Israel J. Math. **93** (1996), 115-144.

On Galois groups and their maximal 2-subgroups

Leila Schneps

Abstract

Let $\mathcal{G}$ be a finite group of even order, having a central element of order 2 which we denote by -1. If $\mathcal{G}$ is a 2-group, let G be a maximal subgroup of $\mathcal{G}$ containing -1, otherwise let G be a 2-Sylow subgroup of $\mathcal{G}$. Let $\mathcal{H} = \mathcal{G}/\{\pm 1\}$ and $H = G/\{\pm 1\}$. Suppose there exists a regular extension L_1 of $\mathbb{Q}(T)$ with Galois group $\mathcal{H}$. Let L be the subfield of L_1 fixed by H. We make the hypothesis that L_1 admits a quadratic extension L_2 which is Galois over L of Galois group G. If $\mathcal{G}$ is not a 2-group we show that L_1 then admits a quadratic extension which is Galois over $\mathbb{Q}(T)$ of Galois group $\mathcal{G}$ and which can be given explicitly in terms of L_2. If $\mathcal{G}$ is a 2-group, we show that there exists an element $a \in \mathbb{Q}(T)$ such that L_1 admits a quadratic extension which is Galois over $\mathbb{Q}(T)$ of Galois group $\mathcal{G}$ if and only if the cyclic algebra $(L/\mathbb{Q}(T), a)$ splits. As an application of these results we explicitly construct several 2-groups as Galois groups of regular extensions of $\mathbb{Q}(T)$.

*

Let $\mathcal{G}$ be a finite group and let K be the field $\mathbb{Q}(T)$. A **regular** extension of $\mathbb{Q}(T)$ is an extension containing no algebraic extension of $\mathbb{Q}$ larger than $\mathbb{Q}$ itself. The inverse Galois problem for $\mathcal{G}$ over K is the question of whether $\mathcal{G}$ occurs as the Galois group of a regular extension of K. If this is the case, then by Hilbert's Irreducibility Theorem, $\mathcal{G}$ occurs as a Galois group over every number field: we say that $\mathcal{G}$ has the property Gal_T. In certain cases, it is known that $\mathcal{G}$ has the property Gal_T, for instance whenever $\mathcal{G}$ is an abelian group or when $\mathcal{G}$ is a semi-direct product $A \rtimes H$ where A is abelian and H is a smaller group which itself has Gal_T, or when $\mathcal{G}$ is a quotient of such a semi-direct product. Whenever

$\mathcal{G}$ is the quotient of a semi-direct product with abelian kernel $A \rtimes \mathcal{H}$, then the question of whether $\mathcal{G}$ has Gal_T is reduced to the same question for $\mathcal{H}$.

Any group having a normal abelian subgroup not lying in its Frattini subgroup can be written as such a quotient. Therefore, in order to prove that all finite groups have Gal_T, it would suffice to prove it for irreducible groups, i.e. groups all of whose abelian normal subgroups lie in their Frattini subgroup. The smallest such group is $SL(2,3)$, of order 24: it is known to have Gal_T (cf. [F] or [S1]). The smallest such 2-groups are ten of the 267 groups of order 64. Seven of these groups have descending central 2-series of length 3 and three of them have series of length 4. The smallest irreducible p-groups have order p^5 when $p \neq 2$ (cf. [D]).

When it is not known how to prove that a group is a Galois group by considering its intrinsic structure, one can attempt to consider the group as an extension of a smaller group and study the embedding problem. We restrict ourselves to the case where $\mathcal{G}$ has a central element of order 2, which we call -1. Let $\mathcal{H} = \mathcal{G}/\{\pm 1\}$. Then $\mathcal{G}$ is an extension of the group $\mathcal{H}$ by $\{\pm 1\}$, i.e.

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

Suppose we have a Galois extension L_1 of a field L having Galois group $\mathcal{H}$. Then we may ask the following question: does there exist a quadratic extension L_2 of L_1 which is Galois over L of Galois group $\mathcal{G}$? It is well known that this is the case if and only if a certain algebra is split: this algebra is known as the obstruction to the embedding problem of $\mathcal{G}$ over $\mathcal{H}$ relative to the fields L and L_1. We call it $T_{L,L_1,\mathcal{H},\mathcal{G}}$: the precise definition is given in §1. In this article we prove the following theorem:

Theorem 1: *Let $\mathcal{G}$ be a finite group having a central element -1 of order 2, and let $\mathcal{H} = \mathcal{G}/\{\pm 1\}$. If $\mathcal{G}$ is a 2-group let G be a maximal subgroup of $\mathcal{G}$ containing -1. If $\mathcal{G}$ is not a 2-group let G be a 2-Sylow subgroup of $\mathcal{G}$. Suppose $\mathcal{H}$ has the property Gal_T, and let L_1 be a regular extension of K of Galois group $\mathcal{H}$. Let $H = G/\{\pm 1\}$ and let L be the fixed field of H in L_1. Suppose that $T_{L,L_1,H,G}$ is split, i.e. that L_1 admits a quadratic extension L_2 which is Galois over L of Galois group G. Then*

(i) If $\mathcal{G}$ is not a 2-group, L_1 admits a quadratic extension L_2' which is Galois over K of Galois group $\mathcal{G}$. The field L_2' can be given explicitly in terms of L_2.

(ii) If $\mathcal{G}$ is a 2-group, there exists an element $a \in K^*$ which can be given

explicitly in terms of L_2, such that L_1 admits a quadratic extension L_2' which is Galois over K of Galois group $\mathcal{G}$ if and only if the cyclic algebra $(L/K, a)$ is split.

In §§2 and 3 we prove a more detailed version of the theorem. In §4 we calculate the element a of part (ii) of the theorem in some small examples. In §5, we give some examples of applications of the theorem, and in §6 we use the theorem to prove that the seven irreducible groups of order 64 with descending central 2-series of length 3 have the property Gal_T and to construct explicit regular extensions of K having these groups as Galois groups.

I would like to thank the ETH in Zürich for its hospitality and financial support during the preparation of this article, and Ralf Dentzer for communicating his list of irreducible 2-groups to me. Special thanks are also due to Jack Sonn whose suggestions gave rise to numerous improvements.

§1. The embedding problem

Let $\mathcal{G}$, $\mathcal{H}$, K and L_1 be as above and suppose that $\mathcal{G}$ is not isomorphic to $\mathcal{H} \times \{\pm 1\}$. We begin by recalling the exact statement of the embedding problem and the definition of its obstruction. Let $E(K, L_1, \mathcal{H}, \mathcal{G})$ be the set of fields L_2 which are quadratic extensions of L_1, Galois over K with Galois group isomorphic to $\mathcal{G}$ such that the diagram

$$\begin{array}{ccc} \mathrm{Gal}(L_2/K) & \longrightarrow & \mathrm{Gal}(L_1/K) \\ \downarrow & & \downarrow \\ \mathcal{G} & \longrightarrow & \mathcal{H} \end{array}$$

commutes. The set $E(K, L_1, \mathcal{H}, \mathcal{G})$ is the set of fields $L(\sqrt{\gamma})$ which are Galois over K of Galois group isomorphic to $\mathcal{G}$, and such that the action of the element $-1 \in \mathcal{G}$ on L_1 fixes L_1 and sends $\sqrt{\gamma}$ to $-\sqrt{\gamma}$. It is known that if for some $\gamma \in L_1$ we have $L_1(\sqrt{\gamma}) \in E(K, L_1, \mathcal{H}, \mathcal{G})$, then $E(K, L_1, \mathcal{H}, \mathcal{G}) = \{L_1(\sqrt{r\gamma}) |\ r \in K^*\}$.

Let $\{v_\sigma |\ \sigma \in \mathcal{H}\}$ be a set of representatives for $\mathcal{G}/\{\pm 1\}$. Define a cocycle $\zeta\colon \mathcal{H} \times \mathcal{H} \to \{\pm 1\}$ by $v_\sigma v_\tau = \zeta_{\sigma,\tau} v_{\sigma\tau}$ (we write $\zeta_{\sigma,\tau}$ rather than $\zeta(\sigma, \tau)$). Let $(L_1/K, \zeta)$ be the crossed-product algebra associated to the cocycle ζ: this algebra

is the obstruction to the embedding problem. We recall that it is an algebra of dimension $|\mathcal{H}|^2$. We can define it explicitly as follows: $(L_1/K, \zeta) = \sum_{\sigma \in H} L_1 v_\sigma$, where multiplication is given by the rules $v_\sigma v_\tau = \zeta_{\sigma,\tau} v_{\sigma,\tau}$ and $v_\sigma \alpha = \sigma(\alpha) v_\sigma$ for all $\alpha \in L_1$.

