

Computing the Intersection Points of Algebraic Plane Curves

Jan Hilmar and Chris Smyth

January 26, 2007

Abstract

We consider the problem of determining the intersection points of two projective algebraic plane curves over an algebraically closed field \mathbf{k} . If the defining polynomials are of degrees m and n , respectively, Bezout's Theorem tells us that the curves will have mn intersection points over \mathbf{k} , counting multiplicities.

Using a result due to Fulton together with the Euclidean algorithm, one can devise an algorithm for computing the intersection points of two curves, and a simple proof of Bezout's Theorem follows. We then use this algorithm to compute the intersection points and find the smallest number field $\mathbf{m}(\theta)$ such that Bezout's theorem holds over $\mathbb{P}\mathbf{m}(\theta)^2$ for two given curves with coefficients in a not algebraically closed field \mathbf{m} .

1 Introduction

Let \mathbf{k} be an algebraically closed field. We denote by $\mathbf{k}[x, y, z]$ the ring of homogeneous polynomials with coefficients in \mathbf{k} . Further, for $a(x, y, z) \in \mathbf{k}[x, y, z]$, we define an algebraic curve A over \mathbf{k} to be the variety $A = \{(x, y, z) \in \mathbb{P}\mathbf{k}^2 \mid a(x, y, z) = 0\}$. By the degree of an algebraic curve ∂A , we mean the degree of the polynomial defining it and denote by $\partial_x A, \partial_y A$ the degree of A in x, y , respectively. Given algebraic curves A, B , we define the following varieties:

$$A + B = \{(x, y, z) \in \mathbb{P}\mathbf{k}^2 \mid a(x, y, z) + b(x, y, z) = 0\} \quad (1)$$

$$AB = \{(x, y, z) \in \mathbb{P}\mathbf{k}^2 \mid a(x, y, z)b(x, y, z) = 0\} \quad (2)$$

A well-known result due to Bezout states that, if $\gcd(a, b) = 1$ (we say that A and B have no common component), then A and B have exactly $\partial A \partial B$ common points, counting multiplicities.

In order to define the multiplicity of intersection of two curves A, B with no common component, we turn to a definition from Fulton:

Definition 1. *Let A, B be algebraic curves with no common component and let $P \in \mathbb{P}\mathbf{k}^2$. We define the intersection multiplicity of A and B at P by*

$$m(P; A, B) = \dim_{\mathbf{k}} \frac{\mathcal{O}_P(\mathbb{P}\mathbf{k}^2)}{(a, b)} \quad (3)$$

where $\mathcal{O}_P(\mathbb{P}^2)$ denotes the local ring of rational functions defined at P and (a, b) denotes the ideal generated by $a(x, y, z)$ and $b(x, y, z)$ over $\mathbf{k}[x, y, z]$.

Fulton shows that the multiplicity thus defined satisfies the following conditions:

Theorem 1 (Fulton). *Let A, B be algebraic curves with no common component and $P \in \mathbb{P}^2$ be a common point. Then*

1. $m(P; A, B) = m(P; B, A)$
2. $m(P; A, BC) = m(P; A, B) + m(P; A, C)$ for any algebraic curve C
3. $m(P; A, B + AD) = m(P; A, B)$ for any algebraic curve D such that $\partial AD = \partial B$.

Proofs of these can be found in [2].

Using the notion of intersection multiplicity, one can now form the formal sum

$$A.B = \sum_{P \in \mathbb{P}^2} m(P; A, B)P$$

for two given algebraic curves A, B . If A and B have no common component, this sum will be finite and will contain all intersection points of A and B . It is easily verified that $A.B$, the *intersection cycle* of A and B , satisfies the conditions of theorem 1. Further, for algebraic curves A, B, C with A, B and A, C having no common components, we define

$$nA.B = \sum_{P \in \mathbb{P}^2} n \cdot m(P; A, B)P \text{ for } n \in \mathbb{N} \quad (4)$$

$$A.B \oplus A.C = \sum_{P \in \mathbb{P}^2} (m(P; A, B) + m(P; A, C))P \quad (5)$$

If $(a, b) \subseteq (a, c)$,

$$A.B \ominus A.C = \sum_{P \in \mathbb{P}^2} (m(P; A, B) - m(P; A, C))P \quad (6)$$

