JOURNAL OF NUMBER THEORY **39**, 5–13 (1991)

Explicit Realisations of Subgroups of $GL_2(\mathbf{F}_3)$ as Galois Groups

LEILA SCHNEPS

Max-Planck Institut für Mathematik,
Gottfried-Clarenstrasse 26, 5300 Bonn 3, Germany

Communicated by D. Zagier

Received July 15, 1988; revised September 1, 1988

Let F be a number field and K an extension of F with Galois group D_4 (resp. A_4 or S_4). In this article we explicitly construct all of the quadratic extensions L of K having Galois group $\tilde{D}_4$, the Sylow subgroup of $GL_2(\mathbf{F}_3)$ (resp. $SL_2(\mathbf{F}_3)$ or $GL_2(\mathbf{F}_3)$) over F, whenever such extensions exist.

1. INTRODUCTION

Let G be a finite group and H an extension of G by $\{\pm 1\}$, i.e.,

$$1 \to \{\pm 1\} \to H \to G \to 1.$$

Suppose $H \neq G \times \{\pm 1\}$. Let $\{v_\sigma \in H \mid \sigma \in G\}$ be a set of representatives for $H/\{\pm 1\}$ such that $v_\sigma \to \sigma$ under reduction mod ± 1. Let F be a number field and K a Galois extension of F having Galois group G. The following result is well known:

LEMMA 1. *Let $A = \sum_\sigma K v_\sigma = (K/F, \zeta_{\sigma,\tau})$ be the crossed-product algebra whose multiplicative law is given by*

$$\alpha v_\sigma = v_\sigma \sigma(\alpha) \quad \text{for} \quad \alpha \in K \quad \text{and} \quad v_\sigma v_\tau = \zeta_{\sigma,\tau} v_{\sigma\tau},$$

where $\zeta_{\sigma,\tau} = \pm 1$ and the second law is given by multiplication in H. Let $E(F, K, G, H)$ be the set of quadratic extensions L of K, Galois over F of Galois group H and such that the diagram

$$\begin{array}{ccc} \mathrm{Gal}(L/F) & \longrightarrow & \mathrm{Gal}(K/F) \\ \downarrow & & \downarrow \\ H & \longrightarrow & G \end{array}$$

0022-314X/91 $3.00

commutes. Then $E(F, K, G, H)$ is non-empty if and only if the class of A in the Brauer group $\mathrm{Br}(F)$ *is equal to the identity class. Moreover if $\gamma \in K$ is such that $K(\sqrt{\gamma}) \in E(F, K, G, H)$, then $E(F, K, G, H) = \{K(\sqrt{r\gamma}) \mid r \in F^*\}$.*

Proof. Suppose there exists $\gamma \in K$ such that $L = K(\sqrt{\gamma})$ is Galois over F of Galois group H. Let $\omega = \sqrt{\gamma}$: for each $\sigma \in \mathrm{Gal}(K/F)$, set $c_\sigma = v_\sigma(\omega)/\omega$. Then $c_\sigma \sigma(c_\tau) c_{\sigma\tau}^{-1} \zeta_{\sigma,\tau} = 1$, so the cocycle defining A is equivalent to the trivial cocycle and A splits. In the other direction, suppose such c_σ exist in K. Then $c_\sigma^2 \sigma(c_\tau)^2 = c_{\sigma\tau}^2$, so by Hilbert's Theorem 90, there exists $\gamma \in K$ such that $c_\sigma^2 = \sigma(\gamma)/\gamma$. But then $K(\omega)$ is Galois over F with Galois group H.

It is easy to see moreover that if $K(\sqrt{\gamma}) \in E(F, K, G, H)$ then so are the $K(\sqrt{r\gamma})$ for $r \in F$: if $K(\sqrt{\gamma})$ and $K(\sqrt{\lambda})$ are both in $E(F, K, G, H)$ one deduces the existence of $r \in F$ such that up to squares, $\lambda = r\gamma$ from Hilbert's Theorem 90.

