MATH. SCAND. 71 (1992), 24–30

ON CYCLIC FIELD EXTENSIONS OF DEGREE 8

LEILA SCHNEPS

Abstract.

A 6-parameter family of cyclic extensions of degree 8 is given over any field. This family parametrizes all C_8 extensions over a number of fields including $\mathbf{Q}$, any field containing $\sqrt{2}$ or $\sqrt{-1}$, all number fields having a single prime over 2, all local fields whose residue field has characteristic different from 2 and all these fields with any number of indeterminates adjoined.

Let G be a finite group and K a field. Let $P(X, t_1, \ldots, t_n)$ be a polynomial defined over $K(t_1, \ldots, t_n)$, where $t_1, \ldots, t_n$ are indeterminates. Let E be the splitting field of P over $K(t_1, \ldots, t_n)$, and suppose that P has the following properties:

(i) the Galois group of E over $K(t_1, \ldots, t_n)$ is G,

(ii) every Galois extension E_0 of K such that $\mathrm{Gal}(E_0/K) \simeq G$ is the splitting field of a polynomial of the form $P(X, \alpha_1, \ldots, \alpha_n)$ for some $\alpha_1, \ldots, \alpha_n \in K$.

We say that the polynomial P parametrizes all G-extensions of K. It is said to be *versal* or *generic* for K if it satisfies the following additional property:

(iii) Let F be any field containing K. Then every Galois extension E_1 of F such that $\mathrm{Gal}(E_1/F) \simeq G$ is the splitting field of a polynomial of the form $P(X, \alpha_1, \ldots, \alpha_n)$ for some $\alpha_1, \ldots, \alpha_n \in F$.

Versal polynomials have been constructed for all cyclic groups of odd order (cf. [Sm]). However the methods fail in the case of cyclic 2-groups of order $\geqq 8$; in fact it is known that there is no versal polynomial for the cyclic group of order 8 over $\mathbf{Q}$, for there exists a Galois C_8-extension of $\mathbf{Q}_2$ which cannot be obtained as the splitting field of a polynomial obtained by specialization to values in $\mathbf{Q}_2$ of any C_8 polynomial defined over $\mathbf{Q}(t_1, \ldots, t_n)$ (cf. [L], [Sa]).

In this article we give an explicit extension E of $K(t_1, \ldots, t_6)$ having Galois group C_8 and which actually parametrizes all C_8-extensions of K (but is not versal) whenever K satisfies a certain hypothesis. I owe particular thanks to J-P. Serre for asking me about C_8 extensions, and noticing that the hypothesis applies to more fields than I thought. I also thank the ETH Zürich for its hospitality and

Received September 12, 1991.

financial support during the preparation of this paper. Finally, certain statements (in particular improvements of some parts of Lemma 4 and the remark at the very end of the article) are due to helpful remarks by the referee.

Let $i = \sqrt{-1}$. Let $\mathrm{Br}_2(K)$ be the kernel of multiplication by 2 in the Brauer group of K. We write this group additively and denote by (a, b) the class of the quaternion algebra (a, b) for $a, b \in K$. We say that K satisfies hypothesis (H) if the following is true for K:

Hypothesis (H): For all $d \in K$ such that $(-1, d) = 0$ in $\mathrm{Br}_2(K)$ and $(2, d) = 0$ in $\mathrm{Br}_2(K(i))$, we have $(2, d) = 0$ in $\mathrm{Br}_2(K)$.

After describing the extension E and proving that it parametrizes all C_8-extensions of K whenever K satisfies (H), we give a list of fields satisfying (H), calculate an explicit family of C_8 extensions and consider what can happen over some fields not satisfying (H).

