ISRAEL JOURNAL OF MATHEMATICS **130** (2002), 11–19

$\mathbb{Q}$-ADEQUACY OF GALOIS 2-EXTENSIONS

BY

HELEN G. GRUNDMAN*

Department of Mathematics, Bryn Mawr College
Bryn Mawr, PA 19010-2899, USA
e-mail: grundman@brynmawr.edu

AND

DAVID B. LEEP

Department of Mathematics, University of Kentucky
Lexington, KY 40506-0027, USA
e-mail: leep@ms.uky.edu

AND

TARA L. SMITH

Department of Mathematical Sciences, University of Cincinnati
Cincinnati, OH 45221-0025, USA
e-mail: tsmith@math.uc.edu

ABSTRACT

The $\mathbb{Q}$-adequacy of any finite Galois 2-extension of $\mathbb{Q}$ is shown to depend only on the $\mathbb{Q}$-adequacy of its maximal elementary abelian intermediate field, which must be either quadratic (and hence always $\mathbb{Q}$-adequate) or biquadratic over $\mathbb{Q}$. A precise description of those biquadratic extensions of $\mathbb{Q}$ which are $\mathbb{Q}$-adequate is given. This then gives a method for explicitly determining whether any given finite Galois 2-extension of $\mathbb{Q}$ can arise as a subfield of a $\mathbb{Q}$-central division algebra.

* Research supported by the Faculty Research Fund of Bryn Mawr College.
Received May 25, 2000

1. Introduction

This paper is concerned with a special case of the following question: If F is a field and L a finite extension of F, does there exist an F-central division algebra D containing L as a maximal commutative subfield? If such a D exists, then L is said to be F-adequate; otherwise L is F-deficient. This question was first explored in depth in [S]. In this paper we present a complete answer to the question of which biquadratic extensions $\mathbb{Q}(\sqrt{m},\sqrt{n})$ of the rational numbers $\mathbb{Q}$ are $\mathbb{Q}$-adequate. Using a result in [LSS] we show in Theorem 2.1 that biquadratic extensions are the key to determining $\mathbb{Q}$-adequacy of any Galois 2-extension of $\mathbb{Q}$. Thus this paper provides an explicit means for testing the $\mathbb{Q}$-adequacy of any such extension.

It is shown in [S], Theorem 2.8, that if G is a group for which every Sylow subgroup is cyclic, then every Galois extension L of a global field F with $\mathrm{Gal}(L/F) \cong G$ is F-adequate. Thus biquadratic extensions of $\mathbb{Q}$ represent the first level of difficulty where such an extension may be $\mathbb{Q}$-deficient.

2. $\mathbb{Q}$-adequacy of Galois 2-extensions

In this section we fix L to be a finite Galois 2-extension of $\mathbb{Q}$ with $G = \mathrm{Gal}(L/\mathbb{Q})$. Let $\Phi(G)$ be the Frattini subgroup of G, and let K be the subfield of L that is fixed by $\Phi(G)$. Since $\Phi(G)$ is a normal subgroup of G, it follows that $K/\mathbb{Q}$ is a Galois extension. Since the quotient of a p-group by its Frattini subgroup is the maximal elementary abelian quotient of the group, it follows that K is the maximal elementary abelian extension of $\mathbb{Q}$ inside L. (See [H], Chapter 12.2 for results on the Frattini subgroup of a p-group.)

THEOREM 2.1: *With the notation above, L is $\mathbb{Q}$-adequate if and only if either $[K:\mathbb{Q}] = 2$ or K is a $\mathbb{Q}$-adequate biquadratic extension of $\mathbb{Q}$.*

Proof: First assume that L is $\mathbb{Q}$-adequate. Then a result of Schacher ([S], Theorem 4.1) implies that G is metacyclic. It follows that

$$[K:\mathbb{Q}] = [G:\Phi(G)] \leq 4.$$

(See [LSS, Proposition 2.6(1)].) By [S], Corollary 2.3, if L is $\mathbb{Q}$-adequate, then K is also $\mathbb{Q}$-adequate.

