Can. J. Math., Vol. XXXII, No. 2, 1980, pp. 281–293

$SL(2, 5)$ AND FROBENIUS GALOIS GROUPS OVER Q

JACK SONN

A finite transitive permutation group G is called a *Frobenius group* if every element of G other than 1 leaves at most one letter fixed, and some element of G other than 1 leaves some letter fixed. It is proved in [**20**] (and sketched below) that if k is a number field such that $SL(2, 5)$ and one other nonsolvable group $\hat{S}_5$ of order 240 are realizable as Galois groups over k, then every Frobenius group is realizable over k. It was also proved in [**20**] that there exists a quadratic (imaginary) field $\mathbf{Q}(\sqrt{D})$ over which these two groups are realizable. In this paper we prove that they are realizable over the rationals $\mathbf{Q}$, hence we obtain

THEOREM 1. *Every Frobenius group is realizable as the Galois group of an extension of the rational numbers* $\mathbf{Q}$.

$SL(2, 5)$ is the group of 2×2 matrices of determinant 1 over the field of five elements. Its center is $\pm I$, and modulo its center it is isomorphic to the simple group A_5, the alternating group on 5 letters. Thus $SL(2, 5)$ is a central extension of A_5 by a cyclic group C_2 of order 2. Similarly, $\hat{S}_5$ is a central extension of the symmetric group S_5 by C_2, and it is the one whose Sylow 2 subgroup is the generalized quaternion group of order 16. ($SL(2, 5)$ and $\hat{S}_5$ are in fact stem covers of A_5 and S_5 respectively [**4**, pp. 212–213]; see also Corollary to Theorem 3 below.)

We will prove that the splitting field K of the quintic

$$f(x) = x^5 + 2x^4 - 3x^3 - 5x^2 + x + 1$$

admits a quadratic extension $K(\sqrt{\alpha})$ Galois over $\mathbf{Q}$, with Galois group $\hat{S}_5$. Similarly, the splitting field of the quintic

$$g(x) = x^5 - 2.5.911x^4 + 2^2.3^5.5^2.911x^3 - 2^7.3^5.5^2.19.911x^2 + 2^6.3^5.5^2.19.911x + 2^7.3^6.5.19.101.911$$

admits a quadratic extension Galois over $\mathbf{Q}$ with Galois group $SL(2, 5)$.

§ 1 contains a collection of known facts on embedding problems; the proofs of the above statements on the quintics $f(x)$ and $g(x)$ appear in § 2.

We remark that there have recently appeared some results concerning arithmetic properties of extensions $K/\mathbf{Q}$ with Frobenius Galois group [**8, 9**].

Received March 22, 1978 and in revised form December 7, 1978. This research was supported in part by NRC grant A8778.

https://doi.org/10.4153/CJM-1980-021-4 Published online by Cambridge University Press

I would like to thank Hershel Kisilevsky for communicating to me the polynomial $f(x)$; it appears in the literature [**6**, p. 64] as a totally real quintic with small discriminant, and more of its interesting arithmetic properties have apparently been worked out by Kottwitz and Tate. Its distinction is that its splitting field K is totally real, unramified over $\mathbf{Q}(\sqrt{D})$, where $D = 36{,}497$ (a prime) is the discriminant of $f(x)$ (and of K), the Galois group of $K/\mathbf{Q}$ is S_5, and the class number of $\mathbf{Q}(\sqrt{D})$ is 1. This is a totally real analogue of the well-known example $x^5 - x + 1$.

I would also like to thank Tom Davison for several helpful discussions, as well as Carl Riehm and the Mathematics Department of McMaster University for their kind support and hospitality during the period in which this paper was written.

1. Embedding problems. Let k be a field, $\tilde{k}$ its separable closure, $G_k = G(\tilde{k}/k)$ the Galois group of $\tilde{k}/k$. Let K/k be a finite Galois extension. An *embedding problem for* K/k is given by an epimorphism

$$e: E \to G(K/k)$$

with E a finite group. A *solution* to this embedding problem is given by a homomorphism

$$f: G_k \to E$$

such that $e \circ f = \operatorname{Res}(\tilde{k}/K): G_k \to G(K/k)$, the restriction map. If f is surjective, then the fixed field of its kernel is a Galois extension L of k containing K with $G(L/k) \simeq E$.

For a group G and G-module A, let $H^i(G, A)$ denote the i^{th} cohomology group of the pair G, A. Suppose A is the kernel of e. Then the exact sequence

$$1 \to A \to E \to G(K/k) \to 1$$

determines uniquely a cohomology class $a \in H^2(G(K/k), A)$. The embedding problem has a solution if and only if $\inf(a) = 0$, where inf is the inflation map

$$\inf: H^2(G(K/k), A) \to H^2(G_k, A)$$

[**5**, p. 82], or [**10**].

Let k be a number field, v a prime of k, $\tilde{v}$ a prime of $\tilde{k}$ above v, $\tilde{k}_v$ an algebraic closure of k_v. A given (fixed) embedding of k into k_v (preserving v) can be extended to an embedding of $\tilde{k}$ into $\tilde{k}_v$ (preserving $\tilde{v}$), relative to which $\tilde{k}_v = \tilde{k}.k_v$, so we may identify $G(\tilde{k}_v/k_v)$ with the decomposition group $G_k(\tilde{v}) = G(\tilde{k}/\tilde{k} \cap k_v)$.