Given two algebraic curves A, B , suppose, without loss of generality, that $\partial_x a \geq \partial_x b$. Then we can use the Euclidean Algorithm (in x) to find $q', r' \in \mathbf{k}[x]$ with $a = q'b + r'$ and $r' = 0$ or $\partial_x r' < \partial_x b$. Upon clearing denominators, we obtain $q, r \in \mathbf{k}[x, y, z], d \in \mathbf{k}[y, z]$ with

$$da = bq + r \quad (7)$$

where $q = q'm, r = r'm$, and $r = 0$ or $\partial_x r < \partial_x b$. Suppose now that $\gcd(b, d) = \gcd(b, r) = 1$ (the general case will be commented on later). Writing equation (7) in terms of the algebraic curves these polynomials define, and forming the intersection cycle of both sides with B , we get

$$\begin{aligned}
B.(DA) &= B.(BQ + R) \\
B.D \oplus B.A &= B.R \\
A.B &= B.R \ominus B.D
\end{aligned}$$

Here, we have used the properties of intersection multiplicity from Theorem 1 and the fact that, due to homogeneity, $\partial bq = \partial r$. Note that the "difference" of intersection cycles on the right is well-defined, as we have a containment of ideals $(b, r) \subset (b, d)$ (see (6)).

If $\gcd(b, d) = \gcd(b, r) = g$ with $\partial g > 0$, we can write (7) as

$$d^*ga = b^*gq + r^*g \quad (8)$$

where $d^*g = d, b^*g = b, r^*g = r$. Forming the intersection cycle of the corresponding equation for algebraic curves with B , we get

$$A.B = (B^*.R^* \ominus B^*.D^*) \oplus A.G. \quad (9)$$

We can now apply the Euclidean Algorithm to B, R and A, G again and get expressions of $B.R$ and $A.G$ in terms of curves of lower x -degree. Continuing this until we have an expression involving only expressions of the form $C_1.C_2$, where $c_1 \in \mathbf{k}[x, y, z], c_2 \in \mathbf{k}[y, z]$, we get a recursive method of calculating the intersection points of A and B .

Suppose now, we are given $a \in \mathbf{k}[x, y, z], b \in \mathbf{k}[y, z]$. In order to find the intersection cycle $A.B$, we can factor b as

$$b(y, z) = b_d z^k \prod_{i=1}^n (y - \beta_i z)^{k_i}.$$

Now, for $k \in \mathbb{N}$, let $Z^k = \{(x, y, z) \in \mathbb{P}\mathbf{k}^2 \mid z^k = 0\}$ and $L_i = \{(x, y, z) \in \mathbb{P}\mathbf{k}^2 \mid y - \beta_i z = 0\}$. Then, using Theorem 1 applied to intersection cycles, we get

$$\begin{aligned}
A.B &= A. \left(Z^k \prod_{i=1}^n L_i^{k_i} \right) \\
&= kA.Z \oplus \sum_{i=1}^n k_i A.L_i
\end{aligned} \quad (10)$$

Now, looking at $a(x, y, z)$, we can expand it as

$$a(x, y, z) = \begin{cases} \sum_{j=0}^{\partial_z a} a_j(x, y) z^j \\ \sum_{j=0}^{\partial_y a} \widetilde{a_{i,j}}(x, z) (y - \beta_i z)^j, 1 \leq i \leq \partial_y b \end{cases}$$

Using Theorem 1 and the fact that all polynomials involved are homogeneous, it is now easy to see that

$$\begin{aligned} A.Z &= A_0.Z \\ A.L_i &= \widetilde{A_{i,0}}.L_i. \end{aligned} \tag{11}$$

We can now use this to prove:

Lemma 1. *Let A, B be algebraic curves over $\mathbb{P}\mathbf{k}^2$ with $a \in \mathbf{k}[x, y, z], b \in \mathbf{k}[y, z]$ and $\gcd(a, b) = 1$. Further, assume that \mathbf{k} is an algebraically closed field. Then A and B intersect in $\partial a \partial b$ points.*

Proof. From (10) and (11), we know that

$$A.B = kA_0.Z \oplus \sum_{i=1}^n k_i \widetilde{A_{i,0}}.L_i.$$

Now, let

$$\#(A.B) = \sum_{P \in \mathbb{P}\mathbf{k}^2} m(P; A, B).$$

Then,

$$\begin{aligned} \#(A.B) &= k\#(A_0.Z) + \sum_{i=1}^n k_i \#(\widetilde{A_{i,0}}.L_i) \\ &= k\partial A + \sum_{i=1}^n k_i \partial A \\ &= \partial A \partial B \end{aligned}$$

by using the fact that $\partial A = \partial A_0 = \partial \widetilde{A_{i,0}}$ by homogeneity. □