Let $\tilde{S}_4$ denote the central extension of S_4 by $\{\pm 1\}$ described in terms of generators and relations by

$$t_i^2 = 1, \qquad w^2 = 1, \qquad wt_i = t_i w, \qquad (t_i t_{i+1})^3 = 1, \qquad t_1 t_3 = w t_3 t_1$$

for generators w, t_1, t_2, t_3 (cf. [2]). From now on we consider $G \subset S_4$ and $H = \tilde{G}$, the lifting of G in $\tilde{S}_4$. The goal of this article is to explicitly construct the groups H as Galois groups over number fields.

We thank the Max-Planck Institute für Mathematik for its hospitality and financial support during the preparation of this paper.

2. The Quaternion Group H_8

Let G be the Vierergruppe $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$, which we identify with the subgroup $\{1, (12)(34), (13)(24), (14)(23)\} \subset S_4$. Then $H = \tilde{G}$ is the quaternion group H_8 of order 8. Let K/F be a biquadratic extension, $\{v_\sigma\}$ a set of representatives for $H_8/\{\pm 1\}$, and A the crossed-product algebra defined in Section 1. Witt (cf. [4]) explicitly constructs a field L containing K and having Galois group H_8 over F whenever A splits. We briefly recall his method here.

Let $1, \sigma_1, \sigma_2$, and σ_3 be the elements of G, and let $\{\xi_\sigma \mid \sigma \in G\}$ be a basis of K/F such that $\xi_1 = 1$, $\xi_\sigma^2 = a_\sigma \in F$, $\prod_{\sigma \in G} \xi_\sigma = 1$, and $\sigma(\xi_\sigma) = \xi_\sigma$. The v_σ generate a subalgebra of A isomorphic to the quaternion algebra $(-1, -1)$ over F and the $\xi_\tau v_\tau$ generate a quaternion algebra of the form $(-a_{\sigma_1}, -a_{\sigma_2})$: since the v_σ commute with the $\xi_\tau v_\tau$, we have $A = (-1, -1) \otimes_F (-a_{\sigma_1}, -a_{\sigma_2})$.

The fact that A splits implies that $(-1, -1) \simeq (-a_{\sigma_1}, -a_{\sigma_2})$ and therefore there exist elements $p_{ij} \in F$ such that by setting $w_{\sigma_i} = \sum_{j=1}^{3} p_{ij} v_{\sigma_j}$, we have $\prod_{i=1}^{3} w_{\sigma_i} = -1$ and $w_{\sigma_i}^2 = -1/a_{\sigma_i}$ for $i = 1, 2, 3$. Let $w_1 = 1$.

Witt extends the scalars of $(-1, -1)$ to K (so K is now the center of this algebra) and sets $j_\sigma = \xi_\sigma w_\sigma$: he then constructs the element $C = \sum_{\sigma \in G} v_\sigma^{-1} j_\sigma$. This element is non-zero and satisfies the identity $C j_\sigma C^{-1} = v_\sigma$ for each $\sigma \in G$. Replacing C by $v_\sigma C^\sigma$ in this equation also works. Now set $\mu_\sigma = v_\sigma C^\sigma C^{-1}$: it is easy to see that $\mu_\sigma \in K$. Let $\gamma = NC$ (the quaternion norm). Then $\gamma \in K$ and $\gamma^\sigma \gamma^{-1} = \mu_\sigma^2$ for all $\sigma \in G$, so $L = K(\sqrt{\gamma})$ is Galois over F. Moreover, the μ_σ satisfy the cocyle relation $\mu_\sigma \mu_\tau^\sigma \mu_{\sigma\tau}^{-1} = \zeta_{\sigma,\tau}$, and $\{\zeta_{\sigma,\tau}\}$ is exactly the factor system describing H_8, so $\mathrm{Gal}(K/F) = H_8$. Direct calculation shows that $\gamma = 1 + p_{11}\xi_{\sigma_1} + p_{22}\xi_{\sigma_2} + p_{33}\xi_{\sigma_3}$, so we have proved the following:

LEMMA 2 (Witt). *Let K be an extension of F of Galois group $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ and suppose the associated algebra A splits. Then $E(F, K, \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}, H_8) = \{K(\sqrt{r\gamma}) \mid r \in F^*\}$ for γ defined as above.*

3. THE GENERALIZED DIHEDRAL GROUP $\tilde{D}_4$

We now let F be a number field and K a Galois extension of F such that $\mathrm{Gal}(K/F) = D_4$, the dihedral group of order 8. Such a field always occurs as the splitting field of a polynmial of the form

$$P(X) = X^4 + bX^2 + d,$$

where d, $b^2 - 4d$, and $d(b^2 - 4d)$ are not squares in F. K contains three quadratic subfields, $F(\sqrt{b^2 - 4d})$, $F(\sqrt{D}) = F(\sqrt{d})$, where $D = 16(b^2 - 4d)^2 d$ is the discriminant of the polynomial $P(X)$, and $F(\sqrt{d(b^2 - 4d)})$.

In Theorem 4 we explicitly give the set of Galois extensions of F containing K and having Galois group $\tilde{D}_4$ (this group is also known as the generalized dihedral group and is generated by elements a and b such that $a^4 = (ab)^2 = -1$ and $b^2 = 1$).

Let α_1, α_2, α_3, and α_4 be the roots of $P(X)$, numbered in such a way that $\alpha_1 + \alpha_3 = 0$. We have

$$\alpha_1^2 = \alpha_3^2 = \frac{-b}{2} - \frac{\sqrt{b^2 - 4d}}{2} \qquad \text{and} \qquad \alpha_2^2 = \alpha_4^2 = \frac{-b}{2} + \frac{\sqrt{b^2 - 4d}}{2}.$$

$\mathrm{Gal}(K/F)$ is then the subgroup $\{1, (12)(34), (13)(24), (14)(23), (13), (24), (1234), (1432)\} \subset S_4$. $F(\alpha_1)$ is fixed by $\rho = (24)$.

Let $\xi_1 = \alpha_1 + \alpha_2$, $\xi_2 = 1/(\alpha + \alpha_2)(\alpha_1 + \alpha_4) = -1/\sqrt{b^2 - 4d}$, and $\xi_3 = \alpha_1 + \alpha_4$ (we write ξ_i for ξ_{σ_i} in the preceding notation). Then 1, ξ_1, ξ_2, and ξ_3 form a basis of K over $F(\sqrt{d})$. Moreover if for $1 \leqslant i \leqslant 3$ we define $a_i = \xi_i^2$, the a_i are in $F(\sqrt{d})$, and $\mathrm{Gal}(K/F(\sqrt{d})) = \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ (identified with the subgroup $\{1, (12)(34), (13)(24), (14)(23)\}$ of D_4), so over $F(\sqrt{d})$ we are in the quaternion case of Witt. We form Witt's algebra $(-1, -1) \otimes_{F(\sqrt{d})} (-a_1, -a_2)$.

LEMMA 3. *Let $(a, b)^\rho$ denote the part of the quaternion algebra (a, b) fixed by the action of ρ, this action being conjugation by v_ρ. Let $A = (-1, -1) \otimes_{F(\sqrt{d})} (-a_1, -a_2)$ be the algebra associated to D_4 and $\tilde{D}_4$ as in Lemma 1. Then $(-1, -1)$ and $(-a_1, -a_2)$ are both stable under the action of ρ and*

$$[A] = [(-1, -1)^\rho \otimes_F (-a_1, -a_2)^\rho],$$

where $[A]$ denotes the class of A in Br(F).

