$i \in \{m+1, \ldots, n\}$ can be written as a K-linear combination of the elements of B. Thus it is given by a polynomial expression of the residue classes of $x_1, \ldots, x_m$.

Now we consider the polynomial ring $P' = K[x_1, \ldots, x_m]$ and the ideal I' in P' obtained by substituting $x_{m+1}, \ldots, x_n$ by their expressions in $x_1, \ldots, x_m$. We have $P'/I' \cong P/I$ and the residue classes of $(T_1, \ldots, T_d)$ are a K-basis of P'/I'. Hence we can run Algorithm 6.2.20 for this setting and compute the first m coordinates of every point in $\mathscr{Z}_K(I)$. Finally, for $i = m+1, \ldots, n$, we use the expressions of x_i in terms of $x_1, \ldots, x_m$ to compute the remaining coordinates of the points in $\mathscr{Z}_K(I)$.

In the next example we show how one can apply this remark in practice.

Example 6.2.24 Let $K = \mathbb{Q}$, let $P = K[x_1, x_2]$, and let I be the ideal of P defined as $I = \langle x_1 - x_2^2 + x_2 - 1, x_2^3 - 8\rangle$. If we calculate the reduced `DegRevLex`-Gröbner basis of I, we get $G = (x_1^2 - 3x_1 - 9x_2 + 18, x_1x_2 + x_1 - 9, x_2^2 - x_1 - x_2 + 1)$. Hence $B = (1, x_1, x_2)$ is a K-basis of $R = P/I$ which satisfies the hypothesis of Algorithm 6.2.20.

On the other hand, the reduced `Lex`-Gröbner basis of I is $G' = (x_1 - x_2^2 + x_2 - 1, x_2^3 - 8)$. Therefore $B' = (1, x_2, x_2^2)$ is also a K-basis of $R = P/I$. The indeterminate x_1 is missing, but we have the equality $x_1 + I = x_2^2 - x_2 + 1 + I$ in R. We run Algorithm 6.2.20 with $P' = K[x_2]$ and $I' = \langle x_2^3 - 8\rangle$ and get the K-rational zero (a_2) of I', where $a_2 = 2$. Now we calculate the corresponding x_1-value from $a_1 = a_2^2 - a_2 + 1 = 3$ and conclude that $\mathscr{Z}_K(I)$ consists of one point (a_1, a_2), namely the point $(a_1, a_2) = (2, 3)$.

6.3 Solving Polynomial Systems over Finite Fields

I didn't say that I didn't say it.
I said that I didn't say that I said it.
I want to make that very clear.
(George Romney)

In this section we start to look for solutions of polynomial systems which aren't there. Are we looking for a black cat in a dark cellar which isn't there? Not if we are working over a finite field. In this case we can easily extend the field to a larger finite field and find the solutions there. In order to make this process very clear, we have to tread carefully.

As a first step, let us reconsider the meaning of the symbol $\mathbb{F}_q$ for a finite field with q elements. Here $q = p^e$ is a power of a prime number p and $e > 0$. But how exactly do the elements of $\mathbb{F}_q$ look like when $e > 1$? Didn't we say at the beginning of Sect. 5.2 that $\mathbb{F}_q$ is an isomorphism class? So, in order to construct a field

in which we can find our desired solutions, we have to construct a *representative* of $\mathbb{F}_q$, i.e., a presentation using generators and relations. Any two representatives are isomorphic, because every field with q elements is a splitting field of the polynomial $z^q - z$ in $\mathbb{F}_p[z]$ (see Definition 6.3.14), and it is known that splitting fields are unique up to isomorphism (see for instance [21], Proposition 2.7). If we are actually given two representatives of $\mathbb{F}_q$, how do we find such an isomorphism? Can we calculate all isomorphisms?

The first subsection deals with this question. Since we are assuming that the polynomial system is given over a finite field K having q elements, we are looking for finite extension fields of K. Thus, in Theorem 6.3.4, we compute all K-algebra isomorphisms between finite extension fields of K. An immediate application is then the possibility to determine all K-automorphisms of a finite extension field L of K. Recall that the set of these K-automorphisms is the Galois group of L/K and that it is known that this is a cyclic group of order $\dim_K(L)$ which is generated by the q-Frobenius automorphism of L.

How can we apply these algorithms to solving polynomial systems? First of all, for a polynomial system defined by polynomials $f_1, \ldots, f_m \in K[x_1, \ldots, x_n]$, we can compute the maximal components of the ideal $I = \langle f_1, \ldots, f_m \rangle$ using the methods presented in Chap. 5. Hence the problem of solving the given system is reduced to the problem of solving a polynomial system whose associated ideal is a maximal ideal $\mathfrak{M}$ of $P = K[x_1, \ldots, x_n]$.

The next step is the central idea: cloning! Since $L = P/\mathfrak{M}$ is an extension field of K, should we try to find the solutions there? Not exactly. It is better to produce a *clone* L' of this field and find the coordinates of the zeros of the ideal $\mathfrak{M}$ in the clone $L' = P'/\mathfrak{M}'$, where $P' = K[y_1, \ldots, y_n]$. Then we know already one solution, namely $(\bar{y}_1, \ldots, \bar{y}_n)$. And now the *power of the Frobenius* automorphism kicks in: all other solutions are nothing but coordinatewise powers of this given solution. There is one disadvantage that could spoil the fun, namely that we may have to bring high powers to their normal form. For this task we offer a good approach via Algorithm 6.3.16.

A second way of using an isomorphism $P/\mathfrak{M} \cong L'$ is studied in the third subsection, where we assume that we know a univariate representation of L', for instance, because L' is represented in our computer algebra system via a built-in polynomial $f(y)$ such that $L' = K[y]/\langle f(y) \rangle$. Finally, the last subsection suggests the iterative approach to split one generator of $\mathfrak{M}$ at a time. This may be a viable alternative if the K-vector space dimension of $P/\mathfrak{M}$ is very large. The iterative approach will also turn out to be useful for solving polynomial systems over $\mathbb{Q}$ in the last section.

As we said before, and we never repeat ourselves, the algorithms in this section are rather tricky. We want to make it very clear that we tried to make them very clear. Don't say that we didn't say it!

Drawing on my fine command of language,
I said nothing.

6.3.A Computing Isomorphisms of Finite Fields

I have just changed my diet.
The cookies are now to the left of the laptop.

In the following we approach the problem of solving polynomial systems over a finite field from a rather general point of view. As we mentioned above, to find the solutions we may have to extend the base field and to perform certain calculations over the extended field. How should we represent this field extension?

Nowadays many computer algebra systems have efficient implementations of finite fields available. Can we make our algorithms somehow feed on their speed? Clearly, the representative of $\mathbb{F}_q$ in your favourite computer algebra system may differ from the representative obtained from the polynomial system. Hence we have to change the representative. But how do you do that? Is it as easy as putting the cookie jar on the other side of the laptop? Or do we have to keep some cookies inside the computer?

Let us do a hop, step and jump. The first part of this subsection provides a quick hop through some material about isomorphisms of affine algebras which extends [15], Sect. 3.6. Then we step into the calculation of all $\mathbb{F}_q$-isomorphisms between two representatives of $\mathbb{F}_{q^d}$. This includes the calculation of all $\mathbb{F}_p$-automorphisms of $\mathbb{F}_q$. Finally, a third jump brings us to a small cookie reward, namely an algorithm for computing the primitive elements of an extension of a finite field which have the same minimal polynomial.

Come to the dark side, we have cookies!

In the following we let K be a field, let $P = K[x_1, \ldots, x_n]$, let I be an ideal in P, let $P' = K[y_1, \ldots, y_m]$ be another polynomial ring, let I' be an ideal in P', and let $\varphi : P/I \longrightarrow P'/I'$ be a K-algebra homomorphism. Our goal is to extend some results of [15], Sect. 3.6. In particular, we shall characterize when φ is an isomorphism. The next lemma provides some background for maps between polynomial rings. In the following arguments we use [15], Sect. 3.6. We note that J has a different meaning here.

Lemma 6.3.1 *In the above setting, assume that $\Phi : P \longrightarrow P'$ is the K-algebra homomorphism which is given by $\Phi(x_i) = f_i$ with $f_i \in P'$ for $i = 1, \ldots, n$. Let Q be the ring $Q = K[x_1, \ldots, x_n, y_1, \ldots, y_m]$ and J the ideal $J = \langle x_1 - f_1, \ldots, x_n - f_n \rangle$ in Q.*

(a) *The map Φ induces a K-algebra homomorphism $\varphi : P/I \longrightarrow P'/I'$ if and only if $IQ \subseteq I'Q + J$.*

For the following claims, assume that the map Φ induces a K-algebra homomorphism $\varphi : P/I \longrightarrow P'/I'$.

(b) *The map $\varphi : P/I \longrightarrow P'/I'$ is injective if and only if we have $I = (I'Q + J) \cap P$.*

(c) *The map* $\varphi : P/I \longrightarrow P'/I'$ *is surjective if and only if there exist polynomials* $g_1, \ldots, g_m \in P$ *such that for the ideal* $J' = \langle y_1 - g_1, \ldots, y_m - g_m \rangle$ *in* Q *we have* $J' \subseteq I'Q + J$. *In this case we have* $\varphi(\bar{g}_i) = \bar{y}_i$ *for* $i = 1, \ldots, m$.

(d) *Assume that the map* $\varphi : P/I \longrightarrow P'/I'$ *is surjective. Let* $g_1, \ldots, g_m \in P$ *be polynomials such that* $\varphi(\bar{g}_i) = \bar{y}_i$ *for* $i = 1, \ldots, m$, *and let* $\Psi : P' \longrightarrow P$ *be the* K*-algebra homomorphism defined by* $y_i \mapsto g_i$. *Then* Ψ *induces a* K*-algebra homomorphism* $\psi : P'/I' \longrightarrow P/I$ *such that* $\varphi \circ \psi = \mathrm{id}_{P'/I'}$.

Proof First we prove (a). Notice that [15], Proposition 3.6.1 yields the relation $g \in g(f_1, \ldots, f_n) + J$ for every $g \in P$. If we have $IQ \subseteq I'Q + J$, then this shows $g(f_1, \ldots, f_n) \in I'Q + J$ for every $g \in I$. Now we substitute $x_i \mapsto f_i$ for $i = 1, \ldots, n$ here and get $g(f_1, \ldots, f_n) \in I'$. Hence the map φ is well-defined. Conversely, assume that φ is well-defined. This means that every $g \in I$ satisfies $g(f_1, \ldots, f_n) \in I'$. Therefore we get $IQ \subseteq I'Q + J$.

Claim (b) follows immediately from (a) and [15], Proposition 3.6.2. In part (c), if the map φ is surjective, then [15], Proposition 3.6.6.d shows that polynomials $g_1, \ldots, g_m \in P$ with $y_i - g_i \in I'Q + J$ exist. Conversely, suppose that such polynomials $g_1, \ldots, g_m \in P$ exist, and let σ be an elimination ordering for $(y_1, \ldots, y_m)$ on $\mathbb{T}(x_1, \ldots, x_n, y_1, \ldots, y_m)$. Then the normal form $\mathrm{NF}_{\sigma, I'Q+J}(y_i)$ equals $\mathrm{NF}_{\sigma, I'Q+J}(g_i)$ and $g_i \in P$ implies that also the latter normal form is in P. Consequently, we have $y_i + I' \in \mathrm{Im}(\varphi)$ by [15], Proposition 3.6.6.a.

Finally, claim (d) follows from (c), since $(\varphi \circ \psi)(\bar{y}_i) = \varphi(\bar{g}_i) = \bar{y}_i$ for all $i = 1, \ldots, m$. □

Based on this lemma, we can characterize isomorphisms of finitely generated K-algebras as follows.

Proposition 6.3.2 (Isomorphisms of Affine K-Algebras)
Let K *be a field, let* P *be the polynomial ring* $P = K[x_1, \ldots, x_n]$, *let* $I \subseteq P$ *be an ideal, let* $P' = K[y_1, \ldots, y_m]$, *and let* $I' \subseteq P'$ *be an ideal. Moreover, given* $f_1, \ldots, f_n \in P'$, *let* $\Phi : P \longrightarrow P'$ *be the* K*-algebra homomorphism defined by* $\Phi(x_i) = f_i$ *for* $i = 1, \ldots, n$, *and let* J *be the ideal* $J = \langle x_1 - f_1, \ldots, x_n - f_n \rangle$ *in* $Q = K[x_1, \ldots, x_n, y_1, \ldots, y_m]$.

Furthermore, let $g_1, \ldots, g_m$ *be polynomials in* P, *let* $\Psi : P' \longrightarrow P$ *be the* K*-algebra homomorphism defined by* $\Psi(y_j) = g_j$ *for* $j = 1, \ldots, m$, *and let* $J' = \langle y_1 - g_1, \ldots, y_m - g_m \rangle \subseteq Q$. *Then the following conditions are equivalent.*

(a) *The homomorphisms* Φ *and* Ψ *defined above induce* K*-algebra isomorphisms* $\varphi : P/I \longrightarrow P'/I'$ *and* $\psi : P'/I' \longrightarrow P/I$ *which are inverse to each other.*

(b) *We have the equality* $IQ + J' = I'Q + J$.

