Lecture 21: Applications of Gauss' lemma

27 October 2020
16:06

Recall: Gauss' Lemma

<u>version 1</u>: Let R be a UFD and $f(x), g(x) \in R[X]^{*}$ then

$c(fg) = c(f)c(g)$.

<u>version 2</u>: 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

$\deg(G) = \deg(g)$ & $\deg(H) = \deg(h)$. In fact $G = ag$, $H = bh$ where $a, b \in R^{\times}$.

<u>Cor</u>: 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 $K[X]$.

<u>Example</u>: 1) $f(X) = 3X - 6 \in \mathbb{Z}[X]$ $\quad$ $f(x) = 3(x-2)$ is red in $\mathbb{Z}x$.

But in $\mathbb{Q}[X]$ $f(x)$ is irred.

2) $\mathbb{Q}[X,Y]$, $\mathbb{Q}(X)[Y]$ where $\mathbb{Q}(X)$ is fraction field of $\mathbb{Q}[X]$

$f(X,Y) = 3Y^3 + 2XY^2 + 7Y + 3X + 5$

Is $f(X,Y)$ irred ?

$f(X,Y) \in \mathbb{Q}(Y)[X]$ $\quad$ $R = \mathbb{Q}[Y]$, $K = \mathbb{Q}(Y)$

$(2Y^2+3)X + 3Y^3 + 7Y + 5$ is irred in $\mathbb{Q}(Y)[X]$

$\gcd(2Y^2+3, 3Y^3+7Y+5) = 1$ ($\because$ $2Y^2+3$ is irred. & $2Y^2+3 \nmid 3Y^3+7Y+5$)

$\xRightarrow{\text{Gauss' Lemma}}$ f is irred in $\mathbb{Q}[X,Y]$

$\xRightarrow{\text{Gauss' lemma}}$ " " " " $\mathbb{Q}(X)[Y]$ (here $R = \mathbb{Q}[X]$, $R[Y] = \mathbb{Q}[X,Y]$)

(*) Note $f(X) = g_1 \cdots g_r$ in $K[X]$ in version 2 then

$f(X) = G_1 \cdots G_r$ in $R[X]$ where $G_i = a_i g_i$ for some $a_i \in R^{\times}$.

Thm: Let R be a UFD then $R[X]$ is a UFD.

Pf: Let $K = QF(R)$ and $f(X) \in R[X]$. Assume $f(X)$ is nonzero nonunit.

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

Since R is a UFD, if $c(f)$ is not a unit $c(f) = p_1 \cdots p_r$ product irred in R

(this exists since R is a UFD)

$F(X) \in R[X] \subseteq K[X]$ and $K[X]$ is a UFD.

Hence if $F(X)$ is non constant. $F(X) = g_1(X) \cdots g_s(X)$ where $g_1, \dots, g_s \in K[X]$ are irred.

By Gauss' lemma

$$F(X) = G_1(X) \cdots G_s(X)$$

where $G_i(X) \in R[X]$ and $\deg g_i = \deg G_i$ infact $G_i(X)$ are irred in $K[X]$ as g_i are irred & $G_i \sim g_i$ in $K[X]$

associate

Also $c(F) = 1$

$\overset{\text{version 1}}{\Rightarrow}$ $c(G_1)c(G_2) \cdots c(G_s) = 1 \Rightarrow c(G_i) = 1$

$\Rightarrow$ G_i's are primitive poly irred in $K[X]$.

$\overset{\text{Cor to Gauss' lemma}}{\Rightarrow}$ G_i's are irred in $R[X]$.

Also p_i's are irred in $R \Rightarrow p_i$'s are irred in $R[X]$.

Hence $f(X) = p_1 \cdots p_r G_1(X) \cdots G_s(X)$ can be written as a product of irred elements of $R[X]$.

For Uniqueness, suppose $f(X) = q_1(X) \cdots q_t(X)$ be product of irred in $R[X]$.

Since $q_i(X) \in R[X]$ are irred. and

$q_i(X) = c(q_i) Q_i(X)$ for some $Q_i(X) \in R[X]$

either $c(q_i) = 1$ or $Q_i(X) = 1$, i.e. $q_i(X)$ is a const or q_i is a primitive poly.