An embedding problem $e : E \to G(K/k)$ induces a local one given by

$$e_v: E_v \to G(K_v/k_v)$$

where $E_v = e^{-1}G(K_v/k_v)$, and $K_v = K.k_v$. A global solution restricts to a local solution, but surjectivity is not necessarily preserved.

https://doi.org/10.4153/CJM-1980-021-4 Published online by Cambridge University Press

Suppose E is a *central* extension of $G(K/k)$; i.e., $A = \ker(e) \subseteq \text{center}(E)$. Then A is a $G(K/k)$-module with trivial action, and is then naturally a G_k-module with trivial action. In this case, the map

$$H^2(G_k, A) \xrightarrow{\delta} \prod_v H^2(G_k(\tilde{v}), A) \quad (\text{one } \tilde{v} \text{ for each } v)$$

is injective, see [**5**, 3.7 and 6.1] or [**10**, Satz 4.7]. The preceding discussion yields

Lemma 1. *If k is a number field and $e: E \to G(K/k)$ is a central extension, then the embedding problem has a global solution if and only if the corresponding local embedding problem at v has a solution, for every prime v of k* [**5**, p. 96], [**10**, Satz 2.2].

Note that Ikeda's theorem [**19**, p. 416] implies that the global solution can be assumed surjective.

Suppose now that k is a number field containing the n^{th} roots of unity, n a positive integer, and that E is a central extension of $G(K/k)$, where $\ker(e) \simeq \mathbf{Z}/n\mathbf{Z}$.

The short exact sequences

$$0 \to \mathbf{Z}/n\mathbf{Z} \to \tilde{k}^* \xrightarrow{n} \tilde{k}^* \to 1$$

$$0 \to \mathbf{Z}/n\mathbf{Z} \to \tilde{k}_v^* \xrightarrow{n} \tilde{k}_v^* \to 1$$

yield, by Hilbert's Theorem 90, monomorphisms

$$H^2(G_k, Z/n\mathbf{Z}) \xrightarrow{i} H^2(G_k, \tilde{k}^*)$$

$$H^2(G_{k_v}, \mathbf{Z}/n\mathbf{Z}) \xrightarrow{i_v} H^2(G_{k_v}, \tilde{k}_v^*).$$

Consider the commutative diagram

$$(1)\qquad \begin{array}{ccccccc}
0 & \longrightarrow & H^2(G_k, \tilde{k}^*) & \xrightarrow[\Pi\gamma_v]{} & \Pi_v H^2(G_{k_v}, \tilde{k}_v^*) & \xrightarrow[\text{inv}]{} & \mathbf{Q}/\mathbf{Z} \\
 & & \uparrow{\scriptstyle i} & & \uparrow{\scriptstyle \Pi i_v} & & \\
 & & H^2(G_k, \mathbf{Z}/n\mathbf{Z}) & \xrightarrow[\Pi\delta_v]{} & \Pi_v H^2(G_{k_v}, \mathbf{Z}/n\mathbf{Z}) & & \\
 & & \uparrow{\scriptstyle \inf} & & \uparrow{\scriptstyle \Pi \inf_v} & & \\
 & & H^2(G(K/k), \mathbf{Z}/n\mathbf{Z}) & \xrightarrow[\Pi\rho_v]{} & \Pi_v H^2(G(K_v/k_v), \mathbf{Z}/n\mathbf{Z}) & &
\end{array}$$

The top row is exact [**21**, p. 196]. Let $a \in H^2(G(K/k), \mathbf{Z}/n\mathbf{Z})$. The image of a in $\mathbf{Q}/\mathbf{Z}$ is therefore zero. Suppose that v_0 is a fixed prime of k and that the embedding problem corresponding to a has a local solution at all $v \neq v_0$. Then $\inf_v \rho_v(a) = 0$ for all $v \neq v_0$, so

$$i_v \inf_v \rho_v(a) = 0, \text{ for } v \neq v_0.$$

https://doi.org/10.4153/CJM-1980-021-4 Published online by Cambridge University Press

But then $\prod_v i_v \inf_v \rho_v(a)$ has zero component for all $v \neq v_0$ and its image under inv is zero. That implies $i_{v_0} \inf_{v_0} \rho_{v_0}(a) = 0$ as well, so

$$\prod_v i_v \inf_v \rho_v(a) = 0 = (\prod \gamma_v) \circ i \circ \inf(a),$$

hence $\inf(a) = 0$ so the global embedding problem has a solution. We therefore have

LEMMA 2. *Let k be a number field containing the n^{th} roots of unity, n a positive integer, and let $e\colon E \to G(K/k)$ be a central extension with* $\ker(e) \simeq \mathbf{Z}/n\mathbf{Z}$. *Then if the embedding problem has a local solution at v for all primes v of k except one, then it has a global solution.* (cf. [**1**, Theorem 7, p. 423].)

We conclude this section with two simple and well-known facts about embedding problems for cyclic extensions of local fields, which will be used in the next section.

LEMMA 3. *Let k be a number field, v a prime of k, k_v the completion of k at v, K_v/k_v a cyclic extension of degree n, $e\colon E \to G(K_v/k_v)$ an embedding problem.*

1. *If K_v/k_v is unramified, then the embedding problem has a solution.*

2. *If K_v/k_v is totally and tamely ramified and E is cyclic, then the embedding problem is solvable if and only if k_v contains the m-th roots of unity, where $|E| = m.m'$, and m' is the largest divisor of $|E|$ prime to n.* (See [**80**], Satz 5.1).

Proof. 1. Let C be a cyclic subgroup of E of minimal order such that $C \ker(e) = E$; then $|C| = n.s$. A solution field (i.e. fixed field of the kernel of a solution map f) is the unramified extension of k_v of degree $n.s$, and the existence of a solution map f is insured by the fact that any automorphism of a factor group of a cyclic group C can be lifted to an automorphism of C.

