Lec17A Square-free factorization. Michael Monagan

March 16, 2021 12:34 PM

Chapter 8 Polynomial Factorization

$\mathbb{Z}[x]$ ✓, $\mathbb{F}_q[x]$ ✓, $\mathbb{Q}(\alpha)[x]$ ✗

8.2 Square-free factorization.

Let $a \in K[x]$, K a field, e.g. $K = \mathbb{Q}$.

Idea $a = x^8 + 2x^6 - 3x^4 - 8x^2 - 4 = (x^4-4)(x^2+1)^2$

not irreducible; is irreducible.

square-free

Def: a is square-free if a has no repeated factors
i.e. $\exists\, b \in K[x]$ s.t. $\deg(b) > 0$ and $b^2 \mid a$.

Lemma 1. a is ~~not~~ square-free $\iff \gcd(a, a') = 1$. ($\neq 1$)

Proof. ① Suppose a is not square-free.
Then $a = b^2 \cdot c$ for some $b, c \in K[x]$ with $\deg(b) > 0$.

$$\gcd(a,a') = \gcd(b^2 c,\ 2\cdot b \cdot b' c + c' \cdot b^2)$$
$$= b \cdot \gcd(bc,\ 2b'c + c'b)$$
$$\neq 1.$$

② Suppose a is square-free.
Then $a = f_1 \cdot f_2 \cdots f_n$ for some irreducible $f_i \in K[x]$
with $\gcd(f_i, f_j) = 1$ $\forall i \neq j$.

$$\gcd(a,a') = \gcd(f_1, a') \cdot \gcd(f_2, a') \cdot \cdots \cdot \gcd(f_n, a).$$

$$\gcd(f_1 a') = \gcd(f_1,\ f_1' f_2 f_3 \cdots f_n + f_1 f_2' f_3 \cdots f_n + \cdots + f_1 f_2 \cdots f_{n-1} f_n')$$
$$= \gcd(f_1,\ f_1' f_2 f_3 \cdots f_n)$$
$$= \gcd(f_1, f_1')$$
$$= 1$$

irreducible; $\deg f_1' \overset{?}{=} \deg f_1 - 1$

True for $\mathbb{Q} \subset K$

? $\boxed{\mathbb{Z}_p \subset K}$

$$[f_1 (f_2 f_3)]' = f_1'(f_2 f_3) + f_1 (f_2' f_3 + f_2 f_3') = f_1' f_2 f_3 + f_1 f_2' f_3 + f_1 f_2 f_3'$$

Consider $f_1 = x^3 + 1 \in \mathbb{Z}_3[x]$.
$f_1' = 3x^2 = 0$
$\gcd(f_1, f_1') = \gcd(x^3+1, 0) = x^3 + 1.$

But $x^3 + 1 = (x+1)^3$ is not square-free.

Exercise Show that $f_1' = 0 \Rightarrow f_1$ is not square-free.

Def. A square-free factorization of $a \in K[x] \setminus K$ is

$$a = \prod_{i=1}^{n} a_i^i \quad \text{where } a_i \in K[x],\ \gcd(a_i, a_i') = 1 \text{ and } \gcd(a_i, a_j) = 1 \ \forall i \neq j.$$

Example $a = \underset{\div 4}{(x+2)}\underset{\times 2}{(x^2+x)^2}\, 1^3 (x^2+2)^4$ Unique upto $\times$ by units.

Lemma 2. Let $a = f_1^1 f_2^2 f_3^3 \cdots f_n^n$ be a square-free factorization.
If $\mathbb{Q} \subset K$ then $\gcd(a, a') = f_2^1 f_3^2 f_4^3 \cdots f_n^{n-1}$.

Proof. $\gcd(a, a') = \gcd(f_1 f_2^2 \cdots f_n^n,\ f_1' f_2^2 f_3^3 \cdots f_n^n + 2 f_2' f_2 f_1 f_3^3 \cdots f_n^n + 3 f_3' f_3^2 f_1 f_2^2 \cdots f_n^n + \cdots + n f_n' f_n^{n-1} f_1 f_2^2 \cdots f_{n-1}^{n-1})$.

$= f_2 f_3^2 \cdots f_n^{n-1} \cdot \gcd(f_1 f_2 \cdots f_n,\ f_1' f_2 f_3 \cdots f_n + 2 f_2' f_1 f_3 \cdots f_n + \cdots + n f_n' f_1 f_2 \cdots f_{n-1})$ $= S$.

Show $\gcd(\underbrace{f_1 f_2 \cdots f_n}, S) = 1$.
factors are square-free & relatively prime.

$\gcd(f_1, S) = \gcd(f_1, f_1' f_2 f_3 \cdots f_n)$
$= 1.$ $\gcd(f_1, f_1') = 1$ $\gcd(f_1, f_j) = 1 \ \forall j \neq 1.$

Similarly for $\gcd(f_i, S) = 1$.

Algorithm SQRFREE
Input $a \in K[x]$, K is a field, $\mathbb{Q} \subset K$, $\deg a \geq 1$.
Output $f_1, f_2, \ldots, f_n$ s.t. $a = f_1 f_2^2 f_3^3 \cdots f_n^n$ is a square-free factorization.

1. If $\deg(a) = 1$ return a.
2. $g \leftarrow \gcd(a, a')$ $\xrightarrow{L2}$ $= f_2 f_3^2 \cdots f_n^{n-1}$
   L1 if $g = 1$ return a.
   $\bar{a} \leftarrow a/g$ $= f_1 f_2 f_3 \cdots f_n$ ←
3. $h \leftarrow \gcd(g, \bar{a})$ $= f_2 f_3 \cdots f_n$ ←
   $f_1 \leftarrow \bar{a}/h$.
4. Let $f_2, f_3, \ldots, f_n = \text{SQRFREE}(g)$

(5) Return $(f_1, \underline{f_2}, \underline{f_3}, \ldots, f_n)$

Remark: Only need poly. $\div$, $\frac{d}{dx}$, gcd in $K[x]$.

Example. $a = x^4 + 3x^3 + 3x^2 + x \quad = x \cdot 1^2 \cdot (x+1)^3$

$g \leftarrow \gcd(a, a') \overset{L2}{=} (x+1)^2 = x^2 + 2x + 1$

$\bar{a} \leftarrow a/g = x \cdot (x+1)$

$h \leftarrow \gcd(\bar{a}, g) = x+1$

$f_1 \leftarrow \bar{a}/h = x.$

CALL SQRFREE$(g = (x+1)^2) \longrightarrow 1, x+1.$

Return$(\underline{x, 1, x+1})$

Recursive call for

$a = x^2 + 2x + 1 \quad = (x+1)^2$

$g = \gcd(a, a') \quad = (x+1)$

$\bar{a} = a/g \quad = (x+1)$

$h = \gcd(g, \bar{a}) \quad = (x+1)$

$f_1 = \bar{a}/h. \quad = 1$

SQRFREE$(g = x+1) \longrightarrow x+1$

Return $1, x+1.$