We construct a C_8-extension E of $K(t_1, \ldots, t_6)$ as follows. Let

$$
\begin{aligned}
D &= t_1^2 + t_2^2 - t_3^2 + 2,\\
x &= (2t_1t_3 - t_1^2 + t_2^2 - t_3^2 + 2)/D,\\
y &= (2t_2t_3 - 2t_1t_2)/D,\\
z &= (t_3^2 - 2t_1t_3 + t_1^2 + t_2^2 + 2)/D,\\
w &= (2t_3 - 2t_1)/D,\\
d &= x^2 + y^2 = z^2 - 2w^2,\\
r &= t_4^2 + t_5^2,\\
u &= t_4x - t_5y - t_4y - t_5x,\\
v &= t_4x - t_5y + t_4y + t_5x\\
u_1 &= (1/x)(vx - uy + u\sqrt{d})\\
v_1 &= (1/x)(ux + vy - v\sqrt{d})\\
\gamma &= (z + \sqrt{d})(2rd + u_1\sqrt{rd + ry\sqrt{d}}).
\end{aligned}
$$

Let $K_6 = K(t_1, \ldots, t_6)$ and $E = K_6(\sqrt{t_6\gamma})$. Let $P(X, t_1, \ldots, t_6)$ be the minimal polynomial of $\sqrt{t_6\gamma}$ over K_6. It is easy to calculate P using a computer, however every coefficient, even factored, takes several lines to write down, so we do not give it here. At the end of the article we give an example of a one-parameter family of C_8 polynomials.

MAIN RESULT: *The Galois group* $\mathrm{Gal}(E/K_6)$ *is* C_8. *Moreover, if K is a field satisfying* (H), *then every extension of K having Galois group C_8 comes from E by specialization of the parameters t_i to values in K: that is, every such extension is the splitting field of a polynomial of the form $P(X, \alpha_1, \ldots, \alpha_n)$ for $\alpha_i \in K$.*

The proof is contained in Lemmas 2 and 3. The essential idea of the construction is the following. We first construct the complete set of C_4 extensions of

K which can be embedded into a C_8 extension. Let L be such a C_4 extension and $K(\sqrt{d})$ its quadratic subfield: we then construct the complete set of C_4 extensions of $K(\sqrt{d})$ containing L. Finally, we give the subset of these fields which are actually Galois over K.

Before proving the main result we recall some general facts about C_8 extensions.

LEMMA 1. *Let $d \in K$. Then*

(i) *There exists a C_4 extension L/K containing $K(\sqrt{d})$ if and only if $(-1, d) = 0$,* i.e. *d is the sum of two squares $x^2 + y^2$. If this is the case the complete set of such fields is given by*

$$\{L_r = K(\sqrt{rd + ry\sqrt{d}}) \mid r \in K^*\}.$$

(ii) *Suppose we have a C_4 extension L_r as in* (i). *Then L_r can be embedded in a C_8 extension E/K if and only if $(2, d) + (-1, rd) = 0$ in* $\mathrm{Br}_2(K)$.

(iii) *Let $d \in K$. Then $K(\sqrt{d})$ can be embedded into a cyclic extension of K of degree 8 if and only if $(-1, d) = 0$ and there exists $r \in K$ such that $(2, d) = (-1, r)$. If K satisfies* (H), *these conditions become: $(-1, d) = (2, d) = 0$.*

PROOF. (i) A field $K(\sqrt{d})(\sqrt{\alpha})$ for $\alpha \in K(\sqrt{d})$ is a Galois C_4 extension of K if and only if $N_{K(\sqrt{d})/K}(\alpha) = da^2$ for some $a \in K^*$. Clearly this is the case for all the fields L_r. If $K(\sqrt{d})(\sqrt{\alpha})$ is a C_4 extension, then all others containing $K(\sqrt{d})$ are given by $K(\sqrt{d})(\sqrt{r\alpha})$ for $r \in K^*$, so when $d = x^2 + y^2$, the L_r give the complete set. Now suppose L is a C_4 extension of K and $K(\sqrt{d})$ is its quadratic subfield. Then we can write $L = K(\sqrt{d})(\sqrt{\alpha})$ where $\alpha \in K(\sqrt{d})$ and $N_{K(\sqrt{d})/K}(\alpha) = da^2$, so writing $\alpha = a_1 + a_2\sqrt{d}$, we have $a_1^2 - da_2^2 = da^2$, so $d = a_1^2(a^2 + a_2^2)^{-1}$, so it is the sum of two squares.

