ISRAEL JOURNAL OF MATHEMATICS, Vol. 37, No. 3, 1980

RATIONAL DIVISION ALGEBRAS AS SOLVABLE CROSSED PRODUCTS

BY
JACK SONN

ABSTRACT

Let G be a finite group. If there exists a division algebra central over the rationals $\mathbf{Q}$ which is a crossed product for G, then according to a theorem of Schacher, the Sylow subgroups of G are all metacyclic.† The converse is proved here to hold in the following cases: (1) G metacyclic; (2) The Sylow 2-subgroups of G are cyclic (this implies G solvable); (3) G is solvable and the Sylow 2-subgroups of G are dihedral of order larger than 8.

Let D be a division algebra finite dimensional and central over $\mathbf{Q}$, the rational number field. D is a *crossed product* for a group G if there is a maximal subfield K of D, Galois over $\mathbf{Q}$, whose Galois group $G(K/\mathbf{Q})$ is isomorphic to G. It is well known that D is a crossed product for the cyclic group C_n of order n, where the dimension of D over $\mathbf{Q}$ is n^2. Schacher [8] posed the question as to which other groups are possible, i.e., for which groups G does there exist a division algebra D finite dimensional and central over $\mathbf{Q}$, such that D is a crossed product for G? Or more briefly, which G are "$\mathbf{Q}$-admissible"? The following arithmetic criterion [8, 2.1, 2.6] is necessary and sufficient for such G: there exists a Galois extension $K/\mathbf{Q}$ with $G(K/\mathbf{Q}) \simeq G$ such that for every prime p dividing the order of G, there are at least two rational primes q_1, q_2 and divisors Q_1, Q_2 of q_1, q_2 respectively in K, such that the decomposition groups $G(Q_1)$ and $G(Q_2)$ contain a Sylow p-subgroup of $G(K/\mathbf{Q})$. As a corollary [8, th. 4.1], if G is $\mathbf{Q}$-admissible then the Sylow subgroups of G are metacyclic. Thus far, the following such groups have been proved $\mathbf{Q}$-admissible: abelian metacyclic groups, the symmetric groups S_3, S_4, S_5 [8], A_4 [1], A_5, odd order nilpotent metacyclic groups [2], SL(2,5) [11].

Let us call a finite group G *Sylow-metacyclic* if all its Sylow subgroups are

† In this paper M is called *metacyclic* if it contains a cyclic normal subgroup N such that M/N is cyclic.

Received February 1, 1980

metacyclic. In this paper we apply Neukirch's theory of the embedding problem with prescribed local solutions to prove that the following solvable Sylow-metacyclic groups are $\mathbf{Q}$-admissible:

(1) metacyclic groups,

(2) Sylow-metacyclic grups having normal 2-complements; in particular, Sylow-metacyclic groups whose Sylow 2-subgroups are cyclic, and solvable Sylow-metacyclic groups whose Sylow 2-subgroups are dihedral of order larger than 8.

There are many Sylow-metacyclic groups, both solvable and nonsolvable, for which the question is still open. The smallest solvable example is the semidirect product of the quaternion group of order 8 with an automorphism of order 3. The finite simple groups PSL$(2, p)$ (p prime) are all Sylow-metacyclic; for $p > 5$ the question is open.

THEOREM 1. *Let G be a finite metacyclic group, N a positive integer. Then there exists a set S of N rational primes and a Galois extension $K/\mathbf{Q}$ such that $G(K/\mathbf{Q}) \simeq G$ and for every $p \in S$, $G(K_p/\mathbf{Q}_p) \simeq G$, where $\mathbf{Q}_p$ denotes the field of p-adic rational numbers, and K_p denotes the completion of K at any divisor of p in K.*