Proof First we show (a) ⇒ (b). By parts (a) and (c) of the lemma, we have the inclusion $IQ + J' \subseteq I'Q + J$. The converse inclusion follows by interchanging the roles of Φ and Ψ.

Now we prove (b) ⇒ (a). By part (a) of the lemma, the maps φ and ψ are well-defined. Since the inclusion $I \subseteq (IQ + J') \cap P$ clearly holds, and since the inclusion

$(IQ + J') \cap P \subseteq I$ can be shown using the same arguments as in the proof of part (a) of the lemma, we have $I = (IQ + J') \cap P$. Then the hypothesis implies the equality $I = (I'Q + J) \cap P$, and part (b) of the lemma shows that φ is injective. From part (c) of the lemma we get that φ is surjective. Hence φ is an isomorphism. By interchanging the roles of Φ and Ψ, it follows that also ψ is an isomorphism. Finally, we note that part (d) of the lemma yields that ψ is inverse to φ. □

In the following we apply this proposition to compute all isomorphisms between two representatives of a finite field $\mathbb{F}_q$ with $q = p^e$ for some prime number p and $e > 0$. In field theory it is shown that the group of all automorphisms of $\mathbb{F}_q$ is a cyclic group of order e generated by the Frobenius homomorphism. Since we are interested in $\mathbb{F}_q$-isomorphisms between fields having q^d elements, we generalize this result as follows.

Lemma 6.3.3 *Let K be a field having q elements, and let L and L' be two representatives of $\mathbb{F}_{q^d}$ for some $d > 0$. Then there exist exactly d distinct isomorphisms of K-algebras $\varphi_i : L \longrightarrow L'$ with $i \in \{1, \ldots, d\}$.*

Proof Let $a \in L$ be a generator of the cyclic group $L^\times = L \setminus \{0\}$. Consequently, the K-algebra homomorphism $K[x] \longrightarrow L$ defined by $x \mapsto a$ is surjective. Hence there exists an irreducible polynomial $f \in K[x]$ such that $\varepsilon : K[x]/\langle f \rangle \longrightarrow L$ is an isomorphism. Similarly, we find an isomorphism $\eta : K[y]/\langle g \rangle \longrightarrow L'$ for some irreducible polynomial $g \in K[y]$.

Now we consider the L'-algebra $R = L'[x]/fL'[x]$. Since f is irreducible and L' is a perfect field, the polynomial f is squarefree in $L'[x]$ (see [15], Proposition 3.9.7.d). Hence R is a reduced ring. From $a^{q^d} = a$ we get the relation $x^{q^d} - x \in fK[x] \subseteq fL'[x]$, and hence $\bar{x}^{q^d} = \bar{x}$ in R. Consequently, every $\bar{h} \in R$ satisfies $\bar{h}^{q^d} = \bar{h}$. By Theorem 5.2.4.c, it follows that the zero ideal of R is the intersection of d linear maximal ideals. Hence $fL'[x]$ is the intersection of d linear maximal ideals in $L'[x]$. They correspond to d distinct zeros $b_1, \ldots, b_d$ of f in L'. For $i \in \{1, \ldots, d\}$, the K-algebra homomorphism $\varphi_i : K[x]/\langle f \rangle \longrightarrow K[y]/\langle g \rangle$ given by $\bar{x} \mapsto \eta^{-1}(b_i)$ is well-defined. Since both fields have the same number of elements, the map φ_i is bijective. Thus we have found d distinct K-algebra isomorphisms between L and L'. The fact that these are all K-algebra isomorphisms follows from the observation that a well-defined map φ_i has to map $\bar{x}$ to a zero of f in $K[y]/\langle g \rangle \cong L'$. □

Now we are ready to state and prove the main theorem of this subsection.

Theorem 6.3.4 (Isomorphisms between Representatives of $\mathbb{F}_{q^d}$)
Let p be a prime number, let $q = p^e$, let K be a field with q elements, and let $d > 0$. Assume that we are given two representatives of $\mathbb{F}_{q^d}$, namely $L = P/\mathfrak{M}$ with a maximal ideal $\mathfrak{M}$ of $P = K[x_1, \ldots, x_n]$ and $L' = P'/\mathfrak{M}'$ with a maximal ideal $\mathfrak{M}'$ of $P' = K[y_1, \ldots, y_m]$.

(a) *In the ring* $Q = K[x_1, \ldots, x_n, y_1, \ldots, y_m]$, *the ideal* $\mathfrak{M}Q + \mathfrak{M}'Q$ *is a radical ideal. It has a primary decomposition of the form* $\mathfrak{M}Q + \mathfrak{M}'Q = \mathfrak{M}_1 \cap \cdots \cap \mathfrak{M}_d$ *with maximal ideals* $\mathfrak{M}_i$.

(b) *There exists polynomials* $f_{ij} \in P'$ *and* $g_{ik} \in P$ *with* $i \in \{1, \ldots, d\}$, *with* $j \in \{1, \ldots, n\}$, *and with* $k \in \{1, \ldots, m\}$ *such that, for* $i = 1, \ldots, d$, *the ideal* $\mathfrak{M}_i$ *in* (*a*) *is given by*

$$\mathfrak{M}_i = \mathfrak{M}'Q + \langle x_1 - f_{i1}, \ldots, x_{in} - f_{in} \rangle = \mathfrak{M}Q + \langle y_1 - g_{i1}, \ldots, y_m - g_{im} \rangle$$

In particular, the primary decomposition of the ideal $\mathfrak{M}L'[x_1, \ldots, x_n]$ *is given by* $\mathfrak{M}L'[x_1, \ldots, x_n] = \bigcap_{i=1}^{d} \langle x_1 - \bar{f}_{i1}, \ldots, x_n - \bar{f}_{in} \rangle$, *and an analogous formula holds for* $\mathfrak{M}'L[y_1, \ldots, y_m]$.

(c) *For* $i = 1, \ldots, d$, *let* $\Phi_i : P \longrightarrow P'$ *be the* K*-algebra homomorphism defined by* $\Phi_i(x_j) = f_{ij}$ *for* $j = 1, \ldots, n$, *and let* $\Psi_i : P' \longrightarrow P$ *be the* K*-algebra homomorphism defined by* $\Psi_i(y_k) = g_{ik}$ *for* $k = 1, \ldots, m$. *Then, for* $i = 1, \ldots, d$, *the maps* Φ_i *and* Ψ_i *induce* K*-algebra isomorphisms* $\varphi_i : P/\mathfrak{M} \longrightarrow P'/\mathfrak{M}'$ *and* $\psi_i : P'/\mathfrak{M}' \longrightarrow P/\mathfrak{M}$ *which are inverse to each other.*

(d) *The isomorphisms* $\varphi_1, \ldots, \varphi_d$ *constructed in* (*c*) *are all isomorphisms between* $P/\mathfrak{M}$ *and* $P'/\mathfrak{M}'$.

Proof To prove (a), we first show that $\mathfrak{M}Q + \mathfrak{M}'Q$ is a radical ideal. This is equivalent to the claim that $\mathfrak{M}L'[x_1, \ldots, x_n]$ is a radical ideal. The minimal polynomials of the elements $\bar{x}_1, \ldots, \bar{x}_n$ in $P/\mathfrak{M}$ are squarefree. Thus we have $\gcd(\mu_{\bar{x}_i}(z), \mu_{\bar{x}_i}(z)') = 1$ for $i = 1, \ldots, n$. By Proposition 1.2.3, these polynomials coincide with the minimal polynomials of the residue classes $\bar{x}_1, \ldots, \bar{x}_n$ in $L'[x_1, \ldots, x_n]/\mathfrak{M}L'[x_1, \ldots, x_n]$. Since they are coprime to their derivatives and L' is a perfect field, they are squarefree polynomials by [15], Proposition 3.7.9.d. Hence Seidenberg's Lemma (see [15], Proposition 3.7.15) implies the claim.

Next we prove that $\mathfrak{M}Q + \mathfrak{M}'Q$ has exactly d maximal components of the form described in (b). By the lemma, we know that there are exactly d K-algebra isomorphisms $\varphi_i : P/\mathfrak{M} \longrightarrow P'/\mathfrak{M}'$. For $i = 1, \ldots, d$ and $j = 1, \ldots, n$, let $\varphi_i(\bar{x}_j) = \bar{f}_{ij}$ with $f_{ij} \in P'$. Then Proposition 6.3.2 shows that $\mathfrak{M}Q + \mathfrak{M}'Q$ is contained in $\mathfrak{M}_i = \mathfrak{M}'Q + \langle x_1 - f_{i1}, \ldots, x_n - f_{in} \rangle$ for $i = 1, \ldots, d$. The ideals $\mathfrak{M}_i$ are maximal ideals of Q, because $Q/\mathfrak{M}_i \cong P'/\mathfrak{M}'$ is a field.

Translating this to $L'[x_1, \ldots, x_n]$, we see that $\mathfrak{M}L'[x_1, \ldots, x_n]$ is contained in d distinct linear maximal ideals. Now we use the Chinese Remainder Theorem 2.2.1 and $\dim_{L'}(L'[x_1, \ldots, x_n]/\mathfrak{M}L'[x_1, \ldots, x_n]) = \dim_K(P/\mathfrak{M}) = d$ to conclude that these are all maximal components of $\mathfrak{M}L'[x_1, \ldots, x_n]$, and hence that the ideals $\mathfrak{M}_1, \ldots, \mathfrak{M}_d$ are all maximal components of $\mathfrak{M}Q + \mathfrak{M}'Q$.

To prove (c), let $J_i = \langle x_1 - f_{i1}, \ldots, x_n - f_{in} \rangle$ and $J_i' = \langle y_1 - g_{i1}, \ldots, y_m - g_{im} \rangle$ in Q for $i = 1, \ldots, d$. Then the equalities in (b) yield $J_i + \mathfrak{M}'Q = J_i' + \mathfrak{M}Q$, and the claim follows from Proposition 6.3.2. Finally, we note that claim (d) follows from (c) and the lemma. □

When we translate this theorem to a result about a tuple of endomorphisms of a finite dimensional vector space, we obtain the following corollary about simultaneous diagonalizability after a suitable base field extension.

Corollary 6.3.5 *Let K be a finite field, let V be a finite-dimensional K-vector space, let $\Phi = (\varphi_1, \ldots, \varphi_n)$ be a tuple of pairwise commuting endomorphisms of V, and let $\mathscr{F} = K[\varphi_1, \ldots, \varphi_n]$ be the commuting family they generate. We assume that $\mathrm{Rel}_P(\Phi)$ is a maximal ideal in $P = K[x_1, \ldots, x_n]$ and let $d = \dim_K(P/\mathrm{Rel}_P(\Phi))$.*

Then we introduce new indeterminates $y_1, \ldots, y_m$, we let $P' = K[y_1, \ldots, y_m]$, and let $\mathfrak{M}'$ be a maximal ideal in P' such that $\dim_K(L') = d$ for $L' = P'/\mathfrak{M}'$. Finally, we let $\Phi_{L'} = ((\varphi_1)_{L'}, \ldots, (\varphi_n)_{L'})$, where $(\varphi_i)_{L'}$ is the extension of φ_i to $V_{L'} = V \otimes_K L'$ for $i = 1, \ldots, n$, and we let $\mathscr{F}_{L'}$ be the commuting family generated by $\Phi_{L'}$. Then the family $\mathscr{F}_{L'}$ is simultaneously diagonalizable.

Proof Using $\mathfrak{M} = \mathrm{Rel}_P(\Phi)$, the proof follows by combining claim (b) of the theorem and Proposition 2.6.1.g. □

Next we turn the theorem into an algorithm for computing all $\mathbb{F}_q$-isomorphisms between two finite fields having q^d elements.

Algorithm 6.3.6 (Computing All Isomorphisms of Finite Fields)
In the setting of Theorem 6.3.4, consider the following sequence of instructions.

(1) *Form the ring $Q = K[x_1, \ldots, x_n, y_1, \ldots, y_m]$ and compute the primary decomposition of the ideal $\mathfrak{M}Q + \mathfrak{M}'Q$. Let $\mathfrak{M}_1, \ldots, \mathfrak{M}_d$ be the resulting maximal ideals.*
(2) *Choose a term ordering σ on $\mathbb{T}(x_1, \ldots, x_n, y_1, \ldots, y_m)$ which is an elimination ordering for $(y_1, \ldots, y_m)$. For $i \in \{1, \ldots, d\}$, compute the reduced σ-Gröbner basis G_i of $\mathfrak{M}_i$ and write $G_i = H_i \cup \{y_1 - g_{i1}, \ldots, y_m - g_{im}\}$ with $H_i \subset P$ and $g_{ik} \in P$.*
(3) *Choose a term ordering σ' on $\mathbb{T}(x_1, \ldots, x_n, y_1, \ldots, y_m)$ which is an elimination ordering for $(x_1, \ldots, x_n)$. For every index $i \in \{1, \ldots, d\}$, compute the reduced σ'-Gröbner basis G'_i of the ideal $\mathfrak{M}_i$ and write $G'_i = H'_i \cup \{x_1 - f_{i1}, \ldots, x_n - f_{in}\}$ with $H'_i \subset P'$ and $f_{ij} \in P'$.*
(4) *Return the pairs $((f_{i1}, \ldots, f_{in}), (g_{i1}, \ldots, g_{im}))$, where $i = 1, \ldots, d$.*

This is an algorithm which computes d pairs of tuples of polynomials. Each pair defines two isomorphisms $\varphi_i : P/\mathfrak{M} \longrightarrow P'/\mathfrak{M}'$ such that $\bar{x}_j \mapsto \bar{f}_{ij}$ and $\psi_i : P'/\mathfrak{M}' \longrightarrow P/\mathfrak{M}$ such that $\bar{y}_k \mapsto \bar{g}_{ik}$ which are inverse to each other.

