신 용 수 교수지도

석 사 학 위 논 문

Polynomial ring of krull dimension 2

2009

성신여자대학교 교육대학원

교육학과 수학교육전공

안 소 영

Polynomial ring of krull dimension 2

신 용 수 교수지도

이 논문을 석사학위논문으로 제출함.

2009월 5월

성신여자대학교 교육대학원

교육학과 수학교육전공

안 소 영

인 준 서

안소영의 석사학위 논문으로 인준함.

심사위원 _____ 인

심사위원 _____ 인

심사위원 _____ 인

성신여자대학교 교육대학원

논 문 개 요

주 이데알 정역이 유일인수분해 정역에 속해있는 것은 잘 알려진 정리이다. F. zanello 정리에 따르면 주 이데알 정역에서 모든 극대 아이디얼 길이의 최대치가 2 라는 것과 무한히 많은 기약의 원소를 가진다는 것은 동치이다.

이 논문에서는 몇 개의 정리와 증명을 사용하여 F. zanello의 정리를 상세 증명하고, 몇 가지 예제를 제시하였다.

우선 section 2 에서는 Zorn's Lemma 를 비롯하여 주 이데알의 다항식환에 관한 주요한 정리들과 예제를 제시하였다. Section 3에서는 F. zanello의 정리를 상세히 증명하기 위한 몇 가지 정리와 예제를 제시하였다.

목 차

1. **Introduction**

It is well-known that any principal ideal domain(for short, PID) is in a unique factorization domain(for short, UFD). In [2], F.Zanello proved that D in a PID has infinitely many irreducibles if and only if every maximal ideal of $D[x]$ has height 2.(See Theorem 42). In this thesis, we review F.Zanello's result adding precise details. Moreover, we also give some examples. In Section 2, we give some preliminaries notations and known results. In Section 3, for precise proofs, we introduce known results with proofs for readers.

2. **Preliminaries**

Definition 1 ([2])**.** Let R be a ring with unity $1 \neq 0$. An element u in R is a ***unit*** of R if it has a multiplicative inverse in R. If every nonzero element of R is a ***division ring***. A ***field*** is a commutative division ring.

Definition 2 (2)**.** An ***integral domain*** D is a commutative ring with unity $1 \neq 0$ and containing no divisors of 0.

Definition 3 (2)**.** An additive subgroup N of a ring R satisfying the properties

$$aN \subseteq N \text{ and } Nb \subseteq N \text{ for all } a, b \in R$$

is an ***ideal***.

Definition 4 (2). ***A partial ordering of a set*** S is given by a relation $\leqq$ defined for certain ordered pairs of elements of s such that the following conditions are satisfied :

1. $a \leqq a$ for all $a \in S$ ***(reflexive law)***
2. If $a \leqq b$ and $b \leqq a$, then $a = b$ ***(antisymmetric law)***
3. If $a \leqq b$ and $b \leqq c$, then $a \leqq c$ ***(transitive law)***

Lemma 5. **[Zorn's Lemma]** *If S is a partially ordered set such that every chain in S has an upper bound in S, then S has at least one maximal element.*

Lemma 6. *Let R be a commutative ring with unity* 1*. Then every proper ideal I in R is contained in a maximal ideal M in R.*

Proof. Let $T = \{J \mid I \leqq J \lneqq R$, and J is an ideal of $R\}$ be the collection of all proper ideals J in R containing I.
Then T is not empty since $I \in T$ and it is a partially ordered set under our usual ideal inclusion. Let $T = \{J_i\}$ be a chain in T, and let $J = \bigcup J_i$. Then now prove that $J \in T$, for; $0 \in J_i$ for every i. For every $a, b \in J$, there is J_i containing a and b since T is a chain in T. That is, $a + b$, $a - b \in J_i \subseteq J$. Moreover for every $r \in R$ and $a \in J$, there is J_i containing a, that is, $ra = ar \in J_i \subseteq J$. Hence J

is an ideal containing I since J_i contains I for every i, and $J_i \subset J$. thus J is the largest element of T.

