Q-ADMISSIBILITY OF CERTAIN NONSOLVABLE GROUPS†

BY

ELIAS ABBOUD

Department of Mathematics, Technion — Israel Institute of Technology, Haifa 32000, Israel

ABSTRACT

A finite group G is called Q-admissible if there exists a finite dimensional central division algebra over Q, containing a maximal subfield which is a Galois extension of Q with Galois group isomorphic to G. It is proved that S_5^-, one of the two nontrivial central extensions of S_5 by $Z/2Z$, is Q-admissible. As a consequence of that result and previous results of Sonn and Stern, every finite Sylow-metacyclic group, having A_5 as a composition factor, is Q-admissible.

Introduction

Let Q be the field of rational numbers. Schacher gave in his paper [2] the following definition:

A finite group G is called Q-admissible $\Leftrightarrow$ There exists a finite dimensional central division algebra over Q containing a maximal subfield which is a Galois extension of Q with Galois group $\simeq G$.

We may replace Q by any field k.

Let S_5^- be the central extension of C_2 by S_5 which contains D_{16}' as a 2-sylow subgroup, where

$$D_{16}' = \langle x, y x^2 = y^8 = 1, x^{-1}yx = y^3 \rangle.$$

In this paper we prove the following theorem: S_5^- is Q-admissible.

† This paper is part of a M.Sc. thesis written at the Technion — Israel Institute of Technology, under the supervision of Professor J. Sonn, whom the author wishes to thank for his valuable guidance.

Received June 3, 1985 and in revised form May 7, 1987

Preliminaries

Let p denote a prime divisor of the field k nd ν a prime integer dividing $|G|$. Schacher in [2] characteriszed k-admissibility in terms of local Galois groups:

CRITERION. A finite group G is k-admissible $\Leftrightarrow$ There exists a Galois extension $L \mid k$ such that $G(L/k) \simeq G$ and for every prime $\nu \mid^{|G|}$, $G(L_p \mid k_p)$ contains a ν-sylow subgroup for two different prime divisors p of k.

Thus, we first seek a method for realizing groups over fields. This leads us to embedding problems.

Sonn has written a brief introduction on embedding problems and some of their properties. We refer the reader to [4] and [5] at least for reading the definitions of the local and global embedding problems.

CONSEQUENCES. On the basis of the theorems and lemmas found in [4] and [5] we can prove the following two corollaries:

COROLLARY 1. *Let there be given the embedding problem*:

$$(*)\qquad \begin{array}{c} G(\bar{Q}_p \mid Q_p) \\ \downarrow \\ 1 \to C_2 \to E_p \xrightarrow{j_p} G(K_p \mid Q_p) \to 1 \end{array}$$

where Q_p is the field of p-adic numbers, $p \neq 5$, and $\bar{Q}_p$ is its separable closure. If $K_p = Q_p(\pi^{1/5})Q_p(\theta)$, where π is a prime element of Q_p, θ a primitive 5th root of unity, then the embedding problem is solvable.

PROOF. $K_p \mid Q_p$ is a Galois extension. If $p \equiv 1(5)$, then $G(K_p \mid Q_p) \simeq C_5$ [6, p. 48]. By [4, Lemma 3] the embedding problem $(*)$ has a solution. Assume $p \not\equiv 1(5)$, then $p^4 \equiv 1(5)$ and the order of p in Z_5 is 2 or 4. Thus, $G(K_p \mid Q_p) \simeq C_5 \cdot C_4$ or $C_5 \cdot C_2$ ($A \cdot H$ means semi-direct product). Let H be a subgroup of order 5 of E_p. Obviously, H is normal in E_p and $H \cap C_2 = \{1\}$.

Now, the embedding problem:

$$1 \to C_2 \to E_p/H \to G(Q_p(\theta)/Q_p) \to 1$$

is solvable by [4, Lemma 3].

Let L_p' be a solution field, then $[L_p' : Q_p]$ is a power of 2. Therefore $L_p' \cap K_p = Q_p(\theta)$ so by [5, Lemma 1] the embedding problem $(*)$ has a solution.