Let us see some examples which illustrate this algorithm.

Example 6.3.7 Let $K = \mathbb{F}_{101}$, and let $L = K[x]/\langle f(x)\rangle$ be the field with $q = 101^4$ elements defined by $f(x) = x^4 + 41x^3 - 36x^2 + 39x - 12$. In order to compute

the four K-algebra automorphisms of the field L, we create an isomorphic copy $L' = K[y]/\langle f(y)\rangle$ of L and use Algorithm 6.3.6 to compute the distinct isomorphisms $\varphi_i : L \longrightarrow L'$. (In Sect. 6.3.B the field L' will be called a *clone* of L.) Let us follow the steps of the algorithm.

(1) First we form $Q = K[x, y]$ and compute the primary decomposition of the ideal $I = \langle f(x), f(y)\rangle$ in Q. The result is $I = \mathfrak{M}_1 \cap \mathfrak{M}_2 \cap \mathfrak{M}_3 \cap \mathfrak{M}_4$, where

$$\begin{aligned}
\mathfrak{M}_1 &= \langle f(y), x - y\rangle \\
\mathfrak{M}_2 &= \langle f(y), x - 34y^3 - 20y^2 + 3y + 41\rangle \\
\mathfrak{M}_3 &= \langle f(y), x - 4y^3 - 47y^2 + 29y + 35\rangle \\
\mathfrak{M}_4 &= \langle f(y), x + 38y^3 - 34y^2 - 31y - 35\rangle
\end{aligned}$$

(2) We choose an elimination ordering σ for y and compute the reduced σ-Gröbner basis of the ideals $\mathfrak{M}_i$. We get

$$\begin{aligned}
\mathfrak{M}_1 &= \langle f(x), y - x\rangle \\
\mathfrak{M}_2 &= \langle f(x), y + 38x^3 - 34x^2 - 31x - 35\rangle \\
\mathfrak{M}_3 &= \langle f(x), y - 4x^3 - 47x^2 + 29x + 35\rangle \\
\mathfrak{M}_4 &= \langle f(x), y - 34x^3 - 20x^2 + 3x + 41\rangle
\end{aligned}$$

(3) Next we choose an elimination ordering σ' for x and compute the reduced σ'-Gröbner bases of the ideals $\mathfrak{M}_i$. We get the generators given in Step (1).
(4) The algorithm returns the four pairs (y, x), $(34y^3 + 20y^2 - 3y - 41, -38x^3 + 34x^2 + 31x + 35)$, $(4y^3 + 47y^2 - 29y - 35, 4x^3 + 47x^2 - 29x - 35)$, and $(-38y^3 + 34y^2 + 31y + 35, 34x^3 + 20x^2 - 3x - 41)$.

Altogether, it follows that there are four isomorphisms between $P/\mathfrak{M}$ and $P'/\mathfrak{M}'$, the second one of which is given by $\bar{x} \mapsto 34\bar{y}^3 + 20\bar{y}^2 - 3\bar{y} - 41$ and $\bar{y} \mapsto -38\bar{x}^3 + 34\bar{x}^2 + 31\bar{x} + 35$, etc. For instance, the second of four automorphisms of L is given by $\bar{x} \mapsto 34\bar{x}^3 + 20\bar{x}^2 - 3\bar{x} - 41$, and its inverse is $\bar{x} \mapsto -38\bar{x}^3 + 34\bar{x}^2 + 31\bar{x} + 35$.

In our second example we find five isomorphisms.

Example 6.3.8 We let $K = \mathbb{F}_{71}$ and let $L = P/\langle f(x)\rangle$, where $P = K[x]$ and $f(x) = x^5 + 2x^4 + 7x^3 - 9x^2 - x + 16 \in K[x]$. Furthermore, we use the ring $L' = P'/\langle g(y)\rangle$, where $P' = K[y]$ and $g(y) = y^5 - 23y^4 + 17y - 21$. Since both $f(x)$ and $g(y)$ are irreducible of degree five, the fields L and L' are isomorphic. They both represent $\mathbb{F}_{71^5}$. Let us compute all K-isomorphisms between L and L' using the algorithm.

(1) In the ring $Q = K[x, y]$ we consider the ideal $I = \langle f(x), g(y)\rangle$ and compute its primary decomposition. We get $I = \mathfrak{M}_1 \cap \mathfrak{M}_2 \cap \mathfrak{M}_3 \cap \mathfrak{M}_4 \cap \mathfrak{M}_5$ where

$$\mathfrak{M}_1 = \langle g(y), x + 22y^4 - 21y^3 + 19y^2 + 23y + 21\rangle$$
$$\mathfrak{M}_2 = \langle g(y), x + 13y^4 - 4y^3 - 17y^2 - 29y - 7\rangle$$
$$\mathfrak{M}_3 = \langle g(y), x - 17y^3 - 10y^2 + 35y + 6\rangle$$
$$\mathfrak{M}_4 = \langle g(y), x - 8y^4 + 26y^3 + 19y^2 - 30y - 23\rangle$$
$$\mathfrak{M}_5 = \langle g(y), x - 27y^4 + 16y^3 - 11y^2 + y + 5\rangle$$

(2) Next we compute the reduced Gröbner basis of the ideals $\mathfrak{M}_1, \ldots, \mathfrak{M}_5$ with respect to an elimination ordering for y and get

$$\mathfrak{M}_1 = \langle f(x), y - 20x^4 - 8x^3 + 14x^2 + 6x - 27\rangle$$
$$\mathfrak{M}_2 = \langle f(x), y - 35x^4 - 20x^3 - 8x^2 + 32x - 27\rangle$$
$$\mathfrak{M}_3 = \langle f(x), y - x^4 + 3x^3 + 29x^2 - x - 11\rangle$$
$$\mathfrak{M}_4 = \langle f(x), y - 29x^4 + 25x^3 - 16x^2 - 4x - 16\rangle$$
$$\mathfrak{M}_5 = \langle f(x), y + 14x^4 - 19x^2 - 33x - 13\rangle$$

(3) The reduced Gröbner bases of the ideals $\mathfrak{M}_1, \ldots, \mathfrak{M}_5$ with respect to an elimination ordering for x are the systems of generators given in Step (1).

(4) Altogether, the algorithm returns the five tuples

$$(-22y^4 + 21y^3 - 19y^2 - 23y - 21, 20x^4 + 8x^3 - 14x^2 - 6x + 27)$$
$$(-13y^4 + 4y^3 + 17y^2 + 29y + 7, 35x^4 + 20x^3 + 8x^2 - 32x + 27)$$
$$(17y^3 + 10y^2 - 35y - 6, x^4 - 3x^3 - 29x^2 + x + 11)$$
$$(8y^4 - 26y^3 - 19y^2 + 30y + 23, 29x^4 - 25x^3 + 16x^2 + 4x + 16)$$
$$(27y^4 - 16y^3 + 11y^2 - y - 5, -14x^4 + 19x^2 + 33x + 13)$$

which define the five isomorphisms $\varphi_i : L \longrightarrow L'$ together with their inverses $\psi_i : L' \longrightarrow L$.

In the last part of this subsection we apply the preceding algorithm to the following problem. Suppose we are given a finite field K and a finite field extension $K \subseteq L$. What are the primitive elements for $K \subseteq L$ (see Definition 3.4.3) which share the same minimal polynomial? The next proposition provides the basic link between primitive elements and irreducible polynomials.

Proposition 6.3.9 *Let K be a finite field with q elements, let $K \subseteq L$ be a finite field extension, and let $\dim_K(L) = d$. We denote the set of primitive elements for $K \subseteq L$*

by $\mathrm{Prim}_K(L)$ *and the set of monic irreducible polynomials of degree* d *in* $K[z]$ *by* $\mathrm{Irr}_K(d)$. *Then the map* $\alpha : \mathrm{Prim}_K(L) \longrightarrow \mathrm{Irr}_K(d)$ *given by* $a \mapsto \mu_a(z)$ *is surjective and* d*-to-*1.

Proof To show that α is surjective, we first note that, for $f \in \mathrm{Irr}_K(d)$, the field $K[x]/\langle f(x)\rangle$ is a d-dimensional K-vector space, and therefore has q^d elements. Hence this field is isomorphic to L and $f(z)$ is the minimal polynomial of the element corresponding to $\bar{x}$.

Now we fix a polynomial $f(z) \in \mathrm{Irr}_K(d)$ and let $a \in L$ be a primitive element for $K \subseteq L$ such that $\mu_a(z) = f(z)$. Then we have $L = K[a] \cong K[x]/\langle \mu_a(x)\rangle$. Therefore the map $\varphi_a : L \longrightarrow K[z]/\langle f(z)\rangle$ defined by $a \mapsto \bar{z}$ is an isomorphism of K-algebras. By Theorem 6.3.4, there are exactly d such isomorphisms and the proof is complete. □

The following algorithm is an application of Algorithm 6.3.6 to the setting of this proposition. Notice that Proposition 5.3.10 provides a similar algorithm. However, since there we do not assume that K is finite, we may get fewer than d elements sharing a minimal polynomial (see for instance Example 5.3.11).

Algorithm 6.3.10 (Primitive Elements Sharing a Minimal Polynomial) *In the setting of the proposition, let* $L = P/\mathfrak{M}$ *with* $P = K[x_1, \ldots, x_n]$ *and a maximal ideal* $\mathfrak{M}$ *in* P, *and let* $f(z) \in \mathrm{Irr}_K(d)$. *Consider the following sequence of instructions.*

(1) *Compute the primary decomposition* $\mathfrak{M}_1 \cap \cdots \cap \mathfrak{M}_d$ *of the ideal* $\mathfrak{M} + \langle f(z)\rangle$ *in* $K[x_1, \ldots, x_n, z]$.
(2) *Choose a term ordering* σ *on* $\mathbb{T}(x_1, \ldots, x_n, z)$ *which is an elimination ordering for* z *and compute the reduced* σ*-Gröbner bases* $G_1, \ldots, G_d$ *of the maximal ideals* $\mathfrak{M}_1, \ldots, \mathfrak{M}_d$, *respectively.*
(3) *For* $i = 1, \ldots, d$, *let* $g_1, \ldots, g_d \in P$ *be such that* $z - g_i$ *is contained in* G_i.
(4) *Return the polynomials* $g_1, \ldots, g_d$.

This is an algorithm which computes polynomials $g_1, \ldots, g_d$ *in* P *such that the residue classes* $\bar{g}_1, \ldots, \bar{g}_d$ *in* $L = P/\mathfrak{M}$ *are precisely those primitive elements of* L *whose minimal polynomial is* $f(z)$.

The final example in this subsection provides an explicit application of the preceding algorithm.

Example 6.3.11 Let $K = \mathbb{F}_{71}$, let $P = K[x_1, x_2]$, and let $\mathfrak{M}$ be the ideal given by $\mathfrak{M} = \langle x_1^2 + x_1 + 1, x_2^3 + 11x_2 + 1\rangle$. Then $\mathfrak{M}$ is a maximal ideal of P and $L = P/\mathfrak{M}$ is a field with $\dim_K(L) = 6$. The minimal polynomial of the element $\bar{x}_1 + \bar{x}_2 \in L$ is $f(z) = z^6 + 3z^5 + 28z^4 - 18z^3 + 21z^2 + 12z - 21$, and this polynomial is irreducible. Hence the field $K[z]/\langle f(z)\rangle$ is isomorphic to L.

Our goal is to find all primitive elements of the field L whose minimal polynomial is $f(z)$. To this end, we apply the above algorithm. The primary decomposition of the ideal $\mathfrak{M}Q + \langle f(z)\rangle$ in $Q = K[x_1, x_2, z]$ is $\mathfrak{M}_1 \cap \cdots \cap \mathfrak{M}_6$, where

$$\begin{aligned}
\mathfrak{M}_1 &= \mathfrak{M} + \langle z - x_1 - x_2\rangle \\
\mathfrak{M}_2 &= \mathfrak{M} + \langle z + x_1 - x_2 + 1\rangle \\
\mathfrak{M}_3 &= \mathfrak{M} + \left\langle z + x_1 + 9x_2^2 - 33x_2 - 4\right\rangle \\
\mathfrak{M}_4 &= \mathfrak{M} + \left\langle z - x_1 + 9x_2^2 - 33x_2 - 5\right\rangle \\
\mathfrak{M}_5 &= \mathfrak{M} + \left\langle z + x_1 - 9x_2^2 + 34x_2 + 6\right\rangle \\
\mathfrak{M}_6 &= \mathfrak{M} + \left\langle z - x_1 - 9x_2^2 + 34x_2 + 5\right\rangle
\end{aligned}$$

Hence there are six elements in L whose minimal polynomial is $f(z)$, namely $\bar{x}_1 + \bar{x}_2$, $-\bar{x}_1 + \bar{x}_2 - 1$, $-\bar{x}_1 - 9\bar{x}_2^2 + 33\bar{x}_2 + 4$, $\bar{x}_1 - 9\bar{x}_2^2 + 33\bar{x}_2 + 5$, $-\bar{x}_1 + 9\bar{x}_2^2 - 34\bar{x}_2 - 6$, and $\bar{x}_1 + 9\bar{x}_2^2 - 34\bar{x}_2 - 5$.

