# *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`

# 35 Lecture 35 Jul 25th 2018

## 35.1 Factorizations in Integral Domains (Continued 5)

### 35.1.1 Gauss' Lemma (Continued 2)

We have shown in Example 33.1.1 that $\mathbb{Z}[x]$ is not a PID. Our goal now is the show that, in spite of that, $\mathbb{Z}[x]$ is a UFD.

**Note**

*Recall the following results from the recent lectures: Let $R$ be a UFD with $F$ being its field of fractions. We have*

- $l(x) \in R[x]$ *is irreducible* $\implies \mathrm{c}(l) \sim 1$ *(Lemma 105);*
- $\mathrm{c}(fg) \sim \mathrm{c}(f)\,\mathrm{c}(g)$ *(Lemma 104);*
- $l(x)$ *is irreducible in* $R[x] \implies l(x)$ *is irreducible in* $F[x]$ *(Theorem 107).*

**Note**

*Recall that the contrapositive of Theorem 107 is: if $l(x)$ is reducible in $F[x]$, then $l(x)$ is reducible in $R[x]$.*

*In other words, for $f(x) \in R[x]$, if $f(x) = g(x)h(x) \in F[x]$, then $\exists \tilde{g}(x), \tilde{h}(x) \in R[x]$ such that*

$$f(x) = \tilde{g}(x)\tilde{h}(x) \in R[x].$$

**Example 35.1.1**

$2x^2 + 7x + 3 \in \mathbb{Z}[x]$, *which we observe that*

$$\begin{aligned} 2x^2 + 7x + 3 &= \left( x + \frac{1}{2} \right) (2x + 6) \\ &= (2x + 1)(x + 3). \end{aligned}$$

We want to take advantage of the fact that $\mathbb{Q}[x]$ is a UFD to show that $\mathbb{Z}[x]$ is also a UFD.

Recall from Example 34.1.1 that $2x + 4 \in \mathbb{Q}[x]$ is irreducible, but is reducible in $\mathbb{Z}[x]$. Therefore, we have that the converse of Theorem 107 is not true.

### Proposition 108

*Let $R$ be a UFD with field of fractions $F$. TFAE:*

1. *$f(x)$ is irreducible in $R[x]$;*
2. *$f(x)$ is primitive and irreducible in $F[x]$.*

### Proof

$(1) \implies (2)$ *follows from Lemma 105, Theorem 106 and Theorem 107.*

$(2) \implies (1)$*: Suppose that $f(x)$ is primitive and irreducibile in $F[x]$ but reducible in $R[x]$. Then a non-trivial factorization of $f(x) \in R[x]$ must take the form $f(x) = dg(x)$ with $d \in R$ and $d \not\sim 1$* [1]*. Since $d \mid f(x)$, $d \not\sim 1$ must then divide each of the coefficients of $f(x)$, which contradicts the assumption that $f(x)$ is primitive.* $\square$

[1] Note that we cannot have both factors to have degree $\geq 1$, otherwise this would be a non-trivial factorization in $F[x]$, contradicting the irreducibility of $f(x)$ in $F[x]$.

### Theorem 109 (Polynomial Ring of a UFD is also a UFD)

*If $R$ is a UFD, then the polynomial ring $R[x]$ is also a UFD.*

### Proof

*By Theorem 95, since $R$ is a UFD and hence satisfies ACCP* [2]*, we have $R[x]$ also satisfies ACCP. Then by Theorem 98, to complete the*

[2] See note on page 192.

*proof, it suffices to show that every irreducible element $l(x) \in R[x]$ is prime. To show that an irreducible element $l(x) \in R[x]$ is prime, we need to show that if $l(x) \mid f(x)g(x)$ in $R[x]$, then $l(x) \mid f(x)$ or $l(x) \mid g(x)$.*

***Claim**: It suffices to show that*

$$l(x) \mid f_1(x)g_1(x) \implies l(x) \mid f_1(x) \vee l(x) \mid g_1(x)$$

*where $f_1(x)$ and $g_1(x)$ are primitive, then given any non-primitive $f(x)$ and $g(x)$ such that $l(x) \mid f(x)g(x)$, we can reduce it to the primitive case, which then $l(x) \mid f(x)$ or $l(x) \mid g(x)$.*

*Suppose $l(x) \mid f(x)g(x)$, which then $\exists h(x) \in R[x]$ such that $l(x)h(x) = f(x)g(x)$. Note that at this point, it is not necessary that $f(x)$ and $g(x)$ are primitive. Then by Lemma 104, we may write*

$$\begin{aligned} f(x) &= \mathrm{c}(f)f_1(x) \\ g(x) &= \mathrm{c}(g)g_1(x) \\ h(x) &= \mathrm{c}(h)h_1(x) \end{aligned}$$

