23. *An Elementary Construction of Galois Quaternion Extension*

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

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

1. Let F be a field and let $\tilde{F}$ be a (fixed) algebraic closure of F. An extension field K of F $(F \subseteq K \subseteq \tilde{F})$ will be said to be a *Galois quaternion extension* of F if K/F is a Galois extension and its Galois group $Gal(K/F)$ is isomorphic to the quaternion group of order 8.

Theorem. *Let F be a field of the characteristic $\neq 2$ and let $F(\sqrt{m})$ $(m \notin F^2 = \{x^2 \mid x \in F\})$ be a quadratic extension of F.*

Suppose,

(i) *m is a sum of 3 non-zero squares in F: $m = p^2 + q^2 + r^2$, $p, q, r \in F$, $pqr \neq 0$,*

(ii) $n = p^2 + q^2 \notin F^2$,

(iii) $mn \notin F^2$.

Let

$$\omega = \sqrt{\sqrt{mn}\,(\sqrt{m}+\sqrt{n})(\sqrt{n}+p)} \in \tilde{F}$$

where we choose $\sqrt{mn} = \sqrt{m}\sqrt{n}$.

Then $K = F(\omega)$ is a Galois quaternion extension of F.

Proof. Let $M = F(\sqrt{m}, \sqrt{n})$ be a bicyclic biquadratic extension of F and let $Gal(M/F) = \{\sigma_0 = 1_M, \sigma_1, \sigma_2, \sigma_3\}$ where $\sigma_0 = 1_M$ (the identity),

σ_1: $(\sqrt{m}, \sqrt{n}) \longrightarrow (-\sqrt{m}, \sqrt{n})$,

σ_2: $(\sqrt{m}, \sqrt{n}) \longrightarrow (\sqrt{m}, -\sqrt{n})$,

σ_3: $(\sqrt{m}, \sqrt{n}) \longrightarrow (-\sqrt{m}, -\sqrt{n})$.

Let $K = M(\omega)$ $(\omega^2 \in M)$ and let $\alpha_i : K \to \tilde{F}$ $(i = 0, 1, 2, 3)$ denote any (but fixed once for all) embeddings of K into $\tilde{F}$ which extend σ_i $(i = 0, 1, 2, 3)$ respectively.

Now, calculating

$$(\omega^{\alpha_i})^2 = (\sqrt{mn}\,(\sqrt{m}+\sqrt{n})(\sqrt{n}+p))^{\sigma_i} \qquad \doteq 0, 1, 2, 3)$$

we have

$$\omega^{\alpha_0} = \omega e_0, \qquad \omega^{\alpha_1} = \omega \frac{\sqrt{m}-\sqrt{n}}{r} e_1,$$

$$\omega^{\alpha_2} = \omega \frac{\sqrt{m}-\sqrt{n}}{r} \frac{\sqrt{n}-p}{q} e_2, \qquad \omega^{\alpha_3} = \omega \frac{\sqrt{n}-p}{q} e_3$$

where $e_i = \pm 1$ $(i = 0, 1, 2, 3)$ are the signs depending on α_i $(i = 0, 1, 2, 3)$ respectively. Since, as seen from the above calculations, ω^{α_i} $(i = 0, 1, 2, 3)$ are all in K for any extension $\alpha_i : K \to \tilde{F}$ of σ_i $(i = 0, 1, 2, 3)$, it follows that $K = M(\omega)$ is a Galois extension of F and α_i $(i = 0, 1, 2, 3)$ are automorphisms of K

over F. Then, simple calculations show that

$$\alpha_i^2|M \ (=\text{the restriction of } \alpha_i^2 \text{ on } M)=\sigma_i^2=1_M$$

and

$$\omega^{\alpha_i^2}=-\omega \qquad (i=0,1,2,3)$$

from which it follows that $\omega \notin M$, $[K:F]=8$. Hence, $K=M(\omega)$ is a Galois extension of F with degree $[K:F]=8$.

Now, it is easily verified that

$$\alpha_0^2=1_K, \quad \alpha_i^2 \neq 1_K, \quad \alpha_i^3 \neq \alpha_i, \quad \alpha_i^3|M=\sigma_i \quad (i=1,2,3).$$

Let $\varepsilon=\alpha_0$ be defined by $\omega^\varepsilon=-\omega$. Then, as seen from the above,

$$1_K, \quad \varepsilon, \quad \alpha_1, \quad \alpha_1^3, \quad \alpha_2, \quad \alpha_2^3, \quad \alpha_3, \quad \alpha_3^3$$

are different automorphisms of K over F, whence

$$Gal(K/F)=\{1_K, \varepsilon, \alpha_1, \alpha_1^3, \alpha_2, \alpha_2^3, \alpha_3, \alpha_3^3\}.$$