6.3.B Solving over Finite Fields via Cloning

The following is an example of a clone.
The following is an example of a clone.

In this subsection we introduce a powerful technique: cloning. In science, cloning refers to the development of offspring that are genetically identical to their parent. Although it is sometimes viewed controversially, according to Wikipedia, cloning is a natural form of reproduction that has allowed life forms to spread for more than 50 thousand years. It is the reproduction method used by many bacteria, plants, and fungi. Can it also be used in computational algebra? Will it help this book to spread for more than 50 thousand years?

Let us continue to use the notation introduced before. In particular, let K be a finite field with q elements, where $q = p^e$ for some prime number p and $e > 0$, let $P = K[x_1, \ldots, x_n]$, let $\mathfrak{M}$ be a maximal ideal of P, and let $L = P/\mathfrak{M}$. In order to find the solutions of the polynomial system given by a set of generators of $\mathfrak{M}$, we have to enlarge K suitably. In the following we investigate a straightforward method to do this. It is based on a construction that is our way of introducing the technique of cloning into this book.

Definition 6.3.12 Let $y_1, \ldots, y_n$ be new indeterminates, let $P' = K[y_1, \ldots, y_n]$, and let $\mathfrak{M}'$ be the maximal ideal of P' which is obtained by applying the substitution $x_1 \mapsto y_1, \ldots, x_n \mapsto y_n$ to the polynomials in $\mathfrak{M}$.

(a) The ideal $\mathfrak{M}'$ is called the **clone** of the ideal $\mathfrak{M}$ in P'.
(b) The field $L' = P'/\mathfrak{M}'$ is called a **clone** of the field $L = P/\mathfrak{M}$.

Recall that in Theorem 6.3.4 we showed that a zero of $\mathfrak{M}$ in an extension field $L' = P'/\mathfrak{M}'$ of $L = P/\mathfrak{M}$, where $P' = K[y_1, \ldots, y_m]$ and $\mathfrak{M}'$ is a maximal ideal of P', corresponds uniquely to a linear maximal component of $\mathfrak{M}L'[x_1, \ldots, x_n]$. The following proposition extends this result as follows: if we know one such zero, we know them all, since the other ones can be obtained by applying powers of the q-Frobenius automorphism of L'.

Proposition 6.3.13 *Let K be field with q elements, let $P = K[x_1, \ldots, x_n]$, let $\mathfrak{M}$ be a maximal ideal of P, and let $L = P/\mathfrak{M}$. Furthermore, let $P' = K[y_1, \ldots, y_m]$, let $\mathfrak{M}'$ be a maximal ideal of P', let $L' = P'/\mathfrak{M}'$, and let $f_1, \ldots, f_n \in P'$ be polynomials such that $\langle x_1 - \bar{f}_1, \ldots, x_n - \bar{f}_n \rangle$ is one of the maximal components of $\mathfrak{M}L'[x_1, \ldots, x_n]$. Then the set of all zeros of $\mathfrak{M}$ in $(L')^n$ is given by*

$$\mathscr{Z}_{L'}(\mathfrak{M}) = \left\{ \left(\bar{f}_1^{q^i}, \ldots, \bar{f}_n^{q^i} \right) \mid i = 0, \ldots, d-1 \right\}$$

Proof First we introduce further indeterminates $t_1, \ldots, t_n$ and consider the polynomial ring $P'' = K[t_1, \ldots, t_n]$. Let $\mathfrak{M}''$ be the clone of $\mathfrak{M}$ in P'', and let $L'' = P''/\mathfrak{M}''$. By Theorem 6.3.4, there exists an isomorphism of K-algebras $\varphi : L' \longrightarrow L''$. It extends to an isomorphism $\tilde{\varphi} : L'[x_1, \ldots, x_n] \longrightarrow L''[x_1, \ldots, x_n]$ of K-algebras which maps $\mathfrak{M}L'[x_1, \ldots, x_n]$ to $\mathfrak{M}L''[x_1, \ldots, x_n]$. A tuple $(\bar{g}_1, \ldots, \bar{g}_n)$ is a zero of $\mathfrak{M}$ in $(L')^n$ if and only if the tuple $(\varphi(\bar{g}_1), \ldots, \varphi(\bar{g}_n))$ is a zero of $\mathfrak{M}$ in $(L'')^n$, and the map φ commutes with the q-Frobenius automorphism ϕ_q. Therefore it suffices to prove the claim for the zeros of $\mathfrak{M}$ in $(L'')^n$.

Clearly, the tuple $(\bar{t}_1, \ldots, \bar{t}_n)$ is a zero of $\mathfrak{M}$ in $(L'')^n$. By applying ϕ_q repeatedly, it follows that all tuples $(\bar{t}_1^{q^i}, \ldots, \bar{t}_n^{q^i})$ with $0 \leq i \leq d-1$ are zeros of $\mathfrak{M}$ in $(L'')^n$. In view of Theorem 6.3.4, it remains to show that these tuples are pairwise distinct. Assume that $0 \leq i < j \leq d-1$ satisfy $(\phi_q^i(\bar{t}_1), \ldots, \phi_q^i(\bar{t}_n)) = (\phi_q^j(\bar{t}_1), \ldots, \phi_q^j(\bar{t}_n))$. Since ϕ_q is bijective, we get $\phi_q^{j-i}(\bar{t}_k) = \bar{t}_k$ for $k = 1, \ldots, n$. Now the fact that the residue classes $\bar{t}_1, \ldots, \bar{t}_n$ form a system of K-algebra generators of L'' implies that $\phi_q^{j-i}(\bar{g}) = \bar{g}$ for all $\bar{g} \in L''$. If we use a generator $\bar{g}$ of the multiplicative cyclic group $L'' \setminus \{0\}$ here, the inequality $j - 1 < d$ yields a contradiction to the fact that the smallest power k such that $\bar{g}^{q^k} = \bar{g}$ is $k = d$. □

Clearly, this proposition can be applied to the setting where $L' = P'/\mathfrak{M}'$ is a clone of $L = P/\mathfrak{M}$. We start by looking at the univariate case.

Definition 6.3.14 Let K be a field, and let $K \subseteq L$ be a field extension.

(a) Given a polynomial $f \in K[x] \setminus K$, we say that f **splits** in L if there exist elements $c_1, \ldots, c_s \in L$ such that we have $f = \mathrm{LC}(f)(x - c_1) \cdots (x - c_s)$ in $L[x]$.
(b) If a polynomial $f \in K[x] \setminus K$ splits in L as in (a), and if $L = K(c_1, \ldots, c_s)$, we say that L is a **splitting field** of K.

It is a standard result in Algebra that the splitting field of a polynomial exists and is uniquely determined up to an isomorphism of K-algebras (see [21], Chap. 2).

It is also known that, if K is a perfect field, the K-vector space dimension of the splitting field L is the number of elements of $\mathrm{Gal}(L/K)$. The first observation is that, by cloning it, we can split an irreducible polynomial over a finite field.

Proposition 6.3.15 (Splitting a Polynomial over a Finite Field)
Let K be a finite field with q elements, let $f(x) \in K[x]$ be a monic irreducible polynomial of degree $d \geq 1$, and let $L' = K[y]/\mathfrak{M}'$ be a clone of the field $K[x]/\mathfrak{M}$, where $\mathfrak{M} = \langle f(x) \rangle$ and $\mathfrak{M}' = \langle f(y) \rangle$.

(a) *The field L' has q^d elements.*
(b) *In $L'[x]$ we have $f(x) = (x - \bar{y})(x - \bar{y}^q) \cdots (x - \bar{y}^{q^{d-1}})$, where $\bar{y}$ denotes the residue class of y in L'. In particular, the field L' is a splitting field of $f(x)$ and the elements $\bar{y}, \bar{y}^q, \ldots, \bar{y}^{q^{d-1}}$ are the d roots of $f(x)$ in L'.*
(c) *Let $I = \langle f(x), f(y) \rangle \subset K[x, y]$. Then the ideal $\mathfrak{M}_i = \langle f(y), x - y^{q^i} \rangle$ is a maximal ideal of $K[x, y]$ for every $i \in \{0, \ldots, d-1\}$, and the primary decomposition of I is given by $I = \mathfrak{M}_0 \cap \cdots \cap \mathfrak{M}_{d-1}$.*
(d) *Let $i \in \{0, \ldots, d-1\}$, and let $g_i(y) = \mathrm{NF}_{\mathfrak{M}'}(y^{q^i})$ be the normal form of y^{q^i} with respect to $\mathfrak{M}'$. Then we can substitute $\bar{y}^{q^i}$ with $g_i(\bar{y})$ in (b) and y^{q^i} with $g_i(y)$ in (c).*

Proof Claim (a) follows from the fact that $\dim_K(L') = \deg(f(y)) = d$. Claim (b) is a special case of Proposition 6.3.13. Then claim (c) follows from Theorem 6.3.4, and claim (d) is a consequence of the observation that y^{q^i} and $g_i(y)$ have the same residue class in L'. □

This proposition yields a direct method for computing the splitting field of an irreducible polynomial over a finite field. Apparently, one drawback in part (d) is that we have to compute the normal forms of big powers of polynomials. But there is a remedy which is described in the following algorithm.

Algorithm 6.3.16 (Computing Big Powers over Finite Fields)
Let K be a finite field with q elements, let $f(y)$ be a monic irreducible polynomial of degree $d \geq 1$ in $K[y]$, let $\mathfrak{M}' = \langle f(y) \rangle$, and let $L' = K[y]/\mathfrak{M}'$. Given $g(y) \in K[y]$, we write $\mathrm{NF}_{\mathfrak{M}'}(g(y)) = c_0 y^0 + \cdots + c_{d-1} y^{d-1}$ with $c_i \in K$. Furthermore, let $\alpha \in \mathbb{N}$.

(1) *Let B be the K-basis $B = (1, \bar{y}, \ldots, \bar{y}^{d-1})$ of L'. Compute the matrix $M_B(\phi_q)$ representing the q-Frobenius endomorphism ϕ_q of L' in this basis.*
(2) *Let $v \in K^d$ be the column vector $v = (c_0, c_1, \ldots, c_{d-1})^{\mathrm{tr}}$. Calculate the column vector $w = M_B(\phi_q)^\alpha \cdot v$.*
(3) *Return the polynomial $(1, y, \ldots, y^{d-1}) \cdot w$.*

This is an algorithm which computes $\mathrm{NF}_{\mathfrak{M}'}(g(y)^{q^\alpha})$.

Proof Since the vector v contains the coordinates of the residue class of $\mathrm{NF}_{\mathfrak{M}'}(g(y))$ in L' with respect to the basis B, the column vector w contains the coordinates of the residue class of $\mathrm{NF}_{\mathfrak{M}'}(g(y)^{q^\alpha})$. From this the claim follows. □

Let us add a few remarks about the efficiency of this algorithm.

Remark 6.3.17 The calculation of $M_B(\phi_q)^\alpha \cdot v = M_B(\phi_q)^{\alpha-1} \cdot (M_B(\phi_q) \cdot v)$ requires at most α matrix-vector products which are computationally less costly than matrix products. Similarly, we can improve the algorithm by noting that it suffices to compute $\log_2(\alpha)$ powers $M_B(\phi_q)^{2^i}$ and at most $\log_2(\alpha)$ matrix-vector products of some of these powers with v.

It is time to see Proposition 6.3.15 and Algorithm 6.3.16 in action.

Example 6.3.18 Let $K = \mathbb{F}_{101}$, let the monic irreducible polynomial $f(x) \in K[x]$ be given by $f(x) = x^4 + 41x^3 - 36x^2 + 39x - 12$, and let $L' = K[y]/\langle f(y)\rangle$ be a clone of $L = K[x]/\langle f(x)\rangle$.

(a) By Proposition 6.3.15.b, we get $f(x) = (x - \bar{y})(x - \bar{y}^{101})(x - \bar{y}^{101^2})(x - \bar{y}^{101^3})$ in $L'[x]$.

