KYUNGPOOK Math. J. 36(1996), 117-124

The Intersection of Two Cyclotomic Extensions of a Quadratic Field

Blair K. Spearman
Department of Mathematics, Okanagan University College, Kelowna, British Columbi Canada V1V 1V7

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

(1991 AMS Classification number : 11R11, 11R18)

Let m and n be positive integers and let (m,n) denote their greatest common divisor. A necessary and sufficient condition is given for the equality

$$K(e^{2\pi i/m}) \cap K(e^{2\pi i/n}) = K\big(e^{2\pi i/(m,n)}\big)$$

to hold in the case of a quadratic field K.

Let K be an algebraic number field of finite degree over the rational field Q. Let m and n be positive integers. We write (m,n) for $GCD(m,n)$, and $[m,n]$ for $LCM(m,n)$, so that $(m,n)[m,n] = mn$. We are interested in knowing for which fields K the equality

$$K(e^{2\pi i/m}) \cap K(e^{2\pi i/n}) = K\big(e^{2\pi i/(m,n)}\big) \tag{1}$$

holds. If $m \equiv 2 \pmod 4$, say $m = 2\ell\,(\ell$ odd), then, as

$$e^{2\pi i/\ell} = (e^{2\pi i/m})^2, \quad e^{2\pi i/m} = -\big(e^{2\pi i/\ell}\big)^{(\ell+1)/2}$$

we see that $K(e^{2\pi i/m}) = K\big(e^{2\pi i/\ell}\big)$. Thus we can suppose throughout that $m \not\equiv 2 \pmod 4$ and $n \not\equiv 2 \pmod 4$. If $K = Q$ it is known that (1) holds, see for example [2, Theorem 4.10 (v)] or [4].

Recalling that

$$Q(e^{2\pi i/m}) \subseteq Q(e^{2\pi i/n}) \Leftrightarrow m|n \tag{2}$$

and

$$Q\big(e^{2\pi i/m}, e^{2\pi i/n}\big) = Q\big(e^{2\pi i/[m,n]}\big), \tag{3}$$

(Received : 11 November 1994)
Research supported by Natural Sciences and Engineering Research Council of Canada Grant A-7233.

it is easy to give other examples of fields K for which (1) holds. For example if $e^{2\pi i/m} \in K$ then $e^{2\pi i/(m,n)} \in K$ and so

$$K(e^{2\pi i/m}) \cap K(e^{2\pi i/n}) = K \cap K(e^{2\pi i/n}) = K = K\left(e^{2\pi i/(m,n)}\right),$$

showing that (1) holds in this case. As a second example, we take $K = Q(e^{2\pi i/r})$, where r is a positive integer $\not\equiv 2 \pmod 4$. Then we have

$$\begin{aligned} & K(e^{2\pi i/m}) \cap K(e^{2\pi i/n}) \\ & = Q\left(e^{2\pi i/r}, e^{2\pi i/m}\right) \cap Q\left(e^{2\pi i/r}, e^{2\pi i/n}\right) \\ & = Q\left(e^{2\pi i/[r,m]}\right) \cap Q\left(e^{2\pi i/[r,n]}\right), && \text{(by (3))} \\ & = Q\left(e^{2\pi i/([r,m],[r,n])}\right) && \text{(by (1) for } K = Q\text{))} \\ & = Q\left(e^{2\pi i/[r,(m,n)]}\right) \\ & = Q\left(e^{2\pi i/r}, e^{2\pi i/(m,n)}\right) && \text{(by (3))} \\ & = K\left(e^{2\pi i/(m,n)}\right), \end{aligned}$$

proving (1) in this case too.

However (1) does not hold for every algebraic number field K. To see this take $K = Q(\sqrt[6]{3})$, $m = 3$, $n = 4$. Here

$$\begin{aligned} \sqrt{3} &= \left(\sqrt[6]{3}\right)^3 \in K \subseteq K\left(e^{2\pi i/3}\right), \\ \sqrt{-3} &\in Q\left(e^{2\pi i/3}\right) \subseteq K\left(e^{2\pi i/3}\right), \end{aligned}$$

so

$$\sqrt{-1} = \frac{1}{3}\sqrt{3}\sqrt{-3} \in K\left(e^{2\pi i/3}\right),$$

and

$$\sqrt{-1} \in Q\left(e^{2\pi i/4}\right) \subseteq K\left(e^{2\pi i/4}\right),$$

showing that $K\left(e^{2\pi i/3}\right) \cap K\left(e^{2\pi i/4}\right)$ is a nonreal field, however $K\left(e^{2\pi i/(3,4)}\right) = K = Q\left(\sqrt[6]{3}\right)$ is a real field.

