Far East J. Math. Sci. (FJMS) 1(1) (1999), 121-126

CYCLIC QUARTIC FIELDS AND F_{20} QUINTICS

BLAIR K. SPEARMAN and KENNETH S. WILLIAMS

(Received September 19, 1998)

Submitted by K. K. Azad

Abstract

It is shown how to determine the unique quartic subfield of the splitting field of an irreducible quintic polynomial with Galois group F_{20}.

Let $f(X) \in Q[X]$ be a monic solvable irreducible quintic polynomial. As $f(X)$ is solvable its Galois group G is Z_5 (the cyclic group of order 5), D_5 (the dihedral group of order 10), or F_{20} (the Frobenius group of order 20). Let L denote the splitting field of f. If $G = Z_5$, then L does not possess a quadratic subfield. If $G = D_5$, then L possesses a unique quadratic subfield k. The determination of this quadratic subfield k has been treated by Jensen and Yui [3, 4], Williamson [7], and by Spearman, Spearman and Williams [6] when $f(X)$ is a trinomial of the form $X^5 + aX + b$. If $G = F_{20}$, then L possesses a unique quadratic subfield k (which must be real) and a unique quartic subfield K (which must be cyclic and contains k). It is well known that $k = Q(\sqrt{d})$, where $d(> 0)$ is the discriminant of $f(X)$. When $f(X) = X^5 + aX + b$, Spearman, Spearman and Williams [6] have given an explicit formula for K. In this

1991 Mathematics Subject Classification: 11C08, 11R16.

Key words and phrases: cyclic quartic fields, quintic polynomials with Galois group F_{20}.

Both authors were supported by NSERC research grants.

paper we show how to determine K for an arbitrary monic irreducible quintic polynomial $f(X)$ with Galois group $G = F_{20}$.

If n is a positive integer, we write (n) to denote a monic irreducible polynomial in $Q[X]$ of degree n, and we set

(1) $$S = \{ p(\text{prime}) \mid p \nmid d,\ f(X) \equiv (1)(2)(2) (\text{mod } p) \}.$$

Let $p \in S$. The two irreducible quadratics in the factorization of $f(X) (\text{mod } p)$ are distinct $(\text{mod } p)$ as $p \nmid d$. Hence $p \neq 2$ as there is a unique irreducible quadratic polynomial $(\text{mod } 2)$ namely $X^2 + X + 1$. Let D be the squarefree part of d. By Stickelberger's theorem [5, p. 153], we have

(2) $$\left(\frac{D}{p}\right) = \left(\frac{d}{p}\right) = (-1)^{5-3} = 1.$$

Hence for $p \in S$ we can let E_p denote an integer such that $D \equiv E_p^2 \ (\text{mod } p)$. We prove

Theorem. *Let $f(X)$ be a monic irreducible quintic polynomial with Galois group F_{20}. Let $d\,(> 0)$ be the discriminant of $f(X)$. Let $D\,(> 0)$ be the squarefree part of d. Then there are unique integers A, B, C with the following properties*:

(3) *A is squarefree and odd,*

(4) $D = B^2 + C^2,\ B > 0,\ C > 0,$

(5) $(A, D) = 1,$

(6) $A \mid d,$

(7) $\left(\dfrac{A(D + BE_p)}{p}\right) = -1$ *for all* $p \in S$ *with* $p \nmid C$.

Then the unique quartic subfield K of the splitting field L of $f(X)$ is

$$K = Q\left(\sqrt{A\left(D + B\sqrt{D}\right)}\right).$$

Proof. The unique quadratic subfield of L is $k = Q(\sqrt{d}) = Q(\sqrt{D})$. As K is a cyclic quartic field with quadratic subfield $Q(\sqrt{D})$, where D is squarefree, there exist unique integers A, B, C satisfying (3), (4), (5) and (8) [2]. Let θ be a root of $f(X)$ and set $M = Q(\theta)$ so that $[M : Q] = 5$. The compositum of K and M is L. Hence the set of primes dividing the discriminant $d(L)$ coincides with the set of primes dividing $d(K)d(M)$ [5, p. 167]. But L is the minimal normal extension of Q containing M so $d(M)$ and $d(L)$ contain the same primes [5, p. 168]. Let q be a prime such that $q \mid A$. As $d(K) = 2^e A^2 D^3$, where $e = 0, 4, 6, 8$, see [2], we have $q \mid d(K)$. Hence $q \mid d(L)$ and so $q \mid d(M)$. But A is squarefree so $A \mid d(M)$. Hence $A \mid d$, which is (6).