Moreover since $J_i \subsetneqq R$, i,e., $1 \notin J_i$ for every i, $1 \notin J$. In other words, $I \subseteqq J \subsetneqq R$, and hence $J \in T$. Thus J is an upper bound for $\{J_i\} \in T$. The hypotheses of Zorn's lemma are fullfilled, so there is a maximal element M in T, and M is a maximal ideal containing I in R, as we wished. □

Example 7. Let $\mathbb{Z}$ be a commutative ring with unity 1 and $I = a\mathbb{Z}$, $a \in R$ is a proper ideal, by Lemma 6. Then there exists a prime $p \in \mathbb{Z}$ such that $p \mid a$, and hence $a\mathbb{Z} \subseteqq p\mathbb{Z}$, which $p\mathbb{Z}$ is a maximal ideal of $\mathbb{Z}$.

Definition 8 (2)**.** An ideal N is not equal R in a commutative ring R is a ***prime ideal*** if $ab \in N$ implies that either $a \in N$ or $b \in N$ for $a, b \in R$.

Definition 9 (2)**.** A ***maximal ideal*** of a ring R is an ideal M different from R such that is no proper ideal N of R properly containing M.

Remark 10. For a commutative ring R with unity 1:

1. M is a maximal ideal of R if and only if R/M is a field.
2. An ideal N of R is prime if and only if R/N is an integral domain.

3. Every maximal ideal of R is a prime ideal.

Definition 11 (1)**.** Let R be a commutative ring with unity 1. Then we denote the collection of all maximal ideals in R by

$$\Omega(R) = \{M \mid M \text{ is a maximal ideal of } R\},$$

and the collection of all prime ideals in R by

$$\mathrm{Spec}(R) = \{\wp \mid \wp \text{ is a prime ideal of } R\}.$$

The ***Jacobson radical ideal*** $\sqrt{R}$ of a ring R is the intersection of all maximal ideals M in R. That is,

$$\sqrt{R} = \bigcap_{M \in \Omega(R)} M.$$

The ***nilradical*** $\sqrt{0}$ of R is the intersection of all prime ideals of R. In other words,

$$\sqrt{0} = \bigcap_{\wp \in \mathrm{Spec}(R)} \wp.$$

Lemma 12 (2)**.** *Let I be an ideal and $I \leqq R$ if and only if $0 \in I$, $a \pm b \in I$, $ar, ra \in I$ for all $a, b \in I$, $r \in R$.*

Proof. If I is an ideal of R, then $0 = 0 \cdot 0 \in I$, and $(a \pm b)I = aI \pm bI \subseteq I$, $I(a \pm b) = Ia \pm Ib \subseteq I$ and ar, $ra \in I$ as ideal's definition.

Conversely, if ar, $ra \in I$, then aI, $Ia \subseteq I$. Hence I is an ideal. $\square$

Definition 13. An element a of a ring R is ***nilpotent*** if $a^n = 0$ for some $n \in Z^+$.

Lemma 14. *Let R be a commutative ring with unity 1. Let $I = \{a \in R \mid a^n = 0$ for some $n \geq 0, n \in \mathbb{Z}\}$. Then I is an ideal of R.*

Proof. Since $0^1 = 0$, $0 \in I$. Since $a, b \in I$, $a^n = 0$, $b^m = 0$, for all $m, n \in N$. Let $M = m + n$, then $(a+b)^M = \sum_{i=0}^{M} \binom{M}{k} a^{M-k} b^k = 0$. for; if $0 \leqq k \leqq m$ then $a^{M-k} = 0$, and if $m \leqq k \leqq M$ then $b^k = 0$. Thus, $a + b \in I$. If $a \in I$, then $(-a)^n = \pm\, a^n = 0$. Thus $-a \in I$, if $a \in I$, $r \in R$, then $(ar)^n = (ra)^n = 0 \in I$. By Lemma 12 , I is an ideal of R. □

Lemma 15. *Let R be a commutative ring with unity 1. Then*

$$\sqrt{0} = \{a \in R \mid a^n = 0 \text{ for some } n \geq 0, n \in \mathbb{Z}\}.$$