COROLLARY 2. *The embedding problem $(*)$ is also solvable if $K_p = F_1F_2$*

(K_p is the compositum of F_1&F_2), where $F_1 \mid Q_p$ is totally and tamely ramified extension of degree 3, $F_2 \mid Q_p$ is unramified extension of degree 2 and F_1F_2 contains the 3rd root of unity.

PROOF. In this case, $G(K_p \mid Q_p) \simeq C_3 \cdot C_2$ and the preceding arguments yield the result.

Realizing S_5 over Q and Laguerre polynomials

Turning back to S_5^-, which is a central extension of C_2 by S_5, we have the following exact row:

$$1 \to C_2 \to S_5^- \to S_5 \to 1$$

First we prove that S_5 is realizable over Q and then go on to verify that the following embedding problem is solvable:

$$\begin{array}{c} G(\bar{Q} \mid Q) \\ \downarrow \\ 1 \to C_2 \to S_5^- \to G(K \mid Q) \simeq S_5 \to 1 \end{array}$$

($\bar{Q}$ is the separable closure of Q). By [4, Lemma 2] it is enough to investigate the local embedding problems at every prime of Q except one.

By Schacher's criterion, the Q-admissibility of S_5^- is not yet accomplished. Thus in what follows we have to make sure that the other conditions in the criterion are satisfied.

Following Sonn [4] in proving the Q-admissibility of SL(2, 5) we realize S_5 over Q, using Laguerre polynomials. For λ, μ integers and $n = 5$ they are defined as follows:

$$F_5(\lambda, \mu, x) = x^5 - \frac{K_5}{1!}x^4 + \frac{K_4K_5}{2!}x^3 - \frac{K_3K_4K_5}{3!}x^2 + \frac{K_2K_3K_4K_5}{4!}x - \frac{K_1K_2K_3K_4K_5}{5!}$$

where $K_m = m(\lambda + \mu m)$, $m = 1, 2, \ldots, 5$.

The discriminant of this polynomial is given by

$$D_5 = \mu^{10} \cdot 2^{10} \cdot 3^3 \cdot 5^5(\lambda + 2\mu)(\lambda + 3\mu)^2(\lambda + 4\mu)^3(\lambda + 5\mu)^4.$$

Now, we describe a "Searching method" looking for pairs (λ, μ) that answer the following demands:

(a) The splitting field of $F_5(\lambda, \mu, x)$ has S_5 as a Galois group over Q.

(b) The local embedding problems in all primes of Q, except one at most, are solvable.

(c) The local conditions in the criterion of Q-admissibility are satisfied.

Let S be the set of pairs (λ, μ) satisfying the following conditions: (1)–(7). The search of (λ, μ) satisfying (a), (b), (c) will be carried out inside S (we do not assert that (1)–(7) imply (a)–(c)).

(1) λ, μ integers.

(2) $\lambda + 5\mu = 2a$, a is prime.

(3) $\lambda + 4\mu = 5pq$, $p, q \equiv 3(8)$ (p, q primes).

(4) $\lambda/\mu > -2$, μ is prime.

(5) $\lambda + 3\mu = 3^s 2^j b$, $s \geqq 1, j \geqq 4$, b (prime) $\equiv 1(3)$ or $b = 1$.

(6) $\lambda + 2\mu = c$, c (prime) $\equiv -1(4)$.

(7) $\sqrt{D_5} \in Q_5$.

The rationale for this is as follows: The prime 2, which appears in (2), is connected with the local embedding problem at $p = 2$. If we choose "a" to be prime then the polynomial $F_5(\lambda, \mu, x)$ will be Eisentein and the embedding problem is solvable at $p = a$.

In (3) we demand $p, q \equiv 3(8)$, assuring the existence of the local conditions at two places (we want the dehedral group of order 8 to be a local Galois at two primes).

By (4), we assure that all roots of the polynomial are real [4] and so its splitting field is totally real. The condition "μ is prime" gives no additional primes in the discriminant.

