Simple Field Extensions of Small Degree via Intersections of Plane Curves

Jialu Wang

Motivation

Inspired by a question posed at the end of [1], I was led to the following general viewpoint. Since intersection points of plane curves correspond to solutions of polynomial systems, it is natural to ask whether roots of a given univariate polynomial $p(x) \in F[x]$ can be realised as x–coordinates of intersection points of two plane curves defined over F.

A simple way to encode $p(x)$ is to fix an curve $y = x^m$, and then choose a second curve $g(x, y) = 0$ so that, after substitution, one obtains $g(x, x^m) = p(x)$. This observation motivates the study of which simple field extensions can be realised via intersections of plane curves.

Definition. Let F be a field and let $m, n \in \mathbb{Z}_{>0}$. We say that a finite field extension $F \subset K$ *can be obtained by the intersection of two plane curves of degrees m and n* if there exist polynomials $f, g \in F[x, y]$ with $\deg f = m$, $\deg g = n$, together with an F-algebra surjection

$$\varphi : \ F[x, y]/(f, g) \twoheadrightarrow K.$$

Example. Let $F = \mathbb{Q}$ and put $f := y - x^2$, $g := y^2 + 3x + 1 \in \mathbb{Q}[x, y]$. Define $\mathbb{Q}$-algebras

$$\begin{aligned} \varphi :\ & \mathbb{Q}[x, y]/(f, g) \longrightarrow \mathbb{Q}[z]/(z^4 + 3z + 1), \qquad \overline{x} \mapsto \overline{z},\ \ \overline{y} \mapsto \overline{z}^{\,2}, \\ \psi :\ & \mathbb{Q}[z]/(z^4 + 3z + 1) \longrightarrow \mathbb{Q}[x, y]/(f, g), \qquad \overline{z} \mapsto \overline{x}. \end{aligned}$$

These maps are well defined since $\overline{y}-\overline{x}^2 \mapsto 0$, $\overline{y}^{\,2}+3\overline{x}+1 \mapsto 0$ under φ, and $\overline{z}^{\,4}+3\overline{z}+1 \mapsto 0$ under ψ. Moreover, $\psi\circ\varphi$ and $\varphi\circ\psi$ act as the identity on the generators, hence $\mathbb{Q}[x, y]/(y-x^2,\ y^2+3x+1) \cong \mathbb{Q}[z]/(z^4 + 3z + 1)$.

Lemma. Let $m, n \in \mathbb{Z}_{>0}$ and let F be a field. For any finite field extension $F \subset K$ with $[K : F] \leq mn$ the following statements are equivalent:

(P) The field extension $F \subset K$ is simple; that is, there exists $\alpha \in K$ such that $K = F[\alpha]$.

(Q) There exists a polynomial $f(x) \in F[x]$ of degree exactly mn and an F-algebra surjection

$$F[x]/(f) \twoheadrightarrow K.$$

Proof. (Q)⇒(P). Assume (Q) and let $F \subset K$ be finite with $[K : F] \leq mn$. Choose $f \in F[x]$ with $\deg f = mn$ and an F-algebra surjection $\pi : F[x]/(f) \twoheadrightarrow K$. Set $\alpha := \pi(\overline{x}) \in K$. Since π is F-algebra, the image of π is $F[\alpha]$. So the surjection gives $K = F[\alpha]$, proving (P).

(P)⇒(Q). Assume (P) and let $F \subset K$ be finite with $d := [K : F] \leq mn$. By (P), there exists $\alpha \in K$ with $K = F[\alpha]$. Let $m_\alpha(x)$ be the minimal polynomial of α over F. Define $f(x) := m_\alpha(x)\, x^{mn-d} \in F[x]$, so that $\deg f = mn$. Define $\pi : F[x]/(f) \to F[\alpha]$ given by $\overline{x} \mapsto \alpha$. Note that $f(\alpha) = 0$, so π is well-defined. To prove that π is surjective, let y be an arbitrary element in $F[\alpha]$. By definition of $F[\alpha]$, there exists a polynomial $p(x) \in F[x]$ such that $y = p(\alpha)$. Then $y = \pi(\overline{p(x)})$, so every element in $F[\alpha]$ lies in the image of π, it follows that π is surjective. This is exactly (Q).

