical epimorphism. The resulting map Inf: $Z^2(G/N, F) \longrightarrow Z^2(G, F)$ is called an inflation. For a concise exposition of some of the properties of this map, the reader is referred to [21], p. 124. We will use this when $N = G'$, the commutator subgroup of G. If $\alpha = \mathrm{Inf}(\beta)$, where $\beta \in Z^2(G/G', F)$, then the following property is an immediate consequence of the definition:

$$\forall g, h \in G, \forall x \in G' : \alpha(gx, h) = \alpha(xg, h) = \alpha(g, xh) = \alpha(g, hx)$$

Since any 2-cocycle is cohomologous to a 2-cocycle which is normalized, we will tacitly assume, without loss of generality, that β is normalized. Then α satisfies the extra condition:

$$\forall g \in G, \forall x \in G' : \alpha(g, x) = \alpha(x, g) = 1$$

Here, we used a multiplicative notation for F, since this is most appropriate for the applications we have in mind.

https://doi.org/10.4153/CJM-1991-033-5 Published online by Cambridge University Press

LEMMA 2.9. *If $\alpha \in Z^2(G,F)$, where F is a torsion free abelian group without G action, then α is cohomologous to some $\beta \in \operatorname{Inf}\big(Z^2(G/G',F)\big)$.*

PROOF. Cf. [6], p. 63, Lemma 3.19. ■

LEMMA 2.10. *Any twisted group ring RG^c is epimorphic image of a twisted group ring RH^d, where $d \in \inf\big(Z^2(H/H',R^*)\big)$.*

PROOF. By Dedekind's units Theorem, $R^* \cong W \times \mathbb{Z}^{\alpha}$, where W is the group of roots of unity of R^*. Then $c = c_1 \cdot c_2$, where $c_1 \in Z^2(G,W)$ and $c_2 \in Z^2(G,\mathbb{Z}^{\alpha})$. Let $H = W \rtimes_{c_1} G$. Then H is a finite group and if we set $e = \inf(c_2)$ then $RH^e \twoheadrightarrow RG^c$: $u_{(w,g)} \mapsto wu_g$ is an epimorphism of twisted group rings. Since $\mathbb{Z}^{\alpha}$ is torsion free, e is cohomologous to d, where $d \in \inf\big(Z^2(H/H',R^*)\big)$. Hence $RH^d \cong RH^e \twoheadrightarrow RG^c$. ■

If $c \in Z^2(G,R^*)$, then we define a map P_c on $Z(G) \times G$ by $P_c(g,h) = c(g,h)/c(h,g)$. A cocycle computation shows that P_c is a pairing.

LEMMA 2.11. *Let G be abelian and assume that $P_c: G \times G \longrightarrow \{\pm 1\}$ is a non-degenerate pairing. Then $RG^c \cong \otimes_{i=1}^n Q_i$ where Q_i is a quaternion algebra over R.*

PROOF. (see also [9], p. 12, Theorem 3.7.) According to a theorem of È. M. Žmud (cf. [26], p. 17, Theorem 3.7) $G \cong \oplus_{i=1}^n (A_i \oplus B_i)$ where $A_i, B_i \cong C_{n_i}$ such that, if $\langle x_i \rangle = A_i$, $\langle y_i \rangle = B_i$, we have:

$$P_c(x_i,x_j) = P_c(x_i,y_j) = P_c(y_i,x_j) = P_c(y_i,y_j) = 1 \quad \text{if } i \neq j$$
$$P_c(x_i,y_i) = \epsilon_{n_i}$$

Since $t(R^*) \cong \{\pm 1\}$, this implies $n_i = 2$. Let $\alpha_i = c(x_i,x_i)$, $\beta_i = c(y_i,y_i)$, Q_i the quaternion algebra determined by α_i and β_i, then translating the above for RG^c, we have $RG^c \cong \otimes_{i=1}^n Q_i$. ■

DEFINITION 2.12. Let S be an R algebra contained in a number field L. Then S is called a Kummer extension if and only if there exist n numbers $\alpha_1,\dots,\alpha_n \in \mathbb{N}$ and n elements $\beta_1,\dots,\beta_n \in R^*$ such that $S \cong R[\sqrt[\alpha_1]{\beta_1},\dots,\sqrt[\alpha_n]{\beta_n}]$

LEMMA 2.13. *Let $K \subseteq L$ be an extension of number fields with ring of integers R and S respectively. Then S is a Kummer extension of R if and only if S is epimorphic image of some twisted group ring RG^c.*

PROOF. Let $\pi: RG^c \longrightarrow S$ be an epimorphism. Let $H = \oplus_{C \in \mathcal{C}} C$, where $\mathcal{C}$ is the collection of cyclic subgroups of G. For any $C \in \mathcal{C}$, we choose a fixed generator x_C and define $\alpha_C = \big(\pi(x_C)\big)^{|C|} \in R^*$. For any $C \in \mathcal{C}$, we define a 2-cocycle d_C on C by:

$$d_C(x_C^i, x_C^j) = 1 \quad \text{if } 0 \leq i,j < |C| \text{ and } i+j < |C|$$
$$d_C(x_C^i, x_C^j) = \alpha_C \quad \text{if } 0 \leq i,j < |C| \text{ and } i+j \geq |C|$$

These d_C allow us to define a 2-cocycle d on H by

$$d(\prod_C x_C^i, x_C^j) = \prod_C d_C(x_C^i, x_C^j)$$

The map $\rho: RH^d \longrightarrow S: x_C \longmapsto \pi(x_C)$ is a ring homomorphism, since S is commutative. Now $\pi(G) \subseteq \rho(H)$, so ρ is surjective, i.e., S is a Kummer extension of R. The other direction is obvious. ∎

LEMMA 2.14. *Let $\pi: RG^c \twoheadrightarrow A$ be a representation of a non-trivial Azumaya algebra which can be embedded in a quaternion skew field over K. Assume that there exists a maximal subfield L of $K \otimes A$ such that the inner automorphisms induced by $\pi(u_g), g \in G$ leave L stable. Let S denote the ring of integers of L. Then $A \cong \binom{S\beta}{R}$ for some $\beta \in R^*$, S is a Kummer extension of R and L is an imaginary and unramified extension of K.*

PROOF. Define $\Gamma: G \longrightarrow \mathrm{Aut}_K(L) = \{1, \sigma\}$ by taking $\Gamma(g)$ equal to the inner automorphism induced by $v_g = \pi(u_g)$. Let $H = \mathrm{Ker}(\Gamma)$. If $h \in H$, then v_h commutes with L, hence $v_h \in L$ since L is a maximal commutative subfield. Also, $v_h \in S$, since v_h is integral over R. So $T = \pi(RH^c) \subseteq S$ and consequently $H \neq G$. Now H is a normal subgroup of G and this implies that T is left stable under inner automorphisms by v_g. Let $g_0 \in G$ be such that $\Gamma(g_0) = \sigma$. Then $v_{g_0}^2 \in S$ is stable under $\Gamma(g_0) = \sigma$, hence $v_{g_0}^2 = \beta \in R^*$. Since $G = H \cup Hg_0$, $\pi(RG^c) \subseteq \binom{T\beta}{R} \subseteq \binom{S\beta}{R}$. Since A is Azumaya, this implies $A = \binom{T\beta}{R} = \binom{S\beta}{R}$ and $T = S$, i.e., S is a Kummer extension. Clearly, L is imaginary and Theorem 1.4. shows that L/K is unramified. ∎