Now assume that either $[K:\mathbb{Q}] = 2$ or K is a $\mathbb{Q}$-adequate biquadratic extension of $\mathbb{Q}$. If $[K:\mathbb{Q}] = 2$, then $\mathrm{Gal}(K/\mathbb{Q})$ is cyclic, and it follows from [S], Theorem 2.8, that K is $\mathbb{Q}$-adequate. The proof is finished by using the following result proved in [LSS], Theorem 2.2 and Proposition 2.3. ∎

THEOREM 2.2: *Let L be a Galois p-extension of a number field F, and let K be the maximal elementary abelian p-extension of F inside L. Then L is F-adequate if K is F-adequate.*

Since the results in the following section describe explicitly how to determine $\mathbb{Q}$-adequacy of biquadratic extensions, these results and Theorem 2.1 allow one to determine $\mathbb{Q}$-adequacy of any finite Galois 2-extension of $\mathbb{Q}$.

3. $\mathbb{Q}$-adequacy of biquadratic extensions

The key result needed for determining adequacy of biquadratic extensions of global fields is the following, obtained from specializing [S], Propositions 2.1 and 2.5, to the biquadratic setting.

PROPOSITION 3.1: *The biquadratic extension $\mathbb{Q}(\sqrt{m},\sqrt{n})$ is $\mathbb{Q}$-adequate if and only if $[\mathbb{Q}_p(\sqrt{m},\sqrt{n}) : \mathbb{Q}_p] = 4$ for two different rational primes p.*

Note that $[\mathbb{Q}_p(\sqrt{m},\sqrt{n}) : \mathbb{Q}_p] = 4$ if and only if none of m, n, mn is a square in $\mathbb{Q}_p$. We can describe when this occurs in terms of congruence conditions mod 8 and mod p for $p \mid mn$. To aid us in this description we recall the definitions and basic results of the Legendre symbol ([IR], p. 51) and the Hilbert symbol ([Se], pp. 19–20).

If p is an odd prime and n is an integer relatively prime to p, then the Legendre symbol $(\frac{n}{p})$ is defined by

$$\left(\frac{n}{p}\right) = \begin{cases} 1 & \text{if } n \text{ is congruent to a square mod } p, \\ -1 & \text{otherwise.} \end{cases}$$

For integers m, n and a fixed prime p, the Hilbert symbol $(m,n)_p$ is defined by

$$(m,n)_p = \begin{cases} 1 & \text{if the quadratic form } \langle m,n\rangle \text{ represents 1 over } \mathbb{Q}_p, \\ -1 & \text{otherwise.} \end{cases}$$

The Hilbert symbol is bimultiplicative. Also, if $p \nmid mn$ and p is odd, we have

$$(p,m)_p = \left(\frac{m}{p}\right) \quad \text{and} \quad (m,n)_p = 1,$$

while for $p = 2$, with mn odd, we have

$$(2,m)_2 = (-1)^{(m^2-1)/8} \quad \text{and} \quad (m,n)_2 = (-1)^{((m-1)/2)\cdot((n-1)/2)}.$$

We use these properties along with the following proposition ([G], p. 71) to determine whether given integers are squares in $\mathbb{Q}_p$, and thus to determine $[\mathbb{Q}_p(\sqrt{m},\sqrt{n}) : \mathbb{Q}_p]$.

PROPOSITION 3.2:

(1) *An odd integer z is a square in $\mathbb{Q}_2$ if and only if $z \equiv 1$ (8).*

(2) *Let p be an odd prime. Then an integer z, relatively prime to p, is a square in $\mathbb{Q}_p$ if and only if $(\frac{z}{p}) = 1$.*

For p an odd prime, the square classes in $\mathbb{Q}_p$ are represented by $\{1, s, p, ps\}$ where s is a nonsquare unit. For $\mathbb{Q}_2$, the square classes are represented by $\{1, -1, 2, -2, 5, -5, 10, -10\}$. (See, e.g., [G], p. 71.)

For the remainder of this section we assume, without loss of generality, that m and n are square-free integers. For an odd prime p, if $p \nmid mn$, then m, n and mn are all units, and so at least one must be a square in $\mathbb{Q}_p$. Thus for odd primes p, if $[\mathbb{Q}_p(\sqrt{m}, \sqrt{n}) : \mathbb{Q}_p] = 4$, then $p \mid mn$. The situation is more complicated for $p = 2$ as it is possible for m, n, and mn all to be nonsquare units. Therefore, to determine whether $[\mathbb{Q}_p(\sqrt{m}, \sqrt{n}) : \mathbb{Q}_p] = 4$ for at least two primes p, we need to consider only $p = 2$ and primes p dividing mn. Observe that since m is square free, if $p \mid m$ then m is not a square in $\mathbb{Q}_p$.