Hence (P) and (Q) are equivalent. □

Theorem. *Let F be a field and let $m, n \in \{1,2,3\}$. Every simple field extension $F \subset K$ with $[K:F] \leq mn$ can be obtained by the intersection of two plane curves of degrees m and n.*

Remark. For $m=1$ and $n=2$, this theorem follows from the fact that every quadratic field extension is obtained by intersecting a line and a circle. (see Artin)

Proof. Let m and n be as in the statement and let $F \subset K$ be a simple extension with $[K:F] \leq mn$. Let $f(x,y) = y - x^m$. We show that there exists a polynomial $g(x,y)$ and a surjection $F[x,y]/(f(x,y), g(x,y)) \twoheadrightarrow K$. Note that we have an isomorphism

$$\sigma : F[x,y]/(f(x,y), g(x,y)) \to F[x]/(g(x,x^m))$$

given by $x \mapsto x$ and $y \mapsto x^m$. Given K, we find $g(x,y)$ and a surjection $F[x]/(g(x,x^m)) \twoheadrightarrow K$. By the lemma, there exists a polynomial $h(x) \in F[x]$ of degree mn and an F-algebra surjection

$$\pi : \ F[x]/(h) \twoheadrightarrow K.$$

We argue by cases on m and n; in each case we construct a polynomial $g(x,y)$ whose coefficients involve the a_i, together with a family of surjections

$$\{\varphi_i\} : \ F[x]/\big(g(x,x^m)\big) \twoheadrightarrow F[x]/\big(a_0 + a_1 x + \cdots + a_{mn}x^{mn}\big).$$

Since $h(x)$ determines the coefficients $\{a_i\}$, there must exist explicit $g(x,y)$ such that the image of φ_i is $F[x]/(h)$; therefore $\pi \circ \varphi_i \circ \sigma$ gives an F-algebra surjection $F[x,y]/(f,g) \twoheadrightarrow K$.

By symmetry, assume $m \leq n$ without loss of generality.

Case 1 ($m=1$): When $n=3$, define F-algebra maps

$$\begin{aligned}
\varphi_1 &: \ F[x,y]/(y-x, a+bx+cx^2+dx^3) \longrightarrow F[z]/(a+bz+cz^2+dz^3), \quad \overline{x} \mapsto \overline{z},\ \overline{y} \mapsto \overline{z} \\
\psi_1 &: \ F[z]/(a+bz+cz^2+dz^3) \longrightarrow F[x,y]/(y-x, a+bx+cx^2+dx^3), \quad \overline{z} \mapsto \overline{x}.
\end{aligned}$$

Then φ_1 is a well-defined F-algebra isomorphism. Let $c=d=0$, we get case $m=1, n=1$. And $d=0$ gives case $m=1, n=2$.

Case 2 ($m=2, n=2$): Define F-algebra maps

$$\begin{aligned}
\varphi_2 &: \ F[x,y]/(y-x^2,\ a+bx+cy+dxy+ey^2) \longrightarrow F[z]/(a+bz+cz^2+dz^3+ez^4), \quad \overline{x} \mapsto \overline{z},\ \overline{y} \mapsto \overline{z}^2 \\
\psi_2 &: \ F[z]/(a+bz+cz^2+dz^3+ez^4) \longrightarrow F[x,y]/(y-x^2, a+bx+cy+dxy+ey^2), \quad \overline{z} \mapsto \overline{x}.
\end{aligned}$$

Then φ_2 is a well-defined F-algebra isomorphism.