2. Suppose k_v contains the m-th roots of unity. $K_v = k_v(\pi^{n^{-1}})$ for some prime π of k_v [**22**, p. 89]. Then a solution field is $k_v(\pi^{m^{-1}})$, keeping in mind the remark at the end of the previous case. Conversely, suppose L is a solution field. Then L/k_v is a cyclic extension containing K_v and $G(L/k_v)$ is isomorphic to a subgroup C of E such that $C \ker(e) = E$. Therefore C must be of order divisible by m, hence L contains a subfield $L_1 \supset K_v$ with $[L_1 : k_v] = m$. L_1/k_v is totally and tamely ramified since K_v/k_v is, hence $L_1 = k_v(\pi^{m^{-1}})$ for some prime π of k_v [**22**, p. 89] and k_v must then contain the m-th roots of unity.

We remark that the preceding proof shows that in the case K_v/k_v totally and tamely ramified, if k_v contains the m-th roots of unity and E is any group containing a cyclic subgroup C of order m such that $C \ker(e) = E$, the embedding problem has a solution. However, the converse to this is false. Take $k_v = \mathbf{Q}_3$, $K_v = \mathbf{Q}_3(\sqrt{3})$, E the quaternion group of order 8. This embedding problem has a solution, but $\mathbf{Q}_3$ does not contain the 4-th roots of unity.

https://doi.org/10.4153/CJM-1980-021-4 Published online by Cambridge University Press

2. Quintics. The results in § 1 make it easy to prove the desired facts about the polynomial $f(x) = x^5 + 2x^4 - 3x^3 - 5x^2 + x + 1$. The discriminant D of $f(x)$ is 36, 497, a prime congruent to 1 mod 4. It is easily checked that $f(x)$ is irreducible mod 2 and factors into the product $(x - 1)(x^4 + x - 1)$ of irreducible factors mod 3. Furthermore,

$$f(x) \equiv (x - 27031)^2(x - 15152)(x - 15789)(x - 24486) \pmod{D}$$

which shows both that the Galois group of $f(x)$ is S_5 and that $K/\mathbf{Q}(\sqrt{D})$ is unramified, where K is the splitting field of $f(x)$. Indeed, the above three factorizations of $f(x)$ mod 2, 3 and D show that $G(K/\mathbf{Q})$ contains a 5-cycle, a 4-cycle, and a transposition, and is therefore S_5. The factorization of $f(x)$ mod D shows that the local degree of $K/\mathbf{Q}$ at D is 2, which is also the local degree of $\mathbf{Q}(\sqrt{D})/Q$ at D. Hence D (or rather $\sqrt{D}$) splits completely in $K/\mathbf{Q}(\sqrt{D})$. Thus every prime of $\mathbf{Q}(\sqrt{D})$ (including ∞) is unramified in K. We therefore obtain the following result as an immediate application of § 1.

THEOREM 2. *Let K be the splitting field of the polynomial*

$$f(x) = x^5 + 2x^4 - 3x^3 - 5x^2 + x + 1$$

over $\mathbf{Q}$. *Then*

1. $G(K/\mathbf{Q}) \simeq S_5$.
2. *Every embedding problem* $e: E \to G(K/\mathbf{Q})$ *with* $\ker(e)$ *of order* 2 *has a (surjective) solution.*

Indeed, Lemma 3 implies that the local embedding problem is solvable at every prime, hence by Lemma 1, the global embedding problem is solvable.

We add that there are four nonisomorphic extensions E of S_5 by C_2, two of which contain $SL(2, 5)$ as a subgroup of index two.

We turn now to $SL(2, 5)$. An explicit example of a totally real polynomial $g(x) \in \mathbf{Q}[x]$ having Galois group A_5 over $\mathbf{Q}$ was given by Schur [**15**] in his investigation of Galois groups of some classes of polynomials in the book of Polya and Szego [**10**, p. 88]. For our purposes we are interested in the class of *generalized Laguerre polynomials* $L_n^{(\alpha)}(x)$, defined for non-negative integers n and real α by the equation

$$(2) \qquad \frac{d^n}{dx^n}(e^{-x}x^{n+\alpha}) = n!e^{-x}x^\alpha L_n^{(\alpha)}(x).$$

When $\alpha = 0$ one gets the ordinary Laguerre polynomials. When α is a rational number λ/μ, $L_n^{(\alpha)}$ has rational coefficients. In this case Schur normalizes $L_n^{(\alpha)}(x)$ to obtain the polynomials

$$(3) \qquad F_n(\lambda, \mu, x) = F_n(x) = (-1)^n n!\mu^n L_n^{(\lambda/\mu)}\left(\frac{x}{\mu}\right) = x^n - \frac{k_n}{1}x^{n-1} + \frac{k_{n-1}k_n}{2!}x^{n-2} - \ldots + (-1)^n\frac{k_1k_2\ldots k_n}{n!}$$

https://doi.org/10.4153/CJM-1980-021-4 Published online by Cambridge University Press

where $k_m = m(\lambda + \mu m)$, $m = 1, \ldots, n$. The recursion equations

(4) $\quad xF_n' = nF_n + k_nF_{n-1} \qquad (n \geqq 1,\ F_0 = 1)$

(5) $\quad F_n = (x - k_n + k_{n-1})F_{n-1} - \mu k_{n-1}F_{n-2} \quad (n \geqq 2)$

can be verified directly. Using (4), (5) and the formulas

(6) $\quad D_n = (-1)^{n(n-1)/2}\prod_a F_n'(\xi_a)$

where D_n is the discriminant of F_n, and ξ_a runs through the roots of F_n, and

(7) $\quad R_n = \mathrm{Res}(F_n, F_{n-1}) = \prod_a F_{n-1}(\xi_a) = \prod_b F_n(\eta_b)$

where R_n is the resultant of F_n and F_{n-1}, and η_b runs through the roots of F_{n-1}, Schur derives the formula

(8) $\quad D_n = n!\,\mu^{n(n-1)/2}k_2k_3{}^2k_4{}^3 \ldots k_n{}^{n-1}.$

For $\lambda = \mu = 1$ and n odd, D_n is a perfect square, and Schur shows that $F_n(1, 1, x)$ has Galois group A_n for n odd. Unfortunately, for $n = 5$, the splitting field of $F_5(1, 1, x)$, which has Galois group A_5, cannot be embedded into an extension having $SL(2, 5)$ as Galois group, because the embedding problem is not locally solvable at some primes (namely at 2 and 3). However, we will find an $F_5(\lambda, \mu, x)$ which fulfills all the necessary requirements.

