Trager's Algorithm

November 21, 2023 8:46 AM

Trager's factorization algorithm. 1976

Suppose $f \in \mathbb{Q}(\alpha)[x]$ is monic.

Idea:

$$\begin{tikzcd}
f \in \mathbb{Q}(\alpha)[x] \arrow[r, "\text{factor}", "\text{over } \mathbb{Q}(\alpha)?"'] \arrow[d, "N"] & f_1 \cdot f_2 \cdots f_k \\
h \in \mathbb{Q}[x] \arrow[r, "\text{factor over } \mathbb{Q}"] & h_1 \cdot h_2 \cdots h_l. \arrow[u, "?\ \gcd(f, h_i)?"']
\end{tikzcd}$$

Def. Let $f \in k[x]$, k a field. f is square-free if $\nexists\, b \in k[x]$ s.t. $\deg(b) > 0$ and $b^2 \nmid f$.

Lemma. f is square-free $\iff$ $\gcd(\underline{f(x)}, \underline{f'(x)}) \neq 1$.

Suppose $f(x,\alpha)$ is square-free.

Compute $N(f(x,\alpha)) = \operatorname{res}(m(z), f(x,z)) \in \mathbb{Q}[x]$.

Factor $N(f)$ over $\mathbb{Q}$.

[Lemma 1 (v) $\deg(N(f)) = \deg(m,z) \cdot \deg(f,x) \Rightarrow$ blowup.]

Theorem 8.16 If $f(x,\alpha)$ is irreducible over $\mathbb{Q}(\alpha)$ then $N(f)$ is a power of an irreducible poly over $\mathbb{Q}$.

$\Rightarrow$ If $\underline{f(x,\alpha) = f_1(x,\alpha) \cdots f_k(x,\alpha)}$ where f_i are irreducible over $\mathbb{Q}(\alpha)$

then $\underline{N(f)} = \underline{N(f_1)} \cdot \underline{N(f_2)} \cdots \underline{N(f_k)} \Rightarrow$

Th 8.18

The factorization of $N(f)$ has at most k factors.

f is square-free

Suppose $N(f)$ is also square-free as in example ①.

Then $N(f)$ has k irreducible factors over $\mathbb{Q}$.

I.e. $N(f) = N(f_1) \cdot N(f_2) \cdots N(f_k)$
$= g_1 \cdot g_2 \cdots g_k \leftarrow$ irreducible.

But. $f_i(x,\alpha) \mid N(f_i) \Rightarrow f(x,\alpha) = \prod_{i=1}^{k} \gcd(f, g_i)$
L1 (iii)

$f(x,\alpha)$ ↑ monic $\gcd$ ↑ monic. g_i ↑ factored $N(f)$.

E.g. ① $\gcd(f(x,\alpha) = x^2 + (1+2\sqrt{2})x + 2+\sqrt{2}, x^2-2 = (x-\sqrt{2})(x+\sqrt{2})) = x+\sqrt{2} = f_1$

$= (x+\sqrt{2})(x+\sqrt{2}+1)$

$\gcd(f, x^2+2x-1) = x+\sqrt{2}+1.$

This gcd is computed in $\mathbb{Q}(\alpha)[x] \cong [\mathbb{Q}[z]/m(z)][x]$.

If we use the Euc. Alg. it's ~~slow~~.

$\boxed{\text{One can devise a modular gcd algorithm that uses the Chinese remainder Theorem and rational reconstruction.}}$

Theorem 8.18. If $f(x,\alpha)$ is square-free then $N(f(x-s\alpha,\alpha))$ is square-free for all but finitely many $s \in \mathbb{C}$. ↑ shift with $s \in \mathbb{Z}$.