In (5) we want $3 \cdot 2^4 \mid \lambda + 3\mu$, this is helpful for solving the embedding problems at $p = 2, 3$. In the quotient $(\lambda + 3\mu)/48$ it is preferable to appear powers of 2, 3. We ask $b \equiv 1(3)$ since then it is easy to solve the local embedding problem at $p = b$. Concerning (6), the condition $c \equiv -1(4)$ is useful whenever the polynomial $F_5(\lambda, \mu, x)$ factors, mod c, into the form

$$F_5(\lambda, \mu, x) \equiv x^2(x - \alpha)(x^2 + \beta x + \gamma) \pmod c$$

so that the local Galois groups, at $p = c$, is $C_2 \times C_2$ and the embedding problem is solvable.

Finally, we demand $\sqrt{D_5} \in Q_5$, so that $G(K_p \mid Q_p)$ is a subgroup of A_5 and the local embedding problem is solvable at $p = 5$.

Now, we simplify the equations that appear in (1)–(7). From (2) and (3) we get:

$$\lambda = 25pq - 8a, \quad \mu = 2a - 5pq$$

so that

$$\lambda + 3\mu = 10pq - 2a, \quad \lambda + 2\mu = 15pq - 4a.$$

In (5) we want $48 \mid \lambda + 3\mu$ or $10pq - 2a = 48k$ so that

$$a = 5pq - 24k \qquad (k \text{ integer}).$$

Thus $\lambda/\mu > -2$ (condition (4)) implies

$$\frac{5pq}{96} < k < \frac{5pq}{48}.$$

These previous equations of λ, μ with the last inequality of k assure the validity of conditions (2), (3), (4) (except for "μ is prime") and $48 \mid \lambda + 3\mu$. The condition $D_5 \in Q^{*2}$ is equivalent to [6, p. 79]

$$3pq(\lambda + 2\mu) \equiv 1, 4(5).$$

For solving the embedding problem at $p = 2$ we avoid the case when $(K_1K_2K_3K_4K_5)/5!$, is divisible by 2^{5+3t} (t positive integer). In addition, if everything goes well, for solving the local embedding problem at $p = c$ it remains to check whether or not

$$F_5(\lambda, \mu, x) \equiv x^2(x - \alpha)(x^2 + \beta x + \gamma) \pmod{c}.$$

Applying this method for $p, q = 11, 59$, one gets $34 \leqq k \leqq 67$. The pairs (a, μ) for which a and μ are primes are: (2309, 1373), (2237, 1229), (2213, 1181), (1973, 701), (1949, 653), (1887, 503), (1709, 173), (1637, 29).

But only two have all the properties (1)–(7), namely: (2213, 1181) and (1637, 29).

Thus the pairs (λ, μ) in question are: (1479, 1181) and (3129, 29).

Thus we have got two pairs (λ, μ) and thus two Laguerre polynomials that may solve the Q-admissibility of S_5^-, but only one pair is proved to solve it.

We introduce here the full solution considering the pair $\lambda = 3129$, $\mu = 29$.

The polynomial and discriminant are, respectively,

$$
\begin{aligned}
f(x) &= F_5(3129, 29, x) \\
&= x^5 - 2\cdot 5\cdot 1637x^4 + 2^2\cdot 5^2\cdot 11\cdot 59\cdot 1637x^3 \\
&\quad - 2^6\cdot 3\cdot 5^2\cdot 11\cdot 59\cdot 67\cdot 1637x^2 \\
&\quad + 2^5\cdot 3\cdot 5^2\cdot 11\cdot 59\cdot 67\cdot 1637\cdot 3187x \\
&\quad - 2^6\cdot 3\cdot 5\cdot 11\cdot 59\cdot 67\cdot 1637\cdot 1579\cdot 3187,
\end{aligned}
$$

$$D = D_5 = 2^{22}\cdot 3^5\cdot 5^8\cdot 11^3\cdot 59^3\cdot 67^2\cdot 29^{10}\cdot 1637^4\cdot 3187.$$

THEOREM. *The group S_5^- is Q-admissible.*

PROOF. Let K be the splitting field of $f(x)$ over Q.

