67. A Remark on Quaternion Extensions of the Rational p-adic Field

By Genjiro FUJISAKI
Department of Mathematics, College of Arts and Sciences,
University of Tokyo

(Communicated by Shokichi IYANAGA, M. J. A., Oct. 12, 1990)

0. Let F be a field. An extension field K of F is called a (*Galois*) *quaternion extension* of F if K/F is a Galois extension with the Galois group $Gal(K/F)$ isomorphic to the quaternion group of order 8.

If F is the rational p-adic field $\boldsymbol{Q}_p$, then there exists a Galois quaternion extension of $F=\boldsymbol{Q}_p$ if and only if $p\equiv 3 \bmod 4$ or $p=2$.

In this note, we shall exhibit all quaternion extensions of $\boldsymbol{Q}_p$ ($p\equiv 3 \bmod 4$ or $p=2$) in a fixed algebraic closure of $\boldsymbol{Q}_p$.

First, we recall some results in [3].

Lemma ([3]). *Let F be a field of characteristic $\neq 2$ and let $a_i \in F-F^2$ $(i=1,2,3)$ with $a_1a_2a_3=a^2$ for some $a\in F-F^2$. Let $M=F(\sqrt{a_1},\sqrt{a_2},\sqrt{a_3})$ be a biquadratic bicyclic extension of F. Let $\alpha\in M-M^2$. Then $K=M(\sqrt{\alpha})$ is a quaternion extension of F if and only if*

$$(*)\qquad \begin{cases} \alpha\alpha^{\sigma}=\alpha_1^2a_2 & \text{with some} \quad \alpha_1\in F(\sqrt{a_1}) \\ \alpha\alpha^{\tau}=\alpha_2^2a_3 & \text{with some} \quad \alpha_2\in F(\sqrt{a_2}) \\ \alpha\alpha^{\sigma\tau}=\alpha_3^2a_1 & \text{with some} \quad \alpha_3\in F(\sqrt{a_3}) \end{cases}$$

where $\sigma,\tau\in Gal(M/F)$ are defined by

$$\sqrt{a_1}^{\sigma}=\sqrt{a_1},\qquad \sqrt{a_2}^{\sigma}=-\sqrt{a_2},\qquad \sqrt{a_3}^{\sigma}=-\sqrt{a_3},$$
$$\sqrt{a_1}^{\tau}=-\sqrt{a_1},\qquad \sqrt{a_2}^{\tau}=\sqrt{a_2},\qquad \sqrt{a_3}^{\tau}=-\sqrt{a_3}.$$

Proof. Suppose $K=M(\sqrt{\alpha})/F$ is a quaternion extension. Then, $M(\sqrt{\alpha})=M(\sqrt{\alpha^{\sigma}})$, whence $\alpha\alpha^{\sigma}=\gamma^2$ with some $\gamma\in M$. Since $\alpha\alpha^{\sigma}=N_{M/F(\sqrt{a_1})}(\alpha)\in F(\sqrt{a_1})$, γ has a form α_1 or $\alpha_1\sqrt{a_2}$ with some $\alpha_1\in F(\sqrt{a_1})$. If $\gamma=\alpha_1\in F(\sqrt{a_1})$, then $K=M(\sqrt{\alpha})/F(\sqrt{a_1})$ is an abelian extension of type (2.2). But, since $K/F(\sqrt{a_1})$ is a cyclic extension, γ must have a form $\alpha_1\sqrt{a_2}$, i.e., $\alpha\alpha^{\sigma}=\alpha_1^2a_2$. Similarly, we have $\alpha\alpha^{\tau}=\alpha_2^2a_3$ ($\alpha_2\in F(\sqrt{a_2})$), $\alpha\alpha^{\sigma\tau}=\alpha_3^2a_1$ ($\alpha_3\in F(\sqrt{a_3})$).

Conversely, if the relations $(*)$ hold, then $K=M(\sqrt{\alpha})/F$ is a Galois extension of degree 8 and the subextensions $K/F(\sqrt{a_i})$ $(i=1,2,3)$ are all cyclic of degree 4. Since, as is well known, a finite group of order 8 which contains three cyclic subgroups of order 4, is the quaternion group, $K=M(\sqrt{\alpha})/F$ is a quaternion extension.

Proposition ([3]). *Let F be a field of characteristic $\neq 2$ and let M/F be a biquadratic bicyclic extension. Suppose that $K=F(\sqrt{\alpha})$ (for some $\alpha\in M$) is a quaternion extension of F which contains M.*

Then, $F(\sqrt{r\alpha})$ with any $r\in F^{\times}$ is a quaternion extension of F contain-

ing M. Conversely, any quaternion extension of F containing M is of the form $F(\sqrt{r\alpha})$ with some $r \in F^{\times}$.

