Gauss' Lemma

Jiang-Hua Lu

The University of Hong Kong

Algebra II, HKU

Monday, Feb 10, 2025

In this file:

1. §1.3.1: Gauss' Lemma on products of primitive elements in $R[x]$;
2. §1.3.2: Gauss' Lemma relating irreducible elements in $F[x]$ and $R[x]$;
3. §1.3.3: Characterization of irreducible elements in $R[x]$ via $R[x] \subset F[x]$

What is Gauss' Lemma about:

Gauss' Lemma is about irreducible elements in $R[x]$, where R is a UFD.

We will also give the following applications of Gauss' Lemma:

1. Theorem: If R is a UFD, so is $R[x]$ and thus also $R[x_1, x_2, \ldots, x_n]$;
2. Testing irreducibility for $f(x) \in \mathbb{Q}[x]$ by testing in $\mathbb{Z}[x]$.

高斯引理的部分作用：证明UFD**上的**n元多项式环是UFD
检验Frac(R)[x]中的元素是否可约，只要检验对应的R[x]**中的元素**

Recall some facts about irreducible elements.:

- If R is any integral domain, a non-zero non-unit $r \in R$ is said to be irreducible if whenever
$$r = ab$$
for some $a, b \in R$, then either a is a unit or b is a unit.
- An element in R is said to be reducible if it is not irreducible, i.e., $r = ab$ for $a, b \in R$ both non-units.
- If R is a UFD, irreducible elements are the same as prime elements.

An irreducible element of $R[x]$ is also called an irreducible polynomial over R.

$\underline{(1+2x)}\,\underline{(1-2x)} = 1-4x^2$ in $\mathbb{Z}/4\mathbb{Z}[x]$

A simple fact on units in $R[x]$:

- If R is an integral domain, units in $R[x]$ are precisely the units of R regarded as constant polynomials.

HW

Examples:

- There are exactly two units in $\mathbb{Z}[x]$: the constant polynomials ± 1;
- For a field F, units are exactly the non-zero constant polynomials.

Consequently,

- $2x + 4 = 2(x + 2) \in \mathbb{Z}[x]$ is reducible;
- $2x + 4 = 2(x + 2) \in \mathbb{Q}[x]$ is irreducible.

§1.3.1: Gauss' Lemma on products of primitive elements in $R[x]$

Definition. Let R be a UFD. For a non-zero $f \in R[x]$, define

$$\mathrm{cont}(f) = \text{a gcd of all the non-zero coefficients of } f,$$

and call it a content of f. Say f is primitive if it has 1 as a content.

Lemma. For every non-zero $f(x) \in R[x]$,

1. $f(x) = \gamma g(x)$, where $\gamma = \mathrm{cont}(f)$, and $g(x) \in R[x]$ is primitive.
2. any other such product is of the form
$$f(x) = (\gamma u^{-1}) u g(x)$$
where $u \in R$ is a unit. Note that $ug(x)$ is primitive.

Proof. Exercise.

Eg:

$$f(x) = 1+2x+3x^2+4x^3+5x^4+6x^5$$
$$g(x) = 7x^2+5$$

$$f(x)g(x) = 42x^7+35x^6+(28+30)x^5+\cdots$$

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n \qquad a_n \neq 0$$
$$g(x) = b_0 + b_1 x + \cdots + b_m x^m \qquad b_m \neq 0$$
$$h(x) = c_0 + c_1 x + \cdots + c_{m+n} x^{m+n}$$
$$c_k = \sum_{i+j=k} a_i b_j$$

Claim: $\gcd(a_0, a_1, \cdots a_n) = \gcd(b_0, b_1, \cdots b_m) = 1$

$$\Longrightarrow \gcd(c_0, c_1, \cdots c_{m+n}) = 1$$

Gauss Lemma

Theorem

(Gauss' Lemma on products of primitive elements in $R[x]$): Let R be a UFD. If $f, g \in R[x]$ are primitive, so is fg.

Proof. Suppose not. Then $\exists p \in R$ irreducible such that $p|(fg)$.

- Since p is irreducible and R is a UFD, p is prime. $\pi : R \to R/pR,\ r \mapsto r+pR$
- Let $R_1 = R/pR$. Then R_1 is an integral domain.
- Consider the ring homomorphism

$$\pi : \quad R[x] \longrightarrow R_1[x], \quad \sum_n r_n x^n \longmapsto \sum_n \pi(r_n) x^n.$$

- $p|(fg)$ implies that $\pi(fg) = 0$, i.e., $\pi(f)\pi(g) = 0$.
- Since $R_1[x]$ is an integral domain, $\pi(f) = 0$ or $\pi(g) = 0$.
- In other words, $p|f$ or $p|g$. Contradiction.

Q.E.D.

§1.3.2: Gauss' Lemma relating irreducible elements in $F[x]$ and $R[x]$

Let R be a UFD and $F = \mathrm{Frac}(R)$ the fraction field of R.

The case of $R = \mathbb{Z}$:

- $\mathbb{Q}$ is the fraction field of $\mathbb{Z}$.
- We can clear the denominators for every non-zero $f(x) \in \mathbb{Q}[x]$.