Proof. Let $I = \{a \in R \mid a^n = 0$ for some $n \geq 0, n \in \mathbb{Z}\}$. For every prime ideal $\wp$, if $a \in I$, i.e., $a^n = 0$ for some $n \in Z^+$, then $a^n \in \wp$. Thus $a \in \wp$, since $\wp$ is a prime ideal. Hence $I \subseteq \bigcap \wp = \sqrt{0}$.
Conversely, assume $a \in R$ such that $a^n = 0$ for every $n \geqq 1$. Let T $=\{J \leqq R \mid a^n \neq 0,$ for all $n \geqq 1\}$. Note that $\{0\}$ in T, that is, T is not empty. And for all $J_1 \leqq J_2$, so T is partially ordered set. Let $S = \{J_i\}$ be a chain, then $\bigcup J_i = J$ is a ideal of T.
In fact, it is obvious that $0 \in J$. For every $a, b \in J$, there is an ideal $J_i \in S$ such that $a, b \in J_i$, since S is a chain. Hence $a \pm b$,

ar, $ra \in J_i$, for every $r \in R$, i.e., $a \pm b$, ar, $ra \in J$ for such $r \in R$. Moreover, if $a^n \in J$ for some $n \in \mathbb{Z}^+$, then $a^n \in J_i$ for some i, a contradiction. In other words, J is an upper bound of S in T. By Zorn's lemma, there exists a maximal element $\wp$ in T. Let $x, y \in R$ such that $xy \in \wp$. Suppose $x \notin \wp$, $y \notin \wp$, then $\wp \subsetneq (x, \wp)$ and $\wp \subsetneq (y, \wp)$. By the maximality of $\wp$, $(x, \wp) \notin T$, $(y, \wp) \notin T$, i.e., $a^n \in (x, \wp)$, $a^m \in (y, = wp)$, for some $n, m \in \mathbb{Z}^+$.

Let $\text{Max}\{n, m\} = N$ Then $N \in (x, \wp) \cap (y, \wp)$, that is,

$$\begin{aligned} a^n &= xr_1 + p_1 = yr_2 + p_2 \text{ where } r_1, r_2 \in R, p_1, p_2 \in \wp, \text{ hence} \\ a^N a^N &= (xr_1 + p_1) \cdot (yr_2 + p_2) \\ &= xy(r_1 r_2) + (xr_1)p_1 + (yr_2)p_2 + p_1 p_2 \in \wp, \text{ a contradiction.} \end{aligned}$$

So, there exists $\wp \in \text{Spec}(R)$ such that, $a \notin \wp$, that is, $a \notin \bigcap \wp = \sqrt{0}$, which completes the proof. □

Example 16. Let $\mathbb{Z}_8 = \{0, 1, 2, \ldots, 7\}$ be a commutative ring with unity 1. Then by Lemma 14, $I = \{0, 2, 4, 6\}$ is an ideal of $\mathbb{Z}_8$. Also, $\sqrt{0} = \bigcap_{\wp \in Spec(\mathbb{Z})} = \{0, 2, 4, 6\} = I$, by Lemma 15.

Definition 17 (1)**.** Let R be a commutative ring with unity 1. The ***height*** of a prime ideal $\wp$ is the supremum of the lengths of all the chains

$$\wp_0 \subset \wp_1 \subset \cdots \subset \wp_t = \wp$$

of prime ideals of R that end at $\wp$.

The ***Krull dimension*** $\dim R$ is the supremum of the lengths of all the chains of primes ideals of $\wp$, or equivalently, the supremum of the heights of all the prime ideals $\wp$ in R.

Remark 18. (a) Let F be a field. Then $\{0\}$ is a unique prime ideal in F, and hence $\dim F = 0$.

(b) Let F be as in (a) and $F[x]$ be a polynomial ring over a field F. Then every maximal ideal M in $F[x]$ is of the from $(p(x))$ where $p(x)$ is irreducible in $F[x]$. In other words, $\dim F = 1$.

Lemma 19. *Let R be a commutative ring with unity 1. Then*

(a) *$a \in \sqrt{R}$ if and only if $1 - ab$ is a unit in R for all $b \in R$;*

(b) *in particular, $1 + a$ is a unit in R for every $a \in \sqrt{0}$.*

Proof. (a) Suppose $1-ab$ is not a unit for some $b \in R$. Then there is a maximal ideal M in R such that $1-ab \in M$. Since M is a ideal and $a \in \sqrt{R} \subset M, b \in R$, then $ab \in M$, that is, $1 = (1 - ab) + ab \in M$, a contradiction.

Conversely, assume $a \notin M$ for some maximal ideal M in R. Then M and a generate the ring R, that is, $(M, a) = R$ so that we have $m + ab = 1$ for some $m \in M$ and $b \in R$. Hence $m = 1 - ab \in M$ is not a unit for some $b \in R$.