In [**12**] it is shown that $L_n^{(\alpha)}(x)$ has all distinct real positive roots for $\alpha > -1$ [**12**, p. 274]. Nevertheless, the $L_n^{(\alpha)}(x)$ are defined for all α by formula (2). Since we will need to take $-2 < \alpha < -1$, we require the following lemma.

LEMMA 4. *$L_n^{(\alpha)}(x)$ has all real roots for $-2 < \alpha < -1$, hence so does $F_n(\lambda, \mu, x)$ for $-2 < \lambda/\mu < -1$.*

Proof. Let $-2 < \alpha < -1$ and write $\beta = \alpha + 1$. Then

$$e^{-x}x^{n+\alpha} = e^{-x}x^{n-1+\beta}.$$

Hence

$$n!e^{-x}x^{\alpha}L_n^{(\alpha)}(x) = \frac{d^n}{dx^n}e^{-x}x^{n+\alpha} = \frac{d}{dx}\frac{d^{n-1}}{dx^{n-1}}e^{-x}x^{n-1+\beta}$$

$$= (n-1)!\frac{d}{dx}e^{-x}x^{\beta}L_{n-1}^{(\beta)}(x).$$

Since $\beta > -1$, $L_{n-1}^{(\beta)}(x)$ has $n - 1$ distinct positive roots so $e^{-x}x^{\beta}L_{n-1}^{(\beta)}(x)$ changes sign $n - 1$ times along the positive real axis. Thus its derivative

$$\frac{n!}{(n-1)!}e^{-x}x^{\alpha}L_n^{(\alpha)}(x)$$

vanishes $n - 2$ times between the first and last roots of $L_{n-1}^{(\beta)}(x)$. Furthermore, if x_{n-1} is the largest root of $L_{n-1}^{(\beta)}(x)$, and if n is odd, say, then the leading coefficient of $L_{n-1}^{(\beta)}$ is positive, so $L_{n-1}^{(\beta)}(x)$ and hence $e^{-x}x^{\beta}L_{n-1}^{(\beta)}(x)$ is

https://doi.org/10.4153/CJM-1980-021-4 Published online by Cambridge University Press

increasing at $x = x_{n-1}$ so $L_n^{(\alpha)}(x_{n-1}) > 0$. The leading coefficient of $L_n^{(\alpha)}(x)$ is negative, so $L_n^{(\alpha)}(x)$ must vanish once more after x_{n-1}, hence $L_n^{(\alpha)}(x)$ has $n - 1$ positive real roots. But $L_n^{(\alpha)}(x)$ has real coefficients, so it must have n real roots. The argument is similar for n even.

This lemma can also be proved by showing that the recursive relations (5) yield a Sturm sequence for F_n.

Let us now take $n = 5$ and rewrite formula (8) according the definition $k_m = m(\lambda + \mu m)$ as

$$D_5 = \mu^{10}.2^{10}.3^3.5^5.(\lambda + 2\mu)(\lambda + 3\mu)^2(\lambda + 4\mu)^3(\lambda + 5\mu)^4. \tag{9}$$

In order that D_5 be a square, it is necessary that 3 and 5 appear to odd powers in $(\lambda + 2\mu)$ $(\lambda + 4\mu)$ and that the remaining primes in $(\lambda + 2\mu)$ $(\lambda + 4\mu)$ appear to even powers. For example, if λ and μ are chosen relatively prime such that $\lambda + 4\mu = 3^i5^j$ with i, j odd, it suffices to solve $3^i5^j - 2\mu = m^2$ for m. In fact in this last equation, if we choose any odd $m^2 < 3^i5^j$ then $\mu = \frac{1}{2}(3^i5^j - m^2)$, $\lambda = m^2 - 2\mu$ will do, provided m is not divisible by 3 or 5. Notice that $-2 < \lambda/\mu$. We now choose $i = 5$, $j = 1$, $m = 1$ (found by trial and error). Then

$$\mu = \tfrac{1}{2}(3^5.5 - 1) = 607, \text{ a prime},$$
$$\lambda = 1 - 2\mu = -1213,$$

$$\begin{aligned} g(x) = F_5(x) = x^5 &- (2.5.911)x^4 + (2^2.3^5.5^2.911)x^3 \\ &- (2^7.3^5.5^2.19.911)x^2 + (2^6.3^5.5^2.19.911)x \\ &+ 2^7.3^6.5.19.101.911. \end{aligned} \tag{10}$$

$g(x)$ has all real roots and its discriminant is

$$D = 2^{24}.3^{18}.5^8.(19)^2.(607)^{10}.(911)^4 \tag{11}$$

which is of course a square, so the Galois group of $g(x)$ is a subgroup of A_5. It will be clear from the ensuing discussion that it is the full group A_5.

Let K be the splitting field of $g(x)$. We investigate the local extensions $K_p/\mathbf{Q}_p$. Since K is totally real, $K_\infty = \mathbf{Q}_\infty = \mathbf{R}$, so the embedding problem is solvable trivially at $p = \infty$. At a prime p which is unramified in K, the embedding problem is locally solvable by Lemma 3. It remains to investigate the prime divisors of D, namely 2, 3, 5, 19, 607, 911, and by Lemma 2, we may omit one of them, 607.