PROOF. We first reduce the proof to the case G is a semidirect product of two cyclic groups. Let G be the given metacyclic group. Then G is generated by two elements x, y, and the cyclic subgroup Y generated by y is normal in G. Let X be the cyclic subgroup generated by x. X acts on Y by conjugation in G. Let G_1 be the semidirect product of X and Y with respect to this action. There is a natural epimorphism $G_1 \to G$ given by $(x^i, y^j) \mapsto x^i y^j$. Suppose the theorem holds for G_1. Then there is a set S of N primes of $\mathbf{Q}$ and a Galois extension $K_1/\mathbf{Q}$ with $G(K_1/\mathbf{Q}) \simeq G_1$ such that for every $p \in S$, $G(K_{1,p}/\mathbf{Q}_p) \simeq G_1$. We therefore have an epimorphism $G(K_1/\mathbf{Q}) \to G$, the fixed field K of whose kernel is Galois over $\mathbf{Q}$ with $G(K/\mathbf{Q}) \simeq G$. For $p \in S$, $G(K_p/\mathbf{Q}_p)$ is isomorphic to a subgroup of $G(K/\mathbf{Q})$. On the other hand, $[K_1:\mathbf{Q}] = [K_{1,p}:\mathbf{Q}_p] = [K_{1,p}:K_p][K_p:\mathbf{Q}_p] \leqq [K_1:K][K:\mathbf{Q}] = [K_1:\mathbf{Q}]$, hence $[K_p:\mathbf{Q}_p] = [K:\mathbf{Q}]$. Thus $G(K_p/\mathbf{Q}_p) \simeq G(K/\mathbf{Q}) \simeq G$, for every $p \in S$.

We assume therefore that G is generated by x and y with defining relations

$$x^m = y^n = 1, \qquad x^{-1}yx = y^t.$$

Let μ_n denote the n-th roots of unity. By Dirichlet's density theorem [5, p. 138] there are infinitely many rational primes $q \equiv 1 \pmod{m}$. Hence we may choose a cyclic extension $T/\mathbf{Q}$ of degree m such that $T \cap \mathbf{Q}(\mu_n) = \mathbf{Q}$. By the

Frobenius density theorem [5, p. 134], there exist infinitely many rational primes p satisfying $p \equiv t \pmod{n}$, and p remains prime in T. Indeed, $G(T(\mu_n)/\mathbf{Q}) \simeq G(T/\mathbf{Q}) \times G(\mathbf{Q}(\mu_n)/\mathbf{Q})$. Let σ generate $G(T/\mathbf{Q})$ and let τ be the automorphism of $\mathbf{Q}(\mu_n)/\mathbf{Q}$ which raises μ_n to the power t. The density theorem states that there are infinitely many p whose Artin symbols are (σ, τ). These p satisfy the desired conditions. Let S be any N of these. For each $p \in S$, $T_p/\mathbf{Q}_p$ is unramified of degree m, where T_p denotes the completion of T at a divisor of p in T. Thus T_p contains the $(p^m - 1)$-th roots of unity. Since $t^m \equiv 1 \pmod{n}$ and $p \equiv t \pmod{n}$, we have $p^m \equiv 1 \pmod{n}$. Hence T_p contains the n-th roots of unity, and $T_p(p^{1/n})$ is Galois over $\mathbf{Q}_p$ with Galois group $\simeq G$.

We construct the desired field K by solving an *embedding problem with prescribed local solutions* at the primes $p \in S$. Let $X \simeq G(T/\mathbf{Q})$ be a fixed isomorphism, relative to which we obtain an epimorphism $e : G \to G(T/\mathbf{Q})$. Our embedding problem is to construct a Galois extension $K/\mathbf{Q}$, $K \supseteq T$ such that

(i) $G(K/\mathbf{Q}) \simeq G$ and this isomorphism causes e to coincide with the restriction map $G(K/\mathbf{Q}) \to G(T/\mathbf{Q})$, and

(ii) for each $p \in S$, $K_p = T_p(p^{1/n})$, where K_p is the completion of K at any divisor of p in K.

