Products of Periods in Kummer 1847

Steve Kieffer

In Kummer's 1847 paper, "*Über die Zerlegung der aus Wurzeln der Einheit gebildeten complexen Zahlen in ihre Primfactoren*," it is simply called "*bekanntlich*" that a product of two periods of length f is equal to a $\mathbb{Z}$-linear combination over all such periods (possibly plus a pure integer). Here I explain why this is so.

Recall that λ is an odd prime, α is an imaginary root of $\alpha^\lambda = 1$, and e and f satisfy $ef = \lambda - 1$.

In order to define the e periods η_r of length f, we begin by picking a generator γ of the multiplicative group mod λ, that is, a primitive root mod λ. Each period is a sum of f terms of the form α^{γ^ℓ}, where ℓ runs from 0 to $ef - 1$.

The way these terms are distributed among the periods is analogous to the way in which cards are dealt to players in a card game. Thus, α^{γ^0} is "dealt" to the first period η_0, then α^{γ^1} to the next period η_1, and so on up to $\alpha^{\gamma^{e-1}}$, which is the first term of η_{e-1}. At this point, each player has received one card, and the deal goes around the table again. In this way we move first down the leftmost column in Figure 1, then down the next column, and so on up to the final fth column.

$$\begin{array}{rcccccccccc}
\eta_0 & = & \alpha^{\gamma^0} & + & \alpha^{\gamma^e} & + & \alpha^{\gamma^{2e}} & + & \cdots & + & \alpha^{\gamma^{(f-1)e}} \\
\eta_1 & = & \alpha^{\gamma^1} & + & \alpha^{\gamma^{e+1}} & + & \alpha^{\gamma^{2e+1}} & + & \cdots & + & \alpha^{\gamma^{(f-1)e+1}} \\
\eta_2 & = & \alpha^{\gamma^2} & + & \alpha^{\gamma^{e+2}} & + & \alpha^{\gamma^{2e+2}} & + & \cdots & + & \alpha^{\gamma^{(f-1)e+2}} \\
\vdots & & & & & & & & & & \\
\eta_{e-1} & = & \alpha^{\gamma^{e-1}} & + & \alpha^{\gamma^{e+e-1}} & + & \alpha^{\gamma^{2e+e-1}} & + & \cdots & + & \alpha^{\gamma^{(f-1)e+e-1}}
\end{array}$$

Figure 1: The e periods of length f.

In general then, we have

$$\eta_r = \sum_{i=0}^{f-1} \alpha^{\gamma^{ie+r}} \tag{1}$$

$$= \sum_{i=0}^{f-1} \alpha^{(\gamma^e)^i(\gamma^r)} \tag{2}$$

Now for any r and k we want to show that the product $\eta_r\eta_{r+k}$ is a $\mathbb{Z}$-linear combination over $\{1, \eta_0, \eta_1, \ldots, \eta_{e-1}\}$. (Subscripts on the η_t are of course to be understood mod e.) We have

$$\eta_r\eta_{r+k} = \sum_{i=0}^{f-1}\sum_{j=0}^{f-1} \alpha^{\gamma^{je+r}+\gamma^{ie+r+k}} \tag{3}$$

$$= \sum_{i=0}^{f-1}\sum_{j=0}^{f-1} \alpha^{\gamma^r[(\gamma^e)^j+(\gamma^k)(\gamma^e)^i]} \tag{4}$$

whereupon it is clear that it suffices to prove the claim in the case that $r = 0$; for if we should prove that

$$\eta_0\eta_k = \mu f + m_0\eta_0 + m_1\eta_1 + \cdots + m_{e-1}\eta_{e-1} \tag{5}$$

then it will follow from (4) that

$$\eta_r\eta_{r+k} = \mu f + m_0\eta_r + m_1\eta_{r+1} + \cdots + m_{e-1}\eta_{r+e-1}. \tag{6}$$

But

$$\eta_0\eta_k = \sum_{i=0}^{f-1}\sum_{j=0}^{f-1} \alpha^{(\gamma^e)^j+(\gamma^k)(\gamma^e)^i} \tag{7}$$

$$= \sum_{i=0}^{f-1}\sum_{j=0}^{f-1} \alpha^{(\gamma^e)^i[(\gamma^e)^{j-i}+(\gamma^k)]} \tag{8}$$

$$= \sum_{i=0}^{f-1}\sum_{\ell=0}^{f-1} \alpha^{(\gamma^e)^i[(\gamma^e)^{\ell}+(\gamma^k)]} \tag{9}$$

$$= \sum_{\ell=0}^{f-1}\sum_{i=0}^{f-1} \alpha^{(\gamma^e)^i[(\gamma^e)^{\ell}+(\gamma^k)]} \tag{10}$$

where we have used in equation (9) the fact that exponents of (γ^e) may be regarded mod f. Now, when ℓ is such that

$$\gamma^{\ell e} + \gamma^k \equiv 0 \bmod e, \tag{11}$$

then the inner sum in (10) is $\sum_{i=0}^{f-1} 1 = f$; otherwise,

$$\gamma^{\ell e} + \gamma^k \equiv \gamma^t \not\equiv 0 \bmod e,$$

and the inner sum is η_t, by (2). This establishes (5).

As for μ, which, as Kummer says, is 0 in all cases except when f is even and $k = 0$, or f is odd and $k = e/2$, this is also now evident. For μ is equal to the number of values of ℓ for which (11) holds. From the theory of primitive residues however, we know that (11) holds just in case $\ell e \equiv k + (\lambda - 1)/2 \bmod \lambda - 1$, or, passing to a coarser congruence, $k + (\lambda - 1)/2 \equiv 0 \bmod e$. Now k, being an index to the periods η_s (or a term therein) is itself to be regarded mod e. Then if $f = (\lambda - 1)/e$ is even, so that $(\lambda - 1)/2e$ is an integer, and $(\lambda - 1)/2$ is thus divisible by e, then k must be 0 mod e. On the other hand, if $f = (\lambda - 1)/e = 2\nu + 1$ is odd, then multiplying by $e/2$ we get $(\lambda - 1)/2 = \nu e + e/2 \equiv e/2 \bmod e$, so in this case we must have $k \equiv e/2 \bmod e$.