Let us denote by $T_{K,L_1,\mathcal{H},\mathcal{G}}$ the equivalence class of $(L_1/K, \zeta)$ in the group $\mathrm{Br}_2(K)$, the kernel of multiplication by 2 in the Brauer group of K. In general, we write this group additively and use the notation (a, b) both for the quaternion algebra (a, b) and its equivalence class in $\mathrm{Br}_2(K)$. We have the classical result, proved via Hilbert's 90th Theorem (see for example [S1] for the proof):

$$E(K, L_1, \mathcal{H}, \mathcal{G}) \neq \emptyset \quad \Leftrightarrow \quad T_{K,L_1,\mathcal{H},\mathcal{G}} = 0 \ \text{ in } \ \mathrm{Br}_2(K).$$

§2. The non-2-group case

Suppose $\mathcal{G}$ is not a 2-group, and let G be a 2-Sylow subgroup of $\mathcal{G}$. We suppose as before that $\mathcal{G}$ has a central element -1 of order 2 and we set $\mathcal{H} = \mathcal{G}/\{\pm 1\}$ and $H = G/\{\pm 1\}$. Let L_1 be a regular extension of K having Galois group $\mathcal{H}$. We make part (i) of the main theorem more explicit in the following lemma:

Lemma 2: *Suppose $T_{L,L_1,H,G} = 0$, so there exists an element $\gamma \in L_1$ such that $L_1(\sqrt{\gamma}) \in E(L, L_1, H, G)$. Let T be a set of representatives for the right cosets for H in $\mathcal{H}$ and set $\beta = \prod_{\tau \in T} \tau(\gamma)$. Then $T_{K,L_1,\mathcal{H},\mathcal{G}} = 0$ and $L_1(\sqrt{\beta}) \in E(K, L_1, \mathcal{H}, \mathcal{G})$.*

Proof: We first show that $L_1(\sqrt{\beta})$ is Galois over K. To see this, it suffices to verify that $\beta\sigma(\beta)$ is a square in L_1 for all $\sigma \in \mathcal{H}$. Now, multiplication by an element of $\mathcal{H}$ induces a permutation on the classes τH, so

$$\beta\sigma(\beta) = \prod_{\tau \in T} \tau(\gamma)\sigma\big(\tau(\gamma)\big) = \prod_{\tau \in T} \tau(\gamma)\tau h_\tau(\gamma) = \prod_{\tau \in T} \tau\big(\gamma h_\tau(\gamma)\big)$$

where the h_τ are in H. But for each h_τ, $\gamma h_\tau(\gamma)$ is a square in L_1 since by assumption, $L_1(\sqrt{\gamma})$ is Galois over L, the fixed field of H. So $\beta\sigma(\beta)$ is a square for all $\sigma \in \mathcal{H}$.

Set $L_2 = L_1(\sqrt{\beta})$. We now show that the Galois group of the extension $L_1(\sqrt{\beta})/K$ is really the desired group $\mathcal{G}$. It suffices to show that $L_1(\sqrt{\beta}) \in E(L, L_1, H, G)$, since any quadratic extension L_2 of L_1 which is Galois over K

and such that $L_2 \in E(L, L_1, H, G)$ must have $\mathrm{Gal}(L_2/K) \simeq \mathcal{G}$. We see this because $\mathrm{Gal}(L_2/K)$ must have the two properties that its quotient by the central element fixing L_1 is isomorphic to $\mathcal{H}$ and its 2-Sylow subgroups are isomorphic to G. But all such groups are isomorphic. For consider the map

$$H^2(\mathcal{H}, \pm 1) \stackrel{\mathrm{Res}}{\to} H^2(H, \pm 1).$$

The group $H^2(\mathcal{H}, \pm 1)$ classifies the central extensions of $\mathcal{H}$ by ± 1 and $H^2(H, \pm 1)$ classifies the central extensions of H by ± 1. The restriction arrow is injective since $[\mathcal{H} : H]$ is odd. Therefore, the preimage of the element of $H^2(H, \pm 1)$ corresponding to the central extension G of H is unique and corresponds to the unique central extension of $\mathcal{H}$ by ± 1 having 2-Sylow isomorphic to G.

To conclude the proof, we only need to show that $L_1(\sqrt{\beta}) \in E(L, L_1, H, G)$. Recall that $\mathrm{Br}_2(L_1/K) \simeq H^2(\mathcal{H}, L_1^*)$, and consider the commutative diagram

$$\begin{array}{ccc} H^2(\mathcal{H}, \pm 1) & \xrightarrow{\mathrm{Res}} & H^2(H, \pm 1) \\ \downarrow & & \downarrow \\ H^2(\mathcal{H}, L_1^*) & \xrightarrow{\mathrm{Res}} & H^2(H, L_1^*). \end{array}$$

Let ζ_G be a 2-cocycle in the class of $H^2(H, \pm 1)$ corresponding to the central extension G of H by ± 1, and $\zeta_{\mathcal{G}}$ a 2-cocycle in the class of $H^2(\mathcal{H}, \pm 1)$ which is the (unique) preimage of the class of ζ_G under Res (so ζ_G corresponds as explained above to the extension $\mathcal{G}$ of $\mathcal{H}$). Then $T_{K, L_1, \mathcal{H}, \mathcal{G}}$ is the equivalence class in $\mathrm{Br}_2(L_1/K)$ of the crossed-product algebra $(L_1/K, \zeta_{\mathcal{G}})$, and $T_{L, L_1, H, G}$ is the class of the crossed-product algebra $(L_1/L, \zeta_G)$. In other words, $T_{K, L_1, \mathcal{H}, \mathcal{G}}$ corresponds to the class of $\zeta_{\mathcal{G}}$ in $H^2(\mathcal{H}, L_1^*)$ under the identification $\mathrm{Br}_2(L_1/K) \simeq H^2(\mathcal{H}, L_1^*)$ and the same is true when $\mathcal{H}$ and $\mathcal{G}$ are replaced by H and G, and K by L. By assumption, $T_{L, L_1, H, G}$ is trivial; therefore, since both restriction arrows are injective on elements of order 2, $T_{K, L_1, \mathcal{H}, \mathcal{G}}$ is also be trivial. Therefore, if $L_1(\sqrt{\gamma}) \in E(L, L_1, H, G)$, there exists $\delta \in L_1$ such that $L_1(\sqrt{\delta}) \in E(K, L_1, \mathcal{H}, \mathcal{G})$. Then (as in §1), we must have $\gamma = \delta r \lambda^2$ for some $r \in L$ and $\lambda \in L_1$. Now, since $L_1(\sqrt{\delta})$ is Galois over K, we must have $\tau(\delta) = \delta {\lambda_\tau}^2$ for all $\tau \in T$, where each $\lambda_\tau \in L_1$. Thus we see that

$$\beta = \prod_{\tau \in T} \tau(\gamma) = \prod_{\tau \in T} \tau(\delta) \prod_{\tau \in T} \tau(r) \prod_{\tau \in T} \tau(\lambda)^2,$$

so

$$\beta = \delta^{[\mathcal{H}:H]} \prod_{\tau \in T} \tau(r) \prod_{\tau \in T} \tau(\lambda)^2 {\lambda_\tau}^2.$$

Since $[\mathcal{H} : H]$ is odd and $\prod_{\tau \in T} \tau(r) \in K^*$, we see that β differs from δ by multiplication by a square and an element of K^*, so since $L_1(\sqrt{\delta}) \in E(K, L_1, \mathcal{H}, \mathcal{G})$ by assumption, we obtain

$$L_2 = L_1(\sqrt{\beta}) \in E(K, L_1, \mathcal{H}, \mathcal{G}).$$

$\diamondsuit$

It is clear from the proof that this method, i.e. assuming the two hypotheses that $\mathcal{H}$ has Gal_T and that $T_{L,L_1,H,G} = 0$ has the advantage of considerably simplifying the obstruction to the embedding problem, reducing it to a much smaller one, and even more important reducing the explicit construction of the field having Galois group $\mathcal{G}$ to that of a field having a smaller group G. However, it has the disadvantage of obliging us to construct fields and obstructions to embedding problems over extensions of $\mathbb{Q}(T)$, which may be more difficult. The group $SL(2,3)$ is a good example (see §5).

§3. The 2-group case

Let $\mathcal{G}$ now be a 2-group. Then $\mathcal{G}$ can always be written as a product GC_{2^n} for some n, where G is a non-trivial normal subgroup of $\mathcal{G}$ (one can always take G to be a maximal subgroup, for instance), and C_{2^n} denotes a cyclic subgroup of order 2^n. Such a product is called a partial semi-direct product: $\mathcal{G}$ is a semi-direct product $G \rtimes C_{2^n}$ if $G \cap C_{2^n} = 1$, otherwise it is a quotient of such a semi-direct product. We make part (ii) of theorem 1 more explicit in the following theorem.