$p = 911$. $g(x)$ is Eisenstein with respect to $p = 911$ hence is irreducible over $\mathbf{Q}_p$. If $g(\alpha) = 0$ then $\mathbf{Q}_p(\alpha)/\mathbf{Q}_p$ is totally and tamely ramified of degree 5, [**22**, p. 86] hence [**22**, p. 89] $\mathbf{Q}_p(\alpha) = \mathbf{Q}_p(\pi^{1/5})$, where π is a prime element of $\mathbf{Q}_p$. But $911 \equiv 1 \pmod 5$ so $\mathbf{Q}_p$ contains the 5th roots of unity. But then $\mathbf{Q}_p(\alpha)$ is Galois over $\mathbf{Q}_p$. K_p is the composite of the $\mathbf{Q}_p(\alpha)$ as α runs through the roots of $g(x)$, so $K_p/\mathbf{Q}_p$ is abelian of exponent 5. Since $G(K_p/\mathbf{Q}_p)$ is a subgroup of A_5 it must be a cyclic group of order 5, so $K_p = \mathbf{Q}_p(\alpha)$. Since 5 is prime to 2, the local embedding problem is solvable trivially at $p = 911$.

https://doi.org/10.4153/CJM-1980-021-4 Published online by Cambridge University Press

$p = 19$. The Newton polygon [**22**, p. 73] of $g(x)$ at $p = 19$ consists of two segments, one from $(0, 1)$ to $(3, 0)$ and one from $(3, 0)$ to $(5, 0)$. Thus $g(x)$ factors over $\mathbf{Q}_p$ into the product of a cubic $a(x)$ whose roots have $\text{ord}_p = 1/3$ and a quadratic $b(x)$ whose roots have $\text{ord}_p = 0$. Since

$$g(x) \equiv x^3(x - 4)(x - 5) \pmod{19}$$

$b(x)$ factors into linear factors over $\mathbf{Q}_p$, by Hensel's Lemma [**22**, p. 45]. Since $\text{ord}_p(\alpha) = 1/3$ for the roots α of $a(x)$, $a(x)$ is irreducible, and $\mathbf{Q}_p(\alpha)$ is totally and tamely ramified over $\mathbf{Q}_p$. Since $19 \equiv 1 \pmod 3$, $\mathbf{Q}_p$ contains the cube roots of unity, so $\mathbf{Q}_p(\alpha)/\mathbf{Q}_p$ is Galois, so by the reasoning of the previous case, $K_p/\mathbf{Q}_p$ is cubic, so the embedding problem is solvable at $p = 19$.

We interrupt here to note that the above two cases show already that $G(K/\mathbf{Q}) \simeq A_5$. For $G(K/\mathbf{Q})$ now contains a 5-cycle and a 3-cycle, hence is a subgroup of A_5 of order divisible by 15. But A_5 contains no subgroups of order 15 or 30, hence $G(K/\mathbf{Q}) \simeq A_5$.

$p = 5$. $g(x)$ is Eisenstein with respect to 5 hence irreducible over $\mathbf{Q}_p$ and for roots α of $g(x)$, $\mathbf{Q}_p(\alpha)$ is totally and wildly ramified over $\mathbf{Q}_p$, of degree 5. Hence the local Galois group is a subgroup of A_5 of order divisible by 5, hence of order 5 or 10, since A_5 has no subgroups of order 15 (groups of order 15 are cyclic), 20 (such a subgroup would have a normal 5-Sylow subgroup, but the normalizer of a 5-Sylow subgroup of A_5 is dihedral of order 10), or 30 (A_5 is simple of order 60). If it is 5, then as in the case $p = 911$, the embedding problem is solvable trivially at $p = 5$. If it is 10, then the local Galois group is the dihedral group of order 10. The extension $K_p/\mathbf{Q}_p$ then contains a quadratic extension $\mathbf{Q}_p(\sqrt{\beta})/\mathbf{Q}_p$, and by [**19**, Theorem 3.1] local embedding problem reduced to embedding this quadratic extension into a cyclic extension of degree 4, since every element of order 2 in A_5 increases its order when lifted to $SL(2, 5)$. If $\mathbf{Q}_p(\sqrt{\beta})/\mathbf{Q}_p$ is unramified, the local embedding problem has a solution by Lemma 3. If $\mathbf{Q}_p(\sqrt{\beta})/\mathbf{Q}_p$ is ramified, then the local embedding problem has a solution by Lemma 3, since $5 \equiv 1 \pmod 4$.

$p = 3$. The Newton polygon of $g(x)$ at $p = 3$ consists of the segment from $(0, 6)$ to $(4, 0)$ and the segment from $(4, 0)$ to $(5, 0)$. Hence $g(x)$ factors over $\mathbf{Q}_p$ into $a(x)b(x)$ with $a(x)$ of degree 4, with roots having $\text{ord}_p = 3/2$ and $b(x)$ linear. Thus either $a(x)$ is irreducible, or factors into two irreducible quadratics. If $a(x)$ is irreducible, then the degree of $K_p/\mathbf{Q}_p$ is divisible by 4, so $G(K_p/\mathbf{Q}_p)$ is either the 4-group V_4, or A_4. But A_4 is not realizable as a Galois group over Q_3 (see [**22**, p. 100]). Hence the only possibility is V_4 if $a(x)$ is irreducible, in which case $K_p/\mathbf{Q}_p$ is tamely ramified. If $a(x)$ factors into irreducible quadratic factors $c(x)d(x)$, its splitting field is the composite L_cL_d of the splitting fields of $c(x)$ and $d(x)$. Since the roots of $a(x)$ have $\text{ord}_3 = 3/2$, L_c and L_d are ramified quadratic extensions of $\mathbf{Q}_3$ of which there are two, namely $\mathbf{Q}_3(\sqrt{3})$ and $\mathbf{Q}_3(\sqrt{-3})$. Without loss of generality assume

https://doi.org/10.4153/CJM-1980-021-4 Published online by Cambridge University Press

