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`

33 Lecture 33 Jul 20th 2018

33.1 Factorizations in Integral Domains (Continued 3)

33.1.1 Unique Factorization Domains and Principal Ideal Domains (Continued)

Note

Recall the definition of a gcd: $d = \gcd(a, b)$ *if*

1. $d \mid a \wedge d \mid b$
2. $\forall e \in R\ e \mid a \wedge e \mid b \implies e \mid d$

Proposition 99 (Bezout's Lemma in PIDs)

Let R *be a PID and let* $a_1, ..., a_n$ *be non-zero elements of* R*. Then* $d \sim \gcd(a_1, ..., a_n)$ *exists and* $\exists r_1, ..., r_n \in R$ *such that*

$$\gcd(a_1, ..., a_n) = r_1 a_1 + \ldots + r_n a_n.$$

Proof

Consider

$$A = \{r_1 a_1 + \ldots + r_n a_n : r_i \in R\}.$$

Note that A *is an ideal of* R*, since* $\forall a \in A\ \forall r \in R$*, we have*

$$aR \ni ar = rr_1 a_1 + \ldots + rr_n a_n \in A.$$

Since R is a PID, $\exists d \in R$ such that $A = \langle\, d \,\rangle$. Thus

$$\exists r_1, ..., r_n \in R \quad d = r_1 a_1 + \ldots r_n a_n.$$

It remains to prove that $d \sim \gcd(a_1, ..., a_n)$. Since $A = \langle\, d \,\rangle$ and $a_i \in R$, clearly so $d \mid a_i$, for all $1 \leq i \leq n$. Also, $\exists r \in R\ 1 \leq i \leq n\ r \mid a_i \implies r \mid (r_1 a_1 + \ldots + r_n a_n) \implies r \mid d$. Then by the definition of a gcd, we have $d \sim \gcd(a_1, ..., a_n)$. □

Theorem 100 (PIDs are UFDs)

Every PID is a UFD.

Proof

If R is a PID, by Theorem 98 and Proposition 99, it suffices to show that R satisfies ACCP. If $\langle\, a_1 \,\rangle \subseteq \langle\, a_2 \,\rangle \subseteq \ldots$ in R, let

$$A = \langle\, a_1 \,\rangle \cup \langle\, a_2 \,\rangle \cup \ldots .$$

Note that A is an ideal, since $\forall a \in A$, $a \in \langle\, a_i \,\rangle$ for some i, and so $\forall r \in R$, we have $ar \in \langle\, a_i \,\rangle \subseteq A$. Now since R is a PID, $\exists a \in R$ such that $A = \langle\, a \,\rangle$. Then $a \in \langle\, a_n \,\rangle$ for some $n \in \mathbb{N}$. Then

$$\langle\, a \,\rangle \subseteq \langle\, a_n \,\rangle \subseteq \langle\, a_{n+1} \,\rangle \subseteq \ldots \subseteq A = \langle\, a \,\rangle.$$

which implies that $\langle\, a_n \,\rangle = \langle\, a_{n+1} \,\rangle = \ldots$ in R, i.e. R satisfies ACCP. Therefore R is a UFD. □

Note

We have the following chain of definitions:

$$\textit{field} \subsetneq \textit{PID} \subsetneq \textit{UFD} \subsetneq \textit{ACCP} \subsetneq \textit{commutative ring} \subsetneq \textit{ring}.$$

If F is a field, then we have shown that both F and $F[x]$ are PIDs.

And so we have the following consequence from ☕ Theorem 100:

Corollary 101 (Polynomial Rings over a Field is a UFD)

If F is a field, then F and $F[x]$ are UFDs.

Example 33.1.1

$\mathbb{Z}[x]$ is not a PID.

Consider

$$A = \{2n + xf(x) : n \in \mathbb{Z},\ f(x) \in \mathbb{Z}[x]\}.$$

Note that A is indeed an ideal, since $\forall a \in A$ and $g(x) \in \mathbb{Z}[x]$, let $g(x) = b_0 + b_1x + \ldots b_mx^m$, and we have

$$\begin{aligned} ag(x) &= (2n + xf(x))g(x) \\ &= 2nb_0 + 2n\,(b_1x + \ldots b_mx^m) + xf(x)g(x) \\ &= 2nb_0 + x(2nb_1 + \ldots + 2nb_mx^{m-1}) + xf(x)g(x) \\ &= 2nb_0 + x[h(x) + f(x)g(x)] \in A \end{aligned}$$

where $h(x) = 2nb_1 + 2nb_2x + \ldots + 2bnb_mx^{m-1}$. Suppose for contradiction that $A = \langle\ g(x)\ \rangle$ for some $g(x) \in \mathbb{Z}[x]$. Since $2 \in A$, we must have $g(x) \mid 2$. It follows that $g(x) = \pm 1$ or ± 2 [1]. Thus $A = \mathbb{Z}[x]$ or $A = \langle\ 2\ \rangle$, respectively for $g(x) = \pm 1$ or ± 2. However, $A = \mathbb{Z}[x]$ means that A is not a principal ideal, and if $A = \langle\ 2\ \rangle$, then there must be no $xf(x)$ in A, i.e. this is an impossible case. Therefore $\mathbb{Z}[x]$ is not a PID.