Theorem 3: *Let $\mathcal{G}$ be a 2-group, and write $\mathcal{G}$ as a partial semi-direct product GC_{2^n} for some non-trivial normal subgroup $G \subset \mathcal{G}$. Let ϵ be a generator of the C_{2^n} factor; we suppose that n is minimal, i.e. that ϵ has order n in $\mathcal{G}$. Let let -1 be a central element of order 2 in $\mathcal{G}$ which is contained in G. Set $\mathcal{H} = \mathcal{G}/\{\pm 1\}$ and $H = G/\{\pm 1\}$. Then $\mathcal{H}$ satisfies an exact sequence*

$$1 \to H \to \mathcal{H} \to C_{2^m} \to 1$$

for some $m \leq n$ (if $m = n$ then $\mathcal{G}$ is a semi-direct product $G \rtimes C_{2^n}$). Suppose that $\mathcal{H}$ has the property Gal_T, so there exists a regular extension L_1 of K having Galois group $\mathcal{H}$. Let L be the fixed field of H in L_1 and suppose that $T_{L,L_1,H,G} = 0$. Then there exists an element $a \in K^*$ such that

(i) $T_{K,L_1,\mathcal{H},\mathcal{G}} = 0$ if and only if the cyclic algebra $(L/K, a)$ is split, i.e. if and only if a is a norm from L to K.

(ii) For any $\gamma \in L_1$ such that $L_1(\sqrt{\gamma}) \in E(L, L_1, H, G)$, there exists $r \in L^*$ and $\lambda \in L_1$ such that

$$a = \lambda^2 r \epsilon^{2^{m-1}}(r)\gamma\epsilon^{2^{m-1}}(\gamma).$$

Proof: (i) Consider the following exact sequence of cohomology groups:

$$1 \overset{\mathrm{Inf}}{\to} H^2(C_{2^m}, L^*) \overset{\mathrm{Res}}{\to} H^2(\mathcal{H}, L_1^*) \to H^2(H, L_1^*).$$

The hypothesis that $T_{L,L_1,H,G}$ splits is equivalent to supposing that if ζ: $\mathcal{H} \times \mathcal{H} \to L_1^*$ is a 2-cocycle associated to $\mathcal{G}$ as in §1, then $\mathrm{Res}(\zeta)$ is L_1-equivalent to the trivial cocycle. Then by the exact sequence, ζ is L_1-equivalent to the inflation of a cocycle in $H^2(C_{2^m}, L^*)$, which means that $T_{K,L,\mathcal{H},\mathcal{G}}$ is equivalent to a cyclic algebra of the form $(L/K, a)$ in $\mathrm{Br}_2(K)$ for some element $a \in K^*$. Such an algebra is given by $(L/K, a) = \sum_{i=0}^{i=2^{m-1}-1} L\tilde{\epsilon}^i$ where $\tilde{\epsilon}^{2^m} = a$, and $\tilde{\epsilon}$ acts on L as a generator of $\mathrm{Gal}(L/K)$. It is well-known that a cyclic algebra splits if and only if a is a norm from L to K (see for example [R]).

(ii) The element of $H^2(C_{2^m}, L^*)$ associated to the algebra $(L/K, a)$ can be given by a cocycle ξ: $C_{2^m} \times C_{2^m} \to L^*$ defined by $\xi_{\epsilon^i,\epsilon^j} = 1$ if $i + j < 2^m$, $\xi_{\epsilon^i,\epsilon^j} = a$ otherwise. Since $T_{K,L,\mathcal{H},\mathcal{G}}$ is L_1-equivalent to $(L/K, a)$, there is a 1-cochain $\{c_\sigma \in L_1^* |\ \sigma \in \mathcal{H}\}$ such that

$$c_\sigma \sigma(c_\tau) c_{\sigma\tau}^{-1} \zeta_{\sigma,\tau} = \xi_{\bar{\sigma},\bar{\tau}} = \begin{cases} 1 & i + j < 2^m \\ a & i + j \geq 2^m, \end{cases}$$

where $\bar{\sigma}$ and $\bar{\tau}$ are σ and τ (mod H), and i and j are such that $\bar{\sigma} = \epsilon^i$, $\bar{\tau} = \epsilon^j$. Now, set

$$\gamma_0 = a \sum_{\sigma \in H} c_\sigma^2 \sigma(w) + \sum_{\sigma \in H} c_{\epsilon^{2^{m-1}}\sigma}^2 \epsilon^{2^{m-1}} \sigma(w)$$

for some $w \in L_1$ such that $\gamma_0 \neq 0$ (such a w exists by Artin's theorem on the linear independence of characters). Then

$$\epsilon^{2^{m-1}}(\gamma_0) = a \sum_{\sigma \in H} \epsilon^{2^{m-1}}(c_\sigma)^2 \epsilon^{2^{m-1}} \sigma(w) + \sum_{\sigma \in H} \epsilon^{2^{m-1}}(c_{\epsilon^{2^{m-1}}\sigma})^2 \epsilon^{2^m} \sigma(w).$$

Now, using the two identities,

$$\epsilon^{2^{m-1}}(c_\sigma)^2 = c^{-2}_{\epsilon^{2^{m-1}}} c^2_{\epsilon^{2^{m-1}}\sigma}$$

and

$$\epsilon^{2^{m-1}}(c_{\epsilon^{2^{m-1}}\sigma})^2 = c^{-2}_{\epsilon^{2^{m-1}}} c^2_{\epsilon^{2^m}\sigma} a^2$$

which follow from the definition of the 1-cochain $\{c_\sigma\}$, we obtain

$$\epsilon^{2^{m-1}}(\gamma_0) = (c_{\epsilon^{2^{m-1}}})^{-2} \big[a \sum_{\sigma \in H} c^2_{\epsilon^{2^{m-1}}\sigma} \epsilon^{2^{m-1}} \sigma(w) + a^2 \sum_{\sigma \in H} c^2_{\epsilon^{2^m}\sigma} \epsilon^{2^m} \sigma(w) \big].$$

Since m is precisely the smallest integer such that $\epsilon^{2^m} \in H$, multiplication of the elements of H by ϵ^{2^m} only permutes them, so this expression can be rewritten as

$$\epsilon^{2^{m-1}}(\gamma_0) = a(c_{\epsilon^{2^{m-1}}})^{-2} \left[\sum_{\sigma \in H} c^2_{\epsilon^{2^{m-1}}\sigma} \epsilon^{2^{m-1}} \sigma(w) + a \sum_{\sigma \in H} c^2_\sigma \sigma(w) \right],$$

so in fact

$$\epsilon^{2^{m-1}}(\gamma_0) = a(c_{\epsilon^{2^{m-1}}})^{-2} \gamma_0.$$

Now, $L_1(\sqrt{\gamma_0}) \in E(L, L_1, H, G)$ since, as is easily checked, $\gamma_0 = c^2_\tau \tau(\gamma_0)$ for all $\tau \in H$. So any $\gamma \in L_1$ such that $L_1(\sqrt{\gamma}) \in E(L, L_1, H, G)$ satisfies $\gamma_0 = r\lambda_0^2 \gamma$ for some $r \in L$, $\lambda_0 \in L_1$. Set $\lambda = c_{\epsilon^{2^{m-1}}} r^{-1} \gamma^{-1} \lambda_0^{-1} \epsilon^{2^{m-1}}(\lambda_0)$. Then as in the statement of the theorem, we have

$$a = \lambda^2 r \epsilon^{2^{m-1}}(r) \gamma \epsilon^{2^{m-1}}(\gamma).$$

$\diamondsuit$

In general, it is easier to work with semi-direct products than with partial ones. Moreover if a semi-direct product $G \rtimes C_{2^n}$ has the property Gal_T, then so do its quotients and in particular the partial semi-direct products GC_{2^n}.

If $\mathcal{G} = G \rtimes C_{2^n}$ and the C_{2^n} factor acts on G via an automorphism of order 2^m strictly smaller than 2^n, we can simplify the construction of a field having Galois group $\mathcal{G}$ via the following Lemma.