Replacing α_i by α_i^3, if necessary, we may suppose all $e_i=1$ $(i=1,2,3)$. Then, it follows by calculations that

$$\alpha_i^4=1_K \quad (\alpha_i^2 \neq 1_K) \quad (i=1,2,3)$$

$$\alpha_i^2=\varepsilon \qquad (i=1,2,3)$$

$$\alpha_1\alpha_2=\alpha_3, \quad \alpha_2\alpha_3=\alpha_1, \quad \alpha_3\alpha_1=\alpha_2$$

($\alpha_1\alpha_2$ is defined by $(x)^{\alpha_1\alpha_2}=(x^{\alpha_1})^{\alpha_2}$ for $x \in K$)

$$\alpha_2^{-1}\alpha_1\alpha_2=\alpha_1^3=\alpha_1^{-1}.$$

These relations show that the Galois group $Gal(K/F)$ is isomorphic to the quaternion group of order 8.

Finally, since we can verify $\omega^\alpha \neq \omega^\beta$ for any $\alpha, \beta \in Gal(K/F)$, $\alpha \neq \beta$, it follows that $K=F(\omega)$.

2. Let $\boldsymbol{Q}$ and $\boldsymbol{Z}$ denote the rational number field and the ring of rational integers respectively. Let $m \in \boldsymbol{Z}$ be a squarefree integer. It is known that if there exists a Galois quaternion extension K of $\boldsymbol{Q}$ such that $\boldsymbol{Q} \subseteq \boldsymbol{Q}(\sqrt{m}) \subseteq K$, then m is a sum of 3 squares in $\boldsymbol{Q}$ (hence, $\boldsymbol{Q}(\sqrt{m})$ is a real quadratic field).

Let $m>0$ be a squarefree positive integer. By a famous theorem of Gauss ([2], [4]), m is a sum of (at most) 3 squares in $\boldsymbol{Z}$ if and only if $m \equiv 1$, 2, 3, 5, 6 mod. 8 and it is also known that m is a sum of 2 squares in $\boldsymbol{Z}$ if and only if m is not divisible by any prime number $p \equiv 3$ mod. 4.

Moreover, m is a sum of 3 squares in $\boldsymbol{Z}$ (or 2 squares in $\boldsymbol{Z}$) if and only if m is a sum of 3 squares in $\boldsymbol{Q}$ (or 2 squares in $\boldsymbol{Q}$). (cf. [4], chap. IV, Appendix).

Let $\boldsymbol{Q}(\sqrt{m})$ be a real quadratic field where m is squarefree and $m \not\equiv 4$, 7 mod. 8.

Case i). Suppose that

$$m=p^2+q^2+r^2, \quad p, q, r>0 \qquad \text{in } \boldsymbol{Z}$$

and m is not a sum of 2 squares in $\boldsymbol{Z}$. If we set $n=p^2+q^2$, then n is not a square and mn is not either. In fact, if $mn=l^2$, then $m=(mp/l)^2+(mq/l)^2 \in \boldsymbol{Q}^2+\boldsymbol{Q}^2 \Rightarrow m \in \boldsymbol{Z}^2+\boldsymbol{Z}^2$, a contradiction.

Case ii). Suppose that

$$m=p^2+q^2, \quad p, q>0 \qquad \text{in } \boldsymbol{Z}.$$

If we set $n=m+1=p^2+q^2+1$, then $n \equiv 2$, 3 mod. 4, from which n is not a square. Moreover, mn is not a square. For, if mn is a square then there exists a prime number t such that $t|m$, $t^2|mn$. Since m is squarefree, t must divide n. But, this implies $t|(m,n)=1$, a contradiction.

We set

$$\omega=\sqrt{\sqrt{mn}(\sqrt{m}+\sqrt{n})(\sqrt{n}+p)} \quad \text{in the } Case \text{ i)},$$
$$\omega=\sqrt{\sqrt{mn}(\sqrt{m}+\sqrt{n})(\sqrt{m}+p)} \quad \text{in the } Case \text{ ii)}.$$

Then, it follows from the theorem in **1** that

$$K=\boldsymbol{Q}(\omega)(\supseteq \boldsymbol{Q}(\sqrt{m},\sqrt{n})\supseteq \boldsymbol{Q}(\sqrt{m}))$$

is a Galois quaternion extension of $\boldsymbol{Q}$.