Using this Lemma, we get a simple proof of Bezout's Theorem:

Theorem 2 (Bezout's Theorem). *Let A, B be algebraic curves over $\mathbb{P}\mathbf{k}^2$ with $a, b \in \mathbf{k}[x, y, z]$ and $\gcd(a, b) = 1$. Further, assume that \mathbf{k} is an algebraically closed field. Then A and B intersect in $\partial a \partial b$ points.*

Proof. We proceed by induction on the x -degree of $b(x, y, z)$. If $\partial_x b = 0$, Lemma 1 gives the result.

Suppose now we know that, for fixed A , the result holds for all B with $\partial_x B < n$ and consider A, B with $\partial_x B = n$. Then, by (9)

$$\begin{aligned} \#(A.B) &= \#(A.G \oplus B^*.R^* \ominus B^*.D^*) \\ &= \partial A \partial G + \partial B^*(\partial R^* - \partial D^*). \end{aligned}$$

Using (8) and the fact that all polynomials involved are homogeneous, we see that $\partial R^* - \partial D^* = \partial A$. Also, as $\partial B^* + \partial G = \partial B$, the result follows. □

The proof of Bezout's Theorem also shows that the algorithm is independent of the variable (x or y) chosen to perform the Euclidean Algorithm, as it finds all $\partial A \partial B$ common points, using either variable.

2 Intersection points over general fields

While Bezout's Theorem only applies to algebraically closed fields, it is also interesting to start with a general field \mathbf{m} and construct the smallest extension $\mathbf{m}(\theta)$ in which two given curves A, B satisfy Bezout's Theorem over $\mathbb{P}\mathbf{m}(\theta)^2$.

As most of the algorithm presented in the previous chapter doesn't use the fact that the field is algebraically closed, it is sufficient to look at the case of intersecting curves A, B with $a \in \mathbf{m}[x, y, z], b \in \mathbf{m}[y, z]$. Assuming, without loss of generality, that $b(y, z)$ is monic, we have a factorization

$$b(y, z) = \prod_i b_i(y, z)^{k_i}$$

where each $b_i(y, z)$ is irreducible over \mathbf{m} . We thus form $\mathbf{m}(\beta_i)$, the smallest extension of \mathbf{m} containing all the roots of $b_i(y, z)$. Intersecting each factor with $a(x, y, z)$, we obtain $a(x, y = \beta_i z, z) = \prod_j a_{i,j}(x, z; \beta_i) \in \mathbf{m}(\beta_i)[x, z]$ and thus get intersection points $P_{i,j} = (\alpha_{i,j}, \beta_i, 1)$, where $\alpha_{i,j}$ are the roots of $a_{i,j}(y, z; \beta_i)$ over $\mathbf{m}(\beta_i, \alpha_{i,j})$, the smallest extension over which $a_{i,j}(y, z; \beta_i)$ factors completely.

A problem arises when we look back at the construction of the intersection cycle $A.B$. Since (in the simplest case) it is the difference of the the intersection cycles $B.D$ and $B.R$, points could occur in different representations in the two cycles, as the following example illustrates:

Let $A : x^4 = 0$, $B : (y^4 + z^4)x^4 + (xz^2 - yz^2 + y^3)(x^2 - 2z^2)z^3 = 0$ be two algebraic curves over $\mathbb{P}\mathbb{Q}^2$. Using the Euclidean algorithm, we may write $da = bq + r$ with

$$\begin{aligned} d(y, z) &= (y^4 + z^4) \\ r(x, y, z) &= -z^3(x^2 - 2z^2)(xz^2 - yz^2 + y^3). \end{aligned}$$

Using properties of intersection multiplicities (see Theorem 1) applied to intersection cycles, we see that $B.R = B'.R$ with $B' : d(y, z)x^4 = 0$ and $B.D = R.D$. Thus, the intersection cycle $B.R$ contains the intersection of the curves

$$S_1 : y^4 + z^4 = 0, \quad S_2 : xz^2 - yz^2 + y^3 = 0$$

which in turn contains the point $P = (\sqrt{2}, \frac{1}{\sqrt{2}}(1+i), 1)$, expressed as $(\beta_1 - \beta_1^3, \beta_1, 1)$ where $\beta_1 = \frac{1}{\sqrt{2}}(1+i)$ is a root of $y^4 + 1$.