THEOREM 2.15. *Let K be a number field having a real embedding. Then a non-trivial projective Schur algebra is realizable in a quaternion skew field over K if and only if K satisfies one or more of the following properties:*

- *i K has an imaginary,unramified extension L of degree 2 such that its ring of integers S is a Kummer extension of R.*
- *ii $(2) = (\mu)^2$ for some $\mu \in R$.*
- *iii $\mathbb{Q}(\sqrt{5}) \subseteq K$.*

The corresponding Azumaya algebras are:

- *i $A \cong \binom{S\beta}{R}$, for some $\beta \in R^*$*
- *ii $A \cong R\langle 1, (1+i)/\mu, (1+j)/\mu, (1+i+j+k)/2\rangle$, where $(\mu)^2 = (2)$*
- *iii $A \cong R\langle 1, \big(-1+\sqrt{5}+2i+(1+\sqrt{5})j\big)/4, j, \big(-1-\sqrt{5}+(-1+\sqrt{5})j+2k\big)/4\rangle$*

PROOF. We first show that the conditions are sufficient. Therefore, we have to verify that the stated R algebras are indeed Azumaya and moreover that they are an epimorphic image of some twisted group ring RG^c.

CASE 1. K satisfies condition iii.
This is obvious, in view of Theorem 2.5, item iii.

CASE 2. K satisfies condition ii.
Let A be the R algebra mentioned in item ii. Then $\mathrm{disc}(A/R) = -4/(\mu)^4 \in R^*$, so A is Azumaya over R. We claim that A is the epimorphic image of RE_{48}^c, for some $c \in Z^2(E_{48}, R^*)$. Note that there exists a natural embedding $\psi: E_{24} \longrightarrow A^*$, if one uses the description of Theorem 2.1 for E_{24}. We view E_{48} as embedded in a quaternion algebra

https://doi.org/10.4153/CJM-1991-033-5 Published online by Cambridge University Press

over $\mathbb{Q}(\sqrt{2})$, as in Theorem 2.5. Then E_{24}, E_{48} and A may be regarded as subsets of $\mathbb{H}$, which facilitates the description of the extension of ψ to E_{48}.

$$\begin{aligned} \tilde{\psi}: E_{48} \longrightarrow A: w &\longmapsto \psi(w) \text{ if } w \in E_{24} \\ w &\longmapsto \frac{\sqrt{2}}{\mu} w \text{ if } w \in E_{48} \setminus E_{24} \end{aligned}$$

One now easily verifies that $\forall g, h \in E_{48} : \tilde{\psi}(g)\tilde{\psi}(h) = c(g,h)\tilde{\psi}(gh)$, for some $c(g,h) \in R^*$. Since A is associative, this implies that $c \in Z^2(E_{48}, R^*)$. Then

$$\pi: RE_{48}^c \longrightarrow A : \sum_{x \in E_{48}} \alpha_x x \longmapsto \sum_{x \in E_{48}} \alpha_x \tilde{\psi}(x)$$

is an epimorphism of R algebras, so A is indeed a projective Schur algebra.

CASE 3. K satisfies condition i.

Applying Theorem 1.4, we see that $\left(\frac{S\beta}{R}\right)$ is an Azumaya algebra over R. By assumption, S is a Kummer extension of R, so by Lemma 2.13 there exists a finite group H, a 2-cocycle $d \in Z^2(H, R^*)$ and an algebra epimorphism $\psi: RH^d \longrightarrow S$. Let $\mathcal{G} = \mathrm{Gal}(L/K) = \{\mathrm{id}, \sigma\}$ and $\mathcal{H} = \mathrm{Map}(\mathcal{G}, H)$, the set of functions from G to H. We define an action of G on H by $\forall x, z \in G, \forall k \in H : (xk)(z) = k(x^{-1} \circ z)$. Using this action, we now define a group G as follows. As a set $G = \mathcal{H} \times \mathcal{G}$ and multiplication is given by

$$\forall h, k \in \mathcal{H}, \forall x, y \in \mathcal{G} : (h,x)(k,y) = \big(h(xk), xy\big)$$

This means that $G = H \wr \mathcal{G}$, the wreath product of H and $\mathcal{G}$. Finally, we define a cocycle c on G by the following rules

$$\begin{aligned} c\big((h,x),(k,y)\big) &= \delta(x,y) \prod_{z \in \mathcal{G}} d\big(h(z), (xk)(z)\big) \\ \delta(x,y) &= \begin{cases} 1 & \text{if } x = \mathrm{id} \text{ or } y = \mathrm{id} \\ \beta & \text{if } x = \sigma \text{ and } y = \sigma. \end{cases} \end{aligned}$$

The group G and the 2-cocycle c may be used to define a group ring RG^c. We define π by

$$\pi: RG^c \longrightarrow \left(\frac{S\beta}{R}\right) : u_{(h,x)} \longmapsto \prod_{z \in \mathcal{G}} z\big(\psi(u_{h(z)})\big) u_x$$

https://doi.org/10.4153/CJM-1991-033-5 Published online by Cambridge University Press

It is easily seen that π is surjective. We verify that π is an algebra homomorphism

$$\begin{aligned}
\pi(u_{(h,x)})\pi(u_{(k,y)}) &= \prod_{z\in\mathcal{G}} z\big(\psi(u_{h(z)})\big)u_x z\big(\psi(u_{k(y)})\big)u_y \\
&= \prod_{z\in\mathcal{G}} z\big(\psi(u_{h(z)})\big)x\circ\big(\psi(u_{k(z)})\big)u_x u_y \\
&= \prod_{z\in\mathcal{G}} z\big(\psi(u_{h(z)})\psi(u_{k(x^{-1}\circ z)})\big)\,\delta(x,y)\,u_{xy} \\
&= \prod_{z\in\mathcal{G}} d\big(h(z),k(x^{-1}\circ z)\big)\,\delta(x,y)\,z\big(\psi(u_{h(z)k(x^{-1}\circ z)})\big)u_{xy} \\
&= \prod_{z\in\mathcal{G}} d\big(h(z),(xk)(z)\big)\,\delta(x,y)\,\pi(u_{(h,x)(k,y)}) \\
&= c\big((h,x),(k,y)\big)\pi(u_{(h,x)(k,y)}) \\
&= \pi(u_{(h,x)}u_{(k,y)})
\end{aligned}$$