Examples. i) $m=3=1^2+1^2+1^2$, $n=1^2+1^2=2$, $mn=6$.

$$K=\boldsymbol{Q}\left(\sqrt{\sqrt{6}(\sqrt{3}+\sqrt{2})(\sqrt{2}+1)}\right).$$

ii) $m=5=1^2+2^2$, $n=m+1=6$, $mn=30$.

$$K=\boldsymbol{Q}\left(\sqrt{\sqrt{30}(\sqrt{5}+\sqrt{6})(\sqrt{5}+1)}\right).$$

iii) $m=10=1^2+3^2$, $n=m+1=11$, $mn=110$.

$$K=\boldsymbol{Q}\left(\sqrt{\sqrt{110}(\sqrt{10}+\sqrt{11})(\sqrt{10}+1)}\right).$$

3. Let $p>2$ be a prime number. Let $\boldsymbol{Q}_p$ and $\boldsymbol{Z}_p$ denote the p-adic number field and the ring of p-adic integers. As is well known, there exist exactly 3 quadratic extensions of $\boldsymbol{Q}_p$ (in a fixed algebraic closure of $\boldsymbol{Q}_p$)

$$\boldsymbol{Q}_p(\sqrt{p}),\quad \boldsymbol{Q}_p(\sqrt{u}),\quad \boldsymbol{Q}_p(\sqrt{pu})$$

where u is a p-adic unit such that $(u/p)=-1$.

From the theorem of Witt ([5]), there exists a Galois quaternion extension of $\boldsymbol{Q}_p$ if and only if $p\equiv 3$ mod. 4.

For $p\equiv 3$ mod. 4, p is a sum of 3 squares, but it is not a sum of 2 squares in $\boldsymbol{Q}_p$.

Now, for any $\alpha\in \boldsymbol{Z}_p$ $(p>2)$, α is a sum of 3 squares (or 2 squares) in $\boldsymbol{Q}_p$ if and only if α is a sum of 3 squares (or 2 squares) in $\boldsymbol{Z}_p$ ([3], Th. 34). Hence, for $p\equiv 3$ mod. 4, p is a sum of 3 squares in $\boldsymbol{Z}_p$, but it is not a sum of 2 squares in $\boldsymbol{Z}_p$.

Assume $p\equiv 3$ mod. 4 and set $m=p=a^2+b^2+c^2$, $a, b, c\in \boldsymbol{Z}_p$. Then, from the facts mentioned above, $abc\neq 0$, $n=a^2+b^2\notin \boldsymbol{Q}_p^2$. Moreover, since $(-1/p)=-1$, it follows that $a^2+b^2\not\equiv 0$ mod. p, i.e., a^2+b^2 is a p-adic unit, from which $mn=p(a^2+b^2)\notin \boldsymbol{Q}_p^2$. Hence, it follows from theorem in **1** that

$$K=\boldsymbol{Q}_p\left(\sqrt{\sqrt{mn}(\sqrt{m}+\sqrt{n})(\sqrt{n}+a)}\right) \qquad (p\equiv 3 \text{ mod. } 4)$$
$$(m=p=a^2+b^2+c^2,\ n=a^2+b^2 \text{ in } \boldsymbol{Z}_p)$$

is a Galois quaternion extension of $\boldsymbol{Q}_p$.

Since a Galois quaternion extension contains exactly 3 quadratic subextensions and $\boldsymbol{Q}_p(\sqrt{p})$, $\boldsymbol{Q}_p(\sqrt{-1})$, $\boldsymbol{Q}_p(\sqrt{-p})$ are all quadratic extensions of $\boldsymbol{Q}_p$ (we may take $u=-1$ for $p\equiv 3$ mod. 4), K contains these 3 quadratic extensions of $\boldsymbol{Q}_p$.

Examples. i) $m=p=3=1^2+1^2+1^2$, $n=1^2+1^2=2$, $mn=6$.

$$K=\boldsymbol{Q}_3\left(\sqrt{\sqrt{6}(\sqrt{3}+\sqrt{2})(\sqrt{2}+1)}\right).$$

ii) $m=p=7=1^2+2^2+(\sqrt{2})^2$ $(\sqrt{2} \in Z_7)$, $n=1^2+2^2=5$, $mn=35$.

$$K=Q_7\left(\sqrt{\sqrt{35}(\sqrt{7}+\sqrt{5})(\sqrt{5}+1)}\right).$$

iii) $m=p=11=1^2+1^2+3^2$, $n=1^2+1^2=2$, $mn=22$.

$$K=Q_{11}\left(\sqrt{\sqrt{22}(\sqrt{11}+\sqrt{2})(\sqrt{2}+1)}\right).$$

References

[1] R. Dedekind: Konstruktion von Quaternionkörpern. Ges. Werke 2, Braunschweig (1931).

[2] K. Ireland and M. Rosen: A Classical Introduction to Modern Number Theory. Springer-Verlag, New York (1982).

[3] B. Jones: The Arithmetic Theory of Quadratic Forms. John Wiley and Sons (1961).

[4] J. P. Serre: A Course in Arithmetics. Springer-Verlag, New York (1973).

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