In this note we determine a necessary and sufficient condition for (1) to hold in the case of a quadratic field K. From this point on we take K to be a quadratic field. We denote the discriminant of K by D so that $K = Q\left(\sqrt{D}\right)$. An integer which is the discriminant of a quadratic field is called a fundamental discriminant. It is known [3, Proposition 9, p.59] that a fundamental discriminant is the product of prime fundamental discriminants. This representation is unique apart from the order of the prime discriminants in the product.

Theorem. *Let m and n be positive integers. Set $d = (m,n)$, $\ell = [m,n]$. Let K be a field of degree 2 over Q. Let D denote the discriminant of K. Then*

$$K(e^{2\pi i/m}) \cap K(e^{2\pi i/n}) = K\left(e^{2\pi i/d}\right) \Leftrightarrow D \nmid \ell \text{ or } D \mid m \text{ or } D \mid n.$$

In the case $D|\ell$, $D \nmid m, D \nmid n$, *let* $D = d_1 \cdots d_k$ *be the unique decomposition of the fundamental discriminant* D *as a product of prime discriminants, and set*

$$D_3 = \prod_{\substack{i=1 \\ d_i|d}}^{k} d_i.$$

Then there exist unique fundamental discriminants D_1 *and* D_2 *such that*

$$D = D_1 D_2 D_3,\ \ D_1|m, D_2|n, D_1 \neq 1 \text{ or } D, D_2 \neq 1 \text{ or } D,$$

and

$$\begin{aligned} &K(e^{2\pi i/m}) \cap K(e^{2\pi i/n}) = K\left(e^{2\pi i/d}, \sqrt{D_1}\right) \neq K\left(e^{2\pi i/d}\right), \\ &[K\left(e^{2\pi i/d}, \sqrt{D_1}\right) : K\left(e^{2\pi i/d}\right)] = 2, \\ &K\left(e^{2\pi i/d}, \sqrt{D_1}\right) = K\left(e^{2\pi i/d}, \sqrt{D_2}\right). \end{aligned}$$

Before proving this theorem we need some preliminary results. We set

(4) $$H = K(e^{2\pi i/m}) \cap K(e^{2\pi i/n}),$$

and note that

(5) $$H \subseteq K(e^{2\pi i/m}),\ H \subseteq K(e^{2\pi i/n}),\ H \supseteq K\left(e^{2\pi i/d}\right).$$

Lemma 1. $K \subseteq Q(e^{2\pi i/m}) \Leftrightarrow D|m$.

Proof. The conductor of K is $|D|$ (see for example [1, p.98]) so the smallest cyclotomic field containing K is $Q\left(e^{2\pi i/|D|}\right)$. The result now follows from (2).

Lemma 2. *Set* $q(D,r) = [K\left(e^{2\pi i/r}\right) : K]$. *Then*

$$q(D,r) = \begin{cases} \phi(r)/2, & \text{if } D|r, \\ \phi(r), & \text{if } D \nmid r, \end{cases}$$

where ϕ *denotes Euler's phi function.*

Proof. By Lemma 1 we have

$$\left[K\left(e^{2\pi i/r}\right) : Q\left(e^{2\pi i/r}\right)\right] = \begin{cases} 1, & \text{if } D|r, \\ 2, & \text{if } D \nmid r. \end{cases}$$

The asserted result now follows as

$$\begin{aligned} q(D,r) &= \left[K\left(e^{2\pi i/r}\right) : K\right] = \frac{\left[K\left(e^{2\pi i/r}\right) : Q\right]}{[K:Q]} \\ &= \frac{\left[K\left(e^{2\pi i/r}\right): Q\left(e^{2\pi i/r}\right)\right]\left[Q(e^{2\pi i r}): Q\right]}{[K:Q]} \\ &= \frac{\phi(r)}{2}\left[K\left(e^{2\pi i/r}\right): Q\left(e^{2\pi i/r}\right)\right]. \end{aligned}$$

Lemma 3. $K(e^{2\pi i/m}) = H(e^{2\pi i/m})$.

