Irish Math. Soc. Bulletin
Number 73, Summer 2014, 47–52
ISSN 0791-5578

THE NUMBER OF QUADRATIC SUBFIELDS

JEAN B NGANOU

Abstract. We use elementary field theory to compute the number of intermediate fields of degree 2 of any finite extension of fields of characteristic not 2. This leads to necessary and sufficient conditions for such extensions to have no intermediate fields of degree 2, or to have a unique intermediate field of degree 2. We obtain several applications including the number of quadratic subfields of cyclotomic extensions.

1. Introduction

The Fundamental Theorem of Galois Theory is by far the most important connection between field and group theory. It asserts that for finite Galois extensions, there is a one-to-one correspondence between the intermediate fields and the subgroups of the Galois group. Moreover, under this correspondence subgroups of index n correspond to intermediate fields of degree n. Therefore, this produces an indirect method for finding the number of intermediate fields of a given degree. One would use group-theoretic facts to find the number of subgroups of the correspoding index. Unfortunately, for non Galois extensions, there is no obvious relationship between the intermediate fields of the extensions and the subgroups of their Galois groups.

The aim of this note is to find a field-theoretic formula for the number of intermediate fields of degree 2 for an arbitrary finite extension K/F with F of characteristic not 2. Such a formula would allow us to answer questions about the existence of subfields of degree 2 without having to compute the Galois group, even for non Galois extensions. Our strategy consists in the following steps: starting

2010 *Mathematics Subject Classification.* 06D99, 08A30.

Key words and phrases. Galois group, Galois extension, finite extension, intermediate fields, quadratic closure, cyclotomic extensions, subgroup of squares.

Received on 22-1-2013; revised 25-2-2014.

I would like to thank the referee for his/her comments, which improved the readability of the article.

with a finite extension K/F, we create a new extension Q/F that is finite Galois such that K/F and Q/F have the same intermediate fields of degree 2. We can now apply the Fundamental Theorem of Galois Theory to compute the number of subfields of degree 2 of the extension Q/F, and therefore those of K/F. We also obtain that the extension Q is the fixed field of the subgroup of squares of the Galois group of K/F. In all that follows, F will denote a field of characteristic different from 2 and K/F a finite extension(K is a finite dimensional vector space over F). In addition, for every integer $k \geq 2$, C_k shall denote the cyclic group of order k.

Given a field extension K/F, the Galois group of K/F is denoted by $\mathcal{G}(K/F)$, and is the set of autormorphisms of K that fix every element in F. Given a subgroup H of $\mathcal{G}(K/F)$, the fixed field of H is the intermediate field of K/F defined by $\mathcal{F}(H) := \{a \in K : \sigma(a) = a, \text{ for all } \sigma \in H\}$. An extension K/F is called algebraic if every element of K is a solution to a polynomial equation with coefficients in F. A Galois extension is any algebraic exetnsion K/F satisfying $\mathcal{F}(\mathcal{G}(K/F)) = F$. For the convenience of the reader, we recall the Fundamental Theorem of Galois Theory.

Let K/F be a finite Galois extension with Galois group G. If E is an intermediate field of K/F, let $\mathcal{G}(K)$ denote $\mathcal{G}(K/E)$. Then $\mathcal{F}$ is a bijection from the the subgroups of G to the intermediate fields, with inverse $\mathcal{G}$ such that for every E, $[E : F] = [G : \mathcal{G}(E)]$ and $[K : E] = |\mathcal{G}(E)|$.

We also recall the following result about the number of subgroups of index 2 in any group. The subgroup of squares of a group G is denoted by G^2, and is the subgroup of G generated by $\{g^2 : g \in G\}$. It is easy to see that $G^2 = \{g_1^2 g_2^2 \cdots g_n^2 : g_i \in G, n \geq 1\}$. It is known that, every arbitrary finite group G has exactly $[G : G^2] - 1$ subgroups of index 2 [4, Corollary 1].

We hope the article is accessible to readers with limited background.