Lemma 4: *Suppose $\mathcal{G} = G \rtimes C_{2^n}$ where the automorphism of G given by ϵ induces an automorphism of order 2^m on G with $m < n$. Suppose there exists a field L_2 such that $\mathrm{Gal}(L_2/K) = G \rtimes C_{2^m}$ under the same action as that of C_{2^n}. Let L be the fixed field of G in L_2. Suppose that L can be embedded into a Galois cyclic C_{2^n} extension L' of K with $L_2 \cap L' = L$. Then $\mathrm{Gal}(L_2L'/K) = G \rtimes C_{2^n}$.*

Proof: This is a direct consequence of the structure of the group $\mathcal{G} = G \rtimes C_{2^n}$. Indeed $\mathcal{G}$ is isomorphic to the subgroup of $G \rtimes C_{2^m} \times C_{2^n}$ given by elements

$$\{(\sigma, x) \in (G \rtimes C_{2^m}) \times C_{2^n} \,|\, \sigma \pmod G \equiv x \pmod{C_{2^{n-m}}}\}.$$

This is the Galois group of an extension obtained by identifying the isomorphic quotient fields of $G \rtimes C_{2^m} \pmod G$ and $C_{2^n} \pmod{C_{2^{n-m}}}$. $\diamondsuit$

§4. The element a

Let $\mathcal{G}$ be a 2-group and fix a choice of -1. As before, we write $\mathcal{G} = GC_{2^n}$ for some normal subgroup G of $\mathcal{G}$ containing -1. As in the previous section, we set $\mathcal{H} = \mathcal{G}/\{\pm 1\}$ and $H = G/\{\pm 1\}$. Suppose L_1 is a Galois extension of $K = \mathbb{Q}(T)$ having Galois group $\mathcal{H}$. Let L be the fixed field of H, so L is a cyclic 2^m extension of K for some $m \leq n$. As in Theorem 3, we make the hypothesis that $T_{L,L_1,H,G} = 0$ in $\mathrm{Br}_2(L)$.

Then by Theorem 3, there exists $a \in K$ such that $T_{K,L_1,\mathcal{H},\mathcal{G}} = (L/K, a)$ in $\mathrm{Br}_2(K)$. We compute the element a explicitly in two examples.

Example 1: $\mathcal{G} = C_8$, $G = C_4$, $H = C_2$, $\mathcal{H} = C_4$ (somewhat inelegantly, we write $\mathcal{G} = GC_8$, i.e. $C_8 = C_4C_8$). It is of course already well-known that the cyclic group of order 8 has Gal_T, cf. [M], [S4]; nevertheless it is a good illustration of the methods described above. Let $d \in K$ (not a square) be such that $(-1, d) = 0$ in $\mathrm{Br}_2(K)$. Then d is the sum of two squares, say $d = x^2 + y^2$. Set $L = K(\sqrt{d})$ and for all $r \in K^*$, set $L_r = K(\sqrt{rd + ry\sqrt{d}})$. Let ω generate $\mathrm{Gal}(L/K)$, so $\omega(\sqrt{d}) = -\sqrt{d}$. Then $\mathrm{Gal}(L_r/K) = \mathcal{H} = C_4$. Indeed L_r/K is a Galois extension since $(rd + ry\sqrt{d})\omega(rd + ry\sqrt{d}) = r^2x^2d$ which is a square in L. But $N_{L_r/K}(\sqrt{rd + ry\sqrt{d}}) = r^2x^2d$, which is not a square in K, so $\mathrm{Gal}(L_4/K) \simeq C_4$

and the action of a generator ϵ of it is given by

$$\sqrt{rd+ry\sqrt{d}} \mapsto \sqrt{rd-ry\sqrt{d}} \mapsto -\sqrt{rd+ry\sqrt{d}} \mapsto -\sqrt{rd-ry\sqrt{d}}.$$

By §1, we know the obstruction to the embedding problem T_{K,L_r,C_4,C_8}. It is the crossed-product algebra

$$\sum_{i=0}^{3} L_r \epsilon^i,$$

where ϵ is a generator of C_8, so $\epsilon^4 = -1$, and multiplication is given by the action of ϵ on L_r as a generator of $\mathrm{Gal}(L_r/K)$. This algebra has dimension 16. We write it as the tensor product of two quaternion algebras, precisely

$$(2,d) \otimes (-1,2rd),$$

generated as follows: set $\sigma = \epsilon - \epsilon^3$ and $\lambda = \sqrt{rd+ry\sqrt{d}} + \sqrt{rd-ry\sqrt{d}}\epsilon^2$; then $(2,d)$ is generated by σ and $\sqrt{d}$, and $(-1,2rd)$ is generated by ϵ^2 and $\lambda = \sqrt{rd-ry\sqrt{d}}\epsilon^2 + \sqrt{rd+ry\sqrt{d}}$. It is easy to check that the two pairs of generators anticommute, and that the elements of each pair commute with those of the other. Since $(-1,d)$ is assumed to be trivial in $\mathrm{Br}_2(K)$ and $(-1,2)$ is also trivial, we see that

$$T_{K,L_r,C_4,C_8} = (2,d) + (-1,r)$$

in $\mathrm{Br}_2(K)$.

We now assume that T_{L,L_r,C_2,C_4} is trivial and show that T_{K,L_r,C_4,C_8} becomes equal to a symbol of the form (a,d). Indeed, $T_{L,L_r,C_2,C_4} = (-1, rd+ry\sqrt{d})$ in $\mathrm{Br}_2(L)$. We easily show that if $(-1,rd+ry\sqrt{d}) = 0$ in $\mathrm{Br}_2(L)$, then $(-1,rd) = 0$ in $\mathrm{Br}_2(L)$ and vice versa, for these two algebras are in fact equivalent in $\mathrm{Br}_2(L)$: if ϵ is a generator of C_8, we can let $(-1,rd+ry\sqrt{d})$ be generated by ϵ^2 and $\sqrt{rd+ry\sqrt{d}}$, and $(-1,rd)$ by ϵ^2 and $\sqrt{rd+ry\sqrt{d}} + \sqrt{rd-ry\sqrt{d}}\epsilon^2$: clearly over L each of these algebras contains the other. So the hypothesis that $T_{L,L_r,C_2,C_4} = 0$ actually implies that $(-1,rd) = 0$ in $\mathrm{Br}_2(L)$, and therefore $(-1,r) = 0$ since $(-1,d) = 0$. So $T_{K,L_r,C_4,C_8} = (2,d) + (-1,r) = (2,d)$ in $\mathrm{Br}_2(K)$, so we can take $a = 2$.

Example 2: $\mathcal{G} = D_8$, $G = D_4$, $H = C_2^2$, $\mathcal{H} = D_4$.

Let $L = K(\sqrt{d})$, $L_1 = L(\sqrt{b+c\sqrt{d}}, \sqrt{b-c\sqrt{d}})$ where $b^2 - dc^2 = \delta$ with $K(\sqrt{\delta}) \not\subset K(\sqrt{d})$. Then $\mathrm{Gal}(L_1/K) = D_4$. By a calculation of generators similar to that in example 1 we compute $T_{K,L_1,D_4,D_8} = (2,d) + (2b, -d\delta)$. Now, $T_{L,L_1,H,G} = T_{L,L_1,C_2^2,D_4} = (b + c\sqrt{d}, b - c\sqrt{d})$ in $\mathrm{Br}_2(L)$. Let us show that $(b + c\sqrt{d}, b - c\sqrt{d}) = (2b, -\delta)$ in $\mathrm{Br}_2(L)$. Let ϵ, ω be generators of D_8 such that $\epsilon^8 = \omega^2 = 1$ and the commutator $[\epsilon, \omega] = -\epsilon^2$. The first algebra is generated by $\sqrt{b+c\sqrt{d}}\omega$ and $\sqrt{b-c\sqrt{d}}\epsilon\omega$, and the second by the sum and the product of these two elements.

Now suppose that $T_{L,L_1,H,G} = (2b, -\delta) = 0$ in $\mathrm{Br}_2(L)$. Then $T_{K,L_1,D_4,D_8} = (2,d) + (2b, -d\delta) = (2,d) + (2b,d) + (2b, -\delta) = (b,d)$ so we can take the element a equal to b.

§5. Two examples of applications of the theorem

We keep the preceding notation, so G is a 2-Sylow subgroup or a maximal subgroup of $\mathcal{G}$, $\mathcal{H} = \mathcal{G}/\{\pm 1\}$, and $H = G/\{\pm 1\}$.

Example 1: $\mathcal{G} = SL(2,3)$ (see [F]).

