Lecture 20: Gauss' lemma

16 October 2020
12:50

Defⁿ: Let R be an int dom which admits gcd & $f(x) = a_n X^n + a_{n-1} X^{n-1} + \dots + a_0 \in R[X]$ be a nonzero poly. Then content of f denoted by $c(f) = \gcd(a_n, a_{n-1}, \dots, a_0)$.

Note $c(f)$ is defined upto an associate, i.e. $c = c(f)$ iff $uc = c(f)$ for any unit $u \in R$.

Also $d = \gcd(a_0, \dots, a_n)$ if $d \mid a_i$ $\forall\, 0 \le i \le n$ and if $d' \in R$ be s.t. $d' \mid a_i$ $0 \le i \le n \Rightarrow d' \mid d$.

Gauss' Lemma

version 1: Let R be a UFD and $f(x), g(x) \in R[X]$ then

$c(fg) = c(f)c(g)$. i.e. $d = \gcd(\text{coeff of } fg)$, $d_1 = \gcd(\text{coeff of } f)$, $d_2 = \gcd(\text{coeff of } g)$, $d \sim d_1 d_2$

version 2: Let R be a UFD & $K = QF(R)$. Let $f(X) \in R[X] \subseteq K[X]$.

If $f(X) = g(X)h(X)$ for some $g, h \in K[X]$

then $f(X) = G(X)H(X)$ for some $G, H \in R[X]$ with

$\deg(G) = \deg(g)$ & $\deg(H) = \deg(h)$

Cor: Let R be a UFD & $K = QF(R)$. A poly $f(X) \in R[X]$ of content 1 is irreducible in $R[X]$ iff $f(X)$ is irred in $K[X]$. (A poly of content 1 is called a primitive poly)

Pf: ($\Leftarrow$) $f(X)$ is reducible in $R[X] \Rightarrow f(X) = g(X)h(X)$ where $g(X), h(X) \in R[X] \subseteq K[X]$ are non units.

Since $c(f) = 1$, $g(x)$ and $h(X)$ are non constant poly. Hence they are non units in $K[X]$. Hence $f(X)$ is reducible in $K[X]$.

Conversely, $f(X)$ is reducible in $K[X] \Rightarrow f(X) = g(X)h(X)$, $g(X), h(X) \in K[X]$ are nonconst poly. Hence by Gauss' lemma $f(X)$ is reducible in $R[X]$.

version 1 $\Rightarrow$ version 2 :

Let $g(X) = b_m X^m + b_{m-1} X^{m-1} + \dots + b_1 X + b_0$ and

$h(X) = c_\ell X^\ell + c_{\ell-1} X^{\ell-1} + \dots + c_1 X + c_0$ where b's & c's $\in K$

say $b_i = \frac{b_i'}{b_i''}$

$b_i', b_i'' \in R$

$b = \prod_{i=0}^{m} b_i''$

collecting denominator $\exists\, b, c \in R$ s.t.

$G_1(X) = b\, g(X) \in R[X]$ & $H_1(X) = c\, h(X) \in R[X]$.

Hence $bc\, f(X) = G_1(X) H_1(X)$ in $R[X]$ $(\because f(X) = g(X) h(X))$

version 1 $\Rightarrow$ $bc\, c(f) = c(G_1)\, c(H_1)$ ... (*)

Now $G_1(X) = c(G_1)\, G(X)$ for some $G(X) \in R[X]$

& $H_1(X) = c(H_1)\, H(X)$ " " $H(X) \in R[X]$

and $f(X) = c(f)\, F(X)$ " " $F(X) \in R[X]$

$bc\, f(X) = G_1(X) H_1(X) \Rightarrow$

$bc\, c(f)\, F(X) = c(G_1)\, c(H_1)\, G(X) H(X)$

$\overset{(*)}{\Rightarrow}$ $F(X) = G(X) H(X)$

$\overset{\cdot c(f)}{\Rightarrow}$ $f(X) = \underbrace{c(f) G(X)}_{\in R[X]} H(X)$ & $\deg(c(f) G(X)) = \deg(g(X))$

& $\deg(H(X)) = \deg h(X)$

(Gauss' original result)

(*) A primitive poly $f(X) \in \mathbb{Z}[X]$

is $g(X) h(X)$ for some $g, h \in \mathbb{Q}[X]$

Then $f(X) = G(X) H(X)$ in $\mathbb{Z}[X]$

with $\deg G = \deg g$ &

$\deg H = \deg h$.

Pf of version 1:

Let $f(X) = g(X)h(X)$ for $f, g, h \in R[X]$

$g(X) = c(g)G(X)$, $h(X) = c(h)H(X)$ for some $G, H \in R[X]$

So

$f(X) = c(g)c(h)G(X)H(X)$

Hence $c(g)c(h) \mid c(f)$

Let $c(g)c(h) = p_1 \cdots p_n$ where $p_i \in R$ are irreducible.

$\Rightarrow$ $c(f) = p_1 \cdots p_n q_1 q_2 \cdots q_m$ for some $m \geq 0$, $q_i \in R$ are irred.

Suppose $m \neq 0$ then q_1 exist.

$c(f) = c(g)c(h)d$ for some $d \in R$

Also $f(x) = c(f)F(X)$ for some $F[X] \in R[X]$

$c(f)F(X) = c(g)c(h)G(X)H(X)$

$dF[X] = G(X)H(X)$ where G, H are primitive. and $d = q_1 \cdots q_m$

$q_1 \mid G(X) H(X)$

$$G(X) = b_m X^m + b_{m-1} X^{m-1} + \dots + b_0$$
$$H(X) = c_\ell X^\ell + c_{\ell-1} X^{\ell-1} + \dots + c_0$$

Let i_0 be the smallest integer s.t. $q_1 \nmid b_{i_0}$

j_0 " " " " " $q_1 \nmid c_{j_0}$

Note $i_0 \leq m$ & $j_0 \leq \ell$. ($\because G, H$ are primitive)

Consider the coeff of $X^{i_0+j_0}$ in

$G(X) H(X)$. $a = b_{i_0} c_{j_0} + b_{i_0+1} c_{j_0-1} + \dots + b_{i_0+j_0} c_0$

$+ b_{i_0-1} c_{j_0+1} + \dots + b_0 c_{i_0+j_0}$

By hyp $q_1 \mid a$. Also q_1 divides all the terms except $b_{i_0} c_{j_0}$.

Hence $q_1 \mid b_{i_0} c_{j_0}$. This contradicts that q_1 is prime element of R

(as $q_1 \nmid b_{i_0}$ & $q_1 \nmid c_{j_0}$ but q_1 is irred element of a UFD.)

∎