Proof. From (5) we have

$$H(e^{2\pi i/m}) \supseteq K(e^{2\pi i/d}, e^{2\pi i/m}) = K(e^{2\pi i/m}) \supseteq H(e^{2\pi i/m}).$$

Lemma 4. *If D and D_1 are fundamental discriminants and d is a positive integer such that*

$$D_1 | D,\ D_1 \not| d,\ D/D_1 \not| d, \tag{6}$$

then

$$\left[K(e^{2\pi i/d}, \sqrt{D_1}) : K(e^{2\pi i/d})\right] = 2.$$

Proof. Suppose on the contrary that $\left[K(2\pi i/d, \sqrt{D_1}) : K(e^{2\pi i/d})\right] \neq 2$. Then $\left[K(e^{2\pi i/d}, \sqrt{D_1}) : K(e^{2\pi i/d})\right] = 1$ and $\sqrt{D_1} \in K(e^{2\pi i/d})$. Thus there are elements α and β of $Q(e^{2\pi i/d})$ such that

$$\sqrt{D_1} = \alpha + \beta\sqrt{D}.$$

Hence

$$\begin{aligned} 2\alpha &= tr_{K(e^{2\pi i/d})/Q(e^{2\pi i/d})}(\alpha + \beta\sqrt{D}) \\ &= tr_{K(e^{2\pi i/d})/Q(e^{2\pi i/d})}(\sqrt{D_1}) \\ &= 0 \text{ or } 2\sqrt{D_1}, \end{aligned}$$

so that $\alpha = 0$ or $\sqrt{D_1}$. If $\alpha = 0$ then $\sqrt{D_1} = \beta\sqrt{D}$ so $\sqrt{\frac{D}{D_1}} = \frac{1}{\beta} \in Q(e^{2\pi i/d})$, and thus $\frac{D}{D_1}\Big| d$, contradicting $D/D_1 \not| d$. If $\alpha = \sqrt{D_1}$ then $\sqrt{D_1} \in Q(e^{2\pi i/d})$ and thus $D_1 | d$, contradicting $D_1 \not| d$.

We are now ready to prove the theorem.

Proof of Theorem. First we show that

$$D \not| \ell \text{ or } D|m \text{ or } D|n \Rightarrow K(e^{2\pi i/m}) \cap K(e^{2\pi i/n}) = K(e^{2\pi i/d}). \tag{7}$$

By (5) we have

$$K(e^{2\pi i/n}) \supseteq H \supseteq K(e^{2\pi i/d}),$$

and thus

$$\begin{aligned} \left[K(e^{2\pi i/d}, e^{2\pi i/m}) : K(e^{2\pi i/d})\right] &\geq \left[H(e^{2\pi i/m}) : H\right] \\ &\geq \left[K(e^{2\pi i/n}, e^{2\pi i/m}) : K(e^{2\pi i/n})\right]. \end{aligned} \tag{8}$$

First we determine the quantity on the left hand side of (8). We have

$$\left[K(e^{2\pi i/d}, e^{2\pi i/m}) : K(e^{2\pi i/d})\right] = \left[K(e^{2\pi i/m}) : K(e^{2\pi i/d})\right] = \frac{q(D,m)}{q(D,d)}.$$

Next we determine the quantity on the right hand side of (8). We have

$$\left[K\left(e^{2\pi i/n}, e^{2\pi i/m}\right): K\left(e^{2\pi i/n}\right)\right] = \left[K\left(e^{2\pi i/\ell}\right): K\left(e^{2\pi i/n}\right)\right] = \frac{q(D,\ell)}{q(D,n)}.$$

The next step is to show that $\frac{q(D,m)}{q(D,d)} = \frac{q(D,\ell)}{q(D,n)}$. We treat four cases. If $D \nmid \ell$ (so that $D \nmid m, D \nmid n, D \nmid d$) we have

$$\frac{q(D,m)}{q(D,d)} = \frac{\phi(m)}{\phi(d)} = \frac{\phi(\ell)}{\phi(n)} = \frac{q(D,\ell)}{q(D,n)}.$$

If $D|\ell, D|m,\ D|n$ (so that $D|d$)

$$\frac{q(D,m)}{q(D,d)} = \frac{\phi(m)/2}{\phi(d)/2} = \frac{\phi(\ell)/2}{\phi(n)/2} = \frac{q(D,\ell)}{q(D,n)}.$$

If $D|\ell, D|m,\ D \nmid n$ (so that $D \nmid d$)

$$\frac{q(D,m)}{q(D,d)} = \frac{\phi(m)/2}{\phi(d)} = \frac{\phi(\ell)/2}{\phi(n)} = \frac{q(D,\ell)}{q(D,n)}.$$

If $D|\ell, D \nmid m,\ D|n$ (so that $D \nmid d$)

$$\frac{q(D,m)}{q(D,d)} = \frac{\phi(m)}{\phi(d)} = \frac{\phi(\ell)/2}{\phi(n)/2} = \frac{q(D,\ell)}{q(D,n)}.$$