This group of order 24 actually has a unique and therefore normal 2-Sylow subgroup G isomorphic to the quaternion group of order 8. The group $\mathcal{H}$ is isomorphic to A_4, and $H = C_2^2$, which can be considered as the subgroup of A_4 given by the permutations (1)(2)(3)(4), (12)(34), (13)(24) and (14)(23). Let $P(x)$ be a polynomial having Galois group A_4 over K, and let r_1, r_2, r_3 and r_4 be its roots, A_4 acting on them via its permutations. Let L be the fixed field of H, so $[L:K] = 3$: we have $L = K\big((r_1 + r_3)^2\big)$ since it is easily seen that H fixes L and that $[L:K] = 3$. Let L_1 be the splitting field of $P(x)$, so L_1 is a biquadratic extension of L, say $L_1 = L(r_1 + r_2, r_1 + r_4)$. The obstruction to the embedding problem T_{L,L_1,C_2^2,Q_8} is given by

$$T_{L,L_1,C_2^2,Q_8} = (-1,-1) + \big(-(r_1+r_2)^2, -(r_1+r_4)^2\big).$$

Let $(-1,-1)$ be generated by u_1 and u_2 with $u_1^2 = u_2^2 = -1$, $u_3 = u_1u_2 = -u_2u_1$, and $\big(-(r_1+r_2)^2, -(r_1+r_4)^2\big)$ be generated by v_1 and v_2 with $v_1^2 = -(r_1+r_2)^2$, $v_2^2 = -(r_1+r_4)^2$ and $v_3 = v_1v_2 = -v_2v_1$. If $T_{L,L_1,C_2^2,Q_8} = 0$ then there exists a

3×3 matrix $W = (w_{ij})$ defined over L such that for $i = 1, 2, 3$, $\sum_{j=1}^{3} w_{ij} v_j = u_j$. By a theorem of Witt (see [W]), if we set $\gamma = 1 + (r_1 + r_2)w_{11} + (r_1 + r_4)w_{22} + 1/(r_1 + r_2)(r_1 + r_4)w_{33}$, then $L_1(\sqrt{\gamma})$ is Galois over L with Galois group Q_8. By Lemma 2, if $\beta = \gamma\gamma^{\tau}\gamma^{\tau^2}$ where $\tau = (234) \in A_4$, then $L_1(\sqrt{\beta})$ is Galois over K of Galois group $SL(2,3)$. This calculation can be carried out numerically, at least if one can find the matrix W (see [S1]).

Example 2: A family of 2-groups of nilpotency class 3.

Let $\mathcal{G}$ be a 2-group which is a semi-direct product of an extra-special 2-group G and C_2 (generated by ϵ of order 2). We recall that an extra-special 2-group is an extension of C_2^n by C_2 having center and commutator subgroup of order 2: there are no such groups for n odd and exactly two for n even, which take the forms of central products $D_4^{n/2}$ and $Q_8 D_4^{(n-2)/2}$. Let us show that $\mathcal{G}$ can be realized as a Galois group over K. Since G is extra-special, $H = C_2^n$ and $\mathcal{H}$ is a semi-direct product $(C_2^n) \rtimes C_2$: we suppose that the action is not trivial. In order to show that $\mathcal{G}$ is a Galois group, we construct an explicit extension L_1 of K such that $\mathrm{Gal}(L_1/K) = \mathcal{H}$ and $T_{K,L_1,\mathcal{H},\mathcal{G}} = 0$, and then give an explicit element $\gamma \in L_1$ such that $L_1(\sqrt{\gamma})$ is Galois over K with Galois group $\mathcal{G}$.

Let us choose a particular set of n generators for C_2^n. Since we suppose that ϵ does not act trivially, we can choose an α_1 such that ϵ does not fix it. Set $\alpha_2 = \epsilon(\alpha_1)$. If there exist elements of C_2^n not in the subgroup generated by α_1 and α_2 on which ϵ does not act trivially, choose one, call it α_3 and set $\alpha_4 = \epsilon(\alpha_3)$. (Note that α_4 cannot lie in the group generated by α_1 and α_2 since ϵ is of order 2). Continue this way until there are no more elements on which ϵ does not act trivially; we have say $\alpha_1, \ldots, \alpha_{2j}$. Now for $2j < i \leq n$, we take generators α_i such that $\epsilon(\alpha_i) = \alpha_i$.

We now construct the field L_1. Let $d \in K$ be a sum of 2 squares such that $L = K(\sqrt{d})$ is a regular quadratic extension of K. Choose $d_1, \ldots, d_n \in L$, independent in $L^*/(L^*)^2$, satisfying the following properties:

(i) d_1 and d_2 are sums of 2 squares in L;

(ii) For $1 \leq i \leq j$, d_{2i-1} and d_{2i} are conjugates over K, and for $2j < i \leq n$, $d_i \in K^*$, where d and $d_{2j+1}, \ldots, d_n$ are all independent in $K^*/(K^*)^2$, so that

$$\mathrm{Gal}\big(K(\sqrt{d}, \sqrt{d_{2j+1}}, \ldots, \sqrt{d_n})/K\big) \simeq (C_2)^{n-2j+1};$$

(iii) The symbols $(d_i, d_{i+1}) = 0$ in $\mathrm{Br}_2(L)$ for all odd i with $1 \leq i < n$.

Properties (i), (ii) and (iii) can be simultaneously satisfied by choosing each d_i successively of the right form and such that $(d_{i-1}, d_i) = 0$.

Set $L_1 = L(\sqrt{d_1}, \ldots, \sqrt{d_n})$. Then L_1 is Galois over K with Galois group $\mathcal{H}$, and $T_{K,L_1,\mathcal{H},\mathcal{G}} = 0$. Indeed, the action of each α_i on L_1 is given by $\alpha_i(\sqrt{d_i}) = -\sqrt{d_i}$ and α_i fixes the other $\sqrt{d_j}$, and the action of ϵ is given by $\epsilon(\sqrt{d}) = -\sqrt{d}$, $\epsilon(\sqrt{d_{2i-1}}) = \sqrt{d_{2i}}$ for $1 \leq i \leq j$, and $\epsilon(\sqrt{d_i}) = \sqrt{d_i}$ for $2j < i \leq n$, so L_1 is Galois over K with Galois group $\mathcal{H}$. Moreover it is known (cf. [S3]) that the obstruction $T_{L,L_1,H,G}$ is given by $\sum_{\text{odd } i}(d_i, d_{i+1})$ if G has no quaternion part and $(-1, d_1 d_2) + \sum_{\text{odd } i}(d_i, d_{i+1})$ if it does, so conditions (i), (ii) and (iii) on the d_i show that $T_{L,L_1,H,G} = 0$; indeed they were created for that purpose. The point of the construction is to give an element $\gamma \in L_1$ such that $L_1(\sqrt{\gamma})$ is Galois over L of Galois group G. This is done as follows: for each odd i, the field $E_i = L(\sqrt{d_i}, \sqrt{d_{i+1}})$ is a biquadratic extension of L, and since we have $T_{L,E_i,C_2^2,D_4} = (d_i, d_{i+1}) = 0$, there exists an element $\delta_i \in E_i$ for each odd i such that $E_i(\sqrt{\delta_i})$ is a D_4 extension of L. If G has a quaternion part, replace δ_1 by an element of E_1 such that $E_1(\sqrt{\delta_1})$ is a Q_8 extension of L; such an element exists because the obstruction to the embedding problem $T_{L,E_1,C_2^2,Q_8} = (-1, d_1 d_2) + (d_1, d_2) = 0$. The δ_i can all be easily calculated explicitly: for the quaternion one see [W], and for the dihedral one, if $(d_i, d_{i+1}) = 0$ then there exist x_i and $y_i \in K$ such that $d_i x_i^2 + d_{i+1} y_i^2 = 1$, and we can set $\delta_i = 1 - x_i \sqrt{d_i}$. Set $\gamma = \prod_{\text{odd } i} \delta_i$: then by construction, $L_1(\sqrt{\gamma})$ is a Galois extension of L having Galois group the extra-special group G. We want to show how to modify this field, if necessary, for it to be Galois over K with Galois group $\mathcal{G}$.

We are now in a position to apply the methods of theorem 3. By this theorem, we know that there exists $a \in K$, depending on L_1, such that $T_{K,L_1,\mathcal{H},\mathcal{G}} = (a, d)$ and that a can be calculated via the equation $\gamma\gamma^\epsilon = a\lambda^2$ for some $\lambda \in L_1$. We will arrange the field L_1, i.e. choose the elements d_i, in such a way as to make $\gamma\gamma^\epsilon$ into a square, so $a = 1$. It will suffice if each $E_i(\sqrt{\delta_i})$ is Galois over K of Galois group D_8 (except for $E_1(\sqrt{\delta_1})$, which must have Galois group $\tilde{D}_4$ if G has a quaternion part: here $\tilde{D}_4$ is the central extension of D_4 by $\{\pm 1\}$ having generators x and y with relations $x^4 = (xy)^2 = -1$ and $y^2 = 1$). This is satisfied if in addition to properties (i), (ii) and (iii), the d_i satisfy

(iv) $T_{K,E_i,D_4,D_8} = (2, d) + \big(d_i + d_{i+1}, -d d_i d_{i+1}\big) = 0$ for i odd, $1 \leq i < n$,

unless G has a quaternion part, in which case we ask that

$$T_{K,E_1,D_4,\tilde{D}_4} = (-2,-d) + \big(-d_1-d_2, -dd_1d_2\big) = 0$$

in $\mathrm{Br}_2(K)$.