We will write $m = rt$, $n = st$ where $t = \gcd(m, n)$, $t > 0$. We may also assume t is odd, for if $2 \mid m$ and $2 \mid n$, we can work with the square-free parts of m, mn instead. Then r, s, t are pairwise relatively prime square-free integers. Let $\Omega_{\mathbb{Q}} = \{\infty\} \cup \{2, 3, 5, 7, 11, \ldots\}$, the set of all places of $\mathbb{Q}$, and let

$$S = \{p \in \Omega_{\mathbb{Q}} | \ p \text{ is odd and } [\mathbb{Q}_p(\sqrt{m}, \sqrt{n}) : \mathbb{Q}_p] = 4\}.$$

Then S is a finite set, since by the remarks above, if $p \in S$ then $p \mid mn$. Proposition 3.1 can then be restated as follows.

PROPOSITION 3.3: *The biquadratic extension $\mathbb{Q}(\sqrt{m}, \sqrt{n})$ is $\mathbb{Q}$-adequate if and only if either*

(1) $[\mathbb{Q}_2(\sqrt{m}, \sqrt{n}) : \mathbb{Q}_2] = 4$ *and* $|S| \geq 1$ *or*

(2) $|S| \geq 2$.

In addition we have the following useful result.

PROPOSITION 3.4: $[\mathbb{Q}_2(\sqrt{m}, \sqrt{n}) : \mathbb{Q}_2] = 4$ *if and only if* $m \not\equiv 1$ (8), $n \not\equiv 1$ (8) *and* $mn \not\equiv 1$ (8).

Proof: This extension has degree 4 if and only if m, n and $mn = rst^2$ are all non-squares in $\mathbb{Q}_2$. Since t is odd and m, n are square-free, none of m, n, mn is divisible by 4. Thus by Proposition 3.2, an element in $\{m, n, mn\}$ is a square in $\mathbb{Q}_2$ if and only if the element is congruent to $1(8)$. ∎

Let $|r| = \prod_{i=1}^{u} r_i$, $|s| = \prod_{j=1}^{v} s_j$, and $t = \prod_{k=1}^{w} t_k$ where r_i, s_j, t_k are all distinct primes. (In case either $|r| = 1, |s| = 1$, or $t = 1$, the corresponding product is the empty product, always taken to be 1.) Observe that the only primes which lie in S are odd primes from among $\{r_i\}, \{s_j\}, \{t_k\}$. The following lemma gives the criteria for determining which of these primes are in S.

LEMMA 3.5: *Let r_i, s_j, t_k be as above, and assume r_i, s_j are odd. Then*

(1) *$r_i \in S$ if and only if $(m,n)_{r_i} = -1$,*
(2) *$s_j \in S$ if and only if $(m,n)_{s_j} = -1$, and*
(3) *$t_k \in S$ if and only if $(m,n)_{t_k}(-1,t_k)_{t_k} = -1$.*

Proof: For a prime p to be in S, we need m, n, and mn all to be non-squares in $\mathbb{Q}_p$, so with the notation given above, rt, st, and rs should all be non-squares. If r_i is odd, then $r_i \in S$ if and only if $(\frac{st}{r_i}) = -1$, which is equivalent to $(m,n)_{r_i} = -1$. Likewise if s_j is odd, then $s_j \in S$ if and only if $(\frac{rt}{s_j}) = -1$, which is equivalent to $(m,n)_{s_j} = -1$. Finally, $t_k \in S$ if and only if $(\frac{rs}{t_k}) = -1$, but $(\frac{rs}{t_k}) = (\frac{-rs}{t_k})(\frac{-1}{t_k}) = (m,n)_{t_k}(-1,t_k)_{t_k}$, since $(m,n)_{t_k} = (\frac{-rs}{t_k})$ and $(-1,t_k)_{t_k} = (\frac{-1}{t_k})$. ∎

Lemma 3.5 allows Propositions 3.3 and 3.4 to be restated as follows:

THEOREM 3.6: *The biquadratic extension $\mathbb{Q}(\sqrt{m},\sqrt{n})$ is $\mathbb{Q}$-adequate if and only if one of the following conditions holds.*

(1) *m, n, $mn \not\equiv 1(8)$ and there is an odd prime $p \mid mn$ such that either $p^2 \nmid mn$ and $(m,n)_p = -1$, or $p^2 \mid mn$ and $(m,n)_p(-1,p)_p = -1$.*
(2) *There are at least two odd primes $p \mid mn$ that satisfy either of the conditions in (1).*

Checking $\mathbb{Q}$-adequacy of biquadratic extensions thus becomes a matter of checking the values of Hilbert symbols (or Legendre symbols if one prefers) for odd prime divisors of m and n and congruence relations modulo 8. In certain cases it is possible to state the congruences that determine $\mathbb{Q}$-adequacy of biquadratic extensions solely in terms of r, s, t, thus eliminating any need to factor m and n beyond finding t through the Euclidean algorithm. This occurs when we know $[\mathbb{Q}_2(\sqrt{m},\sqrt{n}) : \mathbb{Q}_2] = 4$ and $|S|$ is odd. These conditions can be checked using Proposition 3.4 above and Lemma 3.7, given below.

LEMMA 3.7: *$|S|$ is even if and only if $(m,n)_\infty(m,n)_2(-1,t)_2 = 1$.*

Proof: Using Lemma 3.5 and Hilbert reciprocity, we have

$$\begin{aligned} 1 &= \prod_{p\in\Omega_{\mathbb{Q}}} (m,n)_p \\ &= (m,n)_\infty (m,n)_2 \prod_{r_i \text{ odd}} (m,n)_{r_i} \prod_{s_j \text{ odd}} (m,n)_{s_j} \prod_{t_k} (m,n)_{t_k} \\ &= (m,n)_\infty (m,n)_2 (-1)^{|S|} \prod_{t_k} (-1,t_k)_{t_k}. \end{aligned}$$

For each t_k, $1 = \prod_{p\in\Omega_{\mathbb{Q}}}(-1,t_k)_p = (-1,t_k)_\infty(-1,t_k)_2(-1,t_k)_{t_k}$, and $(-1,t_k)_\infty = 1$, since $t_k > 0$. Thus $(-1,t_k)_{t_k} = (-1,t_k)_2$ and so

$$\begin{aligned} 1 &= (m,n)_\infty (m,n)_2 (-1)^{|S|} \prod_{t_k} (-1,t_k)_2 \\ &= (m,n)_\infty (m,n)_2 (-1)^{|S|} (-1,t)_2. \end{aligned}$$

Thus $(-1)^{|S|} = (m,n)_\infty (m,n)_2 (-1,t)_2$, giving the stated result. ∎

COROLLARY 3.8: *The biquadratic extension $\mathbb{Q}(\sqrt{m},\sqrt{n})$ is $\mathbb{Q}$-adequate if $[\mathbb{Q}_2(\sqrt{m},\sqrt{n}) : \mathbb{Q}_2] = 4$ and $|S|$ is odd. This occurs if and only if m, n, $mn \not\equiv 1(8)$ and either at least one of m, n is positive with $(m,n)_2(-1,t)_2 = -1$, or m, n are both negative with $(m,n)_2(-1,t)_2 = 1$.*

Proof: Since $|S| \geq 1$ if $|S|$ is odd, $\mathbb{Q}$-adequacy of the given biquadratic extension follows from Proposition 3.3(1). Proposition 3.4 gives the necessary and sufficient conditions for $[\mathbb{Q}_2(\sqrt{m},\sqrt{n}) : \mathbb{Q}_2] = 4$, and so we are reduced to determining when $|S|$ is odd. By Lemma 3.7, this occurs if and only if $(m,n)_\infty(m,n)_2(-1,t)_2 = -1$. Since $(m,n)_\infty = 1$ if and only if at least one of m,n is positive, we see that $|S|$ is odd if and only if either at least one of m, n is positive with $(m,n)_2(-1,t)_2 = -1$ or m, n are both negative with $(m,n)_2(-1,t)_2 = 1$. ∎

We now consider some special situations where we can use Corollary 3.8 to verify the $\mathbb{Q}$-adequacy of the extension $\mathbb{Q}(\sqrt{m},\sqrt{n})$ solely in terms of simple congruence conditions.