E.g. $\alpha = \sqrt{2}$
$f(x,\alpha) = x^2-2$
Pick $s=2$
$x \to x-2\sqrt{2}$

$f(x-2\sqrt{2}, \sqrt{2}) = (x-2\sqrt{2})^2-2$
$= x^2-4\sqrt{2}x+8-2$
$= (x-\sqrt{2})(x-3\sqrt{2}).$

$N(f(x-2\sqrt{2},\sqrt{2})) = \mathrm{res}(m(z), (x-2z)^2-2)$
which is S.F. $= x^4 - 20x^2 + 36$
factor over $\mathbb{Q}$ $= (x^2-2)(x^2-18).$

$\gcd(f(x-2\sqrt{2}), x^2-2) = x-\sqrt{2} \longrightarrow x+\sqrt{2}$
$\gcd(f(x-2\sqrt{2}), x^2-18) = x-3\sqrt{2} \longrightarrow x-\sqrt{2}$
$x \to x+2\sqrt{2}$

Ex. Use resultants to characterize which $s \in \mathbb{Q}$ make $N(f(x-s\alpha,\alpha))$ not Square-Free.

Hint. Let $R = N(f) = \mathrm{res}(m(z), f(x-sz, z)) \in \mathbb{Q}[s,x].$

R is NOT square-free $\iff \gcd(R(x), R'(x)) \neq 1.$

$\iff \mathrm{res}(R(x), R'(x), x) = 0.$

$\in \mathbb{Q}[s].$

Proof of Th 8:18.

Lemma 2. If $f \in \mathbb{Q}[x]$ and f is square-free then there are only a finite number of $s \in \mathbb{Q}$ s.t. $f(x - s\alpha, \alpha)$ is NOT square-free.

Proof. Let the roots of $f(x)$ be $\beta_1, \beta_2, \dots, \beta_m \in \mathbb{C}$.

The β's are distinct as f is square-free.

$\Rightarrow$ The roots of $f(x - s\alpha)$ are $\beta_1 + s\alpha, \beta_2 + s\alpha, \dots, \beta_m + s\alpha$.

Let the roots of $m(z)$ be $\alpha_1, \alpha_2, \dots, \alpha_d$.

Let $E(x) = N(f(x - s\alpha)) = \prod_{i=1}^{d} f(x - s\alpha_i)$.

So the roots of $E(x)$ are $\beta_j + s\alpha_i \quad 1 \le i \le d,\ 1 \le j \le m.$

$E(x)$ is NOT square-free $\Rightarrow E(x)$ has multiple roots

$\Rightarrow \beta_j + s\alpha_i = \beta_k + s\alpha_\ell.$

$i = \ell \iff j = k$

$\Rightarrow s = \dfrac{\beta_k - \beta_j}{\alpha_i - \alpha_\ell}.$

$\Rightarrow$ There are $\le 1 + \binom{d}{2}\binom{m}{2}$ choices for $s \in \mathbb{Q}$.

$i \neq \ell$.

Lemma 3. If $f(x, \alpha)$ is square-free in $\mathbb{Q}(\alpha)[x]$ then $\exists\, g(x) \in \mathbb{Q}[x]$ s.t. $f(x, \alpha) \mid g(x)$ and $g(x)$ is square-free.

Proof. Let $E(x) = N(f(x, \alpha)) \in \mathbb{Q}(x)$.

Let $\prod_{i=1}^{\ell} g_i(x)^i$ be the square-factorization of $E(x)$ in $\mathbb{Q}(x)$.

Now $f(x,\alpha) \overset{L1}{\mid} N(f(x,\alpha)) = \prod g_i(x)^i \in \mathbb{Q}[x]$.

But f is S.F. $\Rightarrow$ $f \mid \prod g_i = g(x)$ which is S.F.

Ex. In (3) $N(f) = (x^2-2)^2(x^4-2) \Rightarrow g(x) = (x^2-2)(x^4-2)$.

Proof of Th 8.18. Let $g(x)$ be the polynomial in Lemma 3.

By Lemma 2 $N(g(x-s\alpha))$ is not S.F. for finitely many s.

But $f(x,\alpha) \mid g(x) \Rightarrow f(x-s\alpha) \mid g(x-s\alpha)$

L1 (iv) $\Rightarrow$ $N(f(x-s\alpha)) \mid N(g(x-s\alpha))$.

$N(f(x-s\alpha))$ is not S.F. for finitely many s. $\Leftarrow$ $N(g(x-s\alpha))$ is not S.F. for finitely many s by Lemma 2.