(b) Suppose $1 + a = 1 - a(-1)$ is not a unit in R. Then there is a maximal ideal M in R such that $1 + a \in M$. Since $\sqrt{0} \subseteq \sqrt{R} \subset M$, we have $a \in M$, i.e., $a \cdot (-1) \in M$ and hence $1 = (1 + a) - a \in M$, a contradiction, as we wished. □

Definition 20. The set $R[x]$ of all polynomials with coefficients in the ring R is itself a ring (***polynomial ring***) with the usual operations of polynomial addition and multiplication, and that R is a subring of $R[x]$.

Lemma 21. *Let R be a commutative ring with unity 1 and let $f(x) = a_0 + a_1x + \cdots + a_nx^n \in R[x]$. Then $f(x)$ is a unit in $R[x]$ if and only if a_0 is a unit in R and $a_1, \ldots, a_n$ are nilpotent in R.*

Proof. We shall prove this Lemma using induction on n. If $n = 0$, then $a_0 \in R \subseteq R[x]$, and hence a_0 is unit. So we assume $n > 0$. Let $g(x) = b_0 + b_1x + \cdots + b_mx^m \in R[x]$ be the multiplicative inverse of $f(x)$. Then

$$1 = f(x)g(x) = a_0b_0 + (a_1b_0 + a_0b_1)x + \ldots + a_nb_mx^{n+m}$$

Note that $a_0b_0 = 1$, and so a_0 is a unit in R . Now we shall prove that $a_n^{\alpha+1}b_{m-\alpha} = 0$ by induction on α. Since $a_nb_m = 0$, it holds when $\alpha = 0$. Assume $\alpha > 0$. Consider the $(n + m - \alpha)$-th coefficient of

$f(x)g(x)$. Then

$$\begin{aligned} 0 &= a_{n-\alpha}b_m + a_{n-(\alpha-1)}b_{m-1} + \cdots + a_{n-1}b_{m-(\alpha-1)} + a_n b_{m-\alpha} \\ &= a_n^{\alpha}(a_{n-\alpha}b_m + a_{n-(\alpha-1)}b_{m-1} + \cdots + a_{n-1}b_{m-(\alpha-1)} + a_n b_{m-\alpha}) \\ &= a_{n-\alpha}a_n^{\alpha-1}(a_n b_m) + a_{n-(\alpha-1)}a_n^{\alpha-2}(a_n^2 b_{m-1}) + \cdots + \\ & \quad a_{n-1}(a_n^{\alpha}b_{m-(\alpha-1)}) + a_n^{\alpha+1}b_{m-\alpha} \\ &= a_n^{\alpha+1}b_{m-\alpha}(\text{by induction on } \alpha), \end{aligned}$$

and hence $a_n^{\alpha+1}b_{m-\alpha} = 0$ for every $\alpha \geq 0$. In particular, if $\alpha = m$, then we have that $a_n^{m+1} = 0$, and hence a_n is a nilpotent element in R.

Moreover, since $a_n x^n$ is also nilpotent in $R[x]$, by Lemma 19(b), $f(x) - a_n x^n = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$ is also a unit in $R[x]$. Hence, by induction on n, a_0 is a unit and $a_1, \cdots, a_{n-1}$ are all nilpotent in R, as we wanted.

Conversely, since $a_1, \cdots, a_n$ are all nilpotent in R, $a_1 x + \cdots + a_n x^n$ is also nilpotent in $R[x]$, and hence, by Lemma 19(b) again, $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ is unit in $R[x]$,which completes the proof. $\square$

Example 22. Let $\mathbb{Z}_8 = \{0, 1, 2, \ldots, 7\}$ be a commutative ring with unity 1. Then $0, 2, 4, 6$ are nilpotents of $\mathbb{Z}_8$. Let $f(x) = 1 + 6x$, by Lemma 21, then $1+6x$ is a unit in $\mathbb{Z}_8[x]$, for $(1+6x)(1+2x+4x^2) = 1 + 8x + 16x^2 + 24x^3 = 1 \in \mathbb{Z}_8[x]$.