2. Number of intermediate fields of degree 2

Let $Q(K/F) := F(\{\alpha \in K : \alpha^2 \in F\})$, then $F \subseteq Q(K/F) \subseteq K$. Since K/F is finite, there exists a subset $\{\alpha_1, \alpha_2, \ldots, \alpha_n\} \subseteq K$ with $\alpha_i^2 \in F$ such that $\alpha_{i+1} \notin F(\alpha_1, \alpha_2, \ldots, \alpha_i)$ for all $i \leq n-1$ and $Q(K/F) = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$. When it is clear what extension K/F is being considered, we will simply write Q for $Q(K/F)$. We will call

$Q(K/F)$ the *quadratic closure* of F in K, or simply the *quadratic closure* of the extension K/F.
Let E be an intermediate field of K/F such that $[E : F] = 2$, then since $Char(F) \neq 2$, there exists $\beta \in E$ with $\beta^2 \in F$ such $E = F(\beta)$. Hence, $E \subseteq Q$ and therefore, every intermediate field of K/F of degree 2 is an intermediate field of Q/F of degree 2. The converse is clearly true. Therefore, intermediate fields of K/F of degree 2 and intermediate fields of Q/F of degree 2 are the same. On the other hand, note that Q is the splitting field of $(x^2 - \alpha_1^2)(x^2 - \alpha_2^2)\cdots(x^2 - \alpha_n^2)$ over F. We have obtained the following key fact about the extension Q/F, which shall play a central role in the entire article.

Theorem 2.1. *For every finite extension K/F, the extension Q/F is a finite Galois extension. Furthermore, K/F and Q/F have the same intermediate subfields of degree 2 over F.*

The Galois group of Q/F is elementary Abelian of exponent 2 as we prove next.

Theorem 2.2. *Let $G = \mathcal{G}(Q/F)$. Then $G \cong C_2 \times C_2 \times \cdots \times C_2$.*

Proof. To see this, first as observed above, there exists a subset $\{\alpha_1, \alpha_2, \ldots, \alpha_n\} \subseteq K$ with $\alpha_i^2 \in F$ such that $\alpha_{i+1} \notin F(\alpha_1, \alpha_2, \ldots, \alpha_i)$ for all $i \leq n-1$ and $Q = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$. It follows from the tower formula that $[Q : F] = 2^n$, and the Fundamental Theorem of Galois Theory that $|G| = 2^n$. In addition, for every $\sigma \in G$, $\sigma(\alpha_i) = \pm\alpha_i$ for all i and consequently $\sigma^2 = id$. It follows from a well-known exercise that G is Abelian, and since G has exponent 2, by the Fundamental Theorem of Finite Abelian groups, $G \cong C_2 \times C_2 \times \cdots \times C_2$. □

Appealing to the Fundamental Theorem of Galois Theory, we can count the number of intermediate fields of Q/F of degree 2 by counting the number of subgroups of index 2 in $\mathcal{G}(Q/F)$.

Corollary 2.3. *Let K/F be finite extension with quadratic closure Q. Then, Q/F has exactly $[Q : F] - 1$ intermediate fields of degree 2.*

Proof. From Theorem 2.2, we have $\mathcal{G}(Q/F) \cong C_2 \times C_2 \times \cdots \times C_2$, where C_2 is the cyclic group of order 2. Thus, $\mathcal{G}(Q/F)^2$ is the trivial group and by [4, Corollary 1], $\mathcal{G}(Q/F)^2$ has $|\mathcal{G}(Q/F)| - 1$ subgroups of index 2. Now, it follows from Fundamental Theorem of Galois Theory, that Q/F has $[Q : F] - 1$ subfields of degree 2. □

Since K/F and Q/F have the same intermediate fields of degree 2 (Theorem 2.1), we deduce;

Corollary 2.4. *Every finite extension K/F has exactly $[Q : F] - 1$ intermediate fields of degree 2 where Q is the quadratic closure of K/F.*

Corollary 2.5. *A finite extension K/F has a unique intermediate field of degree 2 if and only if $[Q : F] = 2$.*

One can apply the Fundamental Theorem of Galois Theory and the results in [4] about subgroups of index 2 to obtain the following.

