Norske Vid. Selsk. Skr. 2 (1994), 3-8.

A short proof of the formula for the conductor of an abelian cubic field

James G. Huard, Blair K. Spearman and Kenneth S. Williams*

Abstract: *Let Q denote the field of rational numbers and let K be an abelian cubic extension of Q, that is $[K:Q] = 3$ and $Gal(K/Q) \cong Z/3Z$. An explicit formula for the conductor $f(K)$ of K is given in terms of integers A and B, where $K = Q(\theta)$, $\theta^3 + A\theta + B = 0$.*

Let Q denote the field of rational numbers. The smallest field containing both Q and a complex number θ is called the field generated by θ, and is denoted by $Q(\theta)$. If θ is a root of unity, $Q(\theta)$ is called a cyclotomic field. Subfields of cyclotomic fields are called abelian fields. The smallest positive integer f for which a given abelian field K is contained in the cyclotomic field generated by an f-th root of unity is called the conductor of K, and is denoted by $f(K)$. It is known that $f(K)$ is a product of powers of those primes which ramify in K. In the case of an abelian field K of degree 3, Hasse [1] has shown that if $p_1, \ldots, p_n$ are the primes other than 3 which ramify in K then

$$(0) \qquad f(K) = \begin{cases} p_1 \cdots p_n, & \text{if 3 does not ramify in } K, \\ 9p_1 \cdots p_n, & \text{if 3 ramifies in } K. \end{cases}$$

Such a field K can be expressed in the form $K = Q(\theta)$, where θ is a root of an irreducible cubic polynomial $X^3 + AX + B$ with integral coefficients for which the discriminant

$$(1) \qquad -4A^3 - 27B^2 = C^2$$

for some positive integer C. With this representation of K, one can ask for an explicit formula for $f(K)$ in terms of A and B. This is the question we address.

* *Research supported by Natural Sciences and Engineering Research Council of Canada Grant A-7233*

If R is an integer with $R^2 | A$ and $R^3 | B$, then $K = Q(\theta / R)$, so we may assume that

(2) $$R^2 | A, R^3 | B \Rightarrow |R| = 1.$$

From (1) and (2) we deduce that exactly one of the following possibilities occurs:

(3) $$3 \nmid A (\Rightarrow 3 \nmid C) \text{ or } 3 \| A,\ 3 \nmid B (\Rightarrow 3^2 | C) \text{ or } 3^2 \| A,\ 3^2 \| B (\Rightarrow 3^3 \| C).$$

We split the possibilities in (3) into two cases as follows:

(4) $$\begin{cases} \text{case 1:} & 3 \nmid A \quad \text{or} \quad 3 \| A,\ 3 \nmid B,\ 3^3 | C, \\ \text{case 2:} & 3^2 \| A,\ 3^2 \| B \quad \text{or} \quad 3 \| A,\ 3 \nmid B,\ 3^2 \| C, \end{cases}$$

and set

(5) $$\alpha = \begin{cases} 0, & \text{in case 1,} \\ 2, & \text{in case 2.} \end{cases}$$

Using only the basic properties for cubic Gauss sums, and without appealing to Hasse's formula (0), we give a short proof of the following formula for $f(K)$.

Theorem

(6) $$f(K) = 3^{\alpha} \prod_{\substack{p\,(\text{prime}) \equiv 1 \pmod 3 \\ p | A,\, p | B}} p$$

Proof

Let π be a primary Eisenstein prime whose norm is a rational prime $p \equiv 1 \pmod 3$. Let ω denote a complex cube root of unity and let x be an integer not divisible by p. The cubic residue character $\left[\frac{x}{\pi}\right]_3$ is defined by $\left[\frac{x}{\pi}\right]_3 = \omega^k$, where $x^{(p-1)/3} \equiv \omega^k \pmod{\pi}$, $k = 0, 1, 2$, and the cubic Gauss sum $G(\pi)$ by

$$(7) \qquad G(\pi) = \sum_{x=1}^{p-1} \left[\frac{x}{\pi}\right]_3 e^{2\pi i x/p} \in Q\,(e^{2\pi i/3p}).$$

The basic properties of $G(\pi)$ are $G(\pi)\overline{G(\pi)} = p$, $\overline{G(\pi)} = G(\overline{\pi})$, $G(\pi)^3 = p\pi$. Let λ be the Eisenstein integer $\lambda = (-27B + 3C\sqrt{-3})/2$ of norm $N(\lambda) = (-3A)^3$. Clearly $(\sqrt{-3})^c \,\|\, \lambda$, where $3^c \,\|\, N(\lambda)$. Let τ be the product of primary Eisenstein primes such that $\frac{\lambda/(\sqrt{-3})^c}{\tau^3}$ is cubefree. Let F_1 be the largest positive integer dividing $\lambda/((\sqrt{-3})^c\tau^3)$. Let ρ be the product of primary Eisenstein primes such that $\lambda/((\sqrt{-3})^c\tau^3F_1\rho)$ is a unit, say,

$$(8) \qquad \frac{\lambda}{(\sqrt{-3})^c\tau^3F_1\rho} = (-1)^a\omega^b, \quad \text{where} \quad a = 0, 1; \quad b = 0, 1, 2.$$