Lemma 23. *Let R be a commutative ring with unity 1 and $R[x]$ be a polynomial ring over a ring R. Then $f(x) = a_0 + a_1x + \cdots + a_nx^n \in R[x]$ is nilpotent if and only if $a_0, a_1, \ldots, a_n \in R$ are all nilpotent.*

Proof. We shall prove this Lemma by induction on n. If $n = 0$, the statement holds. Now assume $n > 0$. Since $f(x)$ is nilpotent in $R[x]$, there is a positive integer m such that

$$f(x)^m = (a_0 + a_1x + \cdots + a_nx^n)^m = 0.$$

I.e.,

$$0 = a_0^m + m(a_0^{m-1}a_1)x + \cdots + (a_n^m)x^{mn} \Rightarrow a_n^m = 0.$$

Hence a_nx^n is also nilpotent in $R[x]$, and so is $f(x) - a_nx^n = a_0 + a_1x + \ldots + a_{n-1}x^{n-1}$. Thus, by induction on n, a_0, a_1, $\ldots$, a_{n-1} are also nilpotent in R.

Conversely, since a_i are all nilpotent in R for every i, a_ix^i are all nilpotent in $R[x]$ for such i. Therefore, $f(x) = a_0 + a_1x + \ldots + a_nx^n$ is also nilpotent in $R[x]$, as we wished. □

Example 24. Let $\mathbb{Z}_8 = \{0, 1, 2, \ldots, 7\}$ be a commutative ring with unity 1. Then $0, 2, 4, 6$ are nilpotents of $\mathbb{Z}_8$. Let $f(x) = 2 + 4x$, by Lemma 23, then $2 + 4x$ is a nilpotent in $\mathbb{Z}_8[x]$, for $(2 + 4x)^3 = 8 + 48x + 96x^2 + 64x^3 = 0 \in \mathbb{Z}_8[x]$.

Proposition 25. *Let R be a commutative ring with unity 1 and $R[x]$ be a polynomial ring over a ring R. Then $\sqrt{R[x]} = \sqrt{0}$.*

Proof. It is obvious that $\sqrt{0} \subseteq \sqrt{R[x]}$.

Let $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \sqrt{R[x]}$. Then $xf(x)$ is also in $\sqrt{R[x]}$, and thus, by Lemma 19(a), $1+xf(x) = 1+a_0x+a_1x^2+\cdots+a_nx^{n+1}$ is a unit in $R[x]$. In other words, by Lemma 21, $a_0, a_1, \cdots, a_n$ are all nilpotent in R, and so, by Lemma 23, $f(x) = a_0+a_1x+\cdots+a_nx^n$ is nilpotent in $R[x]$, that is, $f(x) \in \sqrt{0}$, as we wished. □

Corollary 26. *Let R be an integral domain. Then $\sqrt{R[x]} = \{0\} = \sqrt{0}$.*

Proof. Since R is an integral domain, $\{0\}$ is a prime ideal, so $\sqrt{0} = \bigcap_{\wp \in Spec(R)} \wp = \{0\}$, and therefore, by Proposition 25, $\sqrt{R[x]} = \sqrt{0} = \{0\}$. □

Definition 27 (2)**.** Let R be a commutative ring with unity and let a, b in R. If there exists c in R such that $b = ac$, then a ***divides*** b (or a ***is a factor of*** b), denoted by $a \mid b$. We read $a \nmid b$ as "a does not divide b ".

Definition 28 (2)**.** An element u of a commutative ring with unity R is a ***unit of*** R if u divides 1, that is , if u has a multiplicative inverse in R. Two elements a, b in R are ***associates in*** R if $a = bu$, where u is a unit in R.

Definition 29 (2)**.** A nonzero element p that is not a unit of an integral domain D is an ***irreducible of*** D if in every factorization $p = ab$ in D has the property that either a or b is a unit.

Definition 30 (2)**.** An integral domain D is a ***unique factorization domain*** (abbreviated UFD) if the following conditions are satisfied:

1. Every element of D that is neither 0 nor a unit can be factored into a product of a finite number of irreducibles.
2. If $p_1,\ldots,p_r$ and $q_1,\ldots,q_s$ are two factorizations of the same element of D into irreducibles, then $r = s$ and the q_j can be renumbered so that p_i and q_j are associates.

Definition 31 (2)**.** An integral domain D is a ***principal ideal domain*** (abbreviated PID) if every ideal in D is a principal ideal.

Definition 32 (2)**.** A nonzero nonunit element p of an integral domain D is a ***prime*** if, for all $a, b \in D$, $p \mid ab$ implies either $p \mid a$ or $p \mid b$.