These two obstructions are well-known; the D_8 one was given in example 2 of §4; for the $\tilde{D}_4$ one, see [S2].

When the d_i satisfy (iv), then the δ_i can be chosen such that $E_i(\delta_i)$ is Galois over K of Galois group D_8 (resp. $\tilde{D}_4$). This implies that $\delta_i\delta_i^\epsilon$ is a square in E_i for each odd i, so of course $\gamma\gamma^\epsilon$ is a square, $a = 1$, $T_{K,L_1,\mathcal{H},\mathcal{G}} = 0$ and $\mathrm{Gal}\big(L_1(\sqrt{\gamma})/K\big) = \mathcal{G}$. Thus we have

Lemma 5: *Semi-direct products of extra-special 2-groups with C_2 have the property* Gal_T.

We remark that it is easy to generalize this result to any extension of C_2^n by C_2 in the place of the extra-special group.

Remark: We note that we could have given condition (iv) together with the other conditions directly, and then proved that $L_1(\sqrt{\gamma})$ was the right extension without mentioning the element a. This would have had the disadvantage of giving no indication as to how the extension was found. In the following section, however, we do give the extension directly and then prove it is the right one without ever mentioning the element a. We point out here that the procedure used to find the extension in each case was analogous to the one used in this example: choose a maximal subgroup $G \subset \mathcal{G}$, build an extension L_1 having $\mathcal{H} = \mathcal{G}/\{\pm 1\}$ as Galois group, let L be the fixed field of the image H of G in $\mathcal{H} = \mathcal{G}/\{\pm 1\}$, and build an extension L_2 of L_1 having Galois group G over L (that you can do this is a strong assumption on L_1 which must be realized). Then calculate the element a such that (a,d) gives the obstruction to L_2 being Galois over K, and arrange L_2 so that this obstruction becomes trivial.

§6. The smallest irreducible 2-groups

The smallest irreducible 2-groups are 10 of the 267 groups of order 64, which were calculated by Ralf Dentzer using the SOGOS system for calculations in solvable groups developed by R. Laue, J. Neubueser and U. Schoenwalder in

Aachen (cf. [LNS]). As mentioned earlier, seven of these groups have descending central 2-series of length 3. In this section we prove that these seven groups all have the property Gal_T and construct explicit regular extensions of K having them as Galois groups. The three groups of length 4 are technically more difficult to obtain but should also give way to similar techniques.

Let $\mathcal{G}_1, \ldots, \mathcal{G}_7$ denote the seven groups of order 64 having no abelian normal subgroup not lying in the Frattini subgroup and descending central 2-series of length 3. In general, we use the following strategy to prove that the groups $\mathcal{G}_i$ have the property Gal_T. We write $\mathcal{G}_i$ as a quotient of a group of the form $G \rtimes C_{2^n}$ where G is a normal subgroup of $\mathcal{G}_i$: in each case we can take a group G of order 16. Let ϵ be a generator of the C_{2^n} factor: if the action of ϵ induces an automorphism of G having order 2^m for $m \leq n$, we explicitly construct a field having Galois group $G \rtimes C_{2^m}$, in such a way that we can then apply Lemma 4 to extend the field to one having Galois group $G \rtimes C_{2^n}$.

We use the following notation. A fixed central element of order 2 of $\mathcal{G}_i$, contained in G, will be denoted by -1. We set $\mathcal{H}_i = \mathcal{G}_i/\{\pm 1\}$ and $H = G/\{\pm 1\}$. We write L_1 for a Galois extension of K having Galois group $\mathcal{H}_i$ and L for the fixed field of H, so L is a cyclic Galois 2^n-extension of K. We always write ϵ for a generator of the C_{2^n} factor in $\mathcal{G}_i$ and $\mathcal{H}_i$ and also for the automorphisms which it induces on G, on L_1 and on $T_{L,L_1,H,G}$. We use the notation $[a,b]$ for the commutator of two elements of a group, and (α, β) for a quaternion algebra or an element of the Brauer group.

We will need the following result on cyclic extensions of degree 8.

Lemma 6: *Let $d \in K$ be such that $K(\sqrt{d})$ is a regular quadratic extension of K. Then $K(\sqrt{d})$ can be embedded in a cyclic Galois K-extension of order 8 if and only if $(-1,d) = 0$ in $\mathrm{Br}_2(K)$ and there exists $c \in K$ such that $(2,d) = (-1,c)$.*

Proof: Suppose that $K(\sqrt{d})$ can be embedded in a Galois 8 extension L. Let L' be the cyclic 4 subextension of L. Then $L' = K(\sqrt{a + b\sqrt{d}})$. As explained in §4, example 1, the obstruction to the embedding problem is given by $T_{K,L',C_4,C_8} = (2,d) + (-1,a)$, so since this embedding problem is trivial by hypothesis, we may take c to be a. Now suppose that we have an element c such that $(2,d) = (-1,c)$. If $(-1,d) = 0$ then $d = x^2 + y^2$ for some $x, y \in K$. Set $L' = K(\sqrt{c + \frac{cx}{d}\sqrt{d}})$. Then it is immediate that $\mathrm{Gal}(L'/K) = C_4$, and moreover $T_{K,L',C_4,C_8} = (2,d) + (-1,c)$ which is zero by hypothesis, so L' can be embedded into a cyclic 8 extension L.

$\diamondsuit$

Case 1: The groups $\mathcal{G}_1$, $\mathcal{G}_2$ and $\mathcal{G}_3$

The first three groups on our list all have a normal subgroup G of the form $D_4 \times C_2$, where D_4 is the dihedral group of order 8. Let a, b and c be generators of G such that $a^2 = b^2 = c^2 = 1$ and $[a,b] = -1$, $[a,c] = [b,c] = 1$. The group $H = G/\{\pm 1\}$ is isomorphic to $(C_2)^3$. Let ϵ be the following automorphism of G:

$$\epsilon(a) = -bc, \quad \epsilon(b) = -a, \quad \epsilon(c) = c.$$

The order of this automorphism is 4, and the order of the automorphism induced on H is also 4. We have:

$$\mathcal{G}_1 = (D_4 \times C_2) \rtimes C_4$$

$$\mathcal{G}_2 = \big((D_4 \times C_2) \rtimes C_8\big)/(\epsilon^4 = c)$$

$$\mathcal{G}_3 = \big((D_4 \times C_2) \rtimes C_8\big)/(\epsilon^4 = -c).$$

where in each case the action of the C_{2^n} factor is given by the above automorphism ϵ, considered to be a generator of C_{2^n} acting by conjugation.

Suppose we show that $\mathcal{G}_1$ has Gal_T. This gives a field L_2 having Galois group $\mathcal{G}_1$ over K. Let L be the fixed field of $G \subset \mathcal{G}$; then L is a cyclic 4 extension of K. To show that $\mathcal{G}_2$ and $\mathcal{G}_3$ satisfy Gal_T, it suffices by Lemma 4 to show that $\mathcal{G}_1$ can be realized in such a way that L can be embedded into a cyclic 8 extension L' of K which is disjoint from L_2 as extensions of L. We construct an L_2 with these properties.

We want $d \in K$, not a square, such that $(-1,d) = (2,d) = 1$. Then d can be written as a sum of two squares in K, say $x^2 + y^2$, and also as $z^2 + 2w^2$. For example, set $X = T^2 - 1 - T^4$, $x = (2T^3 - T^2 - 1 - T^4)/X$, $y = (2T^2 - 2T)/X$, $u = (T^4 - 2T^3 + T^2 - 1)/X$ and $v = (2T^2 - 2T)/X$, and let $d = x^2 + y^2 = u^2 + 2v^2$. Note that $d = r^2 - 2s^2$ with $r = (xu + d)/(x + u)$ and $s = (yv)/(x + u)$. Let $L = K(\sqrt{d + y\sqrt{d}})$. Then by Lemma 6, $\mathrm{Gal}(L/K) \simeq C_4$, and the obstruction to the embedding problem T_{K,L,C_4,C_8} is $(2,d) + (-1,d)$ which is trivial.