To prove necessity, we start from a representation $\pi\colon RG^c = \bigoplus_{g\in G} Ru_g \twoheadrightarrow A$ of a projective Schur algebra A. Throughout, let $v_g = \pi(u_g) \in A^*$. According to Lemma 2.10, we may assume that $c = \mathrm{Inf}(d)$, $d \in Z^2(G/G', R^*)$ and d normalized. Then $W = \pi(G')$ is a finite subgroup of A^* since c is trivial on G', hence of $\mathbb{H}^*$. We first show that W is stable under inner automorphism by v_g. If $g \in G$, $x \in G'$ then:

$$\begin{aligned}
v_g\pi(u_x)v_g^{-1} &= \pi(u_g u_x u_g^{-1}) \\
&= \frac{c(g,x)c(gx,g^{-1})}{c(g,g^{-1})}\pi(u_{gxg^{-1}})
\end{aligned}$$

By the remarks made before Lemma 2.9, $c(g,x) = 1$ and $c(gx,g^{-1}) = c(g,g^{-1})$. So $v_g\pi(u_x)v_g^{-1} = \pi(u_{gxg^{-1}}) \in W$. We now distinguish 5 cases according to 5 types of subgroups W of $\mathbb{H}$.

CASE 1. $|W| \leq 2$.
Then W is trivial or $W \cong C_2$. Let $\bar{\pi}\colon G \longrightarrow A^*/R^*$ be the group homomorphism defined by π. By our assumption $W \subseteq \{\pm 1\}$, hence $G' \subseteq \ker\bar{\pi}$. Let $H = G/\ker\bar{\pi}$. Choose a section $\sigma\colon H \longrightarrow G$ and define d on $H \times H$ by $d(\bar{g},\bar{h})\cdot v_{\sigma(\bar{g}\bar{h})} = v_{\sigma(\bar{g})}v_{\sigma(\bar{h})}$. Then d is a 2-cocycle on the abelian group H and σ and π determine an epimorphism $\phi\colon RH^d \twoheadrightarrow A\colon u_{\bar{g}} \mapsto v_{\sigma(\bar{g})}$. We claim that P_d is non degenerate. If $\bar{x} \in H$ is such that $\forall \bar{y} \in H\colon d(\bar{x},\bar{y}) = d(\bar{y},\bar{x})$, then

$$\begin{aligned}
\phi(u_{\bar{x}})\phi(u_{\bar{y}}) &= d(\bar{x},\bar{y})\phi(u_{\bar{x}\bar{y}}) \\
&= d(\bar{y},\bar{x})\phi(u_{\bar{y}\bar{x}}) \\
&= \phi(u_{\bar{y}})\phi(u_{\bar{x}})
\end{aligned}$$

So $\phi(u_{\bar{x}})$ commutes with every $\phi(u_{\bar{y}})$, hence with A. But then $\phi(u_{\bar{x}}) = \pi(u_{\sigma(\bar{x})}) \in R^*$, i.e. $\sigma(\bar{x}) \in \ker\bar{\pi}$, which proves our assertion. Applying Lemma 2.11, $RH^d \cong \otimes_{i=1}^n Q_i$. But then $\phi\colon K\otimes RH^d \cong \otimes_{i=1}^n K\otimes Q_i \longrightarrow K\otimes A$ is an epimorphism of central simple algebras, hence an isomorphism. However $[A : K] = 4$ and $[K\otimes Q_i : K]$ is a square, so exactly one of the $K \otimes Q_i$ is isomorphic to $K \otimes A$ and all other ones are trivial. This shows that ϕ is injective too and therefore $RH^d \cong Q \cong A$. However, one verifies that $\mathrm{disc}(Q/R) = -16\alpha^2\beta^2$ if Q is the quaternion algebra defined by $x^2 = \alpha$, $y^2 = \beta$, $xy = -yx$. So Q is not Azumaya, which shows that this case actually can not occur.

CASE 2. W is conjugate to $C_n = \langle \epsilon_n \rangle$, $n \geq 3$ or W is conjugate to $H_n = \langle \epsilon_{2n}, i \rangle$, $n \geq 3$.

In this case, $\langle \epsilon_n \rangle$ is a characteristic subgroup of W (note that $\langle \epsilon_n \rangle = H_n'$). Since W is invariant under inner conjugation by v_g, the same holds for $\langle \epsilon_n \rangle$. Let $L = K(\epsilon_n)$, S its ring of integers. Lemma 2.14. now shows that K satisfies hypothesis 1 and $A = \left(\frac{S\beta}{R}\right)$.

CASE 3. W is conjugate to H_2 or W is conjugate to E_{24}
Then $H_2 = \{\pm 1, \pm i, \pm j, \pm k\}$ is a characteristic subgroup of W, namely it is its unique Sylow 2-subgroup. Since W is stable under inner automorphism by v_g, the same then holds for H_2. Let $v_g i v_g^{-1} = \alpha_i \pi(i)$, where $\alpha_i \in \{\pm 1\}$, $\pi(i) \in \{i, j, k\}$ and analogous rules hold for j and k. We now define a homomorphism

$$\Gamma : G \longrightarrow C_2^3 \ltimes S_3 \cong E_{48} : g \longmapsto \begin{pmatrix} i & j & k \\ \alpha_i \pi(i) & \alpha_j \pi(j) & \alpha_k \pi(k) \end{pmatrix}$$

Let $\tau : C_2^3 \rtimes S_3 \longrightarrow S_3$ be the canonical epimorphism. One easily verifies that $\tau \circ \Gamma(g) = \mathrm{id}$ implies $v_g = \alpha x$ for some $\alpha \in R^*$ and $x \in \{1, i, j, k\}$ whereas $\mathrm{ord}(\tau \circ \Gamma(g)) = 3$ implies $v_g = \alpha x$ for some $\alpha \in R^*$ and $x \in \{(\pm 1 \pm i \pm j \pm k)/2\}$. If $\tau \circ \Gamma$ is not surjective, then the above remarks imply that $\pi(RG^c) \subseteq R\langle E_{24} \rangle$, a contradiction since $R\langle E_{24} \rangle$ is not Azumaya. (cf. Theorem 2.5) So $\tau \circ \Gamma$ is surjective and we may choose $g_0 \in G$ such that $\Gamma(g_0)(i) = \pm i$ and $\mathrm{ord}(\tau \circ \Gamma)(g_0) = 2$. If $\Gamma(g_0) = -i$, then we choose $g_1 \in G'$ such that $\pi(g_1) = j \in W$ and replace g_0 by $g_0 g_1$. This is possible, since $H_2 \subseteq W_2 = \pi(G')$ and it does not affect $\mathrm{ord}(\tau \circ \Gamma)(g_0)$. We now have $\Gamma(g_0)(i) = i$. Since $K(i)$ is a maximal subfield of $K \otimes A$, this implies $v_{g_0} = a + ib$, $a, b \in K$. Now assume that $\Gamma(g_0)(j) = k$. This implies $\Gamma(g_0)(k) = \Gamma(g_0)(ij) = -j$. An easy calculation then shows that $a = b$, i.e. $v_g = a(1 + i)$. If $\Gamma(g_0)(j) = -k$, $\Gamma(g_0)(k) = j$, then we have $a = -b$. In both cases, $v_{g_0}^8 = 2^4 \cdot a^8 \in R^*$. Let $\mu = a^{-1}$, then $(2) = (\mu)^2$ in R, i.e. K satisfies hypothesis 2. Note further that $(1 + i)/\mu = (1 - i)/\mu + 2i/\mu$, so anyhow, $(1 + i)/\mu \in A$. If we interchange i and j in the above, we find that $(1 + j)/\nu \in A$, where $(\nu)^2 = (2)$. Since the group of fractional ideals of R is free, this implies $\nu = \mu\delta$, for some $\delta \in R^*$ and $(1 + j)/\mu = (1 + j)\delta/\nu \in A$. Finally, $(1 + i + j + k)/2 = ((1 + i)(1 + j)/\mu^2)(\mu^2/2) \in A$, and we have shown that:

$$R\langle 1, (1 + i)/\mu, (1 + j)/\mu, (1 + i + j + k)/2 \rangle \subseteq A$$

As already shown in Case 2 of the sufficiency part of the proof, the right hand side is Azumaya and so equality holds.

CASE 4. W is conjugate to E_{48}
Then $\sqrt{2} \in R$, so K satisfies hypothesis ii. Since $R\langle E_{48} \rangle$ is already Azumaya, $R\langle E_{48} \rangle = A$.

CASE 5. W is conjugate to E_{120}
This implies $\sqrt{5} \in R$, i.e. K satisfies hypothesis iii. As in Case 4, we find $R\langle E_{120}\rangle = A$ ∎

REMARK 2.16. The Azumaya algebras which can be constructed if K satisfies hypothesis ii, were obtained by L. Childs in [1] by studying the smash product of Hopf algebras of rank 2 over R.

A comparison of the Azumayas constructed in Theorem 2.5 and Theorem 2.15 if K satisfies hypothesis 2 shows that they are very akin, namely one may change the coefficients of some generators in order to pass from one to another. We make this precise in the following definition.

DEFINITION 2.17. *Let K and K' be number fields with ring of integers R and R' respectively. A projective Schur algebra A over R is a twisted version of a Schur algebra B over R' if there exists a finite subgroup G of B^* and a 2-cocycle $c \in Z^2(G, R^*)$ such that A is epimorphic image of RG^c and B is spanned by G as an R' module.*

EXAMPLE 2.18. All projective Schur algebras mentioned in items ii and iii in Theorem 2.15 are twisted versions of Schur algebras which can be embedded in skew fields over K'. For item iii, this is obvious, whereas for item ii, this has been shown in the sufficiency part of the proof of Theorem 2.15.

We now examine condition i closer. If $K \subseteq L$ is an unramified extension of degree 2 and $S = R[\sqrt[\lambda_1]{\delta_1}, \dots, \sqrt[\lambda_n]{\delta_n}]$, then it is easily verified that we can take $\lambda_i = 2$ unless $\delta_i = 1$. So S has the form $S = R[\epsilon_s, \sqrt{\delta_2}, \dots, \sqrt{\delta_n}]$. If $\epsilon_s \notin S$ for $s \geq 3$, then we have $\forall x \in S$: $2 |\operatorname{tr}(x)$, as is easily seen. But then S is not unramified over R. On the other hand, if there exists $\epsilon_s \in S$ where s is truly composite, then $R[\epsilon_s]$ is an unramified extension of R, by Lemma 2.4. and $\left(\frac{S\beta}{R}\right)$ is a twisted version of $\left(\frac{R[\epsilon_s] - 1}{R}\right)$. One may now be tempted to conjecture that any projective Schur algebra constructed in Theorem 2.15 is the twisted version of a Schur algebra constructed in Theorem 2.5. This however is not the case. We will produce infinitely many examples of projective Schur algebras which can not be obtained by this process. We first collect some technical facts in a Lemma.

LEMMA 2.19. *If $G \cong E_{48}$ or $G \cong E_{120}$ and $c \in Z^2(G, \{\pm 1\})$, then $(\{\pm 1\} \rtimes_c G)' \cong G'$. If $G \cong H_m$, $m \geq 2$, then $\operatorname{Inf}: H^2(H_m/H_m', \{\pm 1\}) \longrightarrow H^2(H_m, \{\pm 1\})$ is an epimorphism.*

PROOF. Let $G \cong E_{120}$. Then $H^2(E_{120}, \mathbb{C}^*) \cong H^2\big(\mathrm{Sl}_2(\mathbb{F}_5), \mathbb{C}^*\big) = 1$ (cf. [19], p. 232 Satz ix). The long exact cohomology sequence corresponding to the short exact sequence

$$(*) \qquad 1 \longrightarrow \{\pm 1\} \longrightarrow \mathbb{C}^* \xrightarrow{\text{square}} \mathbb{C}^* \longrightarrow 1$$

then yields that $H^2(E_{120}, \{\pm 1\}) = 1$ and therefore $(\{\pm 1\} \rtimes_c E_{120})' \cong E_{120}'$. If $G \cong E_{48}$ then $E_{24} \trianglelefteq E_{48}$. Since $H^2(E_{24}, \mathbb{C}^*) \cong H^2\big(\mathrm{Sl}_2(\mathbb{F}_3), \mathbb{C}^*\big) = 1$ (cf. [19], p. 232, Satz ix), the same calculation as above yields that $H^2(E_{24}, \{\pm 1\}) = 1$. The inflation restriction sequence

$$0 \longrightarrow H^2\big(E_{48}/E_{24}, \{\pm 1\}\big) \xrightarrow{\text{Inf}} H^2\big(E_{48}, \{\pm 1\}\big) \xrightarrow{\text{Res}} H^2\big(E_{24}, \{\pm 1\}\big)$$

is exact, since $\mathrm{Hom}(E_{24}, \{\pm 1\}) = 1$ (cf. [21], p. 126, Proposition 5). This shows that $\mathrm{Inf}: H^2(E_{48}/E_{24}, \{\pm 1\}) \longrightarrow H^2(E_{48}, \{\pm 1\})$ is surjective. Without loss of generality, we may therefore assume that $c \in \mathrm{Inf}\big(Z^2(E_{48}/E_{24}, \{\pm 1\})\big)$. One now immediately verifies that $(\{\pm 1\} \rtimes_c G)' \cong G'$.