(ii) We briefly recall the main result about obstructions to embedding problems. Let H be a group, G an extension of H by C_2 and L/K a Galois extension with Galois group H. Let $\{v_\sigma \mid \sigma \in H\}$ be a system of representatives for G/C_2 and let ζ be the factor system defined by $v_\sigma v_\tau = \zeta(\sigma, \tau)v_{\sigma\tau}$. The field L can be embedded in a Galois extension E/K of Galois group G if and only if the crossed-product algebra $(L/K, \zeta)$ splits (cf. [R]).

In our case, we have $H = C_4 = \mathrm{Gal}(L/K)$ and $G = C_8$. Let ε be a generator of C_8 so $\varepsilon^4 = -1$, and take $1, \varepsilon, \varepsilon^2$ and ε^3 for the set $\{v_\sigma\}$. The algebra $(L/K, \zeta)$ can be written $\sum_{i=0}^{3} L\varepsilon^i$, where multiplication is given by $\varepsilon\alpha = \varepsilon(\alpha)\varepsilon$, ε acting on L via H. Since the dimension of this algebra is 16 and it is killed by 2, it can be written as a tensor product of the two quaternion algebras. We claim that we can take $(2, d)$ and $(-1, 10rd)$ to be these two algebras, generated as follows. Let $\sigma = \varepsilon - \varepsilon^3$ and

$\lambda = \sqrt{rd + ry\sqrt{d}} + \sqrt{rd - ry\sqrt{d}}\varepsilon^2$. Then $(2, d)$ is generated by σ and $\sqrt{d}$ and $(-1, 10rd)$ is generated by ε^2 and $\lambda + \sigma\lambda\sigma/2$ (note that each pair of generators anticommutes). To check that $(L/K, \zeta)$ is a tensor product of these two algebras it sufficies to check that the generators of $(2, d)$ commute with those of $(-1, 10rd)$ and to notice that each of them is contained in $(L/K, \zeta)$. Note that $(-1, 10) = 0$ in $\mathrm{Br}_2(K)$ so $(-1, 10rd) = (-1, rd)$, and the obstruction to the embedding problem as an element of $\mathrm{Br}_2(K)$ is $(2, d) + (-1, rd)$. For similar considerations, see [K].

(iii) First suppose $(-1, d) = 0$ and there exists r such that $(2, d) = (-1, r)$. Then by (i), $d = x^2 + y^2$ and $L_r = K(\sqrt{rd + ry\sqrt{d}})$ is a C_4 extension of K and by (ii), since $(2, d) + (-1, rd) = (2, d) + (-1, r) = 0$, L_r admits a C_8 extension. Now suppose that E is a C_8 extension of K and let L be its C_4 subfield and $K(\sqrt{d})$ its quadratic subfield. Then since $K(\sqrt{d})$ admits the extension L, by (i) we must have $(-1, d) = 0$, $d = x^2 + y^2$ and $L = L_r$ for some r. Moreover, L_r is embedded in the C_8 extension E, so the obstruction to the embedding problem $(2, d) + (-1, rd)$ must be trivial, so $(2, d) = (-1, r)$. If K satisfies (H), this condition implies that $(2, d) = 0$.

We now prove the main result in Lemmas 2 and 3.

LEMMA 2. $\mathrm{Gal}(E/K_6) = C_8$.

PROOF. E is an extension of degree 8 which contains a cyclic 4 extension of K, namely $L_r = K(\sqrt{rd + ry\sqrt{d}})$. To see that E is a C_8 extension, it suffices to show that $L_r(\sqrt{\gamma})$ is one, which we do by checking the following two properties: firstly, $L_r(\sqrt{\gamma})$ is a Galois C_4 extension of $K(\sqrt{d})$ and secondly, $L_r(\sqrt{\gamma})$ is Galois over K.