COROLLARY 3.9: *Let m,n be relatively prime odd integers. Then $\mathbb{Q}(\sqrt{m},\sqrt{n})$ is $\mathbb{Q}$-adequate if either*

(1) *at least one of m,n is positive, $m \equiv n \equiv 3(4)$ and $mn \equiv 5(8)$, or*
(2) *both m and n are negative and interchanging m,n if necessary, $m \equiv 5(8)$ and $n \equiv 3(4)$.*

Proof: Apply Corollary 3.8 with $t = 1$ and recall

$$(m,n)_2 = (-1)^{((m-1)/2)\cdot((n-1)/2)}. \quad \blacksquare$$

COROLLARY 3.10: *Let $L = \mathbb{Q}(\sqrt{m},\sqrt{n})$ where $m = rt, n = 2s't$, with r, s', t pairwise relatively prime and odd, and t positive. If at least one of m, n is positive, then L is $\mathbb{Q}$-adequate if any of the following conditions hold:*

(1) $m \equiv -1(8)$, $s' \equiv 3(4)$,
(2) $m \equiv -3(8)$, $r \equiv 1(4)$, *or*
(3) $m \equiv 3(8)$, $s' \equiv 1(4)$.

If both m and n are negative, then L is $\mathbb{Q}$-adequate if any of the following conditions hold:

(1) $m \equiv -1(8)$, $s' \equiv 1(4)$,
(2) $m \equiv -3(8)$, $r \equiv 3(4)$, *or*
(3) $m \equiv 3(8)$, $s' \equiv 3(4)$.

Proof: Since $n \equiv 2(4)$, the conditions $m \equiv -1, -3$ or $3(8)$ guarantee

$$[\mathbb{Q}_2(\sqrt{m},\sqrt{n}) : \mathbb{Q}_2] = 4$$

in all cases. We apply Corollary 3.8 by first observing that

$$\begin{aligned}(m,n)_2(-1,t)_2 &= (m,2)_2(m,s')_2(m,t)_2(-1,t)_2 = (m,2)_2(m,s')_2(-rt,t)_2 \\ &= (m,2)_2(m,s')_2(r,t)_2 = (-1)^\epsilon,\end{aligned}$$

where $\epsilon = (\frac{m^2-1}{8}) + (\frac{m-1}{2})(\frac{s'-1}{2}) + (\frac{r-1}{2})(\frac{t-1}{2})$. If $m \equiv -1(8)$, then $r \equiv -t(8)$, and $\epsilon \equiv \frac{s'-1}{2}$ (2). If $m \equiv -3(8)$, then $r \equiv t(4)$, and $\epsilon \equiv 1 + (\frac{r-1}{2})(\frac{t-1}{2})$ (2), so $\epsilon \equiv 0$ (2) if $r \equiv 3(4)$ and $\epsilon \equiv 1(2)$ if $r \equiv 1(4)$. If $m \equiv 3(8)$, then $r \not\equiv t(4)$, and $\epsilon \equiv 1 + \frac{s'-1}{2}$ (2). The results then follow. $\blacksquare$

The analysis of the $\mathbb{Q}$-adequacy of the biquadratic extensions $\mathbb{Q}(\sqrt{p},\sqrt{q})$ and $\mathbb{Q}(\sqrt{-p},\sqrt{q})$ for p, q distinct primes was carried out in [S], §3. When both p and q are odd primes, however, the author neglected to consider the degree over $\mathbb{Q}_2$, leading to some inaccurate conclusions in these cases. The next corollary corrects these results of Schacher ([S], Theorem 3.2, Corollary 3.3 and Theorem 3.4 (3)).