(b) Another representation of the zeros of f can be found by combining Proposition 6.3.15.d with Algorithm 6.3.16. We get

$$f(x) = (x - \bar{y}) \cdot \left(x - 34\bar{y}^3 - 20\bar{y}^2 + 3\bar{y} + 41\right) \cdot \left(x - 4\bar{y}^3 - 47\bar{y}^2 + 29\bar{y} + 35\right) \cdot \left(x + 38\bar{y}^3 - 34\bar{y}^2 - 31\bar{y} - 35\right)$$

(c) A third way to compute the roots of $f(x)$ in L is to use the primary decomposition of the ideal $I = \langle f(x), f(y)\rangle \subset K[x, y]$ and Proposition 6.3.15.c. We obtain the decomposition $I = \mathfrak{M}_1 \cap \mathfrak{M}_2 \cap \mathfrak{M}_3 \cap \mathfrak{M}_4$ where

$$\begin{aligned}
\mathfrak{M}_1 &= \langle f(y), x - y\rangle \\
\mathfrak{M}_2 &= \langle f(y), x - 34y^3 - 20y^2 + 3y + 41\rangle \\
\mathfrak{M}_3 &= \langle f(y), x - 4y^3 - 47y^2 + 29y + 35\rangle \\
\mathfrak{M}_4 &= \langle f(y), x + 38y^3 - 34y^2 - 31y - 35\rangle
\end{aligned}$$

In other words, the roots of $f(x)$ in L' are the residue classes of the polynomials y, $34y^3 + 20y^2 - 3y - 41$, $4y^3 + 47y^2 - 29y - 35$, and $-38y^3 + 34y^2 + 31y + 35$.

Now we treat the case where the maximal ideal $\mathfrak{M}$ is not necessarily principal. The next proposition follows by combining Theorem 6.3.4 and Proposition 6.3.13

in the case where the field L' is a clone of L. Notice that we always know one zero of $\mathfrak{M}$ in $(L')^n$, namely the clone $(\bar{y}_1, \ldots, \bar{y}_n)$ of the tuple $(\bar{x}_1, \ldots, \bar{x}_n)$.

Proposition 6.3.19 *Let K be a finite field with q elements, let $P = K[x_1, \ldots, x_n]$, let $\mathfrak{M}$ be a maximal ideal in P, let $L = P/\mathfrak{M}$, and let $d = \dim_K(L)$. We introduce new indeterminates $y_1, \ldots, y_n$, let $P' = K[y_1, \ldots, y_n]$, denote the clone of $\mathfrak{M}$ in P' by $\mathfrak{M}'$, and let $L' = P'/\mathfrak{M}'$ be the clone of L. Then we have*

$$\mathscr{Z}_{L'}(\mathfrak{M}) = \left\{ \left(\bar{y}_1^{q^i}, \ldots, \bar{y}_n^{q^i} \right) \mid i = 0, \ldots, d-1 \right\}$$

The formula given in this proposition contains some polynomials of potentially very high degrees. When we combine this formula with Algorithm 6.3.16, we get the following algorithm.

Algorithm 6.3.20 (Solving over Finite Fields via Cloning)
In the setting of the proposition, consider the following instructions.

(1) *Introduce new indeterminates $y_1, \ldots, y_n$, let $P' = K[y_1, \ldots, y_n]$, let $\mathfrak{M}'$ be the clone of $\mathfrak{M}$ in P', and let $L' = P'/\mathfrak{M}'$.*
(2) *For every $i \in \{0, \ldots, d-1\}$, use Algorithm 6.3.16 to compute the tuple $(\mathrm{NF}_{\mathfrak{M}'}(y_1^{q^i}), \ldots, \mathrm{NF}_{\mathfrak{M}'}(y_n^{q^i}))$. Then return the set of all these tuples.*

This is an algorithm which computes a set of n-tuples of polynomials in $K[y_1, \ldots, y_n]$ which are in normal form with respect to $\mathfrak{M}'$ and whose residue classes in $(L')^n$ are the distinct zeros of $\mathfrak{M}$.

The following remark provides a variant of this algorithm which relies on the computation of a primary decomposition instead of Algorithm 6.3.16.

Remark 6.3.21 Suppose we are in the setting of the algorithm. Another version of Step (2) is obtained by computing the primary decomposition of $\mathfrak{M}Q + \mathfrak{M}'Q$ in $Q = K[x_1, \ldots, x_n, y_1, \ldots, y_n]$ and using an elimination ordering σ for $(x_1, \ldots, x_n)$ on $\mathbb{T}(x_1, \ldots, x_n, y_1, \ldots, y_n)$ in order to write the reduced σ-Gröbner bases G_i of the primary components in the form $G_i = H_i \cup \{x_1 - f_{i1}, \ldots, x_n - f_{in}\}$ with $H_i \subset P'$ and $f_{ij} \in P'$. Then the residue classes of the tuples $(f_{i1}, \ldots, f_{in})$ in $(L')^n$ are the zeros of $\mathfrak{M}$ by Theorem 6.3.4 and Algorithm 6.3.6.

Notice that the output of this variant is the same set of tuples of polynomials as the output of the algorithm above, since the set H_i contains a reduced Gröbner basis of $\mathfrak{M}'$.

The following example illustrates the preceding algorithm. Later we will see that, if the maximal ideal $\mathfrak{M}$ is given via a triangular set of generators, we can get an even simpler representation of its zeros (see Example 6.3.29).

Example 6.3.22 Let $K = \mathbb{F}_2$, let $P = K[x_1, x_2, x_3]$, and let $\mathfrak{M} = \langle f_1, f_2, f_3 \rangle$, where $f_1 = x_1^2 + x_1 + 1$, $f_2 = x_2^3 + x_1$, and $f_3 = x_3^2 + x_3 + x_1$. Using the methods of Chap. 5, we can check that $\mathfrak{M}$ is a maximal ideal in P. Hence $L = P/\mathfrak{M}$ is a finite field. Our goal is to enlarge the field K such that we find the zeros of $\mathfrak{M}$ in the larger field.

(a) According to Proposition 6.3.19, we form the ring $P' = K[y_1, y_2, y_3]$, the clone $\mathfrak{M}'$ of $\mathfrak{M}$ and the clone $L' = P'/\mathfrak{M}'$ of the field $L = P/\mathfrak{M}$. Since the field K has $q = 2$ elements and $d = \dim_K(L) = 2 \cdot 3 \cdot 2 = 12$, the zeros of $\mathfrak{M}$ in $(L')^3$ are $(\bar{y}_1^{2^i}, \bar{y}_2^{2^i}, \bar{y}_3^{2^i})$ for $i = 0, \ldots, 11$.

(b) Another way of writing these triples uses Algorithm 6.3.20. With the help of Algorithm 6.3.16, we compute the necessary normal forms and get the following representations:

$$
\begin{array}{lll}
(y_1, y_2, y_3), & (y_1+1, y_2^2, y_1+y_3), & (y_1, y_1y_2, y_3+1), \\
(y_1+1, y_1y_2^2+y_2^2, y_1+y_3+1), & (y_1, y_1y_2+y_2, y_3), & (y_1+1, y_1y_2^2, y_3+y_1), \\
(y_1, y_2, y_3+1), & (y_1+1, y_2^2, y_1+y_3+1), & (y_1, y_1y_2, y_3), \\
(y_1+1, y_1y_2^2+y_2^2, y_1+y_3), & (y_1, y_1y_2+y_2, y_3+1), & (y_1+1, y_1y_2^2, y_1+y_3+1)
\end{array}
$$

A further example in which the generators of $\mathfrak{M}$ are not in triangular form is given as follows.

Example 6.3.23 Over the field $K = \mathbb{F}_7$, let us consider the system of polynomial equations defined by

$$
\begin{aligned}
\tilde{f}_1 &= x_1^4 - 2x_1 + 3, \\
\tilde{f}_2 &= x_1^2x_2^3 + 2x_1^2 - 2x_2 - 1
\end{aligned}
$$

To solve it, we let $P = K[x_1, x_2]$ and $\mathfrak{M} = \langle \tilde{f}_1, \tilde{f}_2 \rangle$. To check that $\mathfrak{M}$ is a maximal ideal in P, we first check that $\mathfrak{M}$ is a zero-dimensional ideal. Then we apply Algorithm 5.3.12. The minimal polynomial of $\bar{x}_1$ in $P/\mathfrak{M}$ is $\mu_{\bar{x}_1}(z) = z^4 - 2z + 3$ which is irreducible in $K[z]$. Thus we let $K_1 = K[x_1]/\langle x_1^4 - 2x_1 + 3 \rangle$. Next we compute the minimal polynomial of $\bar{x}_2$ in $K_1[x_2]/\mathfrak{M}K_1[x_2]$. It is given by the polynomial $\mu_{\bar{x}_2, K_1}(z) = z^3 + (2\bar{x}_1^3 + 3\bar{x}_1^2 + 3)z + \bar{x}_1^3 - 2\bar{x}_1^2$ and is irreducible in $K_1[z]$.

Consequently, the preimage of the ideal $\langle \mu_{\bar{x}_2, K_1}(x_2) \rangle$ in $K[x_1, x_2]$, i.e., the ideal $\langle x_1^4 - 2x_1 + 3, x_2^3 + (2x_1^3 + 3x_1^2 + 3)x_2 + x_1^3 - 2x_1^2 \rangle$ is a maximal ideal contained in $\mathfrak{M}$, and hence equal to $\mathfrak{M}$. Thus we have a triangular set of generators of $\mathfrak{M}$, and we get $d = \dim_K(P/\mathfrak{M}) = 12$.

Now we want to solve $\mathfrak{M}$ via cloning. We introduce two new indeterminates y_1 and y_2, we let $P' = K[y_1, y_2]$, we let $\mathfrak{M}'$ be the clone of $\mathfrak{M}$ in P', and we let $L' = P'/\mathfrak{M}'$ be the clone of $L = P/\mathfrak{M}$. Then the set of zeros of $\mathfrak{M}$ in $(L')^2$ is $\{(y_1^{q^i}, y_2^{q^i}) \mid i = 0, \ldots, 11\}$. When we compute the corresponding normal forms via

Algorithm 6.3.16, we get the following representations:

$$
\begin{array}{ll}
(y_1, & y_2) \\
(-3y_1^3 - 3y_1 + 1, & y_1^3 + 3y_1^2y_2 + 3y_1y_2^2 + 3y_2^3 + 3y_1^2 - 3y_1y_2 + y_2^2 + 3y_2 - 3) \\
(-2y_1^3 - 2y_1^2 - 2y_1 + 3, & 3y_1^2y_2^2 - 2y_1^3 - 2y_1y_2^2 - 2y_2^3 + 3y_1^2 - 2y_1y_2 + 3y_2^2 + 3) \\
(-2y_1^3 + 2y_1^2 - 3y_1 + 3, & -2y_1^2y_2^2 + 2y_2^4 + y_1^3 - 3y_1^2y_2 + 2y_1y_2^2 - 2y_2^3 - y_1^2 - 3y_1y_2 + 3y_1 - 2y_2) \\
(y_1, & -y_1^2y_2^2 - y_2^4 - y_1^3 - y_1^2y_2 - 3y_1y_2^2 - 3y_1^2 + y_1y_2 - y_2^2 + 2y_1 + 3y_2 - 3) \\
(-3y_1^3 - 3y_1 + 1, & y_1^2y_2^2 + 2y_1^3 + 3y_1^2y_2 + 2y_1y_2^2 - 2y_2^3 - 3y_1^2 - y_1y_2 + y_2) \\
(-2y_1^3 - 2y_1^2 - 2y_1 + 3, & y_1^2y_2^2 - y_2^4 - y_1^3 + 3y_1^2y_2 + 2y_1y_2^2 + 2y_2^3 + 3y_1^2 - 3y_2^2 + 2y_1 + y_2 + 3) \\
(-2y_1^3 + 2y_1^2 - 3y_1 + 3, & 2y_1^2y_2^2 - y_2^4 - 2y_1^2y_2 + 3y_1y_2^2 + 2y_2^3 - 2y_1^2 - 2y_2^2 + 2y_1 + 2y_2 + 2) \\
(y_1, & y_1^2y_2^2 + y_2^4 + y_1^3 + y_1^2y_2 + 3y_1y_2^2 + 3y_1^2 - y_1y_2 + y_2^2 - 2y_1 + 3y_2 + 3) \\
(-3y_1^3 - 3y_1 + 1, & 3y_1^2y_2^2 + y_2^4 + 3y_1^3 - 3y_1^2y_2 + y_1^2 + 2y_1y_2 - 2y_1 - y_2 + 1) \\
(-2y_1^3 - 2y_1^2 - 2y_1 + 3, & 3y_1^2y_2^2 + y_2^4 + 3y_1^3 - 3y_1^2y_2 + y_1^2 + 2y_1y_2 - 2y_1 - y_2 + 1) \\
(-2y_1^3 + 2y_1^2 - 3y_1 + 3, & -y_2^4 - y_1^3 - 2y_1^2y_2 + 2y_1y_2^2 + 3y_1^2 + 3y_1y_2 + 2y_2^2 + 2y_1 - 2)
\end{array}
$$

6.3.C Solving over Finite Fields via Univariate Representations

Patience is something you admire
in the driver behind you,
but not in the one ahead.
(Bill McClashen)

As before, we let K be a field with $q = p^e$ elements, where p is a prime and $e > 0$, let $P = K[x_1, \ldots, x_n]$, and let $\mathfrak{M}$ be a maximal ideal in P whose zeros we want to compute in a suitably chosen extension field of K.