The field $L_r(\sqrt{\gamma})$ is a cyclic 4 extension of $K(\sqrt{d})$ by the identity

$$4r^2d^2 - u_1^2(rd + ry\sqrt{d}) = v_1^2(rd + ry\sqrt{d}),$$

as in the proof of (i) of Lemma 1. The left hand side is, up to squares, just $N_{L_r/K(\sqrt{d})}(\gamma)$, so the field $L_r(\sqrt{\gamma})$ is given by adjoining to $K(\sqrt{d})(\sqrt{rd + ry\sqrt{d}})$ the square root of an element whose norm is, up to squares, equal to $rd + ry\sqrt{d}$: such an extension is cyclic of degree 4 (as in the proof of (i) in Lemma 1).

In order to verify that $L_r(\sqrt{\gamma})$ is Galois over K it suffices to show that the product of γ with each of its conjugates is a square. This is clear for the conjugates of γ over $K(\sqrt{d})$ since $L_r(\gamma)$ is Galois over $K(\sqrt{d})$. Therefore it suffices to check that $\gamma\gamma'$ is a square where γ' is the conjugate of γ under the map $\sqrt{d} \to -\sqrt{d}$. This follows from the identity

$$\gamma\gamma' = w^2(2rd + \sqrt{4r^2d^2 + 2((v^2 - u^2)x - 2uvy)r\sqrt{d}})^2.$$

Thus, γ times any of its conjugates is a square and therefore $L_r(\sqrt{\gamma})$ is a Galois extension of K_6 of Galois group C_8.

LEMMA 3: *If K satisfies* (H), *then the extension E of K_6 described above parametrizes all C_8-extensions of K.*

PROOF. By Lemma 1, the set of $d \in K$ such that $K(\sqrt{d})$ is contained in a C_8 extension is given by

$$\{d \in K \mid (-1, d) = (2, d) = 0\}.$$

In other words, d can be written in the form $x^2 + y^2$ and also $z^2 - 2w^2$. Since the equation $x^2 + y^2 - z^2 + 2w^2 = 0$ has an obvious solution $(1, 0, 1, 0)$, the complete set of solutions can be parametrized (the result is given in the description of the extension E/K_6).

By Lemma 1, the complete set of cyclic 4 extensions of K containing $K(\sqrt{d})$ for such a d and embeddable into a C_8 extension of K is given by $L_r = K(\sqrt{rd + ry\sqrt{d}})$ for $r \in K^*$ such that $(2, d) + (-1, rd) = (-1, r) = 0$. This condition is parametrized by $r = t_4^2 + t_5^2$. Finally, over any such L_r, we saw in Lemma 2 that $L_r(\sqrt{\gamma})$ is a C_8 extension of K, so the complete set of C_8 extensions of K containing L_r is given by $L_r(\sqrt{s\gamma})$, $s \in K^*$.

We now take a look at which fields actually satisfy the hypothesis. The following list is certainly not exhaustive.

LEMMA 4. *The following fields K satisfy hypothesis* (H):

(i) *K contains $\sqrt{2}$ or $\sqrt{-1}$ or $\sqrt{-2}$*

(ii) *K is a local field whose residue field is of characteristic different from 2*

(iii) $K = \mathbb{Q}$

(iv) *K is a number field with the following property: at most one of the completions K_v at the places v lying over 2 does not satisfy* (H)

(v) *$K = k(t)$ where t is a indeterminate and k is an infinite field of characteristic different from 2 which satisfies* (H).

PROOF. (i) If K contains $\sqrt{2}$ then $(2, d) = 0$ in $\mathrm{Br}_2(K)$. If K contains $\sqrt{-1}$ and $(2, d) = (-1, x)$ then $(2, d) = 0$. Finally if K contains $\sqrt{-2}$, then $(-1, d) = 0 \Rightarrow (2, d) = (-2, d) = 0$.