Proof. In fact, $A = (-1, 1)^\rho \otimes_F (-a_1, -a_2)^\rho) \otimes_F (1, d)$, where $(1, d)$ is generated by v_ρ (note that $v_\rho^2 = 1$) and $\sqrt{d}$. But $[(1, d)]$ is trivial in Br(F).

The part of (a, b) fixed by ρ consists of the elements $x + v_\rho x v_\rho$ for all $x \in (a, b)$. The algebra $(-1, -1)$ is generated over $F(\sqrt{d})$ by v_1, v_2, and $v_3 = -1/v_1 v_2$, so since $v_\rho v_1 v_\rho = -v_3$ and $v_\rho \sqrt{d}\, v_2 v_\rho = \sqrt{d}\, v_2$, $(-1, -1)^\rho$ is generated by $s_1 = v_1 - v_3$ and $s_2 = \sqrt{d}\, v_2$. This gives the quaternion algebra $(-2, -d)$ over F. Similarly, setting $u_1 = \zeta_1 v_1$, $u_2 = \zeta_2 v_2$, and $u_3 = -\zeta_3 v_3 = -1/u_1 u_2$, the u_i generate $(-a_1, -a_2)$ over $F(\sqrt{d})$ and $t_1 = u_1 - u_3$, $t_2 = \sqrt{d}\,(b^2 - 4d) u_2$ generate $(-a_1, -a_2)^\rho = (2b, -d(b^2 - 4d))$ over F. Thus,

$$[A] = [(-2, -d) \otimes_F (2b, -d(b^2 - 4d))]$$

in the Brauer group Br(F). We note that this algebra is equal to

$$\begin{aligned}(-2b, -d) &\otimes_F (2b, b^2 - 4d) \otimes_F (2, d)\\ &= (\text{Witt invariant of } \mathrm{Tr}(x^2)) \otimes_F (2, d),\end{aligned}$$

which confirms that the splitting of A is identical to the condition for the existence of L given in Serre's theorem [3].

If A splits then there exists an isomorphism of algebras ϕ: $(2b, -d(b^2 - 4d)) \to (-2, -d)$ and a matrix $Q = (q_{ij})$ with coefficients in F such that $t_i = \sum_{j=1}^3 q_{ij} \phi(s_j)$. By extension of scalars, the isomorphism ϕ gives rise to a unique isomorphism $\tilde{\phi}$: $(-a_1, -a_2) \to (-1, -1)$ and an associated matrix $P = (p_{ij})$ such that

$$\tilde{\phi}(u_i) = \sum_{j=1}^{3} p_{ij} v_j, \qquad i = 1, 2, 3.$$

The matrix P is a "Witt's matrix," i.e., setting $\gamma = 1 + p_{11}\zeta_1 + p_{22}\zeta_2 + p_{33}\zeta_3$, the field $L = K(\sqrt{\gamma})$ is Galois over $F(\sqrt{d})$ with Galois group H_8.

THEOREM 4. *Let K and γ be as above. Then $E(F, K, D_4, \tilde{D}_4) = \{K(\sqrt{r\gamma}) \mid r \in F^*\}$.*

Proof. We first show that $\gamma^\rho \gamma^{-1}$ is a square in F. Define $w_i = \tilde{\phi}(u_i) = \sum_{j=1}^3 p_{ij} v_j$ for (p_{ij}) as above. Then $w_i^2 = -1/a_i$. Let $j_\sigma = \xi_\sigma w_\sigma$ and let C be the element $\sum_{\sigma \in G} v_\sigma^{-1} j_\sigma$ constructed by Witt in the algebra $(-1, -1)$ with scalars extended to K. For any quaternion $q = a + bv_1 + cv_2 + dv_3$, we have $v_\rho q v_\rho = \rho(a) - \rho(b) v_3 - \rho(c) v_2 - \rho(d) v_1$, so $N(v_\rho q v_\rho) = \rho(N_q)$ (we write $v_\rho q v_\rho$ instead of $v_\rho^{-1} q v_\rho$).