[1] We must have $\deg g = 0$, otherwise there is no way that $g(x) \mid 2$. And as $\deg g = 0$, we have that $|g(x)| \leq 2$ in $\mathbb{Z}$, and hence the result.

Theorem 102 (Quotient over a PID)

Let R be a PID and $0 \neq p \in R$ a non-unit. TFAE:

1. *p is prime;*
2. *$R/\langle\ p\ \rangle$ is a field;*
3. *$R/\langle\ p\ \rangle$ is an integral domain.*

Proof

(1) $\implies$ (2): *Consider a non-zero element* $a + \langle\ p\ \rangle \in R/\langle\ p\ \rangle$. *Clearly then,* $a \notin \langle\ p\ \rangle$ *and so* $p \nmid a$. *Consider*

$$A = \{ra + sp : r, s \in R\},$$

which is (quite clearly so) an ideal in R. *Since* R *is a PID,* $\exists d \in R$ *such that* $A = \langle\ d\ \rangle$. *Since* $p \in A$ [2], *we have* $d \mid p$. *Since* p *is prime,* p *is irreducible*[3], *and so* $d \sim p$ *or* $d \sim 1$ *by* Proposition 92. *If* $d \sim p$, *then* $\langle\ p\ \rangle = \langle\ d\ \rangle = A \implies p \mid a$, *which contradicts the fact that* $p \nmid a$.

[2] Since R is a PID, it is a integral domain and so $0 \in R$. Then $0 \cdot a + 1 \cdot p = p \in A$.

[3] By Proposition 93.

And so we are left with $d \sim 1$. *It follows that* $A = \langle\ 1\ \rangle = R$. *In particular, we have* $1 \in A$, *and say then* $ba + cp = 1$ *for some* $b, c \in R$. *It so follows that*

$$(b + \langle\ p\ \rangle)(a + \langle\ p\ \rangle) = ba + \langle\ p\ \rangle = 1 + \langle\ p\ \rangle \in R/\langle\ p\ \rangle.$$

Therefore $a + \langle\ p\ \rangle$ *is a unit and so* $R/\langle\ p\ \rangle$ *is a field.*

(2) $\implies$ (3): *By* Proposition 74, *every field is an integral domain.*

(3) $\implies$ (1): *Suppose* $p \mid ab \in R$. *Then*

$$(a + \langle\ p\ \rangle)(b + \langle\ p\ \rangle) = ab + \langle\ p\ \rangle = 0 + \langle\ p\ \rangle.$$

Since $R/\langle\ p\ \rangle$ *is an integral domain, WLOG, say we have that* $a + \langle\ p\ \rangle = 0 + \langle\ p\ \rangle$. *Then* $a \in \langle\ p\ \rangle \implies p \mid a$. *Otherwise, we would have* $p \mid b$. □

Conseuqently, alongside with Proposition 77 and Proposition 78, we have:

Corollary 103 (Non-Zero Prime Ideals in a PID are Maximal)

Every non-zero prime ideal of a PID is maximal.[4]

[4] In other words, in a PID, maximal ideals are prime ideals and vice versa (see Corollary 79.)

Note

The results of Theorem 102 may fail if we are simply in a UFD.

Example 33.1.2

$R = \mathbb{Z}[x]$ is a UFD. Consider the principal ideal $\langle\ x\ \rangle \subseteq R$. Then $R/\langle\ x\ \rangle \cong \mathbb{Z}$, which we know is an integral domain but not a field. $\therefore \langle\ x\ \rangle$ is a prime ideal in $\mathbb{Z}[x]$ but not maximal.

33.1.2 Gauss' Lemma

Definition 60 (Content)

*If R is a UFD and if $0 \neq f(x) \in R[x]$, the greatest common divisor of the non-zero coefficients of $f(x)$ is called the **content** of $f(x)$, and denoted by $c(f)$.*

Definition 61 (Primitive Polynomials)

*If R is a UFD and if $0 \neq f(x) \in R[x]$, then if $c(f) \sim 1$, we say that $f(x)$ is a **primitive polynomial**, or simply say that $f(x)$ is **primitive**.*

Example 33.1.3

In $\mathbb{Z}[x]$, we have

$$\text{(primitive)} : c(6 + 10x^2 + 15x^3) \sim 1;$$
$$\text{(non-primitive)} : c(6 + 9x^2 + 15x^3) \sim 3.$$