Decomposition of polynomials

6.1 A polynomial-time algorithm for decomposition

The first polynomial time algorithms for decomposition of polynomials have been presented by Gutierrez et al. (1988) and practically at the same time by D. Kozen and S. Landau (1989). We follow the approach of Kozen and Landau.

The problem to be considered is to decide whether a given polynomial $f(x)$ can be written as the functional composition of other polynomials, i.e., whether

$$f(x) = g(h(x)) = (g \circ h)(x)$$

for some polynomials $g, h$. We assume all the polynomials to have coefficients in a computable field $K$.

Decompositions of polynomials are interesting, e.g., for the solution of polynomial equations. If $f = g \circ h$, we can find the roots of $f$ by solving for the roots $\alpha$ of $g$ and then for the roots of $h - \alpha$.

In factoring polynomials we have to identify factorizations that differ only by a constant. A similar restriction has to be enforced in decomposing polynomials, since for every $a \in K^*$ the linear polynomials

$$l_a^{(1)}(x) = ax + b \quad \text{and} \quad l_a^{(2)}(x) = \frac{1}{a}(x - b)$$

are inverses of each other under composition. Thus, every polynomial admits a trivial decomposition of the form

$$f(x) = l_a^{(1)} \circ l_a^{(2)} \circ f(x).$$

Definition 6.1.1. Let $f(x) \in K[x]$ be monic and of degree $> 1$. A (functional) decomposition of $f$ is a sequence $g_1, \ldots, g_k$ of polynomials in $K[x]$ such that

$$f = g_1 \circ g_2 \circ \ldots \circ g_k, \quad \text{i.e.,} \quad f(x) = g_1(g_2(\ldots g_k(x) \ldots)).$$

The $g_i$ are called the components of the decomposition of $f$. If all decompositions of $f$ are trivial, i.e., all but one of the components are linear, then $f$ is called indecomposable. A complete decomposition is one in which all components are of degree $> 1$ and indecomposable.
Obviously it is sufficient to decompose monic polynomials. If \( f(x) \) admits a decomposition \( f = g \circ h \) and \( c = \text{lc}(h) \), then also \( f = g' \circ h' \), where \( g'(x) = g(c \cdot x) \) and \( h'(x) = h(x)/c \). So it suffices to search for decompositions into monic components. For a similar reason we can assume that \( h(0) = 0 \), i.e., the constant coefficient of \( h \) is 0.

Complete decompositions are not unique, even if we disregard trivial decompositions. Further ambiguities in decomposition are

\[
x^n \circ x^m = x^m \circ x^n \quad \text{for } m, n \in \mathbb{N}
\]
and

\[
T_n \circ T_m = T_m \circ T_n \quad \text{for } m, n \in \mathbb{N},
\]
where \( T_n(x) \) is the \( n \)-th Chebyshev polynomial \((T_0(x) = 1, T_1(x) = x, T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x) \text{ for } n > 1)\). However, J. F. Ritt (1922) has shown that these are the only ambiguities.

**Theorem 6.1.1.** A monic polynomial \( f(x) \in K[x] \), \( \deg(f) > 1 \), has a unique complete decomposition up to trivial decompositions and the ambiguities (6.1.1), provided \( \text{char}(K) = 0 \) or \( \text{char}(K) > \deg(f) \).

Now let \( f(x) \in K[x] \), \( \deg(f) = n \), be the monic polynomial that we want to decompose. Let \( n = rs \) be a non-trivial factorization of the degree of \( f \). Then we want to decide whether \( f \) can be decomposed into polynomials \( g \) and \( h \) of degrees \( r \) and \( s \), respectively, and if so compute such a decomposition.

\[
f = x^{rs} + a_{rs-1}x^{rs-1} + \ldots + a_0,
g = x^r + b_{r-1}x^{r-1} + \ldots + b_0,
h = x^s + c_{s-1}x^{s-1} + \ldots + c_1x.
\]

Let \( \beta_1, \ldots, \beta_r \) be the (not necessarily different) roots of \( g \) in an algebraic extension of \( K \). So

\[
g(x) = \prod_{i=1}^{r} (x - \beta_i),
\]
and therefore

\[
f(x) = g(h(x)) = \prod_{i=1}^{r} (h(x) - \beta_i).
\]

**Lemma 6.1.2.** Let \( f_1, f_2, g \in K[x] \) be monic. If \( f_1 \) and \( f_2 \) agree on their first \( k \) coefficients, then so do \( f_1g \) and \( f_2g \).

**Proof.** Exercise 1.