Let $G_{\mathbf{Q}}$ denote the absolute Galois group $G(\tilde{\mathbf{Q}}/\mathbf{Q})$ of $\mathbf{Q}$ ($\tilde{\mathbf{Q}}$ = algebraic closure of $\mathbf{Q}$). The restriction map $G_{\mathbf{Q}} \to G(T/\mathbf{Q}) \simeq X$ makes Y a $G_{\mathbf{Q}}$-module, and by restriction a $G_{\mathbf{Q}_p}$-module for each $p \in S$. Let $H^1(G_{\mathbf{Q}}, Y)$ denote the first cohomology group of $(G_{\mathbf{Q}}, Y)$. Now there exists a K satisfying (i) by a theorem of Scholz [9; 4, p. 101]. Therefore by a theorem of Neukirch [6, 2.5] there is a K satisfying (i) and (ii) provided the mapping

$$H^1(G_{\mathbf{Q}}, Y) \to \prod_{p \in S} H^1(G_{\mathbf{Q}_p}, Y)$$

is surjective, where the arrow denotes the product of the restriction maps over $p \in S$.

Set $Y' = \mathrm{Hom}(Y, \mu_n)$. $G_{\mathbf{Q}}$ acts on Y' by the rule $f^z(y) = f(y^{z^{-1}})^z$, $y \in Y$, $z \in G_{\mathbf{Q}}$. Let $\mathbf{Q}(Y') = T'$ denote the fixed field of the subgroup $G_{\mathbf{Q}}$ acting trivially on Y'. Then $T' \subseteq T(\mu_n)$. Let $G' = G(T'/\mathbf{Q})$, G'_p the decomposition group of a prime divisor of p in T'. Then $G'_p \simeq G(T'_p/\mathbf{Q}_p)$. Also $T'_p \leqq (T(\mu_n))_p = T_p(\mu_n) = T_p$. Hence G'_p is cyclic for each $p \in S$. It follows from [6, 6.4(b)] that the cohomology map above is surjective, q.e.d.

Taking $N = 2$, we see that Schacher's arithmetic criterion for $\mathbf{Q}$-admissibility is fulfilled for all metacyclic groups, hence

COROLLARY. *Every finite metacyclic group is* $\mathbf{Q}$*-admissible.*

Let G be a finite group, p a prime dividing $|G|$. A *normal p-complement* in G is a normal complement of a Sylow p-subgroup of G, i.e. a normal subgroup of G of order prime to p and index a power of p.

THEOREM 2. *Let G be a Sylow-metacyclic group having a normal 2-complement. Then G is $\mathbf{Q}$-admissible.*

PROOF. Let H be a Sylow 2-subgroup of G, N the normal 2-complement. Then $G = HN$, $H \cap N = 1$. Since H is metacyclic, by Theorem 1, H is $\mathbf{Q}$-admissible. Accordingly let $K/\mathbf{Q}$ be Galois with $G(K/\mathbf{Q}) \simeq H$ and let $q_i = q_i(2)$, $i = 1,2$ be two odd primes such that $G(K_{q_i}/\mathbf{Q}_{q_i}) \simeq H$. From the proof of Theorem 1 we may assume also that $K \cap \mathbf{Q}(\mu_n) = \mathbf{Q}$ and $q_i \nmid n$, $i = 1,2$, $n = |N|$.

Now let p be a prime dividing $|N|$, N_p a p-Sylow subgroup of N. As in the proof of Theorem 1, we can choose primes $q_i(p)$, $i = 1,2$ such that N_p is a Galois group over $\mathbf{Q}_{q_i(p)}$, $i = 1,2$. The conditions that determine $q_i(p)$ can be expressed by prescribing a value of the Frobenius symbol in a field $\mathbf{Q}(\mu_{p^t})$, where t is some positive integer. By choice of K,

$$\mathbf{Q}(\mu_{p^t}) \cap K = \mathbf{Q},$$

hence by the Frobenius density theorem, we may assume that $q_i(p)$ splits completely in K, $i = 1,2$. We may also assume that the set of primes $S = \{q_i(p): i = 1,2;\ p \mid |N|\}$ is distinct.