$L_c = \mathbf{Q}_3(\sqrt{3})$. We claim L_d is then $\mathbf{Q}(\sqrt{-3})$. For suppose $L_c = L_d$. Then the roots of $a(x)$ are all of the form $r + s\sqrt{3}$, r, $s \in \mathbf{Z}_3$. Moreover since $\operatorname{ord}_3(r + s\sqrt{3}) = 3/2$, it follows that $\operatorname{ord}_3(r) \geqq 2$, $\operatorname{ord}_3(s) = 1$. The difference of two such roots has $\operatorname{ord}_3 \geqq 3/2$, so that the product of the squares of the differences of the 4 roots of $a(x)$ has $\operatorname{ord}_3 \geqq 6.2.3/2 = 18$. Since 3 divides D to the power 18, it follows that the difference of any two roots of $a(x)$ has $\operatorname{ord}_3 = 3/2$. If $r + s\sqrt{3}$ and $r' + s'\sqrt{3}$ are two such roots, it follows that $\operatorname{ord}_3(s - s') = 1$, so $s \not\equiv s' \bmod 9$. Since $s \equiv 0 \bmod 3$, there are only two possibilities for $s \bmod 9$, namely 3 and 6. Hence at most two roots of $a(x)$ can be of the form $r + s\sqrt{3}$. Thus the other two are of the form $r + s\sqrt{-3}$, so $L_c \neq L_d$, and again $K_3/\mathbf{Q}_3$ is tamely ramified with Galois group V_4.

The local embedding problem at $p = 3$ is then that of embedding the biquadratic extension $K_3 = \mathbf{Q}_3(\sqrt{3}, \sqrt{-1})$ into an extension $L/\mathbf{Q}_3$ with $G(L/\mathbf{Q}_3) \simeq Q$, the quaternion group of order 8. Actually we should prove that given an epimorphism $\epsilon : Q \to G(K_3/\mathbf{Q}_3)$, there exists a Galois extension $L/\mathbf{Q}_3$ containing K_3 and an isomorphism

$$\sigma : G(L/\mathbf{Q}_3) \to Q$$

such that $\epsilon\sigma = \operatorname{res}(L/K_3)$. However, since every automorphism of $Q/\{\pm 1\} \simeq V_4$ lifts to an automorphism of Q, it is seen that it will suffice to show that some Galois extension $L/\mathbf{Q}_3$ containing K_3 has Q as Galois group. But any $L/\mathbf{Q}_3$ with Galois group Q must contain K_3, which is the only extension of $\mathbf{Q}_3$ with Galois group V_4. So it is enough to prove that Q is a group over $\mathbf{Q}_3$. Now the maximal 2-extension of $\mathbf{Q}_3$ has Galois group G isomorphic to the pro-2 group on 2 generators x, y with one defining relation

$$x^{-1}yx = y^3 \quad [\mathbf{16}, \text{II-34}].$$

It follows that Q is a factor group of G, which is what we need.

$p = 2$. Substituting $x = 2y$ we may replace $g(x)$ by $2^{-5}g(2y) = g_1(y)$ whose Newton polygon consists of the segments from (0, 2) to (3, 0) and from (3, 0) to (5, 0). Then $g_1(x)$ factors over $\mathbf{Q}_2$ into $a(x)b(x)$ with $a(x)$ a cubic with roots having $\operatorname{ord}_2 = 2/3$ and $b(x)$ irreducible quadratic $\equiv x^2 + x + 1 \bmod 2$. The splitting field of $b(x)$ over $\mathbf{Q}_2$ is then unramified quadratic. If α is a root of $a(x)$, then $\mathbf{Q}_2(\alpha)$ is a totally and tamely ramified cubic extension of $\mathbf{Q}_2$, so is of the form $\mathbf{Q}_2(\pi^{1/3})$, π a prime of $\mathbf{Q}_2$. Its splitting field is then $\mathbf{Q}_2(\pi^{1/3}, \rho)$, ρ a primitive cube root of unity. Since $\mathbf{Q}_2(\rho)$ is the splitting field of $b(x)$, $\mathbf{Q}_2(\pi^{1/3}, \rho)$ is the splitting field of $g_1(x)$ over $\mathbf{Q}_2$. Its Galois group is S_3. The local embedding problem reduces [**19**, Theorem 3.1] to embedding $\mathbf{Q}_2(\rho)$ into a cyclic extension of degree 4, which, by Lemma 3, is solvable.

All the local embedding problems (with $p = 607$ omitted) are therefore solvable, so by Lemma 2, the global embedding problem given by $SL(2, 5) \to$

https://doi.org/10.4153/CJM-1980-021-4 Published online by Cambridge University Press

$G(k/\mathbf{Q})$ has a solution, necessarily surjective, and the solution field L has Galois group $SL(2, 5)$ over $\mathbf{Q}$.

We have therefore proved

THEOREM 3. *Let K be the splitting field of the quintic $g(x)$ given by* (10). *Then,*

1. $G(K/\mathbf{Q}) \simeq A_5$.
2. *There is a Galois extension $L/\mathbf{Q}$ containing K with $G(L/\mathbf{Q}) \simeq SL(2, 5)$.*

COROLLARY. *Every central extension of A_5 is realizable as a Galois group over* $\mathbf{Q}$.

This corollary follows from Theorem 3 and the following lemma.