Furthermore, $F(\sqrt{r_1\alpha})=F(\sqrt{r_2\alpha})$, $r_1, r_2 \in F^{\times}$, if and only if $r_1/r_2 \in M^2$.

Proof. If $K=F(\sqrt{\alpha})$ $(=M(\sqrt{\alpha}))$ is a quaternion extension of F, then, by lemma, $F(\sqrt{r\alpha})=M(\sqrt{r\alpha})$ is a quaternion extension of F containing M.

Conversely, let K' be any quaternion extension of F containing M. Then, $K'=M(\sqrt{\beta})$ with some $\beta \in M$ and, as is seen from the relations $(*)$, $M(\sqrt{\beta/\alpha})$ is a Galois extension of F and three extensions $M(\sqrt{\beta/\alpha})/F(\sqrt{a_i})$ $(i=1,2,3)$ are all bicyclic. Since a finite group of order 8 which contains three abelian subgroups of type $(2,2)$, is an abelian group of type $(2,2,2)$, $M(\sqrt{\beta/\alpha})/F$ is an abelian extension of type $(2,2,2)$. Hence, $M(\sqrt{\beta/\alpha})$ has the form $M(\sqrt{r})$ with some $r \in F^{\times}$, whence $M(\sqrt{\beta})=M(\sqrt{r\alpha})$.

Therefore, $K'=M(\sqrt{\beta})=M(\sqrt{r\alpha})=F(\sqrt{r\alpha})$.

Finally, as $F(\sqrt{r\alpha})=M(\sqrt{r\alpha})$ $(r \in F^{\times})$, $F(\sqrt{r_1\alpha})=F(\sqrt{r_2\alpha})$ $(r_1, r_2 \in F^{\times})$ if and only if $r_1/r_2 \in M^2$.

Now, we state the theorem of Witt [4].

Theorem (Witt). *Let F be a field of characteristic $\neq 2$ and let $M=F(\sqrt{a}, \sqrt{b})$ $(a, b \in F^{\times})$ be a biquadratic bicyclic extension of F. Then, M is embeddable into a Galois quaternion extension K of F if and only if the quadratic form $ax^2+by^2+abz^2$ is equivalent over F to $x^2+y^2+z^2$.*

When this is the case, if

$$ {}^{t}P\begin{pmatrix} a & & \\ & b & \\ & & ab \end{pmatrix} P=\begin{pmatrix} 1 & & \\ & 1 & \\ & & 1 \end{pmatrix} $$

with a matrix $P=(p_{ij})$ $(p_{ij} \in F)$, $\det P=(ab)^{-1}$, *then a field*

$$ K=F\left(\sqrt{r(1+p_{11}\sqrt{a}+p_{22}\sqrt{b}+p_{33}\sqrt{ab})}\right) $$

(with any $r \in F^{\times}$) is a quaternion extension of F containing M.

For an elementary proof of this theorem, see the paper [2].

Corollary. *If a quadratic extension $F(\sqrt{m})$ of F is embeddable into a quaternion extension of F, then m is a sum of three squares in F.*

1. Let $p \equiv 3 \pmod 4$ be a prime number. p is expressed as a sum of 3 non-zero squares in $\boldsymbol{Z}_p$ (=the ring of p-adic integers): $p=a^2+b^2+c^2$, $a, b, c \in \boldsymbol{Z}_p$, $abc \neq 0$. (For example, $19=1^2+3^2+3^2$, $23=2^2+4^2+(\sqrt{3})^2$, $\sqrt{3} \in \boldsymbol{Z}_{23}$.)

We put $m=p$, $n=a^2+b^2$, $\alpha=\sqrt{mn}(\sqrt{m}+\sqrt{n})(\sqrt{n}+a)$ (in an algebraic closure of $\boldsymbol{Q}_p$). Then $K=\boldsymbol{Q}_p(\sqrt{\alpha})$ is a quaternion extension of $\boldsymbol{Q}_p$ which contains the biquadratic field $M=\boldsymbol{Q}_p(\sqrt{p}, \sqrt{-1}, \sqrt{-p})$. (cf. [1]).

The field M is the unique biquadratic bicyclic extension of $\boldsymbol{Q}_p$ which contains all quadratic extensions of $\boldsymbol{Q}_p$.