Consider the embedding problem given by $f: G \to G/N \cong G(K/\mathbf{Q})$. A solution is any homomorphism $g: G(\tilde{\mathbf{Q}}/\mathbf{Q}) \to G$ such that $fg = \text{res}(\tilde{\mathbf{Q}}/K)$. Since f splits, there is a trivial solution. For each $q = q_i(p) \in S$, let $L(q)/\mathbf{Q}_q$ be a Galois extension with Galois group N_p. Since $K_q = \mathbf{Q}_q$ for $q \in S$, $L(q)$ is a solution field to the corresponding local embedding problem. By a theorem of Neukirch [7, p. 148], there is a global surjective solution $L/\mathbf{Q}$ to the embedding problem whose localizations L_q coincide with $L(q)$ for each $q \in S$. (Note that N is solvable, e.g. by the Feit–Thompson theorem.) Thus $L/\mathbf{Q}$ satisfies the Schacher criterion for $\mathbf{Q}$-admissibility of G, q.e.d.

COROLLARY. *Any Sylow-metacyclic group whose 2-Sylow subgroups are cyclic is $\mathbf{Q}$-admissible.*

PROOF. Such a group G has a normal 2-complement [10, p. 138].

We are grateful to David Chillag for helpful group-theoretic conversations. In particular, he pointed out to us the work of Gorenstein and Walter [3] on finite

groups with dihedral Sylow 2-subgroups. The main theorem of [3] implies immediately that *if G is a solvable Sylow-metacyclic group whose Sylow 2-subgroups are dihedral of order greater than* 8, *then G has a normal 2-complement, and therefore is* **Q**-*admissible* by Theorem 1.

NOTE. D. Chillag has communicated to the author that every finite solvable Sylow-metacyclic group has a normal $\{2,3\}$-Hall complement. In view of this, Theorem 2 above can be transformed into a reduction theorem, which yields in particular the following result: *every finite solvable Sylow-metacyclic group whose* $\{2,3\}$-*Hall subgroups are metacyclic is* **Q**-*admissible.* Details will appear elsewhere.

REFERENCES

1. B. Gordon and M. Schacher, *Quartic coverings of a cubic*, J. Number Theory, to appear.

2. B. Gordon and M. Schacher, *The admissibility of* A_5, J. Number Theory **11** (1979), 498–504.

3. D. Gorenstein and J. W. Walter, *Finite groups whose Sylow* 2-*subgroups are dihedral*, J. Algebra **2** (1965), 85–151.

4. K. Hoechsmann, *Zum Einbettungsproblem*, J. Reine Angew. Math. **229** (1968), 81–106.

5. G. J. Janusz, *Algebraic Number Fields*, Academic Press, 1973.

6. J. Neukirch, *Uber das Einbettungsproblem der algebraische Zahlentheorie*, Invent. Math. **21** (1973), 59–116.

7. J. Neukirch, *On solvable number fields*, Invent. Math. **53** (1979), 135–164.

8. M. Schacher, *Subfields of division rings I*, J. Algebra **9** (1968), 451–477.

9. A. Scholz, *Über die Bildung algebraischen Zahlkörper mit auflosbarer galoischer Gruppe*, Math. Z. **30** (1929), 332–356.

10. W. R. Scott, *Group Theory*, Prentice-Hall, N.J., 1964.

11. J. Sonn, SL(2, 5) *and Frobenius Galois groups over* **Q**, Canad. J. Math., to appear.

DEPARTMENT OF MATHEMATICS
TECHNION — ISRAEL INSTITUTE OF TECHNOLOGY
HAIFA, ISRAEL