If $q \in (-1, -1)$, write $q = \sum_i a_i \otimes x_i$ for $a_i \in (-2, -d)$ and $x_i \in F(\sqrt{d})$. Then $v_\rho q v_\rho = \sum_i a_i \otimes \rho(x_i)$ since ρ acts trivially on $(-2, -d)$. Thus, the isomorphism ϕ commutes with conjugation by v_ρ $(-1, -1)$. This allows us to calculate the elements $v_\rho w_i v_\rho$ as follows: $v_\rho w_i v_\rho = v_\rho \tilde{\phi}(u_i) v_\rho = \tilde{\phi}(v_\rho u_i v_\rho) = -w_{4-i}$. Now we calculate

$$\begin{aligned} v_\rho C v_\rho &= 1 + v_\rho(v_1^{-1} j_1) v_\rho + v_\rho(b_2^{-1} j_2) v_\rho + v_\rho(v_3^{-1} j_3) v_\rho \\ &= 1 + v_\rho(v_1^{-1} \xi_1 w_1) v_\rho + v_\rho(v_2^{-1} \xi_2 w_2) v_\rho + v_\rho(v_3^{-1} \xi_3 w_3) v_\rho \\ &= 1 + (-v_3^{-1}) \rho(\xi_1)(-w_3) + (-v_2^{-1}) \rho(\xi_2)(-w_2) \\ &\quad + (-v_1^{-1}) \rho(\xi_3)(-w_1) = C \end{aligned}$$

since $\rho(\xi_i) = \xi_{4-i}$. Thus, $\gamma^\rho = (NC)^\rho = N(v_\rho C v_\rho) = NC = \gamma$! One can further verify that if $\mu_\sigma = v_\sigma C^\sigma C^{-1}$ for $\sigma \in \{1, (12)(34), (13)(24), (14)(23)\}$ and $\mu_{\rho\sigma} = \mu_\sigma^\rho \zeta_{\rho,\sigma}$, the μ_σ verify the cocycle relation $\mu_\sigma \mu_\tau^\sigma \mu_{\sigma\tau}^{-1} = \zeta_{\sigma,\tau}$ for all σ, $\tau \in D_4$ and therefore $\mathrm{Gal}(K(\sqrt{\gamma})/F) = \tilde{D}_4$ and $K(\sqrt{\gamma}) \in E(F, K, D_4, \tilde{D}_4)$. Lemma 1 suffices to conclude.

We remark in particular that the γ constructed in this way is in fact an element of $F(\alpha_1)$.

EXAMPLE. *Let $P(X) = X^4 - X^2 + d$,* where d, $1 - 4d$, and $d(1 - 4d)$ are not squares in F. In this case, $(2b, -d(b^2 - 4d)) = (-2, -d(1 - 4d))$, so the condition for the existence of L becomes $(-2, -d(1 - 4d)) \sim (-2, -d)$, or $(-2, 1 - 4d) \sim 1$ in the Brauer group of F. This is equivalent to the condition

there exist $u, v \in F$ such that $-2u^2 + (1 - 4d) v^2 = 1$.

Suppose this condition is satisfied. Then a matrix $Q = (q_{ij})$ as above is given by

$$Q^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1/v(1+4d) & u/v(1-4d) \\ 0 & 2u/v(1-4d) & 1/v(1-4d) \end{pmatrix}$$

and this gives

$$P=\begin{pmatrix} 1/2va_1+1/2 & u/va_1 & 1/2va_1-1/2 \\ u/v & 1/v & u/v \\ 1/2va_3-1/2 & u/va_3 & 1/2va_3+1/2 \end{pmatrix}.$$

Thus we can take

$$\begin{aligned}\gamma &= 1+\left(\frac{1}{2}+\frac{1}{2va_1}\right)\xi_1+\left(\frac{1}{v}\right)\xi_2+\left(\frac{1}{2}+\frac{1}{2va_3}\right)\xi_3 \\ &= 1+\alpha_1-\frac{1}{v\sqrt{1-4d}}-\frac{\alpha_1}{v\sqrt{1-4d}}.\end{aligned}$$

If $Q(X)$ is the minimal polynomial of this element, then $Q(X^2)$ is a polynomial having Galois group $\tilde{D}_4$.