If $G \cong H_m$, then $H^2(H_m, \mathbb{C}^*) = 1$ (cf. [2], p. 302). and after substitution in the long exact cohomology sequence associated to $(*)$ above, this shows that the transfer map $\delta_1: \mathrm{Hom}(H_m, \mathbb{C}^*) \longrightarrow H^2(H_m, \{\pm 1\})$ is an isomorphism. We have a commutative diagram

$$\begin{array}{ccc} \mathrm{Hom}(H_m/H_m', \mathbb{C}^*) & \xrightarrow{\mathrm{Inf}_1} & \mathrm{Hom}(H_m, \mathbb{C}^*) \\ \downarrow \delta_2 & & \downarrow \delta_1 \\ H^2(H_m/H_m', \{\pm 1\}) & \xrightarrow{\mathrm{Inf}_2} & H^2(H_m, \{\pm 1\}) \end{array}$$

Since Inf_1 and δ_1 are isomorphisms, Inf_2 is surjective. ∎

EXAMPLE 2.20. Let p be an odd prime, $p \geq 7$, $r > 0$. In this example, we write θ, ϵ instead of $\theta_{p^r}, \epsilon_{p^r}$. Choose $u \in \mathbb{Z}[\theta]^*$ such that u is not a square and u is positive in at least one embedding of $\mathbb{Q}(\theta)$. Let $K = \mathbb{Q}(\theta)(\sqrt{(2-\theta)u})$, $L = K(\epsilon)$. Then K admits a real embedding and L is an imaginary extension of degree 2 over K. Let R, S be the ring of integers of K and L respectively. Note that $\epsilon = (\theta + \sqrt{\theta^2 - 4})/2$, $\theta - 2 = (\epsilon_{2p^r} - \bar{\epsilon}_{2p^r})^2$ and $\theta + 2 \in \mathbb{Z}[\theta]^*$, since $\mathbb{N}(\theta - 2) = \mathbb{N}(\theta^2 - 4)$. This implies $\sqrt{-u} \in S$. Now $\mathrm{disc}(1, \epsilon) = (\theta^2 - 4)$ and $\mathrm{disc}(1, \sqrt{-u}) = -4u$. Since $(\theta^2 - 4)$ and 4 are coprime, this implies that S is unramified over R. Also $S = R[\epsilon, \sqrt{-u}]$, so S is a Kummer extension of R.

Let $A = \binom{S-1}{R}$, then A is a projective Schur algebra by Theorem 2.15. We claim that A is not the twisted version of any Schur algebra embeddable in a quaternion skew field over K'. To prove this, we first calculate $t(A)$, the group of norm 1 units of A. Clearly, $H_{p^r} \subseteq t(A)$ and by Theorem 2.1, this implies $t(A) = H_k$ for some multiple k of p^r. In the notation of Theorem 2.5., this implies that $t(A)' = C_k$ is stable under inner conjugation by u_σ, $\sigma \neq \mathrm{id}$, so $C_k \subseteq S^*$. If ϕ denotes the Euler function, then we have

$$\phi(k) \leq [L : \mathbb{Q}(\epsilon)]\phi(p^r) = 2\phi(p^r)$$

This inequality implies that $k/p^r = 1, 2, 3$ or 4. If $k/p^r = 3$, then $\epsilon_3 \in L$, (3) ramifies in L and hence in K, contradicting the fact that K can only ramify at 2 and p. If $k/p^r = 2$ or $k/p^r = 4$, then $i \in L$. This implies $\sqrt{u} \in K$. By assumption $\sqrt{u} \notin \mathbb{Q}(\theta)$, so $\sqrt{u} = x\sqrt{2-\theta}$ for some $x \in \mathbb{Q}(\theta)$. This implies that $(2-\theta)$ is the square of an ideal in $\mathbb{Z}[\theta]$, contradicting the fact that it is a maximal ideal. We have now proved that $t(A) = H_{p^r}$.

If our claim is not true, then there exists a finite subgroup G of the multiplicative group of a Schur algebra B such that $\pi': RG' \twoheadrightarrow B$ represents B and $\pi: RG^c \twoheadrightarrow A$ represents A. Theorem 2.5 now shows that $G \cong H_m$, $G \cong E_{48}$ or $G \cong E_{120}$. As in Lemma 2.10, we decompose $c = c_1c_2$, where $c_1 \in Z^2(G, \{\pm 1\})$ and $c_2 \in Z^2(G, F)$, F a free subgroup of R^*.

CASE 1. $G \cong E_{48}$ or $G \cong E_{120}$

Then we replace G by $T = \{\pm 1\} \rtimes_{c_1} G$ and c by $d = \mathrm{Inf}(c_2)$. We then obtain a representation $\gamma: RT^d \twoheadrightarrow A$, where $d \in \mathrm{Inf}\big(Z^2(T/T', R^*)\big)$. To this representation, we may then apply the proof of the necessity part of Theorem 2.15. Cases 3, 4 and 5 are immediately excluded, since $H_{p^r} \cong t(A)$ does not contain H_2. Case 2 is also excluded, since $T' \cong G'$ by Lemma 2.19, $C_3 \not\subseteq t(A)$ and C_n is not the epimorphic image of G' if $n \geq 4$.

CASE 2. $G \cong H_m$.
By Lemma 2.19, we may already assume that $c \in \mathrm{Inf}\big(Z^2(H_m/H_m', \{\pm 1\})\big)$. We may therefore apply Theorem 2.15 to $\pi: RH_m^c \twoheadrightarrow A$ and again all cases but the second are immediately excluded. Let $L = \pi(KC_m^c)$ and Q the ring of integers of L. Then $A \cong \left(\frac{Q\ \beta}{R}\right)$ for some $\beta \in R^*$ and Q is generated over R by $\pi(RC^c)$, where C runs over a subcollection of all cyclic subgroups of G (cf. Lemma 2.13 and Lemma 2.14). Now Q is an unramified Kummer extension of R of degree 2, so $Q = R[\epsilon_{s_1}, \sqrt{\alpha_2}, \ldots, \sqrt{\alpha_n}]$. Let $C_{(i)}$ be a cyclic subgroup of G such that $\pi : RC_{(i)}^c \twoheadrightarrow R[\sqrt{\alpha_i}]$, $i \geq 2$. Then $|C_{(i)}|$ is even and $\alpha_i = c(\zeta, \zeta)$, where ζ is the unique element of order 2 of $C_{(i)}$, hence of G. This proves that all α_i are equal. Moreover, if s_1 is even, then $\alpha_i = -1$ for all $i \geq 2$ and $Q = R[\epsilon_{s_1}]$. But $\epsilon_{s_1} \in t(A)^*$, so $s_1 | 2p^r$ or $s_1 = 4$. Applying Lemma 2.3 this contradicts the fact that Q is unramified over R. If s_1 is odd and $RC_{(1)} \twoheadrightarrow R[\epsilon_{s_1}]$, then there exists an element $\gamma \in G$ such that γ^2 generates $C_{(1)}$. Then $\gamma^{s_1} = \zeta$ and $\alpha_2 = c(\gamma^{s_1}, \gamma^{s_1}) = c(\gamma^2, \gamma^{2(s_1-1)}) = -1$. So again $Q = R[\epsilon_{s_1}]$, and for the same reason as above this leads to a contradiction. ∎