Simple arithmetical arguments show that

$$(9) \qquad b = \begin{cases} 0, & \text{in case } 1, \\ 1 \text{ or } 2, & \text{in case } 2, \end{cases}$$

and

$$(10) \qquad N(\rho) = F_1 = \prod_{\substack{p\,(\text{prime}) \equiv 1 \pmod 3 \\ p|A,\, p|B}} p$$

Let $\rho = \pi_1 \ldots \pi_k$ be the factorization of ρ into primary Eisenstein primes and set

(11) $$H = (-1)^{a+1} e^{2\pi i b/9} (\sqrt{-3})^{(c/3)-2} \tau G(\pi_1) \ldots G(\pi_k).$$

We note from (7) and (10) that $G(\pi_1) \ldots G(\pi_k) \in Q(e^{2\pi i/3F_1})$. Using (8), (10) and (11) it is easy to check that $H^3 = \lambda/27$ so that $H^3 + \bar{H}^3 = -B$, $H\bar{H} = -A/3$. Thus the three roots of the equation $x^3 + Ax + B = 0$ are

(12) $$\theta = H + \bar{H}, \quad \theta' = \omega H + \omega^2 \bar{H}, \quad \theta'' = \omega^2 H + \omega \bar{H},$$

and so $K = Q(\theta) = Q(\theta') = Q(\theta'')$. A little checking using (7) and (11) shows that $\theta \in Q(e^{2\pi i/3^{\alpha}F_1})$, so that $K \subseteq Q(e^{2\pi i/3^{\alpha}F_1})$, and thus

(13) $$f(K) \leq 3^{\alpha} F_1.$$

For any prime p dividing F_1, we have

$$\begin{cases} pO_K = \langle p, \ \theta \rangle^3, & \text{if } p \| B, \\ pO_K = \langle p, \ \theta^2/p \rangle^3, & \text{if } p^2 | B, \ (\text{so that } p^2 | A, \ p^2 \| B), \end{cases}$$

so that p ramifies in K and thus in $Q(e^{2\pi i/f(K)})$, proving $p \mid f(K)$. Hence

(14) $$F_1 \mid f(K).$$

From (13) and (14) we deduce $f(K) = F_1$ in case 1.

In case 2 another simple calculation shows that

$$\begin{cases} 3O_K = \langle 3, \ \theta^2 + (A/3) \rangle^3, & \text{if } 3 \| A, \ 3 \nmid B, \ 3^2 \| C, \\ 3O_K = \langle 3, \ (\theta^2 + A)/3 \rangle^3, & \text{if } 3^2 \| A, \ 3^2 \| B, \ 3^3 \| C, \end{cases}$$

so that 3 ramifies in K and thus in $Q(e^{2\pi i/f(K)})$. Hence $3 \mid f(K)$. From (11) and (12) we deduce

$$e^{2\pi i b/9} = \frac{(\omega^2\theta - \theta')}{(\omega^2 - \omega)(-1)^{a+1} \tau G(\pi_1) \ldots G(\pi_k) (\sqrt{-3})^{(c/3)-2}} \in Q(e^{2\pi i/f(K)}),$$

so that, as $b = 1$ or 2 by (9), we have $Q(e^{2\pi i/9}) \subseteq Q(e^{2\pi i/f(K)})$, and thus $9 \mid f(K)$. Appealing to (14) we deduce that $9F_1 \mid f(K)$ in case 2, and so, by (13), $f(K) = 9F_1$ in case 2. ■

The only primes $p(\neq 3)$ which ramify in K are those primes $p \equiv 1 \pmod 3$ such that $p \mid A$ and $p \mid B$. Moreover, 3 does not ramify in case 1 but does ramify in case 2. This establishes Hasse's formula (0) for $f(K)$.

References

1. H. Hasse, Arithmetische Theorie der kubischen Zahlkörper auf klassenkörpertheoretischer Grundlage, math. Z. 30 (1930), 565-582.

James G. Huard
Department of Mathematics
Canisius College
Buffalo, NY 14208
USA

Blair K. Spearman
Department of Mathematics
Okanagan University College
Kelowna, B.C. V1Y 4X8
Canada

Kenneth S. Williams
Department of Mathematics and Statistics
Carleton University
Ottawa, Ontario K1S 5B6
Canada