4. The Group $\tilde{A}_4 \simeq SL_2(\mathbf{F}_3)$

Let $P(X)$ be a polynomial over F having splitting field K such that $\mathrm{Gal}(K/F)=A_4$. Let $\Gamma=\{1, (12)(34), (13)(24), (14)(23)\}\subset A_4$, and let $R\subset K$ be the fixed field of Γ. Then $[R:F]=3$ and Gal $(K/R)=\Gamma$, so over R we are in the quaternion case of Witt. Let $\tau=(234)\in A_4$, so τ fixes $F(\alpha_1)$.

Theorem 5. *Suppose there exists an element $\gamma\in K$ such that $K(\sqrt{\gamma})$ is Galois over R with Galois group H_8. Set $\beta=\gamma\gamma^{\tau}\gamma^{\tau^2}$. Then $E(K, F, A_4, \tilde{A}_4)=\{K(\sqrt{r\beta})\mid r\in F^*\}$.*

Proof. In order to show that Gal $(K(\sqrt{\beta})/F)=\tilde{A}_4$, we must show that $\beta\beta^{\sigma}$ is a square for all $\sigma\in A_4$. Now, $A_4=\Gamma\rtimes\{1,\tau,\tau^2\}$, so we can write $\sigma=\delta\omega$ with $\delta\in\Gamma$ and $\omega\in\{1,\tau,\tau^2\}$. Then $\beta\beta^{\sigma}=(\gamma\gamma^{\tau}\gamma^{\tau^2})(\gamma^{\delta\omega}\gamma^{\delta\omega\tau}\gamma^{\delta\omega\tau^2})=(\gamma\gamma^{\tau}\gamma^{\tau^2})(\gamma^{\delta}\gamma^{\delta\tau}\gamma^{\delta\tau^2})$ since ω permutes 1, τ, and τ^2. But $\Gamma=\mathrm{Gal}(K|R)$, so $\gamma\gamma^{\delta}$ is a square in K for each $\delta\in\Gamma$. Moreover, by writing $\delta\tau=\tau\delta_1$ and $\delta\tau^2=\tau^2\delta_2$, we find that δ_1 and δ_2 are in Γ, so

$$\begin{aligned}\beta\beta^{\sigma} &= (\gamma\gamma^{\delta})(\gamma^{\tau}\gamma^{\delta\tau})(\gamma^{\tau^2}\gamma^{\delta\tau^2})=(\gamma\gamma^{\delta})(\gamma^{\tau}\gamma^{\tau\delta_1})(\gamma^{\tau^2}\gamma^{\tau^2\delta_2}) \\ &= (\gamma\gamma^{\delta})(\gamma\gamma^{\delta_1})^{\tau}\,(\gamma\gamma^{\delta_2})^{\tau^2},\end{aligned}$$

which is a square. The usual remark on the cocycle relation satisfied by the μ_{δ} shows that $\mathrm{Gal}(K(\sqrt{\beta})/F)$ is really $\tilde{A}_4$ and Lemma 1 suffices to conclude.

We remark that the β obtained in this way is an element of $F(\alpha_1)$.