We will see later that the local degrees of $K \mid Q$ at the primes 67, 11, 1637 are divisible by 3, 5, 8. Since $G(K \mid Q)$ is a subgroup of S_5 it follows that $G(K \mid Q) \simeq S_5$. Consider the following embedding problem:

$$
\begin{array}{c}
G(\bar{Q} \mid Q) \\
\downarrow \text{res} \\
1 \to C_2 \to S_5^- \xrightarrow{j} G(K \mid Q) \simeq S_5 \to 1
\end{array}
$$

Since K is totally real, $K_\infty = Q_\infty = R$ and the embedding problem is trivially solvable at $p = \infty$. At p which is unramified ($p \nmid D$) the local embedding is solvable by [4, Lemma 3]. It remains to investigate the prime divisors of D: 2, 3, 5, 11, 59, 67, 29, 1637, 3187. By [4, Lemma 2] we may omit one of them: $p = \mu = 29$.

$p = 1637$: $f(x) \in Q_p[x]$ is Eisenstein. If ω is a root of $f(x)$, then $Q_p(\omega)/Q_p$ is totally and tamely ramified extension of degree 5 [6, 3-3-1, p. 86]. Hence $Q_p(\omega) = Q_p(\pi^{1/5})$ where π is a prime element of Q_p [6, 3-4-3, p. 89]. Let θ be a primitive 5th root of unity, then $Q_p(\theta)/Q_p$ is unramified extension of degree 4 [6, 3-2-12, p. 85]. Therefore $K_p = Q_p(\omega)Q_p(\theta)$ and the local Galois group is: $G(K_p \mid Q_p) \simeq C_5 \cdot C_4$. By Corollary 1 the local embedding problem has a solution.

$p = 67$: $f(x) \equiv x^3(x^2 - 22x + 3) \pmod{67}$, where $x^2 - 22x + 3$ is irreducible over Z_{67}. By Hensel's Lemma [6, 2-2-1, p. 45] $f(x) = a(x)b(x)$ over the ring of integers of Q_p, $\bar{a}(x) = x^3$, $\bar{b}(x) = x^2 - 22x + 3$ over the residue class ield, Z_{67}, of Q_{67}.

Now, the splitting field F_1 of $b(x)$ is unramifield Galois extension of degree 2

[6, 3-2-6, p. 82]. By Newton's polygon there are three roots, with ord $=\frac{1}{3}$, of $a(x)$ [6, 3-1-1, p. 74].

If $a(\omega)=0$ then $Q_p(\omega)/Q_p$ is totally and tamely ramified of degree 3, so $Q_p(\omega)=Q_p(\pi^{1/3})$. but Q_p contains the third root of unity since $67\equiv 1 \pmod 3$ [6, p. 48].

Thus $Q_p(\omega)/Q_p$ is Galois extension of degree 3, $K_p=Q_p(\omega)F_1$ and $G(K_p/Q_p)\simeq C_3\times C_2$ (direct product).

By Corollary 2 there exists a solution.

$p=2$: Define $f_1(y)=2^{-5}f(2y)$, hence

$$f_1(y)=y^5-a_1y^4+a_2y^3-2^3a_3y^2+2a_4y-2a_5, \qquad (a_i,2)=1$$

so

$$f_1(y)\equiv y^3(y^2-y+1) \pmod 2.$$

By Hensel's lemma $f_1(y)=a(y)b(y)$, $\bar{a}(y)=y^3$, $\bar{b}(y)=y^2-y+1$. Newton's polygon yields 3 roots of $a(y)$ with ord $=\frac{1}{3}$. Let ω be one of them, then $Q_p(\omega)/Q_p$ is totally and tamely ramified extension of degree 3, so $Q_p(\omega)=Q_p(\pi^{1/3})$. Besides, the splitting field of $b(y)$, which is unramified extension, equals $Q_p(\theta)$ where θ is a primitive 3rd root of unity [6, 6-5-5, p. 248].

Consequently, $K_p=Q_p(\omega)Q_p(\theta)$ and $G(K_p\mid Q_p)\simeq C_3\cdot C_2$.

By Corollary 2 the local embedding problem is solvable.