LEMMA 4. *Let k be a number field, G a finite perfect group* (*coincides with its commutator subgroup*). *Let $\hat{G}$ be the unique stem cover* (*Darstellungsgruppe*) *of G* [**7**, p. 634]. *If $\hat{G}$ is realizable as a Galois group over k, then so is every finite central extension of G.*

Proof. Let e: $E \rightarrow G$ be a central extension of G with kernel A, and let U be a *minimal cover* of e, i.e. a subgroup of E such that $UA = E$ and such that for no proper subgroup U_1 of U, $U_1A = E$. Then E is a homomorphic image of the direct product $U \times A$, so it suffices to realize U over k, since A is realizable infinitely often over k. Now U is a central extension of G by $B = U \cap A$, and since $G' = G$, where G' is the commutator subgroup of G, $U'B = U$, hence $U'A = UA = E$, so $U' = U$ by minimality of U as a cover. It follows that $U' = U \geqq B$, so U is a *stem extension* of G [**4**, p. 212]. By [**4**, Proposition 8, p. 213], U is then a homomorphic image of the unique stem cover $\hat{G}$ of G, hence realizable over k.

For $G = A_5$, $\hat{G} = SL(2, 5)$ [**7**, p. 646], hence the corollary follows from Theorem 3 and Lemma 4.

For the convenience of the reader, we sketch a proof of Theorem 2.7 in [**20**], which, together with Theorems 2 and 3 above, implies Theorem 1.

THEOREM (2.7 of [**20**]). *Let k be a number field such that $SL(2, 5)$ and $\hat{S}_5$ are Galois groups over k. Then every Frobenius group is a Galois group over k.*

Sketch of proof. Let G be a Frobenius group. By a theorem of Frobenius [**7**, p. 495] or [**11**, p. 179], the set of all elements of G fixing no letter, together with 1, forms a normal subgroup M of G, the *Frobenius kernel* of G. If H is the subgroup of G fixing some given letter, then H has order prime to that of M, and $HM = G$, so G is a split extension of M by H. H is called a *Frobenius complement* of G. By virtue of Shafarevich's theorem [**18**], every finite solvable group is a Galois group over k, so we may assume G nonsolvable. By a theorem of Thompson [**7**, p. 499], M is nilpotent, hence H is nonsolvable. If H is realizable as $G(K/k)$, then by [**17**], the embedding problem $G \rightarrow G(K/k)$ has a surjective solution, which reduces the problem to realizing H as a Galois group over k. By a theorem of Zassenhaus [**11**, Theorem 18.7], H contains a subgroup

https://doi.org/10.4153/CJM-1980-021-4 Published online by Cambridge University Press

of index 1 or 2 of the form $Z \times SL(2, 5)$, where Z is the semidirect product of two cyclic groups C_m and C_n of orders m and n, respectively, and m and n are relatively prime to each other and to 2, 3, 5. In particular H has even order, so by [**7**, p. 506], M is abelian, hence the solvability of the embedding problem $G \to G(K/k)$ follows from an older theorem of Scholz [**14**]. Two more applications of [**14**] reduce the problem to realizing H/Z over k, and since the Sylow 2-subgroups of H are cyclic or generalized quaternion [**7**, p. 499], H/Z must be either $SL(2, 5)$ or $\hat{S}_5$ (see [**20**]).

In conclusion, let us point out the relevance of these results to the work of Jehne [**8**], who deals with real Frobenius fields $F/\mathbf{Q}$ of maximal type ($G = G(F/\mathbf{Q}) = HM$ is a Frobenius group of maximal type, i.e. $|H| = |M| - 1$). We claim that there exist nonsolvable real Frobenius fields of maximal type. Firstly, there exist nonsolvable Frobenius groups of maximal type, e.g., the semidirect product of $SL(2, 5)$ and the two-dimensional vector space over the field of 11 elements [**7**, p. 500]. ($SL(2, 11)$ contains a subgroup $H \simeq SL(2, 5)$ which acts fixed point free on the non-zero vectors of $(\mathbf{Z}/11\mathbf{Z})^{(2)}$ [**7**, p. 500].) Secondly, the A_5 extension $K/\mathbf{Q}$ of Theorem 3 is (necessarily) real, and therefore the $SL(2, 5)$ extension $L = K(\sqrt{\alpha})$ can be taken as real, for $K(\sqrt{-\alpha})/\mathbf{Q}$ has Galois group $SL(2, 5)$ as well. Finally, since M has odd order, any extension $F \supset L$ with

$$G(F/\mathbf{Q}) \simeq G = SL(2.5).(\mathbf{Z}/11\mathbf{Z})^{(2)}$$

must also be real.

Remark. The quintic $g(x)$ of Theorem 3 has an application to a problem of Schacher [**13**, p. 469] (see also, [**2**, **3**]). A finite group G is $\mathbf{Q}$-*admissible* if G is realizable as the Galois group of an extension $K/\mathbf{Q}$, where K is the maximal commutative subfield of a division ring D with center $\mathbf{Q}$.

THEOREM 4. *$SL(2, 5)$ is $\mathbf{Q}$-admissible.*

Proof. By [**13**, Proposition 2.6] it suffices to prove that for each prime p dividing the order of $SL(2, 5)$, i.e., $p = 2, 3, 5$, the local Galois group $G(L_v/\mathbf{Q}_v)$ contains a p-Sylow subgroup of $SL(2, 5)$ for at least two primes v of $\mathbf{Q}$, where L is the field of Theorem 3 with $G(L/\mathbf{Q}) \simeq SL(2, 5)$. By virtue of Chebotarev's density theorem, this condition is satisfied for cyclic Sylow subgroups, so it is enough to verify it for $p = 2$. The Sylow 2-subgroups of $SL(2, 5)$ are isomorphic to the quaternion group Q_8 of order 8. We have already seen that V_4 is the local Galois group $G(K_v/\mathbf{Q}_v)$ at $v = 3$, where K is the splitting field of the quintic $g(x)$ in Theorem 3. Since L_v is a local solution field to the embedding problem given by e: $SL(2, 5) \to G(K/\mathbf{Q}) \simeq A_5$, it follows that $G(L_v/\mathbf{Q}_v) \simeq Q_8$, for $v = 3$.