The intersection cycle $B.M$, on the other hand, contains the intersection points of the curves $s_1(y, z)$ from above with the curve $T : x^2 - 2z^2 = 0$ which contains the point $P' = (\sqrt{2}, \frac{1}{\sqrt{2}}(1+i), 1)$, this time expressed as $(\alpha_1, \beta_1, 1)$ where $\alpha_1 = \sqrt{2}$ is the first root of $x^2 - 2$ and β_1 is as above.

It is thus clear that we need a canonical way of expressing the intersection points of algebraic curves in order to compute the intersection points using extension fields. We start our construction with the following definition:

Definition 2. Let $n \in \mathbb{N}$, $\mathbf{a} = (\alpha_1, \dots, \alpha_n)$, $\mathbf{b} = (\beta_1, \dots, \beta_n)$ be n -tuples of algebraic elements (from now on referred to as “algebraic n -tuples”) over a field \mathbf{m} . We define an equivalence relation of the set of algebraic n -tuples by $\mathbf{a} \simeq \mathbf{b}$ if there exists an automorphism $\sigma \in \text{Aut}(\mathbf{m}(\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_n))$ such that

$$\sigma \mathbf{a} = (\sigma \alpha_1, \dots, \sigma \alpha_n) = (\beta_1, \dots, \beta_n).$$

It is clear that P and P' , defined above, are equivalent using this definition, as $\mathbb{Q}(\sqrt{2}, \beta_1) = \mathbb{Q}(\beta_1)$. If the n -tuples further represent points on an algebraic curve with coefficients in \mathbf{m} , it is further clear that all conjugate n -tuples also lie on the curve.

Given this equivalence relation, it is further convenient to have a canonical way of representing an equivalence class. As we are dealing with roots of polynomials, a natural way is to represent elements using their minimal polynomials.

As the extension $\mathbf{m}(\alpha_1, \dots, \alpha_n)$ is finite and only has finitely many intermediate subfields, the Primitive Element Theorem (see [1] for example) tells us that there exists a γ such that $\mathbf{m}(\alpha_1, \dots, \alpha_n) = \mathbf{m}(\gamma)$. Now, let $N = [\mathbf{m}(\gamma) : \mathbf{m}]$ and let $c_0, c_1, \dots, c_{N-1} \in \mathbf{m}$ be unknown. Fix some α_i and consider now the equation

$$c_0 + c_1 \gamma + \dots + c_{N-1} \gamma^{N-1} = \alpha_i$$

By applying automorphisms in $\text{Aut}(\mathbf{m}(\gamma))$, one obtains a system of at most N equations, expressing the conjugates $\alpha_{i,j}, j = 1 \dots d_i = \partial \alpha_i$ of α_i , in terms of the polynomial $p(x) = \sum_{i=0}^{N-1} c_i x^i$ evaluated at conjugates of γ . This can be written as

$$\mathbf{\Gamma} \mathbf{c} = \mathbf{a}$$

Here, $\mathbf{\Gamma}$ is the Vandermonde Matrix with entries $\mathbf{\Gamma}_{i,j} = \gamma_i^j$, where γ_i denotes the conjugates of γ , $\mathbf{c} = (c_0, \dots, c_n)$, and $\mathbf{a} = (\alpha_{i,1}, \dots, \alpha_{i,d_i}, \dots, \alpha_{i,1}, \dots, \alpha_{i,d_i})$ contains the conjugates of α_i repeated $[\mathbf{m}(\gamma) : \mathbf{m}(\alpha_i)]$ times.

Upon inverting $\mathbf{\Gamma}$ (see Section 3), one obtains a polynomial expression $p_i(\gamma) = \alpha_i$. Thus, we can represent $(\alpha_1, \dots, \alpha_n)$, together with all conjugate n -tuples, as

$$[\mathbf{a}] = [(p_1(x), \dots, p_n(x)), q_\gamma(x)]$$

where $q_\gamma(x)$ is the minimal polynomial of γ over \mathbf{m} . We call this the *polynomial representation* of the equivalence class of the algebraic n -tuple $(\alpha_1, \dots, \alpha_n)$. In the case of P and P' , we get the polynomial representation $[(x - x^3, x), x^4 + 1]$ for both points.