Hence in all four cases we have $\frac{q(D,m)}{q(D,d)} = \frac{q(D,\ell)}{q(D,n)}$. This shows that equality holds throughout (8), and thus

$$\text{(9)}\quad \begin{aligned}\left[K\left(e^{2\pi i/d}, e^{2\pi i/m}\right): K\left(e^{2\pi i/d}\right)\right] &= \left[H\left(e^{2\pi i/m}\right): H\right] \\ &= \left[K\left(e^{2\pi i/n}, e^{2\pi i/m}\right): K\left(e^{2\pi i/n}\right)\right].\end{aligned}$$

Now by Lemma 3 we have $K\left(e^{2\pi i/d}, e^{2\pi i/m}\right) = K\left(e^{2\pi i/m}\right) = H\left(e^{2\pi i/m}\right)$, and the first equality in (9) gives $\left[H\left(e^{2\pi i/m}\right): K\left(e^{2\pi i/d}\right)\right] = \left[H\left(e^{2\pi i/m}\right): H\right]$. But by (5) we have $H \supseteq K\left(e^{2\pi i/d}\right)$, so we must have $H = K\left(e^{2\pi i/d}\right)$ as claimed. This completes the proof of (7).

Now we show that

$$\text{(10)}\qquad D|\ell,\ D \nmid m,\ D \nmid n \Rightarrow\ K\left(e^{2\pi i/m}\right) \cap K\left(e^{2\pi i/n}\right) \neq K\left(e^{2\pi i/d}\right)$$

and at the same time determine exactly what $K\left(e^{2\pi i/m}\right) \cap K\left(e^{2\pi i/n}\right)$ is. Each d_i in the product

$$\prod_{\substack{i=1 \\ d_i \nmid d}}^{k} d_i = D/D_3$$

divides D and so divides ℓ and thus mn. Clearly such d_i do not divide both m and n as $d_i \nmid d$. Set

$$D_1 = \prod_{\substack{i=1 \\ d_i|m \\ d_i \nmid d}}^{k} d_i, \qquad D_2 = \prod_{\substack{i=1 \\ d_i|n \\ d_i \nmid d}}^{k} d_i.$$

Then $D = D_1D_2D_3$, $D_1|m$, $D_2|n$. Clearly D_1 and D_2 are uniquely defined. Suppose $D_1 = 1$. Since $D_2|n/d$ we have $D_2D_3\big|\frac{n}{d}\cdot d = n$, that is $D|n$, contradicting $D \nmid n$. Hence $D_1 \neq 1$. Similarly $D_2 \neq 1$, and thus $D_1 \neq D$, $D_2 \neq D$.

As $D_1|m$, by Lemma 1, we have $\sqrt{D_1} \in Q(e^{2\pi i/m})$ so that

$$\sqrt{D_1} \in K(e^{2\pi i/m}).$$

Similarly

$$\sqrt{D_2} \in K(e^{2\pi i/n}).$$

Also $D_3|d$ so

$$\sqrt{D_3} \in Q\left(e^{2\pi i/d}\right) \subseteq H.$$

Hence, as $\sqrt{D} \in K \subseteq K\left(e^{2\pi i/d}\right) \subseteq H$, we see that

$$\pm\sqrt{D_1} = \frac{\sqrt{D}}{\sqrt{D_2}\sqrt{D_3}} \in K(e^{2\pi i/n}),$$

and

$$\pm\sqrt{D_2} = \frac{\sqrt{D}}{\sqrt{D_1}\sqrt{D_3}} \in K(e^{2\pi i/m}),$$

and thus

$$\sqrt{D_1} \in H, \quad \sqrt{D_2} \in H.$$

It follows that

$$K(e^{2\pi i/n}) \supseteq H \supseteq K\left(\sqrt{D_1}, e^{2\pi i/d}\right),$$

and so

$$\begin{aligned} \left[K\left(\sqrt{D_1}, e^{2\pi i/d}, e^{2\pi i/m}\right) : K\left(\sqrt{D_1}, e^{2\pi i/d}\right)\right] &\geq \left[H(e^{2\pi i/m}) : H\right] \\ &\geq \left[K\left(e^{2\pi i/n}, e^{2\pi i/m}\right) : K(e^{2\pi i/n})\right]. \end{aligned} \tag{11}$$