Theorem 2.6. *For every finite Galois extension K/F with Galois group G and quadratic closure Q,*

$$Q = \mathcal{F}(G^2) \text{ and } \mathcal{G}(K/Q) = G^2$$

3. Applications

We can apply the results above to compute the number of quadratic subfields in some typical extensions. The quadratic closure Q/F of an extension as introduced here could be difficult to compute, but in many cases as in the following Example, it is quite simple and illustrative.

Example 3.1. Consider the extension $\mathbb{Q}(\sqrt{2}, \sqrt[4]{3})/\mathbb{Q}$, which is not Galois. It is easy to see that $[\mathbb{Q}(\sqrt{2}, \sqrt[4]{3}) : \mathbb{Q}] = 8$. It is also clear that $\sqrt{2}, \sqrt{3} \in Q(\mathbb{Q}(\sqrt{2}, \sqrt[4]{3})/\mathbb{Q})$ and $\sqrt[4]{3} \notin Q(\mathbb{Q}(\sqrt{2}, \sqrt[4]{3})/\mathbb{Q})$. Hence $Q(\mathbb{Q}(\sqrt{2}, \sqrt[4]{3})/\mathbb{Q}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ and $[Q(\mathbb{Q}(\sqrt{2}, \sqrt[4]{3})/\mathbb{Q}) : \mathbb{Q}] = 4$. Therefore, $\mathbb{Q}(\sqrt{2}, \sqrt[4]{3})/\mathbb{Q}$ has three intermediate fields of degree 2.

The next example justifies why the characteristic assumption on the base field cannot be dropped.

Example 3.2. Let $k = \mathbb{F}_2(t)$ be the field of rational functions in t over the Galois field of two elements, $K = k(x, y)$ be the field of rational functions in two variables over k and $F = k(x^2, y^2)$. Then for each $a \in k$, there is a degree 2 field extension $L_a = F(x + ay)$ of F. It is elementary to see $L_a = L_b$ if and only if $a = b$. Thus, since $|k|$ is infinite, there are infinitely many degree 2 subextensions of K/F even though $[K : F] = 4$ is finite.

As another application, we investigate degree 2 subfields of the cyclotomic extensions. A simple and complete treatment of cyclotomic extensions can be found in [3, §7]. Recall that for $n \geq 1$, the nth cyclotomic extension of $\mathbb{Q}$ is $\mathbb{Q}_n := \mathbb{Q}(\omega)$ where ω is a primitive nth root of unity. It is well known that $\mathbb{Q}_n/\mathbb{Q}$ is Galois and $\mathcal{G}(\mathbb{Q}_n/\mathbb{Q}) \cong U(n)$, the group of units of the ring $\mathbb{Z}_n$ of integers modulo n. The order of $U(n)$ is denoted by $\phi(n)$ and is equal to the number of positive integers less than or equal to n that are relatively prime to n.

Example 3.3. Let $N_2(\mathbb{Q}_n/\mathbb{Q})$ denote the exact number of degree 2 intermediate fields of $\mathbb{Q}_n/\mathbb{Q}$. Then we have the following formulae:

1. For every nonnegative integer r
$$N_2(\mathbb{Q}_{2^r}/\mathbb{Q}) = \begin{cases} 0 & \text{if } r = 0, 1 \\ 1 & \text{if } r = 2 \\ 3 & \text{if } r \geq 3 \end{cases}$$
2. If $n = 2^r p_1^{t_1} p_2^{t_2} \cdots p_s^{t_s}$ where $r \geq 0$, $s \geq 1$ and $p_1, p_2, \cdots, p_s$ are distinct odd primes.
$$N_2(\mathbb{Q}_n/\mathbb{Q}) = \begin{cases} 2^s - 1 & \text{if } r = 0, 1 \\ 2^{s+1} - 1 & \text{if } r = 2 \\ 2^{s+2} - 1 & \text{if } r \geq 3 \end{cases}$$