Lemma 33. *Let D be an integral domain. If p is a prime in an integral domain, then p is an irreducible. In particular, if D is a UFD and p is an irreducible in D, then p is a prime.*

Proof. First we will prove p is an irreducible. If $p = ab$, then $p \mid ab$. Since p is a prime, we have either $p \mid a$ or $p \mid b$. If $p \mid a$, then $a = pq$ for some $q \in D$. Hence

$$p = ab = (pq)b = p(qb)$$

and so $qb = 1$, that is, b is a unit. Similarly, if $p \mid b$, then by the same method as above one can show that a is a unit of D. Therefore p is an irreducible.

Now we will prove if D is a UFD and p is an irreducible in D, then p is a prime. Assume $p \mid ab$. Since D is a UFD, we see that $a = p_1 \cdots p_r$ and $b = q_1 \cdots q_s$ where p_i and q_j are all irreducibles. Moreover, since $p \mid ab = p_1 \cdots p_r \cdot q_1 \cdots q_s$, we see that

$$p_1 \cdots p_r \cdot q_1 \cdots q_s = pt$$

for some $t \in D$. On the other hand, since D is a UFD, we have that p is associated to either p_i or q_j, that is, $p \mid p_1 \cdots p_i \cdots p_r = a$ or $p \mid q_1 \cdots q_i \cdots q_r = b$. Therefore p is a prime, as we wished. □

Example 34. Let D be a integral domain and let I be the subdomain $I[x^2, xy, y^2]$ in $I[x, y]$. Then xy is irreducible in $I[x, y]$. However $xy \mid (x^2)(y^2) = (xy)^2$, $xy \nmid x^2$ and $xy \nmid y^2$, that is, xy is not prime in $I[x, y]$, by Lemma 33.

Lemma 35. *A ring of integers $\mathbb{Z}$ has infinitely many prime numbers.*

Proof. Consider the integer $Q_n = n! + 1$, $n \geqq 1$ and $n \in \mathbb{Z}^+$. Since every positive integer larger than 1 has a prime divisor, Q_n has at least one prime divisor, which we donete by q_n.

If $q_n \leqq n$, it would follow that $q_n \mid n!$, and then $q_n \mid (Q_n - n!) = 1$, a contradiction. Hence q_n must be larger than n.

Take any positive integer $n \in \mathbb{Z}^+$. Then there exists a prime factor $q_1 \mid (n!+1)$ with $q_1 > n$. Moreover, there is a prime factor $q_2 \mid (q_1!+1)$ with $q_1 < q_2$. By continuing this process, we find infinitely many primes $q_1 < q_2 < \cdots$, as we wanted. □

The following Lemma is easily proved, so we omit the proof here.

Definition 36 (2)**.** Let D be a UFD. A nonconstant polynomial

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n$$

in $D[x]$ is ***primitive*** if 1 is the greatest common divisor of the a_i for $i = 0, 1, \ldots, n$.

Lemma 37 (2)**.** *If D is a UFD, then for every nonconstant $f(x) \in D[x]$ we have $f(x) = (c)g(x)$, where $c \in D$, $g(x) \in D[x]$, and $g(x)$ is primitive. The element c is unique up to a unit factor in D and is the* **content of** *$f(x)$. Also $g(x)$ is unique up to a unit factor in D.*

Theorem 38 (2)**. (Division Algorithm for F[x])** *Let*

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$$

and

$$g(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_0$$

be two elements of $F[x]$*, with* a_n *and* b_n *both nonzero elements of* F *and* $m > 0$*. Then there are unique polynomials* $q(x)$ *and* $r(x)$ *in* $F[x]$ *such that* $f(x) = g(x)q(x) + r(x)$*, where either* $r(x) = 0$ *or the degree of* $r(x)$ *is less than the degree* m *of* $g(x)$*.*

Remark 39 (2)**.** Recall the following well-known facts.

(a) Every ideal of the ring $\mathbb{Z}$ is of the form $n\mathbb{Z}$, which is generated by n, so every ideal of $\mathbb{Z}$ is principal.

(b) If F is a field, every ideal in $F[x]$ is principal.

(c) If D is a UFD, then $D[x]$ is a UFD.

(d) Every PID is UFD.

3. **A polynomial ring over a PID.**

First of all, we introduce a natural isomorphism from $D[x]/p$ to $(D/\langle p \rangle)$ in the following Lemma, we shall use it to prove the main theorem.