For (ii), it suffices to notice that any local field whose residue field is of characteristic $p \neq 2$ contains the square root of -1, 2 or -2, for these numbers are units in K and thus quadratically dependent. As pointed out by the referee, if a local field contains none of these three square roots, it cannot satisfy (H), for if K satisfies (H) and does not contain $\sqrt{-1}$, then $(2, d) = 0$ in $\mathrm{Br}_2(K(\sqrt{-1}))$ for every $d \in K$ (by local class field theory). In particular, $(-1, d) = 0 \Rightarrow (2, d) = 0$, and thus the square classes represented by -1 and 2 must be dependent, so 2 or -2 is a square in K.

Part (iii) is a direct consequence of (i) and (ii) since if $(2,d)=0$ in $\mathrm{Br}_2(\mathbb{R})$ and $\mathrm{Br}_2(\mathbb{Q}_p)$ for all $p \neq 2$, then by the product formula $(2,d)=0$ in $\mathrm{Br}_2(\mathbb{Q}_2)$ and thus in $\mathrm{Br}_2(\mathbb{Q})$. Part (iv) is the same argument: if $(2,d)=0$ in the Brauer groups of completions of K at all places of K except one (the place over 2), then it is 0 everywhere and therefore also in $\mathrm{Br}_2(K)$.

(v) For this part, we need to use the following two basic facts about the Galois cohomology of function fields (cf. [A]).

(1) Let X denote the set of discrete valuations of K which are trivial on k. For each $v \in X$ let us write $k(v)$ for the residue field of K_v, the completion of K at v. Then we have the following exact sequence:

$$0 \to \mathrm{Br}_2(k) \to \mathrm{Br}_2(K) \to \prod_{v \in X} H^1(k(v), \mathbb{Z}/2\mathbb{Z}).$$

The last arrow is given by $\prod_v \mathrm{Res}_v$ where for each $v \in X$,

$$\mathrm{Br}_2(K) \to \mathrm{Br}_2(K_v) \xrightarrow{\mathrm{Res}_v} H^1(k(v), \mathbb{Z}/2\mathbb{Z}) \simeq k(v)^*/k(v)^{*2}.$$

(2) Let $\alpha = \sum_i (a_i(t), b_i(t))$ be an element of $\mathrm{Br}_2(K)$, and suppose its image under $\prod_v \mathrm{Res}_v$ is trivial. Then by the above exact sequence α is an element of $\mathrm{Br}_2(k)$. For any value $t_0 \in k$ which is not a zero or a pole of any of the $a_i(t)$ or the $b_i(t)$, we have $\alpha = \sum_i (a_i(t_0), b_i(t_0))$.

We can now finish the proof of part (v) of the Lemma. Let $d=d(t)$ and $x=x(t)$ be elements of K such that $(-1,d)=0$ and $(2,d)=(-1,x)$ in $\mathrm{Br}_2(K)$. We first show that the image of $(2,d)$ under the map $\prod \mathrm{Res}_v$ is trivial. For any symbol $(a,b) \in \mathrm{Br}_2(K)$, the local symbol $(a,b)_v$ at a place $v \in X$ is trivial if there exist elements a' and $b' \in K$ such that $(a,b)=(a',b')$ in $\mathrm{Br}_2(K)$ and a' and b' both have even valuations at v. We show that this is the case for the symbol $(2,d)$ at every place $v \in X$. Since 2 and -1 have even valuations and $(2,d)$ is equal to $(-1,x)$ by hypothesis, if either d or x has an even valuation at v the local symbol $(2,d)_v$ is trivial. If both d and x have odd valuations, then since $(-1,d)=0$ by hypothesis, we have $(2,d)=(-1,x)=(-1,dx)$ and dx has an even valuation so again, the local symbol $(2,d)_v$ is trivial. This is true for every $v \in X$ so by the exact sequence in (1), we find that $(2,d)$ is in $\mathrm{Br}_2(k)$.