Recall that $\mathcal{G}(\mathbb{Q}_n/\mathbb{Q}) \cong U(n)$ (see for instance [3, Corollary 7.8]. So, by Corollary 2.3, $N_2(\mathbb{Q}_n/\mathbb{Q}) = [Q(\mathbb{Q}_n/\mathbb{Q}) : \mathbb{Q}] - 1 = [U(n) : U(n)^2] - 1$. Therefore, we need to compute $[U(n) : U(n)^2]$ in each case. We will use the decomposition of the U-groups into cyclic groups as found in [1, pp159-160] or [2]. We will also use the facts that if C is a cyclic group of order m, it follows from [1, Theorem. 4.2] that C^2 is cyclic of order $m/gcd(2, m)$; and that $(G_1 \oplus G_2)^2 = G_1^2 \oplus G_2^2$ for every groups G_1, G_2 [4, Theorem 4].
1. First note that the case $r = 0$ is obvious as $\mathbb{Q}_1 = \mathbb{Q}$. On the other hand, we have $U(2) \cong \{0\}$, $U(4) \cong C_2$, $U(2^r) \cong C_2 \oplus C_{2^{r-2}}$ for $r \geq 3$. So $U(2)^2 \cong U(4)^2 \cong \{0\}$, and $U(2^r)^2 \cong C_{2^{r-3}}$ for $r \geq 3$. Hence $[U(2) : U(2)^2] = 1$ and $[U(4) : U(4)^2] = 2$ and for $r \geq 3$, $[U(2^r) : U(2^r)^2] = 2^{r-1}/2^{r-3} = 4$. Therefore the formula is justified.
2. First assume $r \geq 3$, then $U(n) \cong U(2^r) \oplus U(p_1^{t_1}) \oplus \cdots \oplus U(p_s^{t_s}) \cong C_2 \oplus C_{2^{r-2}} \oplus C_{p_1^{t_1} - p_1^{t_1 - 1}} \oplus \cdots \oplus C_{p_s^{t_s} - p_s^{t_s - 1}}$. Hence, $U(n)^2 \cong C_{2^{r-3}} \oplus C_{(p_1^{t_1} - p_1^{t_1-1})/2} \oplus \cdots \oplus C_{(p_s^{t_s} - p_s^{t_s-1})/2}$. Thus, $|U(n)^2| = \phi(n)/2^{s+2}$ and $[U(n) : U(n)^2] = 2^{s+2}$. For $r = 2$, as above $U(n) \cong C_2 \oplus C_{p_1^{t_1} - p_1^{t_1-1}} \oplus \cdots \oplus C_{p_s^{t_s} - p_s^{t_s-1}}$, so $U(n)^2 \cong C_{(p_1^{t_1} - p_1^{t_1-1})/2} \oplus \cdots \oplus C_{(p_s^{t_s} - p_s^{t_s-1})/2}$. So,

$|U(n)^2| = \phi(n)/2^{s+1}$ and $[U(n) : U(n)^2] = 2^{s+1}$.
We leave the cases $r = 0, 1$ as a simple verification exercise.

References

[1] J. Gallian, Contemporary Abstract Algebra, 7th Ed, Brooks/Cole, Belmont, CA, 2010.

[2] D. R. Guichard, When is $U(n)$ cyclic? An Algebra Approach, *Math. Mag.* **72**(1999) 139-142.

[3] P. Morandi, Field and Galois Theory, *Graduate Tests in Math.*, Springer-Verlag, 1996.

[4] J. B. Nganou, How Rare are Subgroups of Index 2?, *Math. Mag.* **85**, No. 3(2012)215-220.

Jean B Nganou earned his PhD in Mathematics from New Mexico State University, and is currently an Instructor in Mathematics at the University of Oregon. Dr. Nganou's interests include algebraic logic (MV-algebras, BL-algebras, residuated lattices), hyperstructures, non-commutative ring theory, elementary group theory, and mathematics for elementary school teachers.

Department of Mathematics, University of Oregon, Eugene, OR 97403, OR 48710-0001
E-mail address: nganou@uoregon.edu