Suppose we are using a method based on Theorem 6.3.4, and for every calculation, we are impatiently awaiting it to finish. Can we speed up and pass the obstacles before us? If the computer algebra system we are using has a fast implementation of finite fields, it knows an irreducible polynomial $f(y)$ of degree d in $K[y]$, namely the defining polynomial of the built-in representative of $\mathbb{F}_{q^d}$. Using the univariate representation $L' = K[y]/\langle f(y)\rangle$, we can solve the system quickly, as the following algorithm shows. An added advantage is that, after we finish the calculation, we have the solutions represented via the built-in field representative and can use them for further computations without delay.

Algorithm 6.3.24 (Solving via a Univariate Representation)
Let K be a finite field with q elements, let $P = K[x_1, \ldots, x_n]$, let $\mathfrak{M}$ be a maximal ideal of P, let $L = P/\mathfrak{M}$, let $d = \dim_K(L)$, let $f(y) \in K[y]$ be a monic irreducible polynomial of degree d, and let $L' = K[y]/\langle f(y)\rangle$. Consider the following sequence of instructions.

(1) *Compute a triangular set* $\{g_1(x_1), g_2(x_1, x_2), \ldots, g_n(x_1, \ldots, x_n)\}$ *of generators of* $\mathfrak{M}$ (*e.g., use Algorithm* 5.3.12). *Then for* $i = 1, \ldots, n$, *let* $d_i = \deg(g_i)$.
(2) *Let* S_0 *be the set consisting of the empty tuple.*
(3) *For* $i = 1, \ldots, n$, *perform the following steps. Then return* S_n *and stop.*
(4) *Let* $S_i = \emptyset$. *For every tuple* $(h_1(y), \ldots, h_{i-1}(y))$ *in* S_{i-1}, *perform the following steps.*
(5) *Substitute* $x_1 \mapsto h_1(y), \ldots, x_{i-1} \mapsto h_{i-1}(y)$ *in* $g_1, \ldots, g_i$ *and get polynomials* $\tilde{g}_1(y), \ldots, \tilde{g}_{i-1}(y) \in K[y]$ *as well as* $\tilde{g}_i(x_i, y) \in K[x_i, y]$.
(6) *In the ring* $Q = K[x_i, y]$, *calculate the primary decomposition of the ideal* $I_i = \langle f(y), \tilde{g}_1(y), \ldots, \tilde{g}_{i-1}(y), \tilde{g}_i(x_i, y)\rangle$ *and get* $p_j(y) \in K[y]$ *such that*

$$I_i = \big\langle f(y), x_i - p_1(y)\big\rangle \cap \cdots \cap \big\langle f(y), x_i - p_{d_i}(y)\big\rangle$$

(7) *For* $j = 1, \ldots, d_i$, *append the tuple* $(h_1(y), \ldots, h_{i-1}(y), p_j(y))$ *to* S_i.

This is an algorithm which computes a set of d tuples S_n *whose residue classes in* $(L')^n$ *are precisely the zeros of* $\mathfrak{M}$.

Proof By Theorem 6.3.4 and Algorithm 6.3.6, the primary decomposition of the ideal I_i has the indicated form. Moreover, if we let $\mathfrak{M}_i = \langle g_1, \ldots, g_i\rangle$, then the homomorphism $K[x_1, \ldots, x_i]/\mathfrak{M}_i \longrightarrow L'$ given by $\bar{x}_k \mapsto h_k(\bar{y})$ for $k = 1, \ldots, i-1$ and $\bar{x}_i \mapsto p_j(\bar{y})$ is an injective K-algebra homomorphism. Thus the tuples in S_i represent zeros of the ideal $\mathfrak{M}_i$ in $(L')^i$. In particular, the final tuple S_n represents zeros of $\mathfrak{M}$ in $(L')^n$. The construction shows that the tuples in S_n represent $d_1 \cdots d_n$ pairwise isomorphisms $P/\mathfrak{M} \longrightarrow L'$, and hence pairwise distinct zeros of $\mathfrak{M}$. □

Notice that this algorithm requires chiefly factorizations of univariate polynomials over the field $L' = K[y]/\langle f(y)\rangle$. This special type of primary decompositions may be faster to determine than the general one (see Algorithm 5.3.8). Let us see a case in point.

Example 6.3.25 Let $K = \mathbb{F}_{101}$, let $P = K[x_1, x_2]$, let $\mathfrak{M}$ be the maximal ideal of P generated by the triangular set $\{x_1^2 - 2x_1 - 1, x_2^3 - x_2^2 - x_1x_2 - 12\}$, and let $L = P/\mathfrak{M}$. We calculate $\dim_K(L) = 6$. Now assume that we know the monic irreducible polynomial $f(y) = y^6 - y - 1$ in $K[y]$. Then the field $L' = K[y]/\mathfrak{M}'$, where we let $\mathfrak{M}' = \langle f(y)\rangle$, satisfies $\dim_K(L') = 6$, and thus $(L')^2$ contains the six zeros of $\mathfrak{M}$.

(a) First we compute these six zeros by applying Theorem 6.3.4 directly. In the ring $Q = K[x_1, x_2, y]$, we calculate the primary decomposition of the ideal $\mathfrak{M}Q + \mathfrak{M}'Q$ and get six maximal components $\mathfrak{M}_1, \ldots, \mathfrak{M}_6$. We represent these

ideas $\mathfrak{M}_i$ by their reduced Gröbner bases with respect to an elimination ordering for (x_1, x_2). The result is

$$\begin{aligned}
\mathfrak{M}_1 &= \mathfrak{M}'Q + \langle x_1 + 19y^5 - 45y^4 - 35y^3 + 9y^2 + 21y, \\
&\qquad x_2 + 3y^5 + 2y^4 - 12y^3 - 19y^2 + 22y + 14\rangle \\
\mathfrak{M}_2 &= \mathfrak{M}'Q + \langle x_1 + 19y^5 - 45y^4 - 35y^3 + 9y^2 + 21y, \\
&\qquad x_2 + 29y^5 + 42y^4 + 38y^3 + 44y^2 + 31\rangle \\
\mathfrak{M}_3 &= \mathfrak{M}'Q + \langle x_1 + 19y^5 - 45y^4 - 35y^3 + 9y^2 + 21y, \\
&\qquad x_2 - 32y^5 - 44y^4 - 26y^3 - 25y^2 + 48y - 41\rangle \\
\mathfrak{M}_4 &= \mathfrak{M}'Q + \langle x_1 - 19y^5 + 45y^4 + 35y^3 - 9y^2 - 21y - 2, \\
&\qquad x_2 - 46y^5 - 23y^4 - 22y^3 - 31y^2 + 14y + 38\rangle \\
\mathfrak{M}_5 &= \mathfrak{M}'Q + \langle x_1 - 19y^5 + 45y^4 + 35y^3 - 9y^2 - 21y - 2, \\
&\qquad x_2 + 40y^5 + 6y^4 - 41y^2 + 6y\rangle \\
\mathfrak{M}_6 &= \mathfrak{M}'Q + \langle x_1 - 19y^5 + 45y^4 + 35y^3 - 9y^2 - 21y - 2, \\
&\qquad x_2 + 6y^5 + 17y^4 + 22y^3 - 29y^2 - 20y - 39\rangle
\end{aligned}$$

(b) Now we solve the polynomial system defined by the generators of $\mathfrak{M}$ using Algorithm 6.3.24. Let us follows its steps.

(1) The generators $g_1(x_1) = x_1^2 - 2x_1 - 1$ and $g_2(x_1, x_2) = x_2^3 - x_2^2 - x_1x_2 - 12$ of $\mathfrak{M}$ form already a triangular set.
(6) The primary decomposition of the ideal $I_1 = \langle f(y), g_1(x_1)\rangle$ is of the form $I_1 = \langle f(y), x_1 - p_1(y)\rangle \cap \langle f(y), x_1 - p_2(y)\rangle$ where $p_1(y) = -19y^5 + 45y^4 + 35y^3 - 9y^2 - 21y$ and $p_2(y) = 19y^5 - 45y^4 - 35y^3 + 9y^2 + 21y + 2$.
(7) Hence we let $S_1 = \{(p_1(y)), (p_2(y))\}$.
(5) For $i = 2$ and $h_1(y) = p_1(y)$, the substitution $x_1 \mapsto p_1(y)$ yields the polynomial $\tilde{g}_2(x_2, y) = x_2^3 - x_2^2 + 19y^5x_2 - 45y^4x_2 - 35y^3x_2 + 9y^2x_2 + 21yx_2 - 12$.
(6) The primary decomposition of the ideal $\langle f(y), \tilde{g}_2(x_2, y)\rangle$ is of the form $I_{21} \cap I_{22} \cap I_{23}$ where

$$\begin{aligned}
I_{21} &= \langle f(y), x_2 + 3y^5 + 2y^4 - 12y^3 - 19y^2 + 22y + 14\rangle \\
I_{22} &= \langle f(y), x_2 + 29y^5 + 42y^4 + 38y^3 + 44y^2 + 31y + 26\rangle \\
I_{23} &= \langle f(y), x_2 - 32y^5 - 44y^4 - 26y^3 - 25y^2 + 48y - 41\rangle
\end{aligned}$$

(7) Hence we let $S_2 = \{(p_1(y), q_1(y)), (p_1(y), q_2(y)), (p_1(y), q_3(y))\}$, where $q_1(y) = -3y^5 - 2y^4 + 12y^3 + 19y^2 - 22y - 14$, $q_2(y) = -29y^5 - 42y^4 - 38y^3 - 44y^2 - 31y - 26$, and $q_3(y) = 32y^5 + 44y^4 + 26y^3 + 25y^2 - 48y + 41$.

(5) For $i = 2$ and $h_1(y) = p_2(y)$, the substitution $x_1 \mapsto p_2(y)$ yields the polynomial $\tilde{g}_2'(x_2, y) = x_2^3 - x_2^2 - 19y^5x_2 + 45y^4x_2 + 35y^3x_2 - 9y^2x_2 - 21yx_2 - 2x_2 - 12$.

(6) The primary decomposition of $\langle f(y), \tilde{g}_2'(x_2, y)\rangle$ is $I_{31} \cap I_{32} \cap I_{33}$ where

$$I_{31} = \langle f(y), x_2 - 46y^5 - 23y^4 - 22y^3 - 31y^2 + 14y + 38\rangle$$
$$I_{32} = \langle f(y), x_2 + 40y^5 + 6y^4 - 41y^2 + 6y\rangle$$
$$I_{33} = \langle f(y), x_2 + 6y^5 + 17y^4 + 22y^3 - 29y^2 - 20y - 3\rangle$$

(7) Now we append the three pairs $(p_2(y), q_1'(y))$, $(p_2(y), q_2'(y))$, and $(p_2(y), q_3'(y))$ to S_2, where $q_1'(y) = 46y^5 + 23y^4 + 22y^3 + 31y^2 - 14y + 38$, $q_2'(y) = -40y^5 - 6y^4 + 41y^2 - 6y$, and $q_3'(y) = -6y^5 - 17y^4 - 22y^3 + 29y^2 + 20y + 3$.

(3) The algorithm returns the set S_2 consisting of six pairs.

Altogether, we find the six zeros of $\mathfrak{M}$ in L' which are put into S_2 in the two iterations of Step (7) for $i = 2$, and these six zeros correspond to the six linear maximal ideals found in (a).

Now we use Algorithm 6.3.24 to solve a system of polynomial equations over the field $\mathbb{F}_2$.

Example 6.3.26 Let $K = \mathbb{F}_2$, and let us consider the system of polynomial equations defined by

$$f_1 = x_1^2 + x_1 + 1,$$
$$f_2 = x_2^3 + x_2 + 1$$

Let $P = K[x_1, x_2]$, and let $\mathfrak{M} = \langle f_1, f_2\rangle$. Since both f_1 and f_2 are irreducible over K, it follows that $\mathfrak{M}$ is a zero-dimensional radical ideal. By calculating the primary decomposition of $\mathfrak{M}$, we see that $\mathfrak{M}$ is a maximal ideal, and that the field $L = P/\mathfrak{M}$ satisfies $\dim_K(L) = 6$.

Furthermore, we assume that we are given the monic irreducible polynomial $f(y) = y^6 + y + 1$ in $K[y]$. Then also the ideal $\mathfrak{M}' = \langle f(y)\rangle$ is maximal in the ring $P' = K[y]$, and the field $L' = P'/\mathfrak{M}'$ is isomorphic to L. Again we use this information to find the zeros of $\mathfrak{M}$ in $(L')^2$ in two ways.