By remark (2) above, if the symbol $(2,d)=(2,d(t))$ is in $\mathrm{Br}_2(k)$, then for any $t_0 \in k$ which is not a zero or pole of $d(t)$ (and we can always find such a t_0 since k is an infinite field), we have $(-1,d)=(-1,d(t_0))$ and $(2,d)=(2,d(t_0))=(-1,x)=(-1,x(t_0))$. Thus, since k satisfies hypothesis (H), we must have $(2,d)=(2,d(t_0))=0$ in $\mathrm{Br}_2(k)$, so K satisfies hypothesis (H). As remarked by the referee, this kind of argument shows that the field $K = k((t))$ also satisfies (H). This concludes the proof of Lemma 4.

The minimal polynomial of the element $t_6\gamma$ in 6 indeterminates is long and complicated. However, it is easy to calculate various explicit families of C_8 extensions. We give one here over the field $\mathbb{Q}(t)$. Let $d = 1 + t^4$. Then since $d = (1 + t^2)^2 - 2t^2$, we have $(-1, d) = (2, d) = 0$. Let $L = \mathbb{Q}(t)(\sqrt{d + t^2\sqrt{d}})$ be a cyclic 4 extension of $\mathbb{Q}(t)$ containing $\mathbb{Q}(t)(\sqrt{d})$. Set

$$\gamma = (1 + t^2 + \sqrt{d})(2d + (d + (1 - t^2)\sqrt{d})\sqrt{d + t^2\sqrt{d}}).$$

Then $L(\sqrt{\gamma})$ is a Galois C_8 extension of $\mathbb{Q}(t)$. It is the splitting field of the polynomial:

$$X^8 - 8(1 + t^2)(1 + t^4)X^6 + 8t^2(4 + t^2)(1 + t^4)^2 X^4 - 32t^4(1 + t^4)^3 X^2 + \\ + 16t^8(1 + t^4)^3.$$

Over fields K which do not satisfy (H), the extension E/K_6 does not parametrize all C_8-extensions of K. The easiest example is $K = \mathbb{Q}_2$. If we set $d = 5$, we have $(-1, 5)_2 = 0$. But $(2, 5)_2 \neq 0$: yet $(2, 5)_2 = (-1, 3)_2$. In fact for any $d \in \mathbb{Z}$, $d \equiv 5 \pmod 8$, we obtain such a counterexample. It is easy to construct number fields not satisfying (H) as well. For example, let K be an extension of $\mathbb{Q}$ of even degree such that 2 splits and there exist primes p and $q \in \mathbb{Q}$, inert in K, with $p \equiv 3 \pmod 8$ and $q \equiv 5 \pmod 8$. Then $(-1, q) = 0$ and $(2, q) = (-1, p)$. Thus $K(\sqrt{q})$ can be embedded into a C_8 extension not obtained by specialization from E.

REFERENCES

[A] J. Arason, *Cohomologische Invarianten Quadratischer Formen* J. Algebra 36 (1975), 448–491.

[K] I. Kiming, *Explicit classification of some 2-extensions of a field of characteristic field of characteristic different from* 2, Canad. J. Math 42 (1990), 825–855.

[L] H. W. Lenstra, J., *Rational functions invariant under a finite abelian group*, Invent. Math. 25 (1974), 299–325.

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

[Sa] D. Saltman, *Generic Galois extensions and problems in field theory*, Adv. in Math. 43 (1982), 250–283.

[Sm] G. W. Smith, *Construction of generic cyclic polynomials*, Comm. Alg. 19 (12) (1991) 3367–3391.

U.R.A. 741 DU CNRS
LABORATOIRE DE MATHEMATIQUES
FACULTÉ DE SCIENCES DE BESANÇON
25000 BESANÇON CEDEX
FRANCE