Set $z = 1/(r + \sqrt{d + y\sqrt{d}}) \in L$. Let $z' = 1/(r + \sqrt{d - y\sqrt{d}})$, $z'' = 1/(r - \sqrt{d + y\sqrt{d}})$ and $z''' = 1/(r - \sqrt{d - y\sqrt{d}})$. Then we have the following conditions which are necessary to ensure that the extensions we construct exist and do not "collapse":

(i) $K(z) = L$;

(ii) $1/zz'' = 2s^2 - y\sqrt{d}$;

(iii) $N_{L/K}(z)$ is not a square nor d times a square in K (this can be checked by hand – or, better, by computer).

Let $\alpha = 1/zz''$, $\beta = 1/z'z'''$ and $\delta = z''z'''$. Let $L_1 = L(\sqrt{\alpha}, \sqrt{\beta}, \sqrt{\delta})$, and let $\mathcal{H}_1 = \mathcal{G}_1/\{\pm 1\}$.

Lemma 7: *L_1 is Galois over K with* $\mathrm{Gal}(L_1/K) = \mathcal{H}_1$.

Proof: The conditions (i) and (iii) imply that $\mathrm{Gal}(L_1/L) \simeq (C_2)^3$. The action of G (so that of H) on L_1 is given by the following diagram:

	a	b	c
$\sqrt{\alpha}$	$\sqrt{\alpha}$	$-\sqrt{\alpha}$	$\sqrt{\alpha}$
$\sqrt{\beta}$	$-\sqrt{\beta}$	$\sqrt{\beta}$	$\sqrt{\beta}$
$\sqrt{\delta}$	$\sqrt{\delta}$	$\sqrt{\delta}$	$-\sqrt{\delta}$

Let ϵ be the generator of $\mathrm{Gal}(L/K) \simeq C_4$ sending $\sqrt{d + y\sqrt{d}}$ to $\sqrt{d - y\sqrt{d}}$. We extend the action of ϵ to L_1 by: $\epsilon(\sqrt{\alpha}) = -\sqrt{\beta}$, $\epsilon(\sqrt{\beta}) = \sqrt{\alpha}$, $\epsilon(\sqrt{\delta}) = z\sqrt{\alpha\delta}$, which shows that L_1 is Galois over K. In order to show that the Galois group is $\mathcal{H}_1$, we must check that this action of ϵ corresponds to the action of ϵ on the generators a, b and c. This involves checking that $\epsilon^{-1}a\epsilon$, $\epsilon^{-1}b\epsilon$ and $\epsilon^{-1}c\epsilon$ act like $\epsilon(a) = -bc$, $\epsilon(b) = -a$ and $\epsilon(c) = c$ on $\sqrt{\alpha}$, $\sqrt{\beta}$ and $\sqrt{\delta}$. Note that -1 acts trivially on L_1 and can therefore be ignored. It is immediate that $\epsilon^{-1}c\epsilon$ acts like c on $\sqrt{\alpha}$ and $\sqrt{\beta}$. On $\sqrt{\delta}$, we have $\epsilon(\sqrt{\delta}) = z\sqrt{\alpha\delta}$, $\epsilon^2(\sqrt{\delta}) = -zz'\sqrt{\alpha\beta\delta}$ and $\epsilon^3(\sqrt{\delta}) = z'\sqrt{\beta\delta}$, so $\epsilon^{-1}c\epsilon(\sqrt{\delta}) = \epsilon^3 c(z\sqrt{\alpha\delta}) = \epsilon^3(-z\sqrt{\alpha\delta}) = -\beta z'z'''\sqrt{\delta} = -\sqrt{\delta} = c(\sqrt{\delta})$ since $\beta = 1/z'z'''$. The other calculations are analogous. $\diamondsuit$

Note that by construction, the field $L_0 := K(\sqrt{d})(\sqrt{\alpha}, \sqrt{\beta})$ is a Galois extension of K of Galois group D_4. The main point in the construction of the group $\mathcal{G}_1$ is that given $L_1 = L(\sqrt{\alpha}, \sqrt{\beta}, \sqrt{\delta})$, **we can give an element** $\gamma \in K(\sqrt{d})(\sqrt{\alpha}, \sqrt{\beta})$ **such that adjoining** $\sqrt{\gamma}$ **to this subfield gives a** D_8**-**

extension of K, and adjoining it to L_1 gives the desired $\mathcal{G}_1$-extension as in diagram 1. The left-hand column shows the construction of a D_8-extension of K. The obstruction to the embedding problem of a D_4 extension into a D_8 extension was given in example 2 of §4; in this example it is equal to $(2,d)+\big(2\cdot 2s^2,-d(4s^4-dy^2)\big)$, which is trivial since $(2,d)$ is trivial and $2\cdot 2s^2$ is a square. Therefore there exists $\gamma\in L_0$ such that $L_0(\sqrt{\gamma})$ is Galois over K with Galois group D_8. Then the field $L_1(\sqrt{\gamma})$ is the desired $\mathcal{G}_1$-extension. Indeed, $\mathrm{Gal}(L_2/L)$ is the normal subgroup $D_4\times C_2$, so it suffices to extend the action of the generator ϵ of $\mathrm{Gal}(L/K)$ to L_2 and check that it coincides with the presentation of $\mathcal{G}_1$. We know the action of ϵ on L_1 by lemma 7. To extend it to L_2 it suffices to define its action on $\sqrt{\gamma}$. But $L_0(\sqrt{\gamma})\cap L=K(\sqrt{d})$, so to define $\epsilon(\sqrt{\gamma})$, it suffices to choose a lifting η of the automorphism $\sqrt{d}\mapsto-\sqrt{d}$ of $K(\sqrt{d})$ to $\mathrm{Gal}(L_0(\sqrt{\gamma})/K)$ which restricted to L_0 is equal to ϵ, and define $\epsilon(\sqrt{\gamma})=\eta(\sqrt{\gamma})$. Then by construction, $\epsilon^{-1}a\epsilon$, $\epsilon^{-1}b\epsilon$ and $\epsilon^{-1}c\epsilon$ act on $\sqrt{\gamma}$ like $-bc$, $-a$ and c respectively.

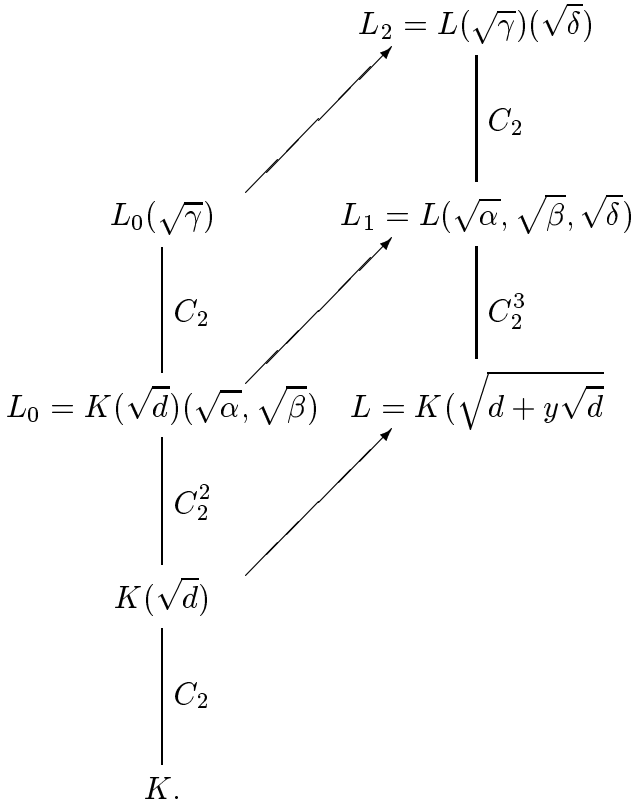

Diagram 1

By the argument in the proof of Lemma 6, L can be embedded into a Galois cyclic 8 extension L' of K. This extension can be chosen disjoint from L_2 as

extensions of L. For L' being a quadratic extension of L, either $L \cap L_2 = L$ or $L' \subset L_2$. But there are infinitely many C_8 extensions L' containing L (recall from §1 that if $L(\sqrt{\lambda})$ is such an extension then the others are all of the form $L(\sqrt{r\lambda})$ for $r \in K^*$). The field L_2 cannot contain them all, so some of them must be L-disjoint from L_2. By lemma 4, this proves that $\mathcal{G}_2$ and $\mathcal{G}_3$ have Gal_T.

Case 2: The groups $\mathcal{G}_4$ and $\mathcal{G}_5$.