Consequently, we see that, for any $r \in \boldsymbol{Q}_p^{\times}$, $\sqrt{r} \in \boldsymbol{Q}_p(\sqrt{r}) \subseteq M$ whence $r \in M^2$ and, in particular, $\sqrt{m}, \sqrt{n} \in M \Rightarrow \alpha \in M$.

Therefore, by the proposition in **0**, $K=\boldsymbol{Q}_p(\sqrt{\alpha})$ with α given above is the unique quaternion extension of $\boldsymbol{Q}_p$ (in a fixed algebraic closure of $\boldsymbol{Q}_p$).

2. For $p=2$, there exist exactly seven quadratic extensions of $\boldsymbol{Q}_2$:

$$\boldsymbol{Q}_2(\sqrt{-1}),\quad \boldsymbol{Q}_2(\sqrt{\pm 2}),\quad \boldsymbol{Q}_2(\sqrt{\pm 5}),\quad \boldsymbol{Q}_2(\sqrt{\pm 10}).$$

Since -1 cannot be expressed as a sum of 3 squares in $\boldsymbol{Q}_2$, $\boldsymbol{Q}_2(\sqrt{-1})$ is not embeddable into any quaternion extension of $\boldsymbol{Q}_2$. All biquadratic bicyclic extensions of $\boldsymbol{Q}_2$ which do not contain $\boldsymbol{Q}_2(\sqrt{-1})$ are $\boldsymbol{Q}_2(\sqrt{2}, \sqrt{5})$, $\boldsymbol{Q}_2(\sqrt{2}, \sqrt{-5})$, $\boldsymbol{Q}_2(\sqrt{5}, \sqrt{-2})$, $\boldsymbol{Q}_2(\sqrt{10}, \sqrt{-2})$. Among these fields, by Witt's theorem, exactly three fields $M_1=\boldsymbol{Q}_2(\sqrt{2}, \sqrt{-5})$, $M_2=\boldsymbol{Q}_2(\sqrt{5}, \sqrt{-2})$, $M_3=\boldsymbol{Q}_2(\sqrt{10}, \sqrt{-2})$ are embeddable into quaternion extensions of $\boldsymbol{Q}_2$. (cf. [2]). In fact, the following six fields

$$\boldsymbol{Q}_2\left(\sqrt{\pm\sqrt{6}(\sqrt{3}+\sqrt{2})(\sqrt{2}+1)}\right) \supseteq M_1=\boldsymbol{Q}_2(\sqrt{2}, \sqrt{-5})=\boldsymbol{Q}_2(\sqrt{2}, \sqrt{3}),$$

$$\boldsymbol{Q}_2\left(\sqrt{\pm\sqrt{30}(\sqrt{6}+\sqrt{5})(\sqrt{5}+1)}\right) \supseteq M_2=\boldsymbol{Q}_2(\sqrt{5}, \sqrt{-2})=\boldsymbol{Q}_2(\sqrt{5}, \sqrt{6}),$$

$$\boldsymbol{Q}_2\left(\sqrt{\pm\sqrt{110}(\sqrt{11}+\sqrt{10})(\sqrt{10}+1)}\right) \supseteq M_3=\boldsymbol{Q}_2(\sqrt{10}, \sqrt{-2})=\boldsymbol{Q}_2(\sqrt{10}, \sqrt{11})$$

are the quaternion extensions of $\boldsymbol{Q}_2$. (cf. Th. in [1]).

If we denote by M any one of three fields M_1, M_2 and M_3, we see that $\sqrt{-1}\notin M$ and, for any $r\in \boldsymbol{Q}_2^{\times}$, either $\sqrt{r}\in M$ or $\sqrt{-r}\in M$.

Therefore, by the proposition in **0**, the six fields given above are exactly all quaternion extensions of $\boldsymbol{Q}_2$ (in a fixed algebraic closure of $\boldsymbol{Q}_2$).

References

[1] G. Fujisaki: An elementary construction of Galois quaternion extension. Proc. Japan Acad., **66**A, 80–83 (1990).

[2] C. Jensen and N. Yui: Quaternion Extensions. Algebraic Geometry and Commutative Algebra. vol. 1, Kinokuniya, pp. 155–182 (1988).

[3] H. Reichardt: Über Normalköper mit Quaternionengruppe. Math. Zeitschrift, **41**, 218–221 (1936).

[4] E. Witt: Konstruktion von galoisschen Köpern der Charakteristik p zu vorgegebener Gruppe der Ordnung p^f. J. Reine Angew. Math., **174**, 237–245 (1936).