First we determine the left hand term in (11). We have

$$\begin{aligned} &\left[K\left(\sqrt{D_1}, e^{2\pi i/d}, e^{2\pi i/m}\right) : K\left(\sqrt{D_1}, e^{2\pi i/d}\right)\right] \\ &= \left[K(e^{2\pi i/m}) : K\left(\sqrt{D_1}, e^{2\pi i/d}\right)\right] \end{aligned}$$

$$= \frac{\left[K(e^{2\pi i/m}) : K\right]}{\left[K\left(\sqrt{D_1}, e^{2\pi i/d}\right) : K\left(e^{2\pi i/d}\right)\right]\left[K\left(e^{2\pi i/d}\right) : K\right]}$$

$$= \frac{q(D,m)}{2q(D,d)}, \quad \text{by Lemma 4.}$$

Next we determine the right hand term in (11). We have

$$\begin{aligned} \left[K\left(e^{2\pi i/n}, e^{2\pi i/m}\right) : K\left(e^{2\pi i/n}\right)\right] &= \left[K\left(e^{2\pi i/\ell}\right) : K\left(e^{2\pi i/n}\right)\right] \\ &= \frac{\left[K\left(e^{2\pi i/\ell}\right) : K\right]}{\left[K(e^{2\pi i/n}) : K\right]} \\ &= \frac{q(D,\ell)}{q(D,n)}. \end{aligned}$$

We now show that

$$\frac{q(D,m)}{2q(D,d)} = \frac{q(D,\ell)}{q(D,n)}.$$

As $D|\ell$, $D \nmid m, D \nmid n$, we have $D \nmid d$ and

$$\frac{q(D,m)}{2q(D,d)} = \frac{\phi(m)}{2\phi(d)} = \frac{\phi(\ell)/2}{\phi(n)} = \frac{q(D,\ell)}{q(D,n)}.$$

Hence equality holds throughout (11), that is

$$\begin{aligned} &\left[K\left(\sqrt{D_1}, e^{2\pi i/d}, e^{2\pi i/m}\right) : K\left(\sqrt{D_1}, e^{2\pi i/d}\right)\right] \\ (12) \qquad &= \left[H(e^{2\pi i/m}) : H\right] \\ &= \left[K\left(e^{2\pi i/n}, e^{2\pi i/m}\right) : K\left(e^{2\pi i/n}\right)\right]. \end{aligned}$$

Now

$$\begin{aligned} K\left(\sqrt{D_1}, e^{2\pi i/d}, e^{2\pi i/m}\right) &= K\left(e^{2\pi i/d}, e^{2\pi i/m}\right) \\ &= K(e^{2\pi i/m}) \\ &= H(e^{2\pi i/m}), \text{ by Lemma 3,} \end{aligned}$$

so (12) gives

$$\left[H(e^{2\pi i/m}) : K\left(\sqrt{D_1}, e^{2\pi i/d}\right)\right] = \left[H(e^{2\pi i/m}) : H\right].$$

But $H \supseteq K\left(\sqrt{D_1}, e^{2\pi i/d}\right)$ so we must have

$$H = K\left(\sqrt{D_1}, e^{2\pi i/d}\right).$$

Note that $D_1 | D$, $D_1 \not| d$, $D_2 D_3 \not| d$, so by Lemma 4 we have

$$\left[K\left(e^{2\pi i/d}, \sqrt{D_1}\right) : K\left(e^{2\pi i/d}\right)\right] = 2,$$

so that

$$H = K\left(e^{2\pi i/d}, \sqrt{D_1}\right) \neq K\left(e^{2\pi i/d}\right).$$

Finally

$$\begin{aligned} K\left(e^{2\pi i/d}, \sqrt{D_1}\right) &= K\left(e^{2\pi i/d}, \sqrt{D}\sqrt{D_2}\sqrt{D_3}\right), && \text{as } D = D_1 D_2 D_3, \\ &= K\left(e^{2\pi i/d}, \sqrt{D_2}\sqrt{D_3}\right) && \text{as } \sqrt{D} \in K, \\ &= K\left(e^{2\pi i/d}, \sqrt{D_2}\right) && \text{as } \sqrt{D_3} \in K\left(e^{2\pi i/d}\right) \end{aligned}$$

This completes the proof of (10), and thus of the theorem.

References

[1] R. L. Long, *Algebraic Number Theory*, Marcel Dekker, Inc., New York and Basel, 1977.

[2] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers (Second Edition)*, Springer-Verlag (Berlin) and Polish Scientific Publishers (Warsaw), 1990.

[3] C. L. Siegel, *Advanced Analytic Number Theory*, Tata Institute of Fundamental Research, Bombay, 1980.

[4] B. K. Spearman and K.S. Williams, *Two short papers in Number Theory*, Centre for Research in Algebra and Number Theory, Carleton University-University of Ottawa, Mathematical Research Series No. 7, October 1991.