Example: For

$$f(x) = \frac{1}{8}x^5 + 4x^3 - \frac{1}{6}x^2 - 1 \in \mathbb{Q}[x],$$

clearing the denominator gives

$$f(x) = \frac{1}{24}(3x^5 + 96x^3 - 4x^2 - 24) \in \mathbb{Q}[x].$$

$$= \frac{1}{48}(6x^5 + 192x^3 - 8x^2 - 48)$$

Cleaning denominators: Let again R be a UFD and $F = \mathrm{Frac}(R)$.

Lemma. For every non-zero $f(x) \in F[x]$,

1. $f(x) = \alpha g(x)$, where $\alpha \in F$, and $g(x) \in R[x]$ is primitive.
2. any other such product is of the form
$$f(x) = (\alpha u^{-1}) u g(x)$$
where $u \in R$ is a unit. Note that $ug(x)$ is primitive.

Proof. Exercise.

Remarks:

1. Write $g = \mathrm{pp}(f) \in R[x]$ and call it the primitive part of f.
2. $\mathrm{pp}(f)$ is well-defined up to multiplication by units of R.

Theorem

(Gauss' Lemma relating irreducible elements in $F[x]$ and $R[x]$): Let R be a UFD and $F = \mathrm{Frac}(R)$. For a non-constant $f \in F[x]$,

2nd Version

$$f \in F[x] \text{ is irreducible} \quad \text{iff} \quad \mathrm{pp}(f) \in R[x] \text{ is irreducible.}$$

Proof. Lemma is equivalent to saying that

$$f \in F[x] \text{ is reducible} \quad \text{iff} \quad \overset{\Longleftarrow\,?}{} \quad \mathrm{pp}(f) \in R[x] \text{ is reducible.}$$

- Assume that $\mathrm{pp}(f) \in R[x]$ is reducible. Then

$$\mathrm{pp}(f) = k(x)h(x)$$

  for some $k(x), h(x) \in R[x]$ with neither a (constant) unit of R.
- Since $\mathrm{pp}(f)$ is primitive, both $k, h \in R[x]$ have positive degrees.
- Thus $f(x) = \lambda k(x)h(x) \in F[x]$ is reducible.

Proof of Gauss' Lemma relating irreducible elements in $F[x]$ and $R[x]$, cont'd:

Assume that $f(x) \in F[x]$ is reducible.

- Then $f(x) = a(x)b(x)$ for $a(x), b(x) \in F[x]$ with positive degrees.
- Write $a(x) = \alpha a_1(x)$ and $b(x) = \beta b_1(x)$, where $\alpha, \beta \in F$ and both $a_1(x), \cancel{a_1} b_1(x) \in R[x]$ are primitive.
- Then $f(x) = \alpha\beta a_1(x)b_1(x)$.
- $a_1(x)\cancel{a_1} b_1(x) \in R[x]$ is primitive by Gauss' Lemma on products of primitive elements in $R[x]$.
- Thus $\mathrm{pp}(f) = a_1(x)b_1(x) \in R[x]$, hence reducible.

$R = \mathbb{C}[x_1, \cdots x_n]$ $\qquad$ $\mathbb{Z}/n\mathbb{Z}$ $\qquad$ **Q.E.D.**

$R[x] = \mathbb{C}[x_1, \cdots, x_n, x] \subset \mathbb{C}(x_1, \cdots x_n)[x]$

§1.3.3: Characterization of irreducible elements in $R[x]$ via $R[x] \subset F[x]$:

Let R be a UFD and $F = \mathrm{Frac}(R)$ the fraction field of R.

Theorem. Irreducible elements in $R[x]$ are precisely of the two types:

1. Type I: constant polynomials defined by irreducible elements of R;
2. Type II: primitive polynomials $f(x) \in R[x]$ irreducible in $F[x]$.

Proof. Assume that $f \in R[x]$ is non-zero and non-unit.

- Case 1: $f(x) = r \in R$ is a constant. Then f is irreducible as an element in $R[x]$ if and only if $r \in R$ is irreducible.
- Case 2: f is not a constant. Write $f = \gamma g$, where $\gamma = \mathrm{cont}(f) \in R$ and $g \in R[x]$ primitive. Then

$$\begin{aligned} f \text{ is irreducible in } R[x] &\iff \gamma \in R \text{ is a unit and } f \text{ is irreducible in } R[x], \\ &\iff f \text{ is primitive and is irreducible in } R[x], \\ &\iff f \text{ is primitive and is irreducible in } F[x]. \end{aligned}$$

By 2nd Version of Gauss Lemma

Q.E.D.

Remarks:

- Define a proper factorization of $g(x) \in R[x]$ to be one of the form

$$g(x) = k(x)h(x),$$

where $k(x), h(x) \in \cancel{\mathbb{Z}}R[x]$ both with positive degrees.

- A primitive $g \in R[x]$ is irreducible iff it has no proper factorization.
- A primitive $g \in R[x]$ is reducible iff it has a proper factorization