Now, let $p \in S$, $p \nmid C$. An easy calculation shows that $p \nmid A(D + BE_p)$. As $\left(\frac{D}{p}\right) = +1$, p splits completely in k, say $p = PP'$. The prime ideal P (and similarly for P') splits in K if and only if

$$\left[\frac{A(D + B\sqrt{D})}{P}\right]_2 = +1$$

$$\Leftrightarrow \left[\frac{A(D + \varepsilon BE_p)}{P}\right]_2 = +1, \text{ where } \sqrt{D} \equiv \varepsilon E_p \pmod{P},\ \varepsilon = \pm 1,$$

$$\Leftrightarrow \left[\frac{A(D + BE_p)}{P}\right]_2 = +1, \text{ as } \left[\frac{A(D + BE_p)}{P}\right]_2 \left[\frac{A(D - BE_p)}{P}\right]_2 = \left[\frac{A^2C^2E_p^2}{P}\right]_2 = +1,$$

$$\Leftrightarrow \left(\frac{A(D + BE_p)}{p}\right) = +1.$$

Suppose $\left(\frac{A(D + BE_p)}{p}\right) = +1$. Then, by the above, P and P' split in K so that p splits completely in K. As L is a normal extension of K of degree 5, p must factor either as $P_1 P_2 P_3 P_4$ with each $N(P_i) = p^5$ or as $P_1 P_2 \cdots P_{20}$ with each $N(P_i) = p$. Now as $p \in S$, we have $p = Q_1 Q_2 Q_3$ in M with $N(Q_1) = p$, $N(Q_2) = N(Q_3) = p^2$. Since L is a quadratic extension of a quadratic extension of M, the prime ideal factors of Q_2 in L have norms p^2, p^4 or p^8, a contradiction. Hence $\left(\frac{A(D + BE_p)}{p}\right) = -1$.

This theorem can easily be put in the form of an algorithm to determine the unique quartic subfield of the splitting field of a given irreducible quintic polynomial with Galois group F_{20}.

INPUT. $f(X)$–irreducible quintic with Galois group F_{20}.

STEP 1. Calculate discriminant d of $f(X)$.

STEP 2. Calculate squarefree part D of d.

STEP 3. Determine all pairs of positive integers (B, C) such that $D = B^2 + C^2$.

STEP 4. Determine all odd squarefree divisors A of d which are coprime with D.

STEP 5. For $p = 3, 5, 7, 11, \ldots$ with $p \nmid dC$

factor $f(X) \pmod p$

if $f(X) \equiv (1)(2)(2) \pmod p$

eliminate (A, B, C) for which $\left(\frac{A(D + BE_p)}{p}\right) = 1$

next p

else

next p

OUTPUT. Stop when a single triple (A, B, C) remains.

Required quartic field is $Q\left(\sqrt{A\left(D + B\sqrt{D}\right)}\right)$.

Example.

$f(X) = X^5 + 250X^2 + 625$

$d = 5^{19} \cdot 59^2$

$D = 5$

$(B, C) = (1, 2), (2, 1)$

$A = \pm 1, \pm 59$

primes p for which $X^5 + 250X^2 + 625 \equiv (1)(2)(3) \pmod{p}$

are $p = 19, 29, 79, 89, \ldots$

$p = 19$ eliminates $(A, B, C) = (-1, 1, 2), (1, 2, 1), (-59, 2, 1), (59, 1, 2)$

$p = 29$ eliminates $(A, B, C) = (1, 1, 2), (-59, 1, 2)$

$p = 89$ eliminates $(A, B, C) = (59, 2, 1)$

surviving (A, B, C) is $(-1, 2, 1)$.

Hence the unique quartic subfield of the splitting field of $X^5 + 250X^2 + 625$ is $Q\left(\sqrt{-\left(5 + 2\sqrt{5}\right)}\right)$.

References

[1] A. Bruen, C. U. Jensen and N. Yui, Polynomials with Frobenius groups of prime degree as Galois groups II, J. Number Theory 24 (1986), 305-359.

[2] R. H. Hudson and K. S. Williams, The integers of a cyclic quartic field, Rocky Mountain J. Math. 20 (1990), 145-150.

[3] C. U. Jensen and N. Yui, Polynomials with D_5 as Galois group, C. R. Math. Rep. Acad. Sci. Canada 2 (1980), 297-302.

[4] C. U. Jensen and N. Yui, Polynomials with D_p as Galois group, J. Number Theory 15 (1982), 347-375.

[5] W. Narkiewicz, Elementary and Analytic Theory of Algebraic Numbers, Springer-Verlag, Berlin, Heidelberg, New York, PWN-Polish Scientific Publishers, Warsaw, Second Edition, 1990.

[6] B. K. Spearman, L. Y. Spearman and K. S. Williams, The subfields of the splitting field of a solvable quintic trinomial, J. Math. Sci. 6 (1995), 15-18.

[7] C. J. Williamson, Odd degree polynomials with dihedral Galois groups, J. Number Theory 34 (1990), 153-173.

Department of Mathematics and Statistics
Okanagan University College
Kelowna, B. C., Canada V1V 1V7
e-mail: bspearman@okanagan.bc.ca

School of Mathematics and Statistics
Carleton University
Ottawa, Ontario, Canada K1S 5B6
e-mail: williams@math.carleton.ca