Case 3 ($m=2, n=3$): Define the F-algebra map

$$\begin{aligned}
\varphi_3 : F[x,y]/&(y-x^2, a+bx+cy+dxy+ey^2+hxy^2+ky^3) \\
&\to F[z]/(a+bz+cz^2+dz^3+ez^4+hz^5+kz^6), \quad \overline{x} \mapsto \overline{z},\ \overline{y} \mapsto \overline{z}^2 \\
\psi_3 : F[z]/&(a+bz+cz^2+dz^3+ez^4+hz^5+kz^6) \\
&\to F[x,y]/(y-x^2, a+bx+cy+dxy+ey^2+hxy^2+ky^3), \quad \overline{z} \mapsto \overline{x}
\end{aligned}$$

Then φ_3 is a well-defined F-algebra isomorphism.

Case 4 ($m=3, n=3$): Note that intersecting a general cubic with $y=x^3$ misses the x^8-term; by the primitive element theorem we may change variables. Define the F-algebra map

$$\begin{aligned}
\tilde{\varphi}_4 : \ F[x,y]/&\big(y-x^3,\ a+bx+dy+cx^2+exy+hx^2y+iy^2+jxy^2+ky^3\big) \\
&\to F[t]/\big(a+bt+ct^2+dt^3+et^4+ht^5+it^6+jt^7+kt^9\big), \quad \overline{x} \mapsto \overline{t},\ \overline{y} \mapsto \overline{t}^3 \\
\tilde{\psi}_4 : \ F[t]/&\big(a+bt+ct^2+dt^3+et^4+ht^5+it^6+jt^7+kt^9\big) \\
&\to F[x,y]/\big(y-x^3,\ a+bx+dy+cx^2+exy+hx^2y+iy^2+jxy^2+ky^3\big), \quad \overline{t} \mapsto \overline{x}
\end{aligned}$$

Then $\tilde{\varphi}_4$ is a well-defined F-algebra isomorphism.

(i) When $k \neq 0$, observe that $a + bt + ct^2 + dt^3 + et^4 + ht^5 + it^6 + jt^7 + kt^9 = a_9\Big(t - \frac{a_8}{9a_9}\Big)^9 + a_8\Big(t - \frac{a_8}{9a_9}\Big)^8 + \cdots + a_0$ for some coefficients $a_9, a_8, \ldots, a_0$ with $a_9 \neq 0$. Then the F-algebra

$$T:\ F[t]/\big(a_9(t-\tfrac{a_8}{9a_9})^9+a_8(t-\tfrac{a_8}{9a_9})^8+\cdots+a_0\big) \to F[z]/(a_9z^9+a_8z^8+a_7z^7+\cdots+a_0), \quad \bar{t}-\tfrac{a_8}{9a_9} \mapsto \bar{z},$$

is an isomorphism.

(ii) When $k = 0$, one has $a+bt+ct^2+dt^3+et^4+ht^5+it^6+jt^7+kt^9 = (t-\frac{b_7}{b_8})\big(b_8t^8+b_7t^7+\cdots+b_0\big)$, for some $b_8, b_7, \ldots, b_0$ with $b_8 \neq 0$ hence the F-algebra

$$S:\ F[t]/\big(t - \tfrac{b_7}{b_8}\big)\big(b_8t^8 + b_7t^7 + \cdots + b_0\big) \longrightarrow F[z]/(b_8z^8 + b_7z^7 + \cdots + b_0), \quad \bar{t} \mapsto \bar{z}$$

is a surjection.

Therefore, $\varphi_4 := T \circ \tilde{\varphi}_4$ is a F-algebra isomorphism when $k \neq 0$, and $\varphi_4' := S \circ \tilde{\varphi}_4$ is a F-algebra surjection when $k = 0$. $\square$

References

[1] Carlos R. Videla. On points constructible from conics. *The Mathematical Intelligencer*, 19(2):53–57, 1997.