(a) First we follow the method suggested by Theorem 6.3.4. We compute the primary decomposition of the ideal $\mathfrak{M}Q + \mathfrak{M}'Q$ in the ring $Q = K[x_1, x_2, y]$ and get the result $\mathfrak{M}Q + \mathfrak{M}'Q = \mathfrak{M}_1 \cap \cdots \cap \mathfrak{M}_6$, where

$$\begin{aligned}
\mathfrak{M}_1 &= \langle y^6 + y + 1,\ x_1 + y^5 + y^4 + y^3 + y + 1,\ x_2 + y^3 + y^2 + y \rangle \\
\mathfrak{M}_2 &= \langle y^6 + y + 1,\ x_1 + y^5 + y^4 + y^3 + y,\ \ x_2 + y^4 + y^3 + 1 \rangle \\
\mathfrak{M}_3 &= \langle y^6 + y + 1,\ x_1 + y^5 + y^4 + y^3 + y + 1,\ x_2 + y^4 + y^2 + y + 1 \rangle \\
\mathfrak{M}_4 &= \langle y^6 + y + 1,\ x_1 + y^5 + y^4 + y^3 + y + 1,\ x_2 + y^4 + y^3 + 1 \rangle \\
\mathfrak{M}_5 &= \langle y^6 + y + 1,\ x_1 + y^5 + y^4 + y^3 + y,\ \ x_2 + y^4 + y^2 + y + 1 \rangle \\
\mathfrak{M}_6 &= \langle y^6 + y + 1,\ x_1 + y^5 + y^4 + y^3 + y,\ \ x_2 + y^3 + y^2 + y \rangle
\end{aligned}$$

For $i = 1, \ldots, 6$, the given generators form a σ-Gröbner basis of the maximal ideal $\mathfrak{M}_i$ for every elimination ordering σ for (x_1, x_2) on $\mathbb{T}(x_1, x_2, y)$. Hence the zeros of $\mathfrak{M}$ in the field $L' = K[y]/\langle f(y) \rangle$ are given by the six pairs

$$\begin{array}{ll}
(\bar{y}^5 + \bar{y}^4 + \bar{y}^3 + \bar{y} + 1,\ \bar{y}^3 + \bar{y}^2 + \bar{y}), & (\bar{y}^5 + \bar{y}^4 + \bar{y}^3 + \bar{y},\ \bar{y}^4 + \bar{y}^3 + 1) \\
(\bar{y}^5 + \bar{y}^4 + \bar{y}^3 + \bar{y} + 1,\ \bar{y}^4 + \bar{y}^2 + \bar{y} + 1), & (\bar{y}^5 + \bar{y}^4 + \bar{y}^3 + \bar{y} + 1,\ \bar{y}^4 + \bar{y}^3 + 1) \\
(\bar{y}^5 + \bar{y}^4 + \bar{y}^3 + \bar{y},\ \bar{y}^4 + \bar{y}^2 + \bar{y} + 1), & (\bar{y}^5 + \bar{y}^4 + \bar{y}^3 + \bar{y},\ \bar{y}^3 + \bar{y}^2 + \bar{y})
\end{array}$$

(b) Next we solve the given polynomial system using Algorithm 6.3.24. The primary decomposition of the ideal $I_1 = \langle f(y), x_1^2 + x_1 + 1 \rangle$ is

$$I_1 = \langle y^6 + y + 1, x_1 + y^5 + y^4 + y^3 + y \rangle \cap \langle y^6 + y + 1, x_1 + y^5 + y^4 + y^3 + y + 1 \rangle$$

Thus the set S_1 consists of $(y^5 + y^4 + y^3 + y)$ and $(y^5 + y^4 + y^3 + y + 1)$.

For each of these elements, the substitution into f_2 yields the same result, because f_2 does not involve x_1. A more thorough treatment of this case will be given in Proposition 6.3.32. So, in both iterations of the loop in Steps (4)–(7), we calculate the primary decomposition of $I_2 = \langle f(y), x_2^3 + x_2 + 1 \rangle$ and get

$$\begin{aligned}
I_2 = &\langle y^6 + y + 1, x_2 + y^3 + y^2 + y \rangle \cap \langle y^6 + y + 1, x_2 + y^4 + y^2 + y + 1 \rangle \\
&\cap \langle y^6 + y + 1, x_2 + y^4 + y^3 + 1 \rangle
\end{aligned}$$

Therefore the set S_2 is obtained by appending each of the three polynomials $y^3 + y^2 + y$, $y^4 + y^2 + y + 1$, and $y^4 + y^3 + 1$ to each of the two tuples in S_1. Altogether, we find the same six pairs as in (a).

Doing 170 km/h, I passed that slowcoach.
Then I had to wait for half an hour
until he administered me first aid.
(Harald Grill)

6.3.D Solving over Finite Fields via Recursion

To define recursion, we must first define recursion.

In the setting of the preceding subsection, suppose that we do not know an irreducible univariate polynomial of degree d over K. Can we still imitate Algorithm 6.3.24 and recursively split the task of computing a potentially huge primary decomposition into smaller ones? To answer this question, we first have to define which kind of recursion we look for.

Let K be a finite field having q elements, let $P = K[x_1, \ldots, x_n]$, and suppose that the polynomials defining the given system form a triangular set of a maximal ideal $\mathfrak{M}$ in P. Then we can split the first polynomial in a suitable extension field of K and work recursively over this field with the maximal ideal defined by substituting the various values of x_1 in the other generators of $\mathfrak{M}$. In the next section, when we try to solve polynomial systems over the rational numbers, this kind of recursive approach will become important.

Our first observation is that some of the powers needed to write down the zeros in Proposition 6.3.19 can be reduced substantially if we know a triangular set of generators of $\mathfrak{M}$, as the next proposition shows.

Proposition 6.3.27 *Let K be a finite field with q elements, let $P = K[x_1, \ldots, x_n]$, let $\mathfrak{M}$ be a maximal ideal of P, and let $L = P/\mathfrak{M}$. Furthermore, assume that we have a triangular set $\{f_1(x_1), f_2(x_1, x_2), \ldots, f_n(x_1, \ldots, x_n)\}$ of generators of $\mathfrak{M}$, and let $d_i = \deg_{x_i}(f_i)$ for $i = 1, \ldots, n$. After introducing new indeterminates $y_1, \ldots, y_n$, let $P' = K[y_1, \ldots, y_n]$, let $\mathfrak{M}'$ be the clone of $\mathfrak{M}$ in P', and let $L' = P'/\mathfrak{M}'$ be the clone of L. Then we have*

$$\mathscr{Z}_{L'}(\mathfrak{M}) = \Big\{ \big(\bar{y}_1^{q^{\beta_1}}, \ldots, \bar{y}_n^{q^{\beta_n}}\big) \in \big(L'\big)^n \;\Big|\; 0 \le \alpha_i \le d_i - 1 \text{ and } \beta_i = \alpha_1 + d_1\alpha_2 + \cdots + (d_1 \cdots d_{i-1})\alpha_i \text{ for } i = 1, \ldots, n \Big\}$$

Proof For $i = 0, \ldots, n$, we let $P'_i = K[y_1, \ldots, y_i]$, let $\mathfrak{M}'_i$ be the clone of the ideal $\mathfrak{M}_i = \langle f_1(x_1), \ldots, f_i(x_1, \ldots, x_i)\rangle$ in P'_i, and let $L'_i = P'_i/\mathfrak{M}'_i$. Here $\mathfrak{M}_i = \mathfrak{M} \cap P_i$ is a maximal ideal, and hence L'_i is a subfield of L'. Notice that the number of elements of L'_i is $q^{d_1 \cdots d_i}$.

Now we prove the proposition by induction on i. For $i = 1$, it follows from Proposition 6.3.15.b that the zeros of the ideal $\mathfrak{M}_1$ in L'_1 are given by $\bar{y}_1^{q^j}$ with $j = 0, \ldots, d_1 - 1$. To prove the induction step, we let $(\bar{y}_1^{q^{\beta_1}}, \ldots, \bar{y}_{i-1}^{q^{\beta_{i-1}}})$ be a zero of $\mathfrak{M}_{i-1}$ in $(L'_{i-1})^{i-1}$. We substitute this zero for $(x_1, \ldots, x_{i-1})$ in the polynomial $f_i(x_1, \ldots, x_i)$ and get an irreducible polynomial $g_i(x_i)$ in $L'_{i-1}[x_i]$.

To find the zeros of this polynomial, we use Proposition 6.3.13. Notice that, in view of the orders of the fields $L'_1, \ldots, L'_{i-1}$, the given zero of $\mathfrak{M}_{i-1}$ is equal to $(\bar{y}_1^{q^{\beta_{i-1}}}, \ldots, \bar{y}_{i-1}^{q^{\beta_{i-1}}})$. Now the fact that $(\bar{y}_1, \ldots, \bar{y}_i)$ is a zero of $\mathfrak{M}_i$ in the field L'_i and a β_{i-1}-fold application of the Frobenius homomorphism show that

$(\bar{y}_1^{q^{\beta_{i-1}}}, \ldots, \bar{y}_i^{q^{\beta_{i-1}}})$ is a zero of $\mathfrak{M}_i$. Hence one zero of $g_i(x_i)$ is $\bar{y}_i^{q^{\beta_{i-1}}}$. Since the field L'_{i-1} has $d_1 \cdots d_{i-1}$ elements, Proposition 6.3.13 implies that the other zeros of $g_i(x_i)$ are $\bar{y}_i^{q^{\beta_{i-1}+d_1\cdots d_{i-1}\alpha_i}}$ with $1 \le \alpha_i \le d_i - 1$. Since $\beta_i = \beta_{i-1} + d_1 \cdots d_{i-1}\alpha_i$, the induction step follows. When we reach $i = n$, the proof is complete. □

For practical computations, it is usually preferable that the output of an algorithm is in normal form, if it consists of residue classes. Thus the preceding proposition yields the following algorithm.

Algorithm 6.3.28 (Solving over $\mathbb{F}_q$ via Recursion)
Let K be a finite field with q elements, let $P = K[x_1, \ldots, x_n]$, let $\mathfrak{M}$ be a maximal ideal of P, let $L = P/\mathfrak{M}$, and let $d = \dim_K(L)$. Consider the following sequence of instructions.

(1) *Compute a triangular set $\{f_1(x_1), f_2(x_1, x_2), \ldots, f_n(x_1, \ldots, x_n)\}$ of generators of $\mathfrak{M}$ (e.g., use Algorithm 5.3.12), and let $d_i = \deg_{x_i}(f_i)$ for $i = 1, \ldots, n$.*
(2) *Let $S_0 = \{(\emptyset, 0)\}$. For $i = 1, \ldots, n$, perform the following steps.*
(3) *Let $S_i = \emptyset$. Introduce a new indeterminate y_i, and in $K[y_1, \ldots, y_i]$ define the ideal $\mathfrak{M}'_i = \langle f_1(y_1), \ldots, f_i(y_1, \ldots, y_i)\rangle$.*
(4) *For every pair (G_{i-1}, β_{i-1}) in S_{i-1}, perform the following step.*
(5) *For every $j \in \{0, \ldots, d_i - 1\}$, let $\beta_i = \beta_{i-1} + d_1 \cdots d_{i-1} j$, compute the normal form $h(y_1, \ldots, y_i) = \mathrm{NF}_{\mathfrak{M}'_i}(y_i^{q^{\beta_i}})$, append this polynomial to G_{i-1} to get a tuple G_i, and put the pair (G_i, β_i) into S_i.*

This is an algorithm which computes a set S_n of tuples of polynomials in $K[y_1, \ldots, y_n]$ whose residue classes in $(L')^n$ are precisely the zeros of $\mathfrak{M}$, where $L' = K[y_1, \ldots, y_n]/\mathfrak{M}'$ is the clone of L.

Proof In view of the proposition, it suffices to note that $y_i^{q^j}$ and $\mathrm{NF}_{\mathfrak{M}'_i}(y_i^{q^j})$ have the same residue class in the field $L'_i = K[y_1, \ldots, y_i]/\mathfrak{M}'_i$, and that L'_i is a subfield of L'. □

The following example shows that Proposition 6.3.27 allows us to reduce the powers necessary in Proposition 6.3.19.

Example 6.3.29 In the setting of Example 6.3.22, notice that the given set of generators $f_1 = x_1^2 + x_1 + 1$, $f_2 = x_2^3 + x_1$, and $f_3 = x_3^2 + x_3 + x_1$ is a triangular set of generators of the maximal ideal $\mathfrak{M}$ in $P = K[x_1, x_2, x_3]$. Thus we can apply Proposition 6.3.27 and get the following twelve zeros of $\mathfrak{M} = \langle f_1, f_2, f_3\rangle$ in the clone

$L' = K[y_1, y_2, y_3]/\mathfrak{M}'$ of $L = P/\mathfrak{M}$.

$$\begin{array}{llll} (y_1, y_2, y_3), & (y_1, y_2, y_3^{2^6}), & (y_1, y_2^{2^2}, y_3^{2^2}), & (y_1, y_2^{2^2}, y_3^{2^8}), \\ (y_1, y_2^{2^4}, y_3^{2^4}), & (y_1, y_2^{2^4}, y_3^{2^{10}}), & (y_1^2, y_2^2, y_3^2), & (y_1^2, y_2^2, y_3^{2^7}) \\ (y_1^2, y_2^{2^3}, y_3^{2^3}), & (y_1^2, y_2^{2^3}, y_3^{2^9}), & (y_1^2, y_2^{2^5}, y_3^{2^5}), & (y_1^2, y_2^{2^5}, y_3^{2^{11}}) \end{array}$$

When we apply Algorithm 6.3.28 to this system, we get the representations of the zeros of $\mathfrak{M}$ given in Example 6.3.22.b.

Another way to perform the last step of Algorithm 6.3.28 is given in the following version of the algorithm.