3. **Schur algebras and hermitian forms.** As shown in §2, the construction of Schur algebras in skew fields over K is only possible in very limited circumstances. So we now turn our attention to Schur algebras embeddable in matrix rings over skew fields. Since proving some analogue of Theorem 2.1. for $M_n(\mathbb{H})$ or $M_n(\mathbb{R})$ is clearly an impossible task, there is no hope that a procedure similar to the one of the previous paragraph may lead to the determination of the Schur or projective Schur algebras over R. However, the theory of hermitian and quadratic forms sheds some light on this question. In this paragraph, we will prove that any Schur algebra for which the class in the Brauer group is non-trivial is spanned by the automorphism group of some positive definite, modular hermitian form. If the class in the Brauer group is trivial, then a similar theorem may be proved, using quadratic instead of hermitian forms. Moreover, these forms are even, which puts a severe restriction on the possible Schur algebras and if $R = \mathbb{Z}$, this even suffices to determine them all. It also shows that easy groups, in some sense, must not be expected to span a Schur algebra. We will make this precise in the final theorem. First, we recall some facts from the theory of involutions on quaternion algebras and the hermitian forms associated to them. In this paragraph, the conventions made in the beginning of § 1 remain in force; in particular, the field K admits at least one real embedding.

DEFINITION 3.1. *Let D be a skew field over K. An involution $\tau: D \longrightarrow D$ is a K linear map such that $\tau^2 = \mathrm{id}$ and $\tau(ab) = \tau(b)\tau(a)$.*

REMARK 3.2. In the theory of central simple algebras, one distinguishes between involutions of the first kind, which are the ones we defined, and involutions of the second kind, which induce a non-trivial automorphism on K. Since the involutions of the second kind will not play a role in what follows, we will use the term involution only in the sense of Definition 3.1.

Actually, we do not need involutions on skew fields, but involutions on maximal R orders contained in them. In general, it is very difficult to find out whether an involution invariant order exists (cf. [18], p. 150, § 4). Fortunately, for Azumaya algebras in quaternion fields, there is a nice method, due to D. J. Saltman, to circumvent these difficulties. The proof that follows is essentially the same as in [17], p. 534.

THEOREM 3.2. *Let D be a quaternion algebra over a number field K. Let A be an Azumaya algebra contained in D. Then A is stable under the unique symplectic involution of D.*

PROOF. Let $\tau : D \longrightarrow D : \delta \longmapsto \mathrm{tr}(\delta)1 - \delta$, where tr denotes the reduced trace. If L is a splitting field for D, then $L \otimes D \cong M_2(L)$ and

$$\tau : M_2(L) \longrightarrow M_2(L) : \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \longmapsto \begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix}$$

This shows that τ is an involution. The uniqueness of τ is stated in [18], p. 148, Theorem 2.6. If A is an Azumaya algebra, then clearly $\tau(A) \subseteq A$. ∎

In what follows, τ will denote this symplectic involution.

DEFINITION 3.3. *Let V be a finite dimensional right vector space over a skew field D over K and let τ be an involution on D. An hermitian form $\langle\ ,\ \rangle$ on V is a K bilinear map into D such that $\forall v, w \in V, \forall \delta \in D : \langle v\delta, w \rangle = \tau(\delta)\langle v, w\rangle, \langle v, w\delta \rangle = \langle v, w \rangle \delta, \tau(\langle v, w \rangle) = \langle w, v \rangle$*

If for every real embedding $K \overset{\iota}{\hookrightarrow} \mathbb{R}$ we have that $\forall v \in V \setminus \{0\} : \iota(\langle v, v \rangle) > 0$, then the form will be called positive definite. With the notations of the previous definition, let A be an Azumaya algebra contained in D and let N be a right A module contained in V. Let I be the ideal generated by $\{\langle m, n \rangle, m, n \in N\}$. Since $\tau(A) \subseteq A$, I is a 2 sided A module contained in D. But A is an Azumaya algebra, so there exists a 2 sided fractional R ideal I of K such that $IA = I$ (cf. [5], p. 54, Corollary 3.7).

We give N a left A module structure by $\forall \alpha \in A, \forall n \in N : a \cdot n = n\tau(a)$. A hermitian form on N may then be viewed as a right A module map

$$\psi : N_A \longrightarrow \mathrm{Hom}_A({}_AN, {}_AI) : n \longmapsto (m \longmapsto \langle m, n \rangle)$$

The subscripts in the above formula indicate the sidedness of the A modules under consideration. The form $\langle\ ,\ \rangle$ on N will be called modular if the above map is an isomorphism. Now let G be a finite group and assume that N is a (RG, A)-bimodule. If $\mathcal{J}$ is any 2 sided A ideal, then $N\mathcal{J}$ is also a (RG, A)-bimodule.

DEFINITION 3.5. *Let $\mathcal{J}$ be any 2 sided ideal of A. A (RG, A)-bimodule will be called simple (mod $\mathcal{J}$) if $N/N\mathcal{J}$ is a simple (RG, A)-bimodule, that is, if it contains no non-trivial (RG, A)-bimodules. N will be called everywhere simple if it is $\mathcal{J}$ simple for any non-zero 2 sided prime ideal $\mathcal{J}$ of A.*

We now have all definitions at our disposal to state the theorem which gives a connection between Schur algebras and hermitian forms.

THEOREM 3.6. *Let $\pi: RG \twoheadrightarrow B$ be an epimorphism from a group ring RG onto a non-trivial Azumaya algebra B. If $[B] \neq 0$ in $\mathrm{Br}(R)$, then there exists an Azumaya algebra A contained in a quaternion skew field D over K, a 2 sided A lattice I contained in D, a (RG, A)-bimodule N and an hermitian form $\langle\ ,\ \rangle: N \times N \longrightarrow I$ such that*

i $B \cong \mathrm{End}_A(N_A)$

ii $\forall g \in G, \forall m, n \in N : \langle gm, gn\rangle = \langle m, n\rangle$

iii *N is everywhere simple.*

iv *$\langle\ ,\ \rangle$ is a positive definite, modular, hermitian form.*

PROOF. Let B be a non-trivial Schur algebra and assume that $[B] \neq 0$ in $\mathrm{Br}(R)$. Let $K \otimes B \cong M_n(D)$ for some skew field D over K. We already know that D is a quaternion algebra over K. Let A be a maximal order contained in D. Then A and B are Morita equivalent over R (cf. [13], p. 189 Corollary 21.7). An easy application of Theorem 4.4 of [5] then shows that A is Azumaya too. Let V be an n dimensional right vector space over D. Then $K \otimes B$ acts on the left of V, so G also acts on the left of V via π. By Theorem 21.6 of [13], there exists a right A lattice N in V such that $B = \mathrm{End}_A(N_A, N_A)$. Let $\tau: D \longrightarrow D: \delta \longmapsto \mathrm{tr}(\delta)1 - \delta$ denote the unique non-trivial symplectic involution on D. Pick a basis $e_1, \ldots, e_n$ in V and define

$$\langle\ ,\ \rangle_O: V \times V \longrightarrow D: \left(\sum_{i=1}^{n} e_i x_i, \sum_{i=1}^{n} e_i y_i\right) \longmapsto \sum_{i=1}^{n} \tau(x_i) y_i$$

It is easy to verify that $\langle\ ,\ \rangle_O$ is an hermitian form.