EXAMPLE. Let $P(X)=x^4-12X^2-8X+9$. The the discriminant of P is 1008^2 and it is easy to check that the Galois group of P over $\mathbf{Q}$ is A_4. Let α_1, α_2, α_3, and α_4 be the roots of $P(X)$. Let $\xi_1=\alpha_1+\alpha_3$, $\xi_2=\alpha_1+\alpha_4$, and $\xi_3=-(\alpha_1+\alpha_2)/8$. Then $\xi_1\xi_2\xi_3=1$, and together with 1, these elements form Witt's basis over the field $R=\mathbf{Q}((\alpha_1+\alpha_3)^2)$. Let K be the splitting field of $P(X)$. For $1\leqslant i\leqslant 3$, let $a_i=\xi_i^2$. Witt's methods give the following expression for an element γ such that $K(\sqrt{\gamma})$ is Galois over R of Galois group H_8:

$$\gamma=672+(-8-192a_2a_3+4a_1)\xi_1+(-192+320a_1a_3+12a_2)\xi_2$$
$$+(1472-8a_1a_2-4096a_3)\xi_3.$$

Let τ be the permutation of the roots given by the 3-cycle (234), and let $\beta=(\gamma\gamma^\tau\gamma^{\tau^2})/(2^{11}7^2)$. Then if $Q(X)$ is the minimal polynomial of β, $Q(X^2)$ has Galois group $\tilde{A}_4$ over $\mathbf{Q}$: we have

$$\begin{aligned}Q(X^2)&=X^8-12884X^6+41492682X^4\\&\quad-7985480580X^2-5051798406522\\&=X^8-2^2\cdot 3221X^6+2\cdot 3^3\cdot 7\cdot 11\cdot 17\cdot 587X^4\\&\quad-2^2\cdot 3^7\cdot 5\cdot 7\cdot 11\cdot 2371X^2-2\cdot 3^6\cdot 7\cdot 494983187.\end{aligned}$$

5. THE GROUP $\tilde{S}_4=GL_2(\mathbf{F}_3)$

The argument is analogous to that for A_4, using D_4 instead of Γ. Let $\mathrm{Gal}(K/F)=S_4$, and let $D_4\subset S_4$ be given by $\{1, (12)(34), (13)(24), (14)(23), (13), (24), (1234), (1432)\}\subset S_4$. Let R be the fixed field of D_4. Then $[R:F]=3$, but R is not Galois over F. Let $\tau=(234)\in S_4$. Then $\tau^{-1}D_4\tau=\mathrm{Gal}(K/R^\tau)$ and $\tau D_4\tau^{-1}=\mathrm{Gal}(K/R^{\tau^2})$.

THEOREM 6. *Suppose there exists $\gamma\in K$ such that $K(\sqrt{\gamma})$ is Galois over R with Galois group D_4. Let $\beta=\gamma\gamma^\tau\gamma^{\tau^2}$. Then $K(\sqrt{\beta})$ is Galois over F with Galois group $\tilde{S}_4$, and therefore $E(K, F, S_4, \tilde{S}_4)=\{K(\sqrt{r\beta})\mid r\in F^*\}$.*

Proof. As before, we must show that $\beta\beta^\sigma$ is a square in K for all $\sigma\in K$. We first suppose that $\sigma\in S_3=\{1, (234), (243), (23), (24), (34)\}$, i.e., the set of elements of S_4 fixing $F(\alpha_1)$. Now, by the argument for D_4, we know that $\gamma\in R(\alpha_1)$ and therefore $\beta\in F(\alpha_1)$, so $\beta\beta^\sigma=\beta^2\in K$. Next we let $\sigma\in\Gamma=\{1, (12)(34), (13)(24), (14)(23)\}$. This subgroup is normal in S_4 and therefore $\beta\beta^\sigma$ is a square in K by the same argument as that in the case of A_4. Now, $S_4=\Gamma\rtimes S_3$, so any $\sigma\in S_4$ can be written $\sigma=\delta\omega$ with $\delta\in\Gamma$, $\omega\in S_3$, Then $\beta\beta^\sigma=\beta\beta^{\delta\omega}=\beta\beta^\delta\beta^\delta\beta^{\delta\omega}(\beta^\delta)^{-2}=(\beta\beta^\delta)(\beta\beta^\omega)^\delta\,(\beta^\delta)^{-2}$, which is a square in K.