Algorithm 6.3.30 (Solving over $\mathbb{F}_q$ via Recursive Factorizations)
In the preceding algorithm, replace Steps (4) *and* (5) *by the following steps.*

(4') *For every tuple G in S_{i-1}, perform the following step.*

(5') *Let $L_i' = K[y_1, \ldots, y_i]/\mathfrak{M}_i'$. Substitute the entries of G for $x_1, \ldots, x_{i-1}$ in f_i and get a polynomial $\bar{f}_i(x_i)$ in $L_{i-1}'[x_i]$. Then compute the factorization $\bar{f}_i(x_i) = (x_i - \bar{h}_{i1}) \cdots (x_i - \bar{h}_{id_i})$ with $\bar{h}_{ij} \in L_i'$ and represent $\bar{h}_{ij}$ by a polynomial h_{ij} in $K[y_1, \ldots, y_i]$. For $j = 1, \ldots, d_i$, append the polynomial h_{ij} to G and put the resulting tuple into S_i.*

The result is an algorithm which computes a set S_n of tuples of polynomials in $K[y_1, \ldots, y_n]$ whose residue classes in $(L')^n$ are precisely the zeros of $\mathfrak{M}$.

Proof Clearly, a zero $(\bar{p}_1, \ldots, \bar{p}_n)$ of $\mathfrak{M}$ in $(L')^n$ yields a zero $G = (\bar{p}_1, \ldots, \bar{p}_{i-1})$ of $\mathfrak{M}_{i-1}$ in $(L_{i-1}')^{i-1}$ and a zero $\bar{p}_i$ of the polynomial $\bar{f}_i(x_i)$ in L_i', where $\bar{f}_i(x_i)$ is obtained by substituting G for $(x_1, \ldots, x_{i-1})$. Thus the zero $(\bar{p}_1, \ldots, \bar{p}_n)$ is computed during the course of the algorithm. Conversely, it is clear that every tuple $(h_1, \ldots, h_i)$ in S_i yields a zero $(\bar{h}_1, \ldots, \bar{h}_i)$ of $\mathfrak{M}_i$ in $(L')^n$. This proves the correctness of the algorithm. □

Comparing the last algorithm to Theorem 6.3.4, we see that it reduces the task of finding the primary decomposition of a big ideal $\mathfrak{M}Q + \mathfrak{M}'Q$ in a big polynomial ring $Q = K[x_1, \ldots, x_n, y_1, \ldots, y_m]$ to a number of univariate factorizations over extension fields of K.

In the next example we apply several solving methods to the polynomial system given in Example 6.3.23.

Example 6.3.31 Let $K = \mathbb{F}_7$, and let us consider the system of polynomial equations defined by

$$\tilde{f}_1 = x_1^4 - 2x_1 + 3,$$
$$\tilde{f}_2 = x_1^2 x_2^3 + 2x_1^2 - 2x_2 - 1$$

Let $P = K[x_1, x_2]$, let $\mathfrak{M} = \langle \tilde{f}_1, \tilde{f}_2 \rangle$, and let $L = P/\mathfrak{M}$. In Example 6.3.23 we checked that $\mathfrak{M}$ is a maximal ideal in the ring P, noted that the field L satisfies $d = \dim_K(L) = 12$, and found the twelve zeros of $\mathfrak{M}$ in a suitable extension of L. Here our goal is to find these zeros using different strategies.

(a) First we solve the task via Theorem 6.3.4. We have to form the polynomial ring $Q = K[x_1, x_2, y_1, y_2]$ and to compute the primary decomposition of the ideal $\mathfrak{M}Q + \mathfrak{M}'Q$, where $\mathfrak{M}'$ is the clone of $\mathfrak{M}$ in $P' = K[y_1, y_2]$. In this way we find again the 12 solutions listed in Example 6.3.23.

(b) Next we use Algorithm 6.3.28. We calculate a triangular set of generators of the ideal $\mathfrak{M}$ and get $\mathfrak{M} = \langle f_1(x_1), f_2(x_1, x_2) \rangle$, where $f_1(x_1) = \tilde{f}_1(x_1)$ and $f_2(x_1, x_2) = x_2^3 + 2x_1^3x_2 + 3x_1^2x_2 + 3x_2 + x_1^3 - 2x_1^2$. Thus we have $d_1 = 4$ and $d_2 = 3$, and the zeros of $\mathfrak{M}$ in $(L')^2$ are given by $(\bar{y}_1^{q^\alpha}, \bar{y}_2^{q^{4\beta}})$ with $0 \le \alpha \le 3$ and $0 \le \beta \le 2$.

(c) Finally, we use Algorithm 6.3.30. For $i = 1$, we have to factorize the polynomial $f_1(x_1) = x_1^4 - 2x_1 + 3$ over the field $L_1' = K[y_1]/\langle y_1^4 - 2y_1 + 3 \rangle$. We get

$$\begin{aligned} f_1(x_1) = (x_1 - \bar{y}_1)\big(x_1 + 3\bar{y}_1^3 + 3\bar{y}_1 - 1\big)\big(x_1 + 2\bar{y}_1^3 + 2\bar{y}_1^2 + 2\bar{y}_1 - 3\big) \\ \cdot \big(x_1 + 2\bar{y}_1^3 - 2\bar{y}_1^2 + 3\bar{y}_1 - 3\big) \end{aligned}$$

Therefore, when we start with $i = 2$, we have $S_1 = \{(y_1), (-3y_1^3 - 3y_1 + 1), (-2y_1^3 - 2y_1^2 - 2y_1 + 3), (-2y_1^3 + 2y_1^2 - 3y_1 + 3)\}$ and $L_1' = K[y_1]/\langle f_1(y_1) \rangle$. In the first iteration of Step (5'), we have to factorize the polynomial $f_2(\bar{y}_1, x_2) = x_2^3 + 2\bar{y}_1^3x_2 + 3\bar{y}_1^2x_2 + 3x_2 + \bar{y}_1^3 - 2\bar{y}_1^2$, and we get three irreducible factors, namely

$$\begin{aligned} &x_2 - \bar{y}_2 \\ &x_2 - \bar{y}_1^2\bar{y}_2^2 - \bar{y}_2^4 - \bar{y}_1^3 - \bar{y}_1^2\bar{y}_2 - 3\bar{y}_1\bar{y}_2^2 - 3\bar{y}_1^2 + \bar{y}_1\bar{y}_2 - \bar{y}_2^2 + 2\bar{y}_1 - 3\bar{y}_2 - 3 \\ &x_2 + \bar{y}_1^2\bar{y}_2^2 + \bar{y}_2^4 + \bar{y}_1^3 + \bar{y}_1^2\bar{y}_2 + 3\bar{y}_1\bar{y}_2^2 + 3\bar{y}_1^2 - \bar{y}_1\bar{y}_2 + \bar{y}_2^2 - 2\bar{y}_1 - 3\bar{y}_2 + 3 \end{aligned}$$

They correspond to the three zeros $(\bar{y}_1, \bar{y}_2)$, $(\bar{y}_1, \bar{y}_1^2\bar{y}_2^2 + \bar{y}_2^4 + \bar{y}_1^3 + \bar{y}_1^2\bar{y}_2 + 3\bar{y}_1\bar{y}_2^2 + 3\bar{y}_1^2 - \bar{y}_1\bar{y}_2 + \bar{y}_2^2 - 2\bar{y}_1 + 3\bar{y}_2 + 3)$, and $(\bar{y}_1, -\bar{y}_1^2\bar{y}_2^2 - \bar{y}_2^4 - \bar{y}_1^3 - \bar{y}_1^2\bar{y}_2 - 3\bar{y}_1\bar{y}_2^2 - 3\bar{y}_1^2 + \bar{y}_1\bar{y}_2 - \bar{y}_2^2 + 2\bar{y}_1 + 3\bar{y}_2 - 3)$ of $\mathfrak{M}$ in $(L')^2$.

In the next iteration of Step (5'), we factorize $f_2(-3\bar{y}_1^3 - 3\bar{y}_1 + 1, x_2)$, and we get another three zeros of $\mathfrak{M}$, and so on. Altogether, we find again the 12 solutions listed in Example 6.3.23.

There is still one very nice situation in which we do not have to make any recursive calls at all. It is described in the following proposition which takes care of

maximal ideals generated by special triangular sets, namely triangular sets consisting of univariate polynomials.

Proposition 6.3.32 (Solving Sequences of Univariate Polynomials)
Let K be a finite field with q elements, let $P = K[x_1, \ldots, x_n]$, and let $\mathfrak{M}$ be a maximal ideal in P of the form $\mathfrak{M} = \langle f_1(x_1), \ldots, f_n(x_n)\rangle$, where $f_i(x_i) \in P$. Moreover, for $i = 1, \ldots, n$, let $d_i = \deg(f_i)$, and let $d = \prod_{i=1}^{n} d_i$.

(a) *For every subset $\{i_1, \ldots, i_k\} \subseteq \{1, \ldots, n\}$, the ideal $\langle f_{i_1}(x_{i_1}), \ldots, f_{i_k}(x_{i_k})\rangle$ is a maximal ideal in the polynomial ring $K[x_{i_1}, \ldots, x_{i_k}]$.*
(b) *Let $\{i_1, \ldots, i_k\} \subset \{1, \ldots, n\}$, and let $j \in \{1, \ldots, n\} \setminus \{i_1, \ldots, i_k\}$. Then the image of $f_j(x_j)$ in $(K[x_{i_1}, \ldots, x_{i_k}]/\langle f_{i_1}(x_{i_1}), \ldots, f_{i_k}(x_{i_k})\rangle)[x_j]$ is irreducible.*
(c) *Let $P' = K[y_1, \ldots, y_n]$, let $\mathfrak{M}' = \langle f_1(y_1), f_2(y_2), \ldots, f_n(y_n)\rangle$ be the clone of $\mathfrak{M}$ in P', and let $L' = P'/\mathfrak{M}'$ be a clone of $P/\mathfrak{M}$. Then the ideal $\mathfrak{M}$ has d zeros in $(L')^n$, namely*

$$\mathscr{Z}_{L'}(\mathfrak{M}) = \left\{ \left(\bar{y}_1^{q^{i_1}}, \ldots, \bar{y}_n^{q^{i_n}} \right) \;\middle|\; 0 \le i_j \le d_j - 1 \text{ for } j = 1, \ldots, n \right\}$$

Proof Clearly, the ring $K[x_{i_1}, \ldots, x_{i_k}]/\langle f_{i_1}(x_{i_1}), \ldots, f_{i_k}(x_{i_k})\rangle$ is a zero-dimensional affine K-algebra. It is an integral domain, since it is contained in the field $P/\mathfrak{M}$. Consequently, it is a field by Corollary 2.2.6, and this proves (a).

Since claim (b) follows from (a), it remains to prove (c). By Proposition 6.3.13, for every $j \in \{1, \ldots, n\}$, the residue classes $\bar{y}_j^{q^0}, \bar{y}_j^{q^1}, \ldots, \bar{y}_j^{q^{d_j-1}}$ are pairwise distinct zeros of $f_j(x_j)$ in $K[y_j]/\langle f_j(y_j)\rangle$. Therefore they are distinct zeros of $f_j(x_j)$ in the larger field L'. Consequently, we have found d distinct zeros of $\mathfrak{M}$ in $(L')^n$, and the proof is complete. □

Let us reconsider Example 6.3.26.

Example 6.3.33 As in Example 6.3.26, we let $K = \mathbb{F}_2$, let $P = K[x_1, x_2]$, and let $\mathfrak{M} = \langle f_1(x_1), f_2(x_2)\rangle$, where $f_1(x_1) = x_1^2 + x_1 + 1$ and $f_2(x_2) = x_2^3 + x_2 + 1$. Then $\mathfrak{M}$ is a maximal ideal of P which satisfies the hypothesis of the proposition. Therefore, to find the zeros of $\mathfrak{M}$, we let $P' = K[y_1, y_2]$, let $\mathfrak{M}'$ be the clone of $\mathfrak{M}$ in P', and let $L' = P'/\mathfrak{M}'$. By the proposition, the set of zeros of $\mathfrak{M}$ in $(L')^2$ is

$$\mathscr{Z}_{L'}(\mathfrak{M}) = \left\{ (\bar{y}_1, \bar{y}_2), \left(\bar{y}_1, \bar{y}_2^2\right), \left(\bar{y}_1, \bar{y}_2^{2^2}\right), \left(\bar{y}_1^2, \bar{y}_2\right), \left(\bar{y}_1^2, \bar{y}_2^2\right), \left(\bar{y}_1^2, \bar{y}_2^{2^2}\right) \right\}$$

Using normal forms with respect to $\mathfrak{M}'$, we can also write this set of zeros as $\mathscr{Z}_{L'}(\mathfrak{M}) = \{(\bar{y}_1, \bar{y}_2), (\bar{y}_1, \bar{y}_2^2), (\bar{y}_1, \bar{y}_2^2 + \bar{y}_2), (\bar{y}_1 + 1, \bar{y}_2), (\bar{y}_1 + 1, \bar{y}_2^2), (\bar{y}_1 + 1, \bar{y}_2^2 + \bar{y}_2)\}$.

http://www.springer.com/978-3-319-43599-2

Computational Linear and Commutative Algebra

Kreuzer, M.; Robbiano, L.

2016, XVIII, 321 p. 1 illus., Hardcover
ISBN: 978-3-319-43599-2