In cases where the polynomial representations of two equivalence classes cannot be determined to be the same by simply comparing the polynomials

directly, we can construct necessary and sufficient conditions. In the following, for two polynomials $f, g \in \mathbf{m}[x, y]$, we let $\text{Res}_x(f, g)$ and $\text{Res}_y(f, g)$ denote the x - and y -Resultants, respectively.

Theorem 3. *Let $[\mathbf{a}] = [(p_1(x), \dots, p_n(x)), q_\theta(x)]$, $[\mathbf{b}] = [(r_1(x), \dots, r_n(x)), q_\delta(x)]$ be equivalence classes of algebraic n -tuples of algebraic elements in polynomial representation. Then*

$$[\mathbf{a}] = [\mathbf{b}] \iff H(t_1, \dots, t_n) = 0 \text{ for all } t_i \in \mathbf{m}$$

where

$$H(t_1, \dots, t_n) = \text{Res}_y \left(\text{Res}_x \left(\sum_{j=1}^n t_j (p_j(y) - r_j(x)), q_\theta(x) \right), q_\delta(y) \right)$$

Proof. Denote by θ_j any conjugate of θ and by δ_k a conjugate of δ . Then for $[\mathbf{a}] = [\mathbf{b}]$, we need

$$\begin{aligned} \text{For all } i : 1 \leq i \leq n, \text{ there exist } j, k \text{ s.t. } & p_i(\theta_j) = r_i(\delta_k) \\ & \iff p_i(\theta_j) - r_i(\delta_k) = 0 \\ & \iff \sum_{i=1}^n t_i (p_i(\theta_j) - r_i(\delta_k)) = 0 \quad \forall t_i \in \mathbf{m} \\ & \iff \text{Res}_x \left(\sum_{i=1}^n t_i (p_i(x) - r_i(\delta_k)), q_\theta(x) \right) = 0 \quad \forall t_i \in \mathbf{m} \\ \iff \text{Res}_y \left(\text{Res}_x \left(\sum_{i=1}^n t_i (p_i(x) - r_i(y)), q_\theta(x) \right), q_\delta(y) \right) & = 0 \quad \forall t_i \in \mathbf{m} \end{aligned}$$

□

By expressing points defined over extension fields on algebraic curves via the polynomial representation of their equivalence classes, we obtain a simple way of comparing points across different representations.

If we are given that $P \simeq Q$ for two common points on the curves A, B , we have $m(P; A, B) = m(Q; A, B)$ (as can be seen by applying the automorphism σ to the polynomials defining the curves). Thus, given two algebraic curves A, B , the intersection cycle $A.B$ will thus look like

$$A.B = \sum_{k=1}^K P_k (\partial \gamma_k \cdot m(P_k; A, B)) \oplus \sum_{l=1}^L P_l (\partial \delta_l \cdot m(P_l; A, B))$$

where

$$\begin{aligned} [P_k] &= [(p_{\alpha_k}(x), p_{\beta_k}(x), 1), q_{\gamma_k}(x)] \\ [P_l] &= [(x, 1, 0), q_{\delta_l}(x)]. \end{aligned}$$

Here $q_\omega(x)$ represents the minimal polynomial of ω over \mathbf{m} . Consider now the element

$$\theta = \gamma_1 + \sum_{k=2}^K c_k \gamma_k + \sum_{l=1}^L d_l \delta_l$$

where the $c_k, d_i \in \mathbf{m}$ are chosen such that $\sigma\theta \neq \theta$ for any $\sigma \in \text{Aut}(\mathbf{m}(\gamma_1, \dots, \gamma_K, \delta_1, \dots, \delta_L))$. Then it easily checked that θ is indeed the primitive element for the extension.