COROLLARY 3.11: *Let p, q be distinct odd primes.*

(1) *$\mathbb{Q}(\sqrt{p},\sqrt{q})$ is $\mathbb{Q}$-adequate if and only if either $(\frac{p}{q}) = (\frac{q}{p}) = -1$ or $p \equiv q \equiv 3\,(4)$, $pq \equiv 5\ (8)$.*
(2) *$\mathbb{Q}(\sqrt{p},\sqrt{q})$ is $\mathbb{Q}$-deficient if and only if either $(\frac{p}{q}) = (\frac{q}{p}) = 1$ or $p \equiv q \equiv 3\,(4)$, $pq \equiv 1\ (8)$.*

(3) *$\mathbb{Q}(\sqrt{-p},\sqrt{q})$ is $\mathbb{Q}$-adequate if and only if either $(\frac{-p}{q}) = (\frac{q}{p}) = -1$ or $p \equiv 1\ (4), q \equiv 3\ (4), pq \equiv 3\,(8)$.*

Proof: We prove statement (3) only; statement (1) is proved similarly and (2) follows easily from (1). We have $|S| \geq 2$ if and only if $|S| = 2$, which occurs if and only if $(\frac{-p}{q}) = (\frac{q}{p}) = -1$. We have $|S| = 1$ if and only if $|S|$ is odd, which occurs if and only if $(-p,q)_2 = -1$ by Lemma 3.7. Since $(-p,q)_2 = (-1)^{\frac{-p-1}{2}\cdot\frac{q-1}{2}}$, it follows that $(-p,q)_2 = -1$ if and only if $p \equiv 1\ (4), q \equiv 3\ (4)$. Observe $[\mathbb{Q}_2(\sqrt{-p},\sqrt{q}) : \mathbb{Q}_2] = 4$ if and only if $-p, q, -pq \not\equiv 1\ (8)$. The result now follows from Proposition 3.3. ∎

The following two corollaries consider several other special cases where Theorem 3.6 can be applied to determine precisely when the given extension is $\mathbb{Q}$-adequate.

COROLLARY 3.12:

(1) *Let m be an odd integer, possibly negative. Then $\mathbb{Q}(\sqrt{m},\sqrt{2})$ is $\mathbb{Q}$-adequate if and only if m has at least one prime factor $r_i \equiv \pm 3\ (8)$. This always occurs if $m \equiv \pm 3\ (8)$.*

(2) *Let m be a positive odd integer. Then $\mathbb{Q}(\sqrt{m},\sqrt{-2})$ is $\mathbb{Q}$-adequate if and only if m has at least one prime factor r_i such that either $r_i \equiv -1\ (8)$ or $r_i \equiv -3\ (8)$. This always occurs if either $m \equiv -1\ (8)$ or $m \equiv -3\ (8)$.*

(3) *Let m be a negative odd integer. Then $\mathbb{Q}(\sqrt{m},\sqrt{-2})$ is $\mathbb{Q}$-adequate if and only if either $m \not\equiv 1\ (8)$ and m has at least one prime factor r_i with $r_i \equiv -1$ or $-3\ (8)$, or $m \equiv 1(8)$ and m has at least two prime factors congruent to -1 or $-3\ (8)$. This always occurs if $m \equiv 3(8)$.*

Proof: Apply Theorem 3.6 to the situation where $n = \pm 2$, $t = 1$. ∎

COROLLARY 3.13:

(1) *Let n be a positive odd integer. The extension $\mathbb{Q}(\sqrt{-1},\sqrt{n})$ is $\mathbb{Q}$-adequate if and only if either $n \equiv 3(8)$ or at least two prime factors of n are congruent to $3(4)$.*

(2) *Let n be a positive even integer. Then $\mathbb{Q}(\sqrt{-1},\sqrt{n})$, is $\mathbb{Q}$-adequate if and only if n has at least one prime factor $s_j \equiv 3\ (4)$. This always occurs if $n \equiv 6\ (8)$.*

Proof: Apply Theorem 3.6 to the situation where $m = -1$, $t = 1$. ∎

References

[G] F. Q. Gouvêa, *p-Adic Numbers, An Introduction*, Springer-Verlag, Berlin, 1993.

[H] M. Hall, Jr., *The Theory of Groups*, 2nd edition, Chelsea, New York, 1976.

[IR] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd edition, Graduate Texts in Mathematics Vol. 84, Springer-Verlag, New York, 1990.

[LSS] D. B. Leep, T. L. Smith and R. Solomon, *Frattini closed groups and adequate extensions of global fields*, Israel Journal of Mathematics, this volume.

[S] M. Schacher, *Subfields of division rings, I*, Journal of Algebra **9** (1968), 451–477.

[Se] J.-P. Serre, *A Course in Arithmetic*, Graduate Texts in Mathematics Vol. 7, Springer-Verlag, New York, 1973.