$p=3$: $f(x)\equiv x^3(x^2-2x+2) \pmod 3$. By Hensel's lemma $f(x)=a(x)b(x)$, $\bar{a}=x^3$, $\bar{b}=x^2-2x+2$.

The splitting field of $b(x)$ $L_p\mid Q_p$ is unramified of degree 2. The extension $Q_p(\sqrt{D})/Q_p$ is totally ramified of degree 2 [6, 3-3-1, p. 86]. Thus 4 divides the order of the group $G(K_p/Q_p)$. By Newton's polygon $a(x)$ has 3 roots of ord $=\frac{1}{3}$. Let $a(\omega)=0$ then $Q_p(\omega)\mid Q_p$ is totally and tamely ramified of degree 3. Now, the same argument as in [5, $p\cdot 3$] yields that $G(K_p\mid Q_p)\simeq S_3\times C_2$ and reduces the case to solving the following embedding problem,

$$1\to C_2\to Q_8\to C_2\times C_2\to 1$$

where Q_8 is the quaternion group of order 8, $Q_8=\langle x,y\mid x^4=1,\ x^2=y^2,\ yxy^{-1}=x^{-1}\rangle$. Since $[Q_p^*:Q_p^{*2}]=4$ [6, 6-5-1, p. 246], it follows that there is a unique Galois extension $K_p'\mid Q_p$ with Galois group $C_2\times C_2$ (see McCarthy, *Algebraic Extensions of Fields*, p. 50). In addition, the Galois group of the maximal 2-extension is isomorphic to the pro-2-group generated by x,y with defining relation $x^{-1}yx = y^3$ [3, p. 34]. But $3 \equiv -1(4)$, so that Q_8 is a quotient group of that of the maximal 2-extension and by Galois theory Q_8 is realizable over Q_p (field of p-adic integers). Let L_p/Q_p be an extension with Galois group Q_8, then $L_p \supseteq K'_p$. Now, since every automorphism of $C_2 \times C_2$ lifts to an automorphism of Q_8, the embedding problem is solvable (see also [5]).

$p = 5$: $f(x) \in Q_p[x]$ is Eisenstein and the order of $G(K_p \mid Q_p)$ is divisible by 5. Moreover,

$$Q_p(\sqrt{D}) = Q_p(\sqrt{3 \cdot 11 \cdot 59 \cdot 3187}),\ 3 \cdot 11 \cdot 59 \cdot 3187 \equiv 4 \pmod 5,$$

so that $\sqrt{D} \in Q_p$ [4, p. 79]. As a result, $G(K_p \mid Q_p)$ can be embedded in A_5. But A_5 does not contain subgroups of order 15, 20, 30 thus $|G(K_p \mid Q_p)|$ is equal to 5 or 10. If $|G(K_p \mid Q_p)| = 5$, then by [4, Lemma 3] the embedding problem is solvable, otherwise $|G(K_p \mid Q_p)| = 10$ and $G(K_p \mid Q_p) \simeq C_5 \cdot C_2$.

By [5, Lemma 1] it suffices to prove that the following embedding problem is solvable:

$$1 \to C_2 \to E_p/H \overset{j}{\to} G(F'/Q_p) \to 1$$

where $[F' : Q_p] = 2$. If E_p/H isomorphic to $C_2 \times C_2$ then the embedding problem $1 \to C_2 \to C_2 \times C_2 \to C_2 \to 1$ is trivially solvable, so assume $E_p/H \simeq C_4$.

Now Q_p contains the 4th root of unity, furthermore, F'/Q_p is either unramified or totally and tamely ramified. By [4, Lemma 3], in both cases, the embedding problem is solvable.

$p = 3187$: $f(x) \equiv x^2(x - 462)\,(x^2 + 27x - 806) \pmod{3187}$, $x^2 + 27x - 806$ is irreducible over Z_p. By Hensel's lemma it follows that $f(x) = a(x)(x - \alpha)(b(x))$ over the ring of integers of Q_p and $\bar{a} = x^2$, $\bar{b} = x^2 + 27x - 806$ over Z_p. By Newton's polygon $a(x)$ has two roots of ord $= \frac{1}{2}$, thus its splitting field is totally and tamely ramified extension of degree 2 and that of $b(x)$ is unramified of degree 2 over Q_p. Hence, $G(K_p \mid Q_p) \simeq C_2 \times C_2$.

