Corrigendum to the proof of Lemma 4.2 of ”Ideal arithmetic and infrastructure in purely cubic function fields”

R. Scheidler

Lemma 4.2 Let \( \mathfrak{a} = [L(a), \mu, \nu] \) be a primitive ideal where \( \mu = m_0 + m_1 \rho + m_2 \omega, \) \( \nu = n_0 + n_1 \rho + n_2 \omega \) with \( m_0, m_1, m_2, n_0, n_1, n_2 \in \mathbb{k}[x] \). Then \( \mathfrak{a} \) has a triangular basis which can be obtained as follows. Set

\[
\begin{align*}
    s'' &= \gcd(m_2, n_2), \\
    s' &= (m_1 n_2 - n_1 m_2)/s'', \\
    s &= L(a),
\end{align*}
\]

and let \( a', b', t \in \mathbb{k}[x] \) satisfy \( a' m_2 + b' n_2 = s'' \) and \( s' t \equiv a' m_1 + b' n_1 \pmod{s''} \). Set \( a = a' - t n_2/s'' \), \( b = b' + t m_2/s'' \),

\[
\begin{align*}
    u &= \frac{m_0 n_2 - n_0 m_2}{s''}, \\
    v &= \frac{a m_0 + b n_0}{s''}, \\
    w &= \frac{a m_1 + b n_1}{s''}.
\end{align*}
\]

Then \( \{s, s'(u + \rho), s''(v + w \rho + \omega)\} \) is a triangular basis of \( \mathfrak{a} \).

Proof: Let \( U = (m_0 n_2 - n_0 m_2)/s'', \) \( V = a' m_0 + b' n_0, \) and \( W = a' m_1 + b' n_1. \) Then \( U, V, W \in \mathbb{k}[x], \) and if \( \alpha = (n_2 \rho - m_2 \nu)/s'' \) and \( \beta = a' \mu + b' \nu = V + W \rho + s'' \omega, \) then \( \{s, \alpha, \beta\} \) is a basis of \( \mathfrak{a} \).

Since \( \alpha \rho, \alpha \omega, \beta \rho, \beta \omega \in \mathfrak{a}, \) each of these four elements can be written as a \( k[x]\)-linear combination of \( \alpha \) and \( \beta. \) By considering the coefficient of \( \omega \) in these linear combinations, we see that \( s'' \mid H s', \) \( s'' \mid U, \) \( s'' \mid WH, \) and \( s'' \mid V. \) Moreover, by writing \( \alpha \rho = A \alpha + B \beta \) with \( A, B \in \mathbb{k}[x] \) and considering the coefficients of \( \omega \) and \( \rho, \) we obtain \( B = H s'/s'' \) and \( U = A s' + BW = s'(A + HW/s''). \) It follows that \( s' \mid U, \) implying \( u = U/s' \in k[x]. \)

We claim that \( \gcd(s', s'') = 1. \) To that end, write \( \beta \rho = C \rho + E \omega \) with \( C, E \in k[x]. \) Considering again the coefficients of \( \omega \) and \( \rho \) in \( \beta \rho \) shows that \( E = HW/s'' \) and \( V = Cs' + EW. \) Let \( d = \gcd(s', s''). \) Then \( d \mid s' \mid U \) and \( d \mid s'' \mid V. \) Furthermore, \( N(\mathfrak{a}) = ss'' \) implies \( s' s''/s \mid s, \) so \( d \mid s. \) Thus, \( \gcd(d, W) = 1 \) since \( \mathfrak{a} \) is primitive. Then \( s' \mid V - EW \) yields \( d \mid EW, \) and hence \( d \mid E = HW/s''. \) Then \( d^2 \mid ds'' \mid HW, \) so \( d \mid H. \) Since \( H \) is squarefree, we must have \( d = 1. \)

It follows that \( t \) as defined in the Lemma exists, and \( W \equiv s' t \pmod{s''}. \) Set \( \gamma = \beta - t \alpha. \) Then \( \{s, \alpha, \gamma\} \) is a basis of \( \mathfrak{a}, \) \( \alpha = s'(u + \rho), s'' \mid \gamma, \) and a simple computation shows that \( \gamma = s''(v + w \rho + \omega). \) \hfill \Box