Let $\iota: K \longrightarrow \mathbb{R}$ be any real embedding of K. Then $\mathbb{R} \otimes_K D \cong \mathbb{H}$, since $\mathrm{Inv}[D] = \mathrm{Inv}[B] = 1/2$, at all infinite places. This is a consequence of the assumption that $[B] \neq 0$ and the fact that the Hasse invariants are equally distributed. (cf. [25], p. 89 Theorem 6.1) It also follows that there exists a quadratic extension L of K such that $L \otimes_K D$ is split (cf. [13], Theorem 7.15 p. 97). From this one easily deduces that D is itself a quaternion algebra. Now $\mathbb{R} \otimes_K D \cong \mathbb{H}$ implies that $\forall x \in D \setminus \{0\} : \iota\big(\tau(x)x\big) = \iota\big(nr(x)\big) > 0$. This shows that $\langle\ ,\ \rangle_O$ is positive definite.

Define a new form $\langle\ ,\ \rangle$ on V by

$$\langle\ ,\ \rangle: V \times V \longrightarrow D: (x, y) \longmapsto \sum_{g \in G} \langle gx, gy\rangle_O$$

Then $\langle\ ,\ \rangle$ is still a positive definite, hermitian form and moreover, it is invariant under the action of G. If I denotes the 2 sided ideal generated by $\{\langle m, n\rangle ; m, n \in N\}$, then we may restrict $\langle\ ,\ \rangle$ to N to obtain

$$\langle\ ,\ \rangle: N \times N \longrightarrow I: (n, m) \longmapsto \langle n, m\rangle$$

Clearly, G acts on the left on N via π. This provides N with a left RG, right A module structure. We have to prove that N is simple everywhere. The left B, right A module structure on N may be interpreted as a left $B \otimes A^\circ$ module structure. This yields a homomorphism $\gamma : B \otimes A^\circ \longrightarrow \mathrm{End}_R(N)$. Since B is the commutator of A° in $\mathrm{End}_R(N)$, the double commutator property may be applied to show that γ is an isomorphism (cf. [5], p. 57, Theorem 4.3). Let $\mathcal{J}$ be any non-zero 2 sided prime ideal of A, $J = \mathcal{J} \cap R$. Then $N/NJ = N/N\mathcal{J}$ is a simple $\mathrm{End}_R(N)$ module. By the above discussion, N/NJ does not contain a non-trivial (RG, A)-bimodule, i.e. N is everywhere simple.

Finally, we show that $\langle\ ,\ \rangle$ is modular. To prove that

$$\psi : N_A \longrightarrow \mathrm{Hom}_A({}_AN, {}_AI) : n \longmapsto (m \longmapsto \langle m, n \rangle)$$

is an isomorphism, it suffices to verify this mod J for any non-zero prime ideal J of R. Let a bar denote reduction mod J. Since $\bar{\psi}$ is a right A module homomorphism, $\mathrm{Ker}(\bar{\psi})$ is a right A module. Also, G leaves $\langle\ ,\ \rangle$ invariant, so $\mathrm{Ker}(\bar{\psi})$ is a left RG module also. But N is simple everywhere, so $\mathrm{Ker}(\bar{\psi}) = 0$ or $\mathrm{Ker}(\bar{\psi}) = N$. Now $\mathrm{Ker}(\bar{\psi}) = N$ is easily seen to imply $A/JA \cong I/JI = 0$, a contradiction. Therefore, $\bar{\psi}$ is injective. A comparison of dimensions over $\bar{R}$ then shows that $\bar{\psi}$ is surjective too, which proves our assertion. ∎

If $D = K$ and $\tau = \mathrm{id}$, all the definitions before Theorem 3.6 still make sense, mutatis mutandis, and instead of hermitian forms, we obtain the usual quadratic forms. However, we need one extra definition.

DEFINITION 3.7. *Let $\langle\ ,\ \rangle$ be a quadratic form on a projective R module N and let I be the fractional R ideal generated by $\{\langle m, n\rangle ; m, n \in N\}$. The form $\langle\ ,\ \rangle$ will be called even if and only if for any prime ideal J of R such that $2 \in J$ and $\forall m, n \in N: \langle m, n \rangle \in IJ$.*

THEOREM 3.8. *Let $\pi : RG \twoheadrightarrow B$ be an epimorphism from a group ring RG onto a non-trivial Azumaya algebra B. If $[B] = 0$ in $\mathrm{Br}(R)$, then there exists a projective R module N, an ideal I of R and a quadratic form $\langle\ ,\ \rangle : N \times N \longrightarrow I$ such that*

i $B \cong \mathrm{End}_R(N)$

ii $\forall g \in G, \forall m, n \in N: \langle gm, gn \rangle = \langle m, n \rangle$

iii *N is everywhere simple.*

iv *$\langle\ ,\ \rangle$ is a positive definite, even, modular, quadratic form.*

PROOF. The proof of Theorem 3.6 may be copied almost verbatim. Note that the existence of an R lattice N such that $\mathrm{End}_R(N) \cong B$ is now an immediate consequence of the fact that $[B] = 0$ in $\mathrm{Br}(R)$. We still have to verify that $\langle\ ,\ \rangle$ is even. Let J be any prime ideal of R such that $2 \in J$ and let a bar denote reduction mod$J$. Then $\phi : \bar{N} \longrightarrow \bar{I} : n \longmapsto \langle n, n \rangle$ is a homomorphism. Since $\langle\ ,\ \rangle$ is modular, there exists a unique $q \in \bar{N}$ such that $\phi(n) = \langle q, n \rangle$. Since G leaves $\langle\ ,\ \rangle$ invariant, $gq = q$ and therefore $\bar{R}q$ is a RG submodule of $\bar{N}$. Now $\bar{N}$ is simple, so $\bar{R}q = \bar{N}$ or $\bar{R}q = 0$. If $\bar{R}q = \bar{N}$, then $\bar{B} = \mathrm{End}_{\bar{R}}(\bar{N}) = \bar{R}$, which contradicts our assumption that B is non-trivial. So $q = 0$ and $\forall n \in N: \langle n, n \rangle \in IJ$. ∎

The extra information that $\langle\ ,\ \rangle$ is even when $[B] = 0$ in $\mathrm{Br}(R)$ has no analogue when $[B] \neq 0$. This is due to the fact that, for any non-trivial Azumaya algebra A, the 2 sided ideal generated by $\{a + \tau(a)\}$ is equal to tr(A)A. Since A is Azumaya, tr(A)$A = A$. This may easily be verified by localization, a chore which is left for the reader.