Given this θ and its minimal polynomial $q_\theta(x)$ over \mathbf{m} , we can rewrite the polynomial representations of the points above simply as

$$\begin{aligned} [P_k] &= [(\widetilde{p_{\alpha_k}}(x), \widetilde{p_{\beta_k}}(x), 1)] \\ [P_l] &= [(\widetilde{p_{\delta_l}}(x)1, 0)] \end{aligned}$$

where

$$\begin{aligned} p_{\alpha_k}(p_{\gamma_k}(x)) &= \widetilde{p_{\alpha_k}}(x) \pmod{q_\theta(x)} \\ p_{\beta_k}(p_{\gamma_k}(x)) &= \widetilde{p_{\beta_k}}(x) \pmod{q_\theta(x)} \\ p_{\delta_l}(x) &= \widetilde{p_{\delta_l}}(x) \pmod{q_\theta(x)} \end{aligned} \tag{12}$$

and $p_{\gamma_k}(\theta) = \gamma_k, p_{\delta_l}(\theta) = \delta_l$. This way of representing the points allows us to read off the primitive element of the smallest extension over which Bezout's Theorem holds for the given algebraic curves and expresses all points over that extension:

Theorem 4. *Let A, B be algebraic curves over a field \mathbf{m} . Then the extension $\mathbf{m}(\theta)$, obtained above, is the smallest extension of \mathbf{m} such that*

$$\sum_{P \in \mathbb{P}\mathbf{m}(\theta)^2} m(P; A, B) = \partial A \partial B$$

Proof. That all common points indeed lie in $\mathbb{P}\mathbf{m}(\theta)^2$ is clear from the explicit expression of their coordinates as polynomials in θ in (12).

As $\mathbf{m}(\theta) = \mathbf{m}(\gamma_1, \dots, \gamma_M, \delta_1, \dots, \delta_L)$ is the smallest field containing $\mathbf{m}(\gamma_k), \mathbf{m}(\delta_l)$ for $1 \leq k \leq K, 1 \leq l \leq L$ and $\mathbf{m}(\gamma_k) = \mathbf{m}(\alpha_{1,k}, \dots, \alpha_{n_k,k}, \beta_{1,k}, \dots, \beta_{m_k,k})$ is the smallest field containing $\mathbf{m}(\alpha_{k,i}), \mathbf{m}(\beta_{k,j}), 1 \leq i \leq n_k = \partial\beta_k, 1 \leq j \leq m_k = \partial\alpha_k$, the minimality of $\mathbf{m}(\theta)$ follows. \square

3 Inverting the Vandermonde Matrix

Let, as in the previous section, $\alpha_1, \dots, \alpha_d$ be a full set of conjugates of an algebraic element α over a field \mathbf{m} and $\mathbf{m}(\gamma)$ be an extension of $\mathbf{m}(\alpha)$ and let $[\mathbf{m}(\alpha) : \mathbf{m}] = d, [\mathbf{m}(\gamma) : \mathbf{m}] = N$. Again, consider the matrix equation

$$\mathbf{a} = \Gamma \mathbf{c}$$

with $\mathbf{a} = (\underbrace{\alpha_1, \dots, \alpha_d, \dots, \alpha_1, \dots, \alpha_d}_{N/d \text{ times}}), \mathbf{c} = (c_0, \dots, c_{N-1})$ and

$$\mathbf{\Gamma} = \begin{bmatrix} 1 & \gamma_1 & \gamma_1^2 & \cdots & \gamma_1^{N-1} \\ 1 & \gamma_2 & \gamma_2^2 & \cdots & \gamma_2^{N-1} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & \gamma_N & \gamma_N^2 & \cdots & \gamma_N^{N-1} \end{bmatrix}$$

We are interested in finding the inverse of $\mathbf{\Gamma}$ explicitly. Let $\mathbf{\Gamma}^{-1} = (g)_{ij}$. In multiplying $\mathbf{\Gamma}$ by its inverse on the right, we thus obtain the following equations:

$$a_{ij} = \sum_{k=1}^N g_{kj} \gamma_i^{k-1} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases}$$

Now, let $p(x)$ be the minimal polynomial of γ and $p'(x)$ its derivative. Since $p(x)$ has no repeated roots, we can find $a(x), b(x) \in \mathbf{m}[x]$ such that

$$a(x)p'(x) + b(x)p(x) = 1$$

Also, we can find $q(x, \gamma)$ and $r(\gamma)$ such that

$$\frac{p(x)}{x - \gamma} = q(x, \gamma) + \frac{r(\gamma)}{x - \gamma}$$

Now, let us define the function

$$H(x, \gamma) = a(x)q(x, \gamma)$$

We have:

Theorem 5. For γ_i, γ_j roots of $p(x)$,

$$H(\gamma_i, \gamma_j) = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases}$$

Proof. Note that, $1 = a(\gamma_i)p'(\gamma_i) + b(\gamma_i)p(\gamma_i) = a(\gamma_i)p'(\gamma_i)$ for $i = 1 \dots N$ so that

$$a(\gamma_i) = \frac{1}{p'(\gamma_i)}.$$

Also, for $j = 1 \dots N$, we have that

$$\frac{p(x)}{x - \gamma_j} = q(x, \gamma_j)$$

so that $r(\gamma_j) = 0$ (which also implies that $p(x) \mid r(x)$).

