MATH4302, Algebra II, Spring 2022

Jiang-Hua Lu

The University of Hong Kong

Week 3, Thursday February 10, 2022

Topics for today:

1. §1.3.1: Gauss' lemma

Eg: 1) $R = \mathbb{Z}$
2) $R = \mathbb{C}[x]$

What is Gauss' Lemma about:

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

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.

Some simple facts on units in $R[x]$:

$\mathbb{Z}[x] \ni f(x) = 15$

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

Examples:

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

Why do we care about irreducible elements?

Recall an important way of constructing new fields from old ones:

Lemma. If F is a field and $f(x) \in F[x]$ is irreducible, then

$$K = F(x)/\langle f \rangle$$

is a field containing F as a sub-field via

$$F \longrightarrow K, \ \lambda \longmapsto \lambda + \langle f \rangle.$$

↑ const. polynomial in $F[x]$

Defintiion:

A field K containing F as a sub-field is called a field extension of F.

Why do we care about irreducible elements?

- It is very useful to find irreducible elements in $F[x]$ for a field F.
- Irreducible elements in $F[x]$ are called, irreducible polynomials over F.

Examples:

- Irreducible polynomials in $\mathbb{C}[x]$ are exactly $f(x) = ax+b$, $a, b \in \mathbb{C}$, $a \neq 0$.
- Irreducible polynomials in $\mathbb{R}[x]$ are $f(x) = ax+b$, or ax^2+bx+c, $b^2-4ac<0$.
- Irreducible polynomials in ~~$\mathbb{Q}[x]$~~ over $\mathbb{Q}$? They give extensions of $\mathbb{Q}$. important in number theory.
- Note that $\mathbb{Q}$ is the fraction field of $\mathbb{Z}$.

$b \neq 0$ $d \neq 0$ $\frac{a}{b} \sim \frac{c}{d} \iff ad = bc$.

What is Gauss' Lemma about, cont'd:

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

- We have said
  - Gauss' Lemma is about irreducible elements in $R[x]$.
- More precisely,
  - Gauss' Lemma relates irreducible elements in $R[x]$ and in $F[x]$.

Two applications of Gauss' Lemma:

$\mathbb{Q}[x]$ $\mathbb{Z}[x]$

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

$R[x_1][x_2] = R[x_1, x_2]$

Strategies in 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

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

$$= \frac{1}{24}\left(3x^5 + 96x^3 - 4x^2 - 24\right)$$

Example: Factor out the gcd:

$$f(x) = 2x + 4 = 2(x+2) \in \mathbb{Z}[x]$$

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. $f(x) = 2x+4 = 2(x+2) = -2(-x-2)$

Let R be a UFD.

$f(x) = 5x^3 + 7x - 2$ $\quad g(x) = 9x^6 - 3x^2 + 4x - 1$

$f(x)g(x) = 54x^9 + 63x^7 - 18x^6 - 15x^5 + \cdots + 2$

Gauss' Lemma, version 0. 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.
- Let $R_1 = R/pR$. Then R_1 is an integral domain. $\quad \pi: R \to R_1$
- Consider the ring homomorphism $\quad \pi(r_n) = r_n + pR \in R_1$

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

- $p|(fg)$ 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.

$R = \mathbb{C}[x]$

Clea~~ning~~ ring denominators: Let again R be a UFD and $F = \mathrm{Frac}(R)$. $\ni \frac{a}{b}$, $b \neq 0$, $a, b \in R$

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. deg $g(x)$ = deg $f(x)$
2. any other such product is of the form
$$f(x) = (\gamma u^{-1}) ug(x)$$
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.

$F = \mathbb{Q}$

$R = \mathbb{Z}$

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

Gauss' Lemma, version 1: For any non-zero non-unit $f \in F[x]$.

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

Equivalently,

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

Remarks:

- A non-primitive $g(x) \in R[x]$ is reducible: for example, $g(x) = 2x + 4 = 2(x + 4) \in \mathbb{Z}[x]$ is reducible.
- If $g \in R[x]$ is primitive, then g is reducible iff $g(x)$ can be written as

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

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

Proof of Gauss' Lemma:

The easy direction:

- Assume that $\mathrm{pp}(f) \in \mathbb{Z}[x]$ is reducible.
- Since $\mathrm{pp}(f)$ is primitive, we have

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

  for some $k, h \in R[x]$ with positive degrees.
- Thus $f(x) = \lambda k(x)h(x) \in F[x]$ is reducible.

Proof of Gauss' Lemma, 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 $a_1(x), \cancel{a_2}\, b_1(x) \in R[x]$ are primitive.
- Then $f(x) = \alpha\beta \boxed{a_1(x) b_1(x)}$.
- By Gauss' Lemma, version 0, $a_1(x)a_2(x) \in R[x]$ is primitive.
- Thus $\mathrm{pp}(f) = a_1(x)b_1(x) \in R[x]$, hence reducible.

Q.E.D.