*for some primitive polynomials $f_1(x)$, $g_1(x)$ and $h_1(x)$ in $R[x]$. Since $l(x)$ is irreducible, by Lemma 105, we have $\mathrm{c}(l) \sim 1$. It thus follows that $\mathrm{c}(h) \sim \mathrm{c}(f)\,\mathrm{c}(g)$. Since*

$$\mathrm{c}(h)h_1(x) = \mathrm{c}(f)\,\mathrm{c}(g)f_1(x)g_1(x),$$

*we have that*

$$h_1(x)l(x) \sim f_1(x)g_1(x).$$

*Then we have that $l(x) \mid f_1(x)g_1(x)$, and so by the assumption, we have that $l(x) \mid f_1(x)$ or $l(x) \mid g_1(x)$, and so we have $l(x) \mid f(x)$ or $l(x) \mid g(x)$.*

*We may now assume that $l(x) \mid f(x)g(x)$ where $f(x)$, $g(x)$ are primitive in $R[x]$. Let $F$ denote the field of fractions of $R$, and consider $R \subseteq F$ is a subring of $F$. Then by extension, we have that $l(x) \mid f(x)g(x)$ in $F[x]$. Since $l(x)$ is irreducible in $R[x]$, we also have that $l(x)$ is irreducible in $F[x]$, by ☕ Theorem 107. Then by 💧 Proposition 86, since $F[x]$ is a field, we have $l(x) \mid f(x)$ or $l(x) \mid g(x)$.*

*Suppose that $l(x) \mid f(x)$ in $F[x]$, say $\exists k(x) \in F[x]$ such that*

$$f(x) = l(x)k(x).$$

*If $d \in R$ is the product of all denominators of the non-zero coefficients of $k(x)$, then $k_0(x) = dk(x) \in R[x]$, and so we have*

$$df(x) = dl(x)k(x) = l(x)k_0(x).$$

*Since $f(x)$ is primitive and $l(x)$ is irreducible, by Lemma 105 and Theorem 106, we have*

$$d \sim \mathrm{c}(df) \sim \mathrm{c}(lk_0) \sim \mathrm{c}(l)\,\mathrm{c}(k_0) \sim \mathrm{c}(k_0). \tag{35.1}$$

*Now if we write $k_0(x) = \mathrm{c}(k_0)k_1(x)$ using Lemma 104, for some primitive $k_1(x) \in R[x]$, then*

$$df(x) = l(x)k_0(x) = \mathrm{c}(k_0)l(x)k_1(x).$$

*Then from Equation (35.1), we have*

$$f(x) \sim l(x)k_1(x).$$

*Thus we have $l(x) \mid f(x)$ in $R[x]$. Similarly so, if $l(x) \mid g(x)$ in $F[x]$, we can show that $l(x) \mid g(x)$ in $R[x]$. It follows that $l(x)$ is therefore prime and so $R[x]$ is a UFD.* □

---

Let $R$ be a UFD, and $x_1, ..., x_n$ be $n$ commuting variables, i.e. $\forall i, j \in \{1, ..., n\}$ we have

$$x_i x_j = x_j x_i.$$

We may then inductively define the ring $R[x_1, ..., x_n]$ of polynomials in $n$ variables by

$$\mathrm{R}[\mathrm{x}_1, ..., x_n] = \left(R[x_1, ..., x_{n-1}]\right)[x_n]$$

for $n \geq 1$. Then, as a direct corollary of Theorem 109, we have:

---

**Corollary 110 (Multiparametered Polynomial Ring of a UFD is also a UFD)**

*If $R$ is a UFD, then $\forall n \in \mathbb{N}$, $R[x_1, ..., x_n]$ is also a UFD.*

Now since $\mathbb{Z}$ is a UFD, we have, therefore:

**Corollary 111 (Polynomial Ring over Integers is a UFD)**

*$\mathbb{Z}[x]$ and $\mathbb{Z}[x_1, ..., x_n]$ are UFDs.*

Another application of Gauss' Lemma is:

**Theorem 112 (Eisenstein's Criterion of $\mathbb{Z}[x]$)**

*Let $f(x) = a_n x^n + \ldots + a_0 \in \mathbb{Z}[x]$ and $p$ a prime. Suppose that*

$$p \nmid a_n, \quad p \mid a_i \text{ for } 0 \leq i \leq n-1 \quad \text{and} \quad p^2 \nmid a_0.$$

*Then $f(x)$ is irreducible in $\mathbb{Q}[x]$. In particular, if $f(x)$ is primitive, then $f(x)$ is irreducible in $\mathbb{Z}[x]$.*[3]

[3] e.g. $f(x)$ is monic $\implies f(x)$ is primitive.

**Proof**

*Take PMATH348!!*[4]

[4] And so we have a teaser right at the end!!