The local embedding problem is

$$1 \to C_2 \to Q_8 \to C_2 \times C_2 \to 1$$

(Q_8 is the group of quaternions of order 8).

Q_8 is realizable over Q_p, since it is a quotient group of $G(Q_p(2)/Q_p)$ — the Galois group of the maximal 2-extension — which is isomorphic to the pro-2-group on 2 generators x, y with the defining relation $x^{-1}yx = y^{3187}$ [3, II-34].

Now $3187 \equiv -1 \pmod 4$ and the same argument as in $p = 3$ yields that the embedding problem is solvable.

$p = 11, 59$: $f(x) \equiv x^4(x - a) \pmod p$. By Hensel's lemma, $f(x) = a(x)(x - \alpha)$ where $\bar{a}(x) = x^4$. By Newton's polygon the 4 roots, ω, of $a(x)$ have $v(\omega) = \mathrm{ord}_\omega = \frac{1}{4}$.

$v(Q_p(\omega))$ is a discrete subgroup of $(R, +)$ (real numbers under addition) so $v(Q_p(\omega)) = \alpha Z$ for some $\alpha \in R^+$. Since $\mathrm{ord}_\omega = \frac{1}{4}$ it follows that $\alpha < \frac{1}{4}$, $e = (\alpha Z : Z) \geqq 4$. On the other hand $e \leqq 4$. Therefore $e = 4$ and $Q_p(\omega)/Q_p$ is totally and tamely ramified extension of degree 4. By [6, 3-4-3, p. 89] $E = Q_p(\pi^{1/4})$ where π is a prime element of Q_p. Let θ be a primitive 4th root of unity, then $Q_p(\theta) \mid Q_p$ is unramified of degree 2 [6, 3-2-12, p. 85]. So $K_p = Q_p(\omega)Q_p(\theta)$, $G(K_p \mid Q_p) \simeq C_4 \cdot C_2$. But $C_4 \cdot C_2 \simeq D_8$ hence $G(K_p \mid Q_p) \simeq D_8$ (dihedral group of order 8).

Consequently, the local embedding problem at $p = 11, 59$ is

$$1 \to C_2 \to D'_{16} \to D_8 \to 1$$

($C_2 =$ center D'_{16}). Let $G = G(Q_p(2) \mid Q_p)$ then G is generated by σ, τ with $\sigma^{-1}\tau\sigma = \tau^p$ [3, II-34]. One can readily verify that if the following embedding problem is solvable,

$$(*) \qquad \begin{array}{c} G \\ \downarrow \mathrm{res} \\ 1 \to C_2 \to D'_{16} \xrightarrow{j} D_8 \to 1 \end{array}$$

then

$$(**) \qquad \begin{array}{c} G(\bar{Q}_p \mid Q_p) \\ \downarrow \\ 1 \to C_2 \to D'_{16} \to D_8 \to 1 \end{array}$$

is solvable also.

Let us recall that

$$D_8 = \langle x, y \mid x^2 = y^4 = 1, xyx^{-1} = y^{-1} \rangle$$

$$D'_{16} = \langle u, v \mid u^2 = v^8 = 1, uvu^{-1} = v^3 \rangle.$$

Concerning (*), denote $\mathrm{res}\,\sigma = x_1$, $\mathrm{res}\,\tau = y_1$. Clearly x_1, y_1 generate D_8 and $x_1^{-1}y_1x_1 = y_1^p$.

If y_1 is of order 2 then $p \equiv 3(8)$ implies $p \equiv 1(2)$ and $x_1^{-1}y_1x_1 = y_1$ so that D_8

is abelian. Thus y_1 is of order 4, $x_1^{-1}y_1x_1 = y_1^{-1}$. In addition, $x_1 \notin \langle y_1 \rangle$ so that the order of x_1 is 2. As a result,

$$D_8 = \langle x_1, y_1 \mid x_1^2 = y_1^4 = 1, x_1^{-1}y_1x_1 = y_1^{-1} \rangle.$$

Now j is epimorphism, choose $v_1 = j^{-1}(y_1)$, $u_1 = j^{-1}(x_1)$. We will see that u_1, v_1 are generators of D'_{16} and satisfy the relation $u^{-1}v_1u_1 = u_1^p$, so that a solution of (*) can be selected by sending the pair (σ, τ) to (u_1, v_1), getting a commutative diagram.