These two groups have a normal subgroup G of the form $Q_8 \times C_2$, where Q_8 is the quaternion group. Let a, b and c be generators of G such that $a^2 = b^2 = -1$, $c^2 = 1$, $[a, b] = -1$. Let ϵ be the following isomorphism of G:

$$\epsilon(a) = -bc, \quad \epsilon(b) = -a, \quad \epsilon(c) = c.$$

Then we have:

$$\mathcal{G}_4 = (Q_8 \times C_2) \rtimes C_4$$

$$\mathcal{G}_5 = \big((Q_8 \times C_2) \rtimes C_8\big)/(\epsilon^4 = c).$$

Thus it suffices to construct $\mathcal{G}_4$, as in Case 1, in such a way that the fixed field of G can be embedded in a cyclic 8 extension. In fact, since H is the same as for the group $\mathcal{G}_1$ and the action of ϵ on H is identical, we may take the same fields L, L' and L_1 as in the construction of $\mathcal{G}_1$. In fact, Case 2 is identical to Case 1 except that the role of D_8 is replaced by $\tilde{D}_4$, the generalized dihedral group. We need to find d and z as above, such that $K(z)$ is a cyclic regular Galois extension of K containing $K(\sqrt{d})$, and such that setting $\alpha = 1/zz''$, $\beta = 1/z'z'''$ and $L_0 = K(\sqrt{\alpha}, \sqrt{\beta})$, we have the following two conditions:

(i) $T_{K,L_1,\mathcal{H}_4,\mathcal{G}_4} = T_{K,L_0,D_4,\tilde{D}_4} = (-\alpha - \beta, -d\alpha\beta) + (-2, -d) = 0$;

(ii) $T_{K,L,C_4,C_8} = 0$.

If condition (i) is satisfied, then $\mathcal{G}_4$ has Gal_T, and conditions (i) and (ii) give the result for $\mathcal{G}_5$ by Lemma 4. We give an explicit example of a choice of d and z such that conditions (i) and (ii) are fulfilled. Let

$$x = \frac{27r^2 + 12r + 3}{24r^2 + 12r} \quad \text{and} \quad a = \frac{12r^2 + 6r}{9r^2 - 1},$$

for any $r \in K^*$. Then we take $d = 1 + x^4$ such that $K(\sqrt{d})$ is a regular extension of K. Note that $(-1, d) = 0$ because d is a sum of two squares and $(2, d) = 0$ because $2x^2 + d = (1 + x^2)^2$.

We set

$$z = 1/\big(\frac{3}{2}\sqrt{d} + \sqrt{\frac{5}{4}(d + \sqrt{d})}\big).$$

It is immediate that $L = K(z) = K\big(\sqrt{\frac{5}{4}(d + \sqrt{d})}\big)$ is a cyclic Galois 4 extension of K. We set $\alpha = 1/zz'' = d - \frac{5}{4}\sqrt{d}$ and $\beta = 1/z'z''' = d + \frac{5}{4}\sqrt{d}$. Then since $\alpha\beta = d^2 - \frac{25}{16}d$, the field $L(\sqrt{\alpha}, \sqrt{\beta})$ is a biquadratic extension of L. The choice of d and z satisfies conditions (i) and (ii) as follows.

(i) We see that

$$(-\alpha - \beta, -d\alpha\beta) + (-2, -d) = \big(-2d, -d(d^2 - \frac{25}{16}d)\big) + (-2, -1)$$

$$= (-2, d - \frac{25}{16}) = (-2, x^4 - \frac{9}{16}).$$

We obtain a solution to the equation

$$-2X^2 + x^4 - \frac{9}{16} = Y^2$$

by setting $X = (9 - 6a)/4a$ and $Y = (9 - 12a)/4a^2$ and expressing x, X and Y in terms of r. The second condition is immediate:

(ii) $T_{K,L,C_4,C_8} = (-1, \frac{5}{4}d) + (2, d) = (-1, \frac{5}{4}) + (-1, d) + (2, d) = 0$.

This concludes the proof that $\mathcal{G}_4$ and $\mathcal{G}_5$ have the property Gal_T. As the explicit construction of the field L_2, it is reduced to the construction of a $\tilde{D}_4$, which is known (cf. [S2]).

Case 3: The groups $\mathcal{G}_6$ and $\mathcal{G}_7$

These groups have normal subgroup $G = C_4 \rtimes C_4$ generated by elements a and b such that $a^2 = -1$, $b^4 = 1$ and $[a, b] = -1$. The action of ϵ is given by

$$\epsilon(a) = -ab^2, \qquad \epsilon(b) = -ab.$$

The groups are given by

$\mathcal{G}_6 = \big((C_4 \rtimes C_4) \rtimes C_8\big)/(\epsilon^4 = b^2)$

$\mathcal{G}_7 = \big((C_4 \rtimes C_4) \rtimes C_8\big)/(\epsilon^4 = -b^2)$.

The action of ϵ is of order 4 so our procedure will be to construct the group $\mathcal{G} := G \rtimes C_4$ in such a way that the C_4 extension can be embedded into a C_8 as usual, which will give the result for $\mathcal{G}_6$ and $\mathcal{G}_7$. The group $\mathcal{G}$ is generated by elements a, b and ϵ such that $a^2 = -1$, $b^4 = 1$ and $\epsilon^4 = 1$, while $[a, b] = -1$, $[a, \epsilon] = -b^2$ and $[b, \epsilon] = a$.

Let $d \in K$ be such that $(-1, d) = 0$. Let $L' = K(\sqrt{x + y\sqrt{d}})$ be a cyclic 4 extension of K. Let a, $b \in K$ and let $L_0 = K(\sqrt{a + b\sqrt{d}}, \sqrt{a - b\sqrt{d}})$, so $\mathrm{Gal}(L_0/K) = D_4$. Then

(i) $T_{K,L_0,D_4,D_8} = \big(2a, -d(a^2 - db^2)\big)$

(ii) $T_{K,L_0L,C_2^2 \rtimes C_4,(C_2 \times C_4) \rtimes C_4} = (d, 2a) + (-x, a^2 - db^2)$.

Note that the group $(C_2 \times C_4) \rtimes C_4$ is precisely the group $\mathcal{H} = \mathcal{G}/\{\pm 1\}$. Set $d = 1 + T^4$, $x = 1$, $y = 1/d$, $a = 2$ and $b = -2/(1 + d)$. Then the elements d, x, y, a and b are such that L' can be embedded into a cyclic 8 extension L of K and the embedding problems (i) and (ii) split. This means that we have obtained the group $G \rtimes C_8$ for the following reason. Let L_1 be the quadratic extension of L_0L' having Galois group $\mathcal{H}$. Let $L_2 = L_1(\sqrt{\gamma})$ where γ is an element of L_0 such that $L_0(\sqrt{\gamma})$ is Galois over K of Galois group D_8 (the field $L_0(\sqrt{\gamma})$ will be the fixed field of the subgroup of $\mathcal{G}$ generated by a^2, b^2 and ϵ^2). Then $\mathrm{Gal}(L_2/K) = \mathcal{G}$ and L_2L has Galois group $G \rtimes C_8$ over K. So $\mathcal{G}_6$ and $\mathcal{G}_7$ have the property Gal_T.

References

[C] T. Crespo. Explicit construction of $\tilde{A}_n$ type fields, *J. Alg.* **127** (1989), 452-461.

[D] R. Dentzer. On split embedding problems with abelian kernel, Heidelberg Preprint Series 91-10 (1991).

[F] D.K. Faddeev, Construction of fields of algebraical numbers whose Galois group is a group of quaternion units, *Doklady* **47** (1945).

[LNS] R. Laue, J. Neubueser and U. Schoenwalder. Algorithms for finite solvable groups and the SOGOS system. Proc. of the LMS Symposium on Computational Group Theory (Durham 1982), M.D. Atkinson, ed., 105-135.

[M] B.H. Matzat. *Konstruktive Galoistheorie*, LNM 1284, Springer-Verlag.

[R] I. Reiner. Maximal Orders. Academic Press, London-New York-San Francisco, 1975.

[S1] L. Schneps. Explicit realisations of subgroups of $GL_2(\mathbf{F}_3)$ as Galois groups, *J. Number Theory* **39**, 5-13.

[S2] ———, $\tilde{D}_4$ et $\hat{D}_4$ comme groupes de Galois, Note aux *C. R. Acad. Sci. Paris*, t. **308**, Série I (1989).

[S3] ———, Construction explicite de 2-groupes extra-spéciaux comme groupes de Galois, *Publications de la Faculté des Sciences de Besançon* (Théorie des Nombres), 1992-93.

[S4] ———, On cyclic field extensions of degree 8, *Math. Scand.* **71** (1992), 24-30.

[W] E. Witt. Konstruktion von galoisschen Körpern der Charakteristik p zu vorgegebener Gruppe der Ordnung p^f. *J. reine angew. math.* **174**, 1935, 237-245.

Leila Schneps
URA 741 du CNRS, Laboratoire de Mathématiques
Faculté des Sciences de Besançon
25030 Besançon Cedex, France