Let $q_1, \ldots, q_n$ be const. & $q_{n+1}, \ldots, q_t$ be primitive poly

then $c(f) = q_1 \cdots q_n$ (Gauss' lemma $\Rightarrow$ $q_{n+1} \cdots q_t$ is prim poly)

But R is a UFD $\Rightarrow$ $n = r$ & after reordering

$p_i \sim q_i$ in R $\Rightarrow$ $p_i \sim q_i$ in $R[X]$

Also $F(X) = q_{n+1}(X) \cdots q_t(X) = G_1(X) \cdots G_s(X)$

and $q_{n+i}(X)$ are irred in $K[X]$

(Gauss' lemma & q_{n+i}'s are irred prim poly in $R[X]$)

Hence $t = n+s = r+s$ & after reordering

$q_{n+i} \sim G_i$ in $K[X]$ for $1 \le i \le s$

i.e. $q_{n+i} = u_i G_i$ for some $u_i \in K \setminus \{0\}$, $u_i = \frac{a_i}{b_i}$, $a_i, b_i \in R$, $b_i \neq 0$

$b_i q_{n+i} = a_i G_i$

But q_{n+i} & G_i are primitive in $R[X]$

$b_i = c(b_i q_{n+i}) = c(a_i G_i) = a_i$

$\Rightarrow u_i$ is a unit in R.

i.e. $b_i \sim a_i$ in R

$\Rightarrow q_{n+i} \sim G_i$ in $R[X]$.

$\Rightarrow u_i = \frac{a_i}{b_i}$ is a unit in R $\blacksquare$

Noetherian Rings

Prop: Let R be a commutative ring with unity. The following are equivalent:

(1) Every R-ideal is finitely generated.

(2) Every increasing chain of R-ideals is eventually constant.

i.e. $I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots$ be a seq of R-ideals then $\exists N$ s.t. $\forall n \geq N$ $I_n = I_N$.

(3) Every non-empty collection of R-ideals has a maximal element. w.r.t inclusion

Def^n A ring satisfying the above equivalent conditions is called a noetherian ring.

Examples: Fields, PID. Hilbert basis thm: R is noeth $\Rightarrow R[x]$ is noeth.

(*) Localization of noetherian is noetherian.

(*) R is noeth I R-ideal then R/I is noeth.

(*) $R_1, \dots, R_n$ noeth. $\Rightarrow R_1 \times \cdots \times R_n$ is noeth.

Proof of the proposition:

(1) $\Rightarrow$ (2): Let $I_0 \subseteq I_1 \subseteq \cdots$ be inc seq of R-ideals

$I = \bigcup_{n \geq 0} I_n$ is an ideal of R.

By (1) $I = (x_1, \dots, x_m)$ for some $m \geq 1$ & $x_1, \dots, x_m \in R$.

So $x_i \in I = \bigcup_{n \geq 0} I_n$

$\Rightarrow x_i \in I_{n_i}$ $\quad n_i \geq 0 \quad 1 \leq i \leq m$

Then take $N = \max\{n_i \mid 1 \leq i \leq m\}$

$I \subseteq I_N$ $(\because x_i \in I_N \ \forall 1 \leq i \leq m)$

$\Rightarrow I_N = I = I_n \quad \forall n \geq N.$

(2) $\Rightarrow$ (3): Let Ω be a nonempty collection of R-ideals. Suppose Ω has no maximal element.

Let $I_0 \in \Omega$. Since I_0 is not maximal element of Ω $\exists I_1 \in \Omega$ s.t. $I_0 \subsetneq I_1$ continue this way to construct a seq of R-ideals

$$I_0 \subsetneq I_1 \subsetneq I_2 \subsetneq I_3 \cdots$$

But this contradicts (2).

③ $\Rightarrow$ ①: Let

$I \subseteq R$ be an ideal.

Let $x_0 \in I$

If $I_0 = (x_0) = I$ then done

otherwise let $x_1 \in I \setminus I_0$.

Let $I_1 = (x_0, x_1) \subseteq I$

again if $I_1 = I$ then done

otherwise let $x_2 \in I \setminus I_1$ &

$I_2 = (x_0, x_1, x_2)$. Continuing

this way, we construct a collection

of ideals $I_0, I_1, I_2, \ldots$

If this process doesn't stop

then $\Omega = \{ I_k \mid k \geq 0 \}$

is a nonempty collection of ideals

no maximal element.

$\left(\because I_0 \subsetneq I_1 \subsetneq I_2 \subsetneq \cdots \right)$

contradicting ③