ON AN EXCEPTIONAL PHENOMENON IN CERTAIN QUADRATIC EXTENSIONS

H. B. MANN

Let Ω be a cyclic extension of degree l over the field Σ. Correcting an error which for some time had been haunting the literature, Hasse (**1**, p. 272) noted that for $l = 2$, the field Ω may contain a unit ξ such that

$$\xi^{l^\beta} \in \Sigma,\ \xi^{l^{\beta-1}} \notin \Sigma,\ \beta > 1.$$

Hasse also gave the example $\Sigma = \Re(\sqrt{-2})$, $\Omega = \Sigma(\sqrt{-1})$, where $\Re$ is the rational field and $\Omega \ni \sqrt[4]{-1}$. In this note, we shall give necessary and sufficient conditions under which this exceptional case arises.

THEOREM 1. *Let Ω be any field separable and cyclic of degree l (a prime) over a field Σ. There exists an element $\omega \in \Omega$ such that $\omega^{l^\beta} \in \Sigma$, $\omega^{l^{\beta-1}} \notin \Sigma$, $\beta \geqslant 2$, if and only if*

$$\text{(i)}\quad l = 2,$$

$$\text{(ii)}\quad \Omega = \Sigma(\sqrt{-1}),$$

$$\text{(iii)}\quad \Sigma \ni \theta + \theta^{-1},$$

where θ is a primitive 2^βth root of unity. Moreover

(iv) *Ω contains the 2^βth roots of unity,*

(v) $\omega = \alpha(1 + \theta), \quad \alpha \in \Sigma.$

Proof. Since Ω is cyclic, hence normal, over Σ and since

$$\Omega = \Sigma(\sqrt[l]{\omega^{l^\beta}}),$$

it is clear that the lth roots of unity must be in Σ. If l is odd, then

$$\omega^{l^\beta} = N(\omega^{l^{\beta-1}}) = N(\omega^{l^{\beta-2}})^l,$$

hence

$$\omega^{l^{\beta-1}} \in \Sigma$$

contrary to hypothesis. (N denotes the relative norm in Ω over Σ.) Hence $l = 2$. We then have

$$-\omega^{2^\beta} = N(\omega^{2^{\beta-1}}) = N(\omega^{2^{\beta-2}})^2$$

which shows that $\sqrt{-1} \notin \Sigma$ and $\Omega = \Sigma(\sqrt{-1})$. Furthermore, we must have $\omega^S = \theta\omega$, where S is the generating automorphism of Ω over Σ and θ a 2^βth

Received November 25, 1953; in revised form February 19, 1954. This research was supported by the United States Air Force through the Office of Scientific Research.

root of unity. Moreover, θ cannot be a $2^{\beta-1}$th root of unity, otherwise we should have

$$(\omega^{2^{\beta-1}})^S = \omega^{2^{\beta-1}} \in \Sigma.$$

The equation $\omega^S = \theta\omega$ shows $N(\theta) = 1$. Hence $\theta^S = \theta^{-1}$, so that $\theta + \theta^{-1} \in \Sigma$ and $(1 + \theta^{-1})^S = \theta(1 + \theta^{-1})$. This gives

$$\left(\frac{\omega}{1+\theta^{-1}}\right)^S = \frac{\omega}{1+\theta^{-1}},$$

and shows that

$$\omega = \alpha(1 + \theta^{-1}), \quad \alpha \in \Sigma.$$

On the other hand, let the conditions (i), (ii), and (iii) be satisfied. Since $\theta^2 - \theta(\theta + \theta^{-1}) + 1 = 0$ and since $\Sigma(\theta) \ni \sqrt{-1}$, it follows that $\Omega \ni \theta$ and $\theta^S = \theta^{-1}$. Therefore

$$((1+\theta)^{2^{\beta-1}})^S = -(1+\theta)^{2^{\beta-1}} \notin \Sigma,$$
$$((1+\theta)^{2^{\beta}})^S = (1+\theta)^{2^{\beta}} \in \Sigma.$$

This completes the proof of Theorem 1.

The condition (v) shows that β is bounded if Ω is a finite extension of $\mathfrak{R}$. We thus have

COROLLARY 1.1. *If Ω is a finite extension of the rationals, then β is bounded. If β is the largest value such that there exists a number ω in Ω for which $\omega^{2^\beta} \in \Sigma$, $\omega^{2^{\beta-1}} \notin \Sigma$, then $\omega \neq \alpha\omega_1{}^{1-S}$, $\alpha \in \Sigma$, $\omega_1 \in \Omega$.*

Otherwise $\omega = \alpha\omega_1{}^{1-S} = \alpha\omega_1{}^{1+S}\,\omega_1{}^{-2S} = \alpha^*\,\omega_1{}^{*2}$. But this shows $\omega_1{}^{*2^\beta} \notin \Sigma$, $\omega_1{}^{*2^{\beta+1}} \in \Sigma$ contrary to the significance of β.

The same argument also shows

COROLLARY 1.2. *If under the conditions of corollary 1, β is the largest value such that there is a unit $H \in \Omega$ for which $H^{2^\beta} \in \Sigma$, $H^{2^{\beta-1}} \notin \Sigma$, then H is not of the form $H_1{}^{1-S}\,\epsilon$, where H_1 is a unit of Ω, ϵ a unit of Σ.*

THEOREM 2. *The number ω in Theorem 1 can (under the conditions of Corollary 1) be chosen as a unit if and only if the ideal (2) is, in Σ, the $2^{\beta-1}$th power of a principal ideal (α).*

Proof. We have

$$(2) = (1+\theta)^{2^{\beta-1}}.$$

If $(2) = (\alpha^{2^{\beta-1}})$, then $(1+\theta)/\alpha = \omega$ is a unit. On the other hand, if ω is a unit, then by Theorem 1.

$$\omega = \alpha(1+\theta), \quad \alpha \in \Sigma.$$

Hence

$$(\alpha^{-1}) = (1+\theta), \ (2) = (\alpha^{-1})^{2^{\beta-1}}.$$

If β is chosen maximal, then the $2^{\beta+1}$th roots of unity are in Ω if and only if $\Sigma \ni \theta_1 - \theta_1{}^{-1}$, where θ_1 is a primitive $2^{\beta+1}$th root of unity. In this case, it is trivial that ω can be chosen as a unit. A less trivial example is $\Sigma = \Re(\sqrt{7})$, $\Omega = \Re(\sqrt{7}, i)$, where the unit

$$H = \frac{1 + i}{3 + \sqrt{7}}$$

has the property $H^2 \notin \Sigma$, $H^4 \in \Sigma$.

Reference

1. H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, Jahresbericht der Deutschen Mathematiker Vereinigung, *36* (1927), 233–311.

Ohio State University

https://doi.org/10.4153/CJM-1954-050-4 Published online by Cambridge University Press