All together, we get that

$$H(\gamma_i, \gamma_j) = a(\gamma_i)q(\gamma_i, \gamma_j) = \frac{p(\gamma_i)}{(\gamma_i - \gamma_j)p'(\gamma_i)}.$$

If $i \neq j$, then this is well-defined and equals 0. Otherwise, consider the limit

$$\lim_{x \rightarrow \gamma_j} \frac{p(x)}{(x - \gamma_j)p'(x)} = \lim_{x \rightarrow \gamma_j} \frac{p'(x)}{p'(x)} = 1$$

by L'Hopital's Rule. \square

Therefore, we may write

$$a_{ij} = \sum_{k=1}^N g_k(\gamma_j) \gamma_i^{k-1} = H(\gamma_i, \gamma_j). \quad (13)$$

Degree considerations from the previous theorem show that γ_j actually also must occur up to degree $N - 1$, so that we actually get

$$g_k(\gamma_j) = \sum_{s=1}^N h_{ks} \gamma_j^{s-1}.$$

By applying an automorphism in $\text{Aut}(\mathbf{m}(\gamma))$ to (13), we see the following:

Lemma 2. *In the expression*

$$\sum_{k=1}^N g_{kj} \gamma_i^{k-1} = \sum_{k=1}^N \sum_{l=1}^N h_{kjl} \gamma_j^{l-1} \gamma_i^{k-1} = H(\gamma_i, \gamma_j)$$

the coefficients h_{kjl} do not depend on the choice of γ_i and γ_j at all. We actually have

$$\sum_{k=1}^N g_{kj} \gamma_i^{k-1} = \sum_{k=1}^N \sum_{l=1}^N h_{kl} \gamma_j^{l-1} \gamma_i^{k-1}$$

We can read off these coefficients h_{kl} by comparing coefficients of γ_i and γ_j on both sides, while the $g_{kj}(\gamma_j)$ give the entries of $\mathbf{\Gamma}^{-1}$.

Given $\mathbf{\Gamma}^{-1}$ (and remembering that square-matrix inverses are always two-sided) we can then use it to solve the equation via

$$\mathbf{\Gamma}^{-1} \mathbf{a} = \mathbf{c}.$$

This gives an expression for c_i :

$$c_i = \sum_{r=1}^N g_{ir}(\gamma_r) \alpha_r = \sum_{r=1}^N \sum_{k=1}^N h_{rk} \gamma_r^{k-1} \alpha_r$$

If we now let β be such that $\gamma = \alpha + c\beta$ for some $c \in \mathbf{m}$, we get

$$\begin{aligned} c_i &= \sum_{k=1}^n h_{rk} \sum_{l=1}^{\partial \alpha} \sum_{m=1}^{\partial \beta} (\alpha_l + c\beta_m)^{k-1} \alpha_l \\ &= \sum_{k=1}^n h_{rk} \sum_{l=1}^{\partial \alpha} \sum_{m=1}^{\partial \beta} \sum_{s=1}^{k-1} \binom{k-1}{s} \alpha_l^{k-1-s} c^s \beta_m^s \alpha_l \\ &= \sum_{k=1}^n h_{rk} \sum_{s=1}^{k-1} \binom{k-1}{s} c^s \sum_{l=1}^{\partial \alpha} \alpha_l^{k-s} \sum_{m=1}^{\partial \beta} \beta_m^s \end{aligned}$$

The two sums involving powers of α and β can be evaluated using Newton's Identities.

References

- [1] DUMMIT, D. S., AND FOOTE, R. M. *Abstract Algebra*, third ed. John Wiley & Sons, Inc., 2004.
- [2] FULTON, W. *Algebraic Curves*. W.A. Benjamin, Inc., New York, NY, 1969.