Foreword

Usage

- Notes are presented in two columns: main notes on the left, and sidenotes on the right. Main notes will have a larger margin.
- The following is the color code for the notes:

Blue	Definitions
Red	Important points
Yellow	Points to watch out for / comment for incompletion
Green	External definitions, theorems, etc.
Light Blue	Regular highlighting
Brown	Secondary highlighting

- The following is the color code for boxes, that begin and end with a line of the same color:

Blue	Definitions
Red	Warning
Yellow	Notes, remarks, etc.
Brown	Proofs
Magenta	Theorems, Propositions, Lemmas, etc.

- Hyperlinks are underlined in magenta. If your PDF reader supports it, you can follow the links to either be redirected to an external website, or a theorem, definition, etc., in the same document. Note that this is only reliable if you have the full set of notes as a single document, which you can find on:
  `https://japorized.github.io/TeX_notes`

34 Lecture 34 Jul 23rd 2018

34.1 Factorizations in Integral Domains (Continued 4)

34.1.1 Gauss' Lemma (Continued)

Lemma 104 (Role of the Content)

Let R be a UFD and let $0 \neq f(x) \in R[x]$.

1. *$f(x)$ can be written as*

$$f(x) = \mathrm{c}(f) f_1(x)$$

   where $f_1(x)$ is primitive.

2. *If $0 \neq b \in R$, then $\mathrm{c}(bf) = b\,\mathrm{c}(f)$.*

Proof

1. *Let $c = \mathrm{c}(f) \sim \gcd(a_0, a_1, ..., a_m)$, where we let $f(x) = a_m x^m + \ldots + a_0$. Since c is the gcd, for $0 \leq i \leq m$, write*

$$a_i = c b_i.$$

   Then $f(x) = c f_1(x)$ where

$$f_1(x) = b_m x^m + \ldots + b_0.$$

   Then by Proposition 97, we have

$$c \sim \gcd(a_0, a_1, ..., a_m) \sim \gcd(cb_0, ..., cb_m) \sim c \gcd(b_0, ..., b_m).$$

It follows that $\gcd(b_0, ..., b_m) \sim 1$ *and so* $f_1(x)$ *is primitive.*

2. *This is an immediate result from* 🔥 *Proposition 97.*

□

🌲 Lemma 105 (Non-Trivial Irreducible Polynomials are Primitive)

Let R *be a UFD and* $l(x) \in R[x]$ *be irreducible with* $\deg l \geq 1$. *Then* $\mathrm{c}(l) \sim 1$.

✎ Proof

By Lemma 104, we can write

$$l(x) = \mathrm{c}(l) l_1(x)$$

for some $l_1(x) \in R[x]$. *Since* $l(x)$ *is irreducible, by* 🔥 *Proposition 92, we have either* $\mathrm{c}(l) \sim 1$ *or* $l_1(x) \sim 1$. *However, since* $\deg l = \deg l_1 \geq 1$, *we have that* $l_1(x) \not\sim 1$ *and so* $\mathrm{c}(l) \sim 1$. □

Example 34.1.1

The polynomial $2x + 4 \in \mathbb{Q}[x]$ *is irreducible*[1]. *However, the polynomial* $2x + 4 \in \mathbb{Z}[x]$ *is not irreducible. For instance,*

$$2x + 4 = 2(x + 2)$$

but both 2 *and* $(x + 2)$ *are not units of* $\mathbb{Z}[x]$.

[1] Any factorization of $2x + 4$ in $\mathbb{Q}[x]$ will always result in one of the factors being a unit.

☕ Theorem 106 (Gauss' Lemma)

Let R *be a UFD. For any non-zero* $f(x), g(x) \in R[x]$, *we have*

$$\mathrm{c}(fg) \sim \mathrm{c}(f)\,\mathrm{c}(g)$$

Proof

By Lemma 104, let

$$f(x) = \mathrm{c}(f) f_1(x)$$
$$g(x) = \mathrm{c}(g) g_1(x),$$

where $f_1(x)$ and $g_1(x)$ are primitive. Then by part (2) of Lemma 104, we have

$$\mathrm{c}(fg) = \mathrm{c}(\mathrm{c}(f) f_1 \, \mathrm{c}(g) g_1) = \mathrm{c}(f) \, \mathrm{c}(g) \, \mathrm{c}(f_1 g_1).$$

From here, if $(f_1 g_1) \sim 1$, our proof is complete. Thus, it suffices to show that $f(x)g(x)$ is primitive when $f(x)$ and $g(x)$ are primitive, i.e. $\mathrm{c}(f) \sim 1 \, \mathrm{c}(g)$.