We now claim that the same is true at $v = \mu = 607$. For this it suffices to show that $G(K_v/\mathbf{Q}_v) \simeq V_4$. Recall that $g(x) = F_5(\lambda, \mu, x)$ with $\lambda = 1213$,

https://doi.org/10.4153/CJM-1980-021-4 Published online by Cambridge University Press

$\mu = 607$. Using $\lambda + 2\mu = 1$ and formula (3), we obtain

$$g(x+1) = x^5 - 15\mu x^4 + 10\mu(6\mu - 1)x^3 + 10\mu^2(7 - 6\mu)x^2 + 15\mu^2(1 - 6\mu)x + \mu^3(6\mu - 25).$$

The Newton polygon of $g(x+1)$ consists of the segment from $(0, 3)$ to $(1, 2)$ and the segment from $(1, 2)$ to $(5, 0)$. Hence $g(x+1)$ and therefore $g(x)$ have a linear factor over $\mathbf{Q}_v$, and $v = 607$ ramifies in K. Therefore $K_v/\mathbf{Q}_v$ is a tamely ramified extension with $G(K_v/\mathbf{Q}_v)$ a metacyclic subgroup of A_4, of which there are three (nontrivial): C_2, C_3, and V_4. From the Newton polygon, it cannot be C_3. If it were C_2, then by Lemma 3, $K_v/\mathbf{Q}_v$ could not be embedded into a cyclic extension of $\mathbf{Q}_v$ of degree 4. But this would be the local embedding problem at $v = 607$ corresponding to the global embedding problem given by

$$e: SL(2, 5) \to G(K/\mathbf{Q}),$$

which is solvable by Theorem 3, a contradiction. If follows that $G(K_v/\mathbf{Q}_v) \simeq V_4$.

We observe in concluding that Lemma 2 has been used as a substitute for direct computation of the local Galois group of $K_v/\mathbf{Q}_v$ at $v = 607$. A technique used in [**3**, proof of Theorem 1] can be applied to $g(x+1)$ to show that $g(x+1)$ has an irreducible quartic factor over $\mathbf{Q}_v$, $v = 607$, which implies that $G(K_v/\mathbf{Q}_v) \simeq V_4$. Then the local embedding problem at $v = 607$ is solvable, by the argument used at $v = 3$, since $607 \equiv 3 \pmod 4$. The same technique can be used to show that $g(x)$ has an irreducible quartic factor at $v = 3$, instead of the argument given in the proof of Theorem 3.

REFERENCES

1. R. Gillard, *Plongement d'une extension d'ordre p ou p^2 dans une surextension non abelienne d'ordre p^3*, J.R. Ang. Math. *268/269* (1974), 418–426.
2. B. Gordon and M. Schacher, *Quartic coverings of a cubic*, J. Number Th. (to appear).
3. ——— *The admissibility of A_5*, J. Number Th. (to appear).
4. K. W. Gruenberg, *Cohomological topics in group theory*, Lecture Notes, Springer-Verlag (1970).
5. K. Hoechsmann, *Zum Einbettungsproblem*, J.R. Ang. Math. *229* (1968), 81–106.
6. J. Hunter, *The minimum discriminants of quintic fields*, Proc. Glasgow Math. Assoc. *3* (1956), 57–67.
7. B. Huppert, *Endliche Gruppen I*, Springer-Verlag (1967).
8. W. Jehne, *Uber die Einheiten-und Divisorenklassengruppe von reelen Frobeniuskörpern von Maximaltyp*, Math. Z. *152* (1976), 223–252.
9. L. R. McCulloh, *Frobenius groups and integral bases*, J.R. Ang. Math. *248* (1971), 123–126.
10. J. Neukirch, *Über das Einbettungsproblem der algebraischen Zahlentheorie*, Inv. Math. *21* (1973), 59–116.
11. D. Passman, *Permutation groups* (Benjamin, N.Y., 1968).
12. G. Pólya and G. Szegö, *Problems and theorems in analysis*, Vol. II, Springer-Verlag (1976).
13. M. Schacher, *Subfields of division rings, I*, J. Alg. *9* (1968), 451–477.
14. A. Scholz, *Über die Bildung algebraischer Zahlköper mit auflösbarer Galoissche Gruppe*, Math Z. *30* (1929), 332–356.
15. J. Schur, *Affectlöse Gleichungen in der Theorie der Laguerreschen und Hermiteschen Polynome*, J.f.R. Ang. Math. *165* (1931), 52–58.

https://doi.org/10.4153/CJM-1980-021-4 Published online by Cambridge University Press

16. J. P. Serre, *Cohomologie galoisienne*, Lecture Notes, Springer-Verlag (1965).
17. I. R. Shafarevich, *On the problem of imbedding fields*, Transl. A.M.S., Ser. 2. *4* (1956), 151–183.
18. ——— *Construction of fields of algebraic numbers with given solvable Galois group*, Transl. A.M.S., Ser. 2, *4* (1956), 185–237.
19. J. Sonn, *On the embedding problem for nonsolvable Galois groups of algebraic number fields: reduction theorems*, J. Number Th. *4* (1972), 411–436.
20. ——— *Frobenius Galois groups over quadratic fields*, Israel J. Math. *31* (1978), 91–96.
21. J. T. Tate, *Global class field theory*, in *Algebraic number theory*, Ed. J. W. S. Cassels and A. Fröhlich, Thompson (1967).
22. E. Weiss, *Algebraic number theory*, McGraw-Hill (1963).

Technion, Israeli Institute of Technology,
Haifa, Israel

https://doi.org/10.4153/CJM-1980-021-4 Published online by Cambridge University Press