We note that we may use these methods to derive Serre's theorem directly for $n=4$ (see [3]).

LEMMA 7. *Let $P(X)$ be a polynomial over F with splitting field K and Galois group S_4: we assume P has the form X^4+bX^2+cX+d. Let $W_2(P)$ be the Witt invariant of the quadratic form $\mathrm{Tr}_{K/F}(x^2)$. Then there exists a quadratic extension L of K such that L is Galois over F with Galois group $\tilde{S}_4$ if and only if the algebra $B=W_2(P)\otimes_F(2, D)$ splits in $\mathrm{Br}(F)$, where D is the discriminant of P.*

Proof. Let α_1, α_2, α_3, and α_4 be the roots of $P(X)$, and let $Y=(\alpha_1+\alpha_3)^2$. Let R be the field $F(Y)$. Then $[R:F]=3$, and a polynomial over R having K as splitting field and D_4 as Galois group is

$$X^4+(2Y-4b)X^2+(16d-4bY-3Y^2),$$

obtained by taking $Q(X^2)$, where $Q(X)$ is the minimal polynomial of $(\alpha_1-\alpha_3)^2$ over R. Let $W_2(Q)$ be the Witt invariant of $\mathrm{Tr}_{K/R}(x^2)$. By Theorem 5, in order to show existence of L, it suffices to prove the existence of some L' containing K such that $\mathrm{Gal}(L'/R)=\tilde{D}_4$. In Section 3, we saw that L exists if and only if $A=W_2(Q)\otimes_R(2, D_Q)$ splits in $\mathrm{Br}(R)$, where D_Q is the discriminant of $Q(X^2)$. But $W_2(Q)=W_2(P)\otimes_F R$ and $(2, D_Q)=(2, D)\otimes_F R$, so $A=B\otimes_F R$. But if A splits, either B splits or R is a neutralising field for this B. Since $[R:F]=3$, R cannot be isomorphic to a maximal commutative subfield of B, so B must split over F.

COROLLARY. *Suppose $P(X)$ has the form X^4+cX+d. Let D be the discriminant of P. Then the condition for L to exist is that $(-2, -D)$ must split, i.e., there exist elements u and v in F such that $-D=2u^2+v^2$.*

Proof. In this case the polynomial over R whose splitting field is K is given by

$$X^4+2(\alpha_1+\alpha_3)^2X^2+(16d-3(\alpha_1+\alpha_3)^4).$$

It is easy to see that up to squares in R, if we let $Y=(\alpha_1+\alpha_3)^2$, then $Y=Y^2-4d$ and $D=16d-3Y^2$. An extension L of K with $\mathrm{Gal}(L/R)=\tilde{D}_4$ exists if and only if $(-2, -D)(Y, -DY)$ splits; but in this case, $(Y, -DY)=(Y, D)=(Y^2-4d,\ 16d-3Y^2)$ splits because $4(Y^2-4d)+(16d-3Y^2)=Y^2$, which is a square in R. So L exists if and only if $(-2, -D)$ splits.

REFERENCES

1. I. REINER, "Maximal Orders," Academic Press, London/New York/San Francisco, 1975.
2. I. SCHUR, Ueber die Darstellung der symmetrischen und der alternierenden Gruppe durch gebrochene lineare Substitutionen, *J. Reine Angew. Math.* **139** (1911), 155–250.
3. J-P. SERRE, L'invariant de Witt de la forme $\mathrm{Tr}(x^2)$, *Comment. Math. Helv.* **59** (1984), 651–676.
4. E. WITT, Konstruktion von galoisschen Körpern der Charakteristik p zu vorgegebener Gruppe der Ordnung p^f, *J. Reine Angew. Math.* **174** (1935), 237–245.