Indeed, if $v_1 = u$ then $v_1^2 = e$, $y_1^2 = j(v_1^2) = e$ which is impossible. Similarly, if $v_1 = uv^j$ then $v_1^2 = (uv^j)^2 = v^{4j}$, but $c_2 = \{e_1 v^4\}$ is the center of D'_{16} so that $v_1^2 \in \{e, v^4\} = \ker j$ implies $y_1^2 = j(v_1^2) = e$, a contradiction. Thus $v_1 = v^j$. If $j = 2k$ then $v_1^2 = v^{4k} \in \ker j$, so $v_1 = v^j$ where j is odd. Now u_1 must be of the form uv^k and one can easily prove that v^j, uv^k (j is odd) form two generators of D'_{16}. Moreover,

$$u_1^{-1}v_1u_1 = v^{-k}u^{-1}v^juv^k = v^{-k}v^{3j}v^k = (v^j)^3 = v_1^3.$$

Finally the order of v_1 is 8 and for $p \equiv 3(8)$, $v_1^3 = v_1^p$ so that $u_1^{-1}v_1u_1 = v_1^p$.

We have demonstrated that S_5^- is realizable over Q. Let L be a solution field: $G(L \mid Q) \simeq S_5^-$. In order to prove its Q-admissibility we have to show, by the criterion, that for every $v = 2, 3, 5$, $G(L_p/Q_p)$ contains a v-sylow subgroup for two prime divisors p of Q. By virtue of Chebotarev's density theorem this condition is satisfied for cyclic sylow subgroups, i.e. for $v = 3, 5$. The 2-sylow subgroup is D'_{16}, we have seen that D_8 is local Galois group, $G(K_p \mid Q_p)$, at two places: $p = 11, 59$ (K is the splitting filed of $f(x)$). Now L_p is a local solution field of

$$1 \to C_2 \to S_5^- \xrightarrow{j} G(K \mid Q) \simeq S_5 \to 1$$

and since the extension of groups

$$1 \to C_2 \to D'_{16} \to D_8 \to 1$$

does not split, the local solution is surjective.

Consequently, $G(L_p \mid Q_p) \simeq D'_{16}$ at two primes: $p = 11, 59$.

Finally, we have:

COROLLARY. *Every finite Sylow metacyclic group, G, which has A_5 as a composition factor is Q-admissible.*

Proof. By a hint of Sonn in [5], S_5^- is sharply Q-admissible. By [1, Th.1.2] G is of the form $A \cdot N$, where A is one of: A_5, S_5, S_5^+, S_5^-, SL(2, 5).

Now, A_5 and SL(2, 5) are strong Q-admissible [1], in particular they are sharply Q-admissible. In addition, S_5^+ and S_5^- are sharply Q-admissible and S_5 is a homomorphic image of S_5^- (or S_5^+) so it has the same type of Q-admissibility. by [1, Th.2.1] with the version of sharply Q-admissibility, it follows that G is such a group, in particular G is Q-admissible.

References

1. D. Chillag and J. Sonn, *Sylow-metacyclic groups and Q-admissibility*, Isr. J. Math. **40** (1981), 307–323.

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

3. J. P. Serre, *Cohomologie Galoisienne*, Lecture Notes in Mathematics, Spring-Verlag, Berlin, 1965.

4. J. Sonn, SL(2, 5) *and Frobenius Galois groups over Q*, Can. J. Math. **32** (1980), 281–293.

5. L. Stern, *Q-Admissibility of Sylow-metacyclic groups having* S_5^+, *as quotient group*, preprint.

6. E. Weiss, *Algebraic Number Theory*, McGraw-Hill, New York, 1963.