Suppose that we have that $f(x)$ and $g(x)$ are primitive but $f(x)g(x)$ is not primitive. Since R is a UFD, by Theorem 98, $\exists p \in R$ such that p divides each coefficient of $f(x)g(x)$. Write

$$f(x) = a_0 + a_1 x + \ldots a_m x^m$$
$$g(x) = b_0 + b_1 x + \ldots b_n x^n.$$

Since $f(x)$ and $g(x)$ are primitive, p does not divide each a_i or each b_j [2]. *Then $\exists k, s \in \mathbb{N} \cup \{0\}$ such that*

- *$p \nmid a_k$ but $p \mid a_i$ for $0 \leq i < k$ and*
- *$p \nmid b_s$ but $p \mid b_j$ for $0 \leq j < s$.*

Note that the coefficient of x^{k+s} in $f(x)g(x)$ is

$$c_{k+s} = \sum_{i+j=k+s} a_i b_j.$$

From the two bullet points, we have that p divides all a_i and b_j with $i + j = k + s$ except $a_k b_s$. It follows that $p \nmid c_{k+s}$, which contradicts the fact that p divides all coefficient of $f(x)g(x)$. Therefore, $f(x)g(x)$ is primitive. □

[2] Otherwise, $f(x)$ and $g(x)$ would not be primitives since if p does divide all of the coefficients, then $\mathrm{c}(f) \not\sim 1$ or $\mathrm{c}(g) \not\sim 1$, i.e. they are not primitives.

Theorem 107 (Reducibility in the Field of Fractions)

Let R be a UFD whose field of fractions is F [3]. *If $l(x) \in R[x]$ is irreducible in $R[x]$, then $l(x)$ is irreducible in $F[x]$.*

The contrapositive of this theorem is rather interesting: If $f(x) \in F[x]$ is reducible, then $f(x)$ is also reducible in $R[x]$!

[3] Note that we regard $R \subseteq F$ as a subring of F, as per usual.

Proof

Let $l(x) \in R[x]$ be irreducible. Suppose $l(x) = g(x)h(x) \in F[x]$ for some $g(x)$, $h(x) \in F[x]$. If a and b [4] are the products of the denominators of the coefficients of $g(x)$ and $h(x)$, respectively, then

[4] They are both in F.

$$\left.\begin{aligned} g_1(x) &= ag(x) \\ h_1(x) &= bh(x) \end{aligned}\right\} \in R[x].$$

Then $abl(x) = g_1(x)h_1(x)$ is a factorization in $R[x]$. Since $l(x)$ is irreducible in $R[x]$, we have that $\mathrm{c}(l) \sim 1$ by Lemma 105. Then by Theorem 106, we have

$$ab \sim ab\,\mathrm{c}(l) \sim \mathrm{c}(abl) \sim \mathrm{c}(g_1h_1) \sim \mathrm{c}(g_1)\,\mathrm{c}(h_1). \tag{34.1}$$

By Lemma 104, write

$$\begin{aligned} g_1(x) &= \mathrm{c}(g_1)g_2(x) \\ h_1(x) &= \mathrm{c}(h_1)h_2(x) \end{aligned}$$

where $g_2(x)$, $h_2(x) \in R[x]$ are primitive. Then we have

$$abl(x) = g_1(x)h_1(x) = \mathrm{c}(g_1)\,\mathrm{c}(h_1)g_2(x)h_2(x).$$

Then by Equation (34.1), we have

$$l(x) \sim g_2(x)h_2(x).$$

Since $l(x)$ is irreducible in $R[x]$, it follows, WLOG, that $g_2(x) \sim 1$, which then

$$ag(x) = g_1(x) = \mathrm{c}(g_1)g_2(x) = \mathrm{c}(g_1)v$$

for some unit $v \in R$. And so

$$g(x) = a^{-1}\,\mathrm{c}(g_1)v$$

is also a unit. Therefore, we have that

$$l(x) = g(x)h(x) \in F[x]$$

implies that either $g(x)$ or $h(x)$ is a unit, i.e. $l(x)$ is irreducible in $F[x]$. □