Since even modular quadratic forms occur rather seldomly, Theorem 3.8 puts a severe restriction on the possible Schur algebras such that $[B] = 0$ in Br(R). We illustrate this for the case $R = \mathbb{Z}$.

COROLLARY 3.9. *If $M_n(\mathbb{Z})$ is a Schur algebra, then $n = 1$ or $8|n$.*

PROOF. Even modular forms of rank n only exist when $8|n$ (cf. [20], p. 92, Corollary 2).

REMARK 3.10. The above corollary was already proved, in a different form, by Thompson (cf. [23]). Actually, the condition $8|n$ is also sufficient. For $R = \mathbb{Z}$, all Schur algebras are therefore known. For a proof of this the reader is referred to [10].

As automorphism groups of positive definite, even quadratic forms tend to have an intricate structure, one may wonder whether it is possible to represent Schur algebras by means of easy groups such as solvable or nilpotent groups. Theorem 2.1. shows that E_{48}, a solvable group, spans a Schur algebra over $\mathbb{Z}[\sqrt{2}]$. We now show that Schur algebras over number rings can not be obtained as epimorphic image of group rings where the group is nilpotent.

THEOREM 3.11. *If G is nilpotent, then RG has no non-trivial epimorphic image which is Azumaya over R.*

PROOF. Let $\pi : RG \twoheadrightarrow A$ be a representation of a Schur algebra, assume that G is nilpotent and $A \neq R$. Choose a prime p such that p divides $|G|$ and $\pi(RG_p) \neq R$, where G_p denotes the unique Sylow p-group of G. It is easy to see that such a prime exists. Since G is nilpotent, there exists a subgroup H of G such that $G \cong G_p \times H$ (cf. [7], p. 139, Theorème 17.1.4). Let bar denote reduction mod J, where J is any prime ideal of R containing p, $\pi(\bar{R}G_p) = \bar{B}$, $\pi(\bar{R}H) = \bar{C}$. Since G_p and H commute, $\bar{B} \otimes \bar{C} \longrightarrow \bar{A} : \bar{b} \otimes \bar{c} \longmapsto \bar{b}\bar{c}$ is a ring epimorphism. By Maschke's Theorem, $\bar{R}H$ is semi-simple, hence so is $\bar{C}$. Also, $Z(\bar{C}) \subseteq Z(\bar{A})$, so $\bar{C}$ is actually simple. By the double commutator theorem, (cf. [5], p. 57 Theorem 4.3) it follows that $\bar{B}$ is simple too. Then $\bar{R}G_p \twoheadrightarrow \bar{B}$ factors through $\bar{R}G_p / \operatorname{rad}(\bar{R}G_p)$. But G_p is a p-group, so $\bar{R}G_p / \operatorname{rad}(\bar{R}G_p) \cong \bar{R}$ (cf. [2], p. 114, Theorem 5.20). Hence $\bar{R} = \bar{B}$, which implies $R = B$. This contradicts our choice of p. ∎

ACKNOWLEDGMENT. The author wishes to thank Prof. Dr. K. Roggenkamp for a private communication concerning the contents of § 3. He also thanks Prof. Dr. F. Van Oystaeyen for stimulating conversations and the referee for his very careful reading of the manuscript.

REFERENCES

1. L. Childs, *Azumayas over number rings as crossed products*, preprint 1986.

2. C. W. Curtis and I. Reiner, *Methods of representation theory with applications to finite groups and orders*. Pure & Applied Mathematics. Wiley Interscience Series of Texts, Monographs and Tracts, 1981.

3. F. De Meyer and R. Mollin, *The Schur group, orders and their applications.* Lecture Notes Mathematics **1142**, Springer-Verlag, Berlin, 205–209, 1985.
4. ———, *The Schur group of a commutative ring*, Journal of Pure and Applied Algebra **35**(1985), 117–122.
5. F. De Meyer and E. Ingraham, *Separable algebras over commutative rings.* Lecture Notes in Mathematics, **181**, Springer-Verlag, Berlin, 1971.
6. G. Karpilovsky, *Projective representations of finite groups.* Marcel Dekker Inc., 1985.
7. M. Kargapolov and I. Merzliakov, *Éléments de la théorie des groupes.* Traduction Française, Éditions Mir, Moscou, 1985.
8. F. Lorenz and H. Opolka, *Einfache Algebren und projective Darstellungen endlicher Gruppen*, Mathematische Zeitschrift **162**(1978), 175-186.
9. P. Nelis and F. M. J. Van Oystaeyen, *The projective Schur subgroup of the Brauer group and root groups of finite groups*, Journal of Algebra, to appear.
10. P. Nelis, *Integral matrices spanned by finite groups*, U.I.A. preprint, **12**, 1990.
11. ———, *The Schur group conjecture for the ring of integers of a number field*, Proc. American Math. Soc., to appear.
12. M. Orzech and C. Small, *The Brauer Group of Commutative Rings.* Lecture Notes in Pure and Applied Mathematics, **11**, 1975.
13. I. Reiner, *Maximal orders.* L. M. S. Monographs **5**, 1975.
14. C. R. Riehm, *Linear and quadratic Schur subgroups*, Lecture Notes, 1988, preprint.
15. ———, *The linear and quadratic Schur subgroups over the S-integers of a number field*, American Mathematical Society, **107–1**(1989), 83–87.
16. ———, *The Schur subgroup of the Brauer group of cylotomic rings of integers*, American Mathematical Society, **103–1**(1988), 27–30.
17. D. J. Saltman, *Azumaya algebras with involution*, Journal of Algebra, **52**(1978), 526–539.
18. W. Scharlau, *Involutions on simple algebras and orders*, Canadian Mathematical Society Conference Proceedings, **4**(1984), 141–157.
19. I. Schur, *Untersuchungen über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen.* Gesammelte Abhandlungen **1**, 198–250, Springer Verlag, Berlin, 1973.
20. J. P. Serre, *Cours d'Arithmétique*, le Mathématicien (P. U. F.), **2**(1970).
21. ———, *Corps Locaux.* Hermann, Paris, 1962.
22. R. G. Swan, *Projective modules over group rings and maximal orders*, Annals of Mathematics, **76–1**(1962), 55–61.
23. J. G. Thompson, *Finite groups and even lattices*, Journal of Algebra, **38**(1970), 523–524.
24. M. F. Vigneras, *Arithmétique des Algèbres de Quaternions.* Lecture Notes in Mathematics, **800**, Springer-Verlag, Berlin, 1980.
25. T. Yamada, *The Schur subgroup of the Brauer group.* Lecture Notes in Mathematics, **397**, Springer-Verlag, Berlin, 1974.
26. È. M. Žmud, *Symplectic geometries of finite abelian groups*, Mat. Sbornik **86-1 (128)**(1971), English translation: Mathematics of the USSR Sbornik, American Mathematical Society, **15-1**(1971), 7–29.

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