Lemma 40. *Let D be a PID and p be an irreducible element of D. Set*

$$\begin{aligned} P &:= \{pf(x) \mid f(x) \in D[x]\} \leqq D[x], \quad \textit{and} \\ Q &:= \{pc \mid c \in D\} \leqq D \end{aligned}$$

Then there is a natural isomorphism φ from $D[x]/P$ into $(D/Q)[x]$, defined by

$$\varphi((\sum a_i x^i) + P) = \sum (a_i + Q)x^i,$$

where $a_i \in D$ for every i.

Proof. First of all, assume $(\sum a_i x) + P = (\sum b_i x^i) + P$ where $a_i, b_i \in D$ for every i. Then we have that

$$\sum (a_i - b_i)x^i \in P \Rightarrow a_i - b_i \in Q \Rightarrow a_i + Q = b_i + Q$$

for every i, which implies that

$$\sum (a_i + Q)x^i = \sum (b_i + Q)x^i,$$

and hence φ is well-defined.

For every $(\sum a_i x^i)+P$ and $(\sum b_i x^i)+P$ in $D[x]/P$ where $a_i, b_i \in D$. Then

$$\begin{aligned}
& \varphi(((\textstyle\sum a_i x^i) + P) + ((\sum b_i x^i) + P)) \\
= \;& \varphi((\textstyle\sum (a_i + b_i)x^i) + P) \\
= \;& \textstyle\sum (a_i + b_i + Q)x^i \\
= \;& \textstyle\sum ((a_i + Q) + (b_i + Q))x^i \\
= \;& \textstyle\sum (a_i + Q)x^i + \sum (b_i + Q)x^i \\
= \;& \varphi((\textstyle\sum a_i x^i) + P) + \varphi((\sum b_i x^i) + P), \quad \textit{and} \\
& \varphi(((\textstyle\sum a_i x^i) + P) \cdot ((\sum b_i x^i) + P)) \\
= \;& \varphi((\textstyle\sum a_i x^i) \cdot (\sum b_i x^i) + P) \\
= \;& (\textstyle\sum (a_i + Q)x^i) \cdot (\sum (b_i + Q)x^i) \\
= \;& \varphi((\textstyle\sum a_i x^i) + P) \cdot \varphi((\sum b_i x^i) + P),
\end{aligned}$$

which means that φ is a homomorphism from $D[x]/P$ into $(D/Q)[x]$. Now suppose $\varphi((\sum a_i x^i) + P) = \varphi((\sum b_i x^i) + P)$ where $a_i, b_i \in D$. Then

$$\begin{aligned}
& \textstyle\sum (a_i + Q)x^i = \sum (b_i + Q)x^i, \\
\Rightarrow \;& a_i + Q = b_i + Q, \forall i \\
\Rightarrow \;& a_i - b_i \in Q, \forall i \\
\Rightarrow \;& \textstyle\sum (a_i - b_i)x^i = (\sum a_i x^i) - (\sum b_i x^i) \in P, \\
\Rightarrow \;& (\textstyle\sum a_i x^i) + P = (\sum b_i x^i) + P,
\end{aligned}$$

i.e., φ is one to one. Moreover, the map φ is obviously onto, and hence φ is an isomorphism, as we wished. $\square$

The following Lemma is also used to prove the main theorem.

Lemma 41. *Let D be a PID and p be an irreducible element in D. If $\langle g(x), p\rangle = D[x]$ where $g(x) = \sum a_i x^i$ is a polynomial in $D[x]$ with $a_i \in D$ for every i, then $p \mid a_i$ for every $i \geqq 1$ and $p \nmid a_0$.*

Proof. With notations as in Lemma 40, let $\bar{g}(x) = g(x) + P \in D[x]/P$. Since $1 \in \langle g(x), p\rangle = D[x]$, $\bar{g}(x)$ is a unit in $D[x]/P$, and hence, by Lemma 40, $\varphi(\bar{g}(x)) = \sum(a_i + Q)x^i$ is a unit in $(D/Q)[x]$. Since p is an irreducible in D, i.e., $Q = \langle p\rangle$ is a maximal ideal in D, one can see that D/Q is a field. In other words, $\varphi(\bar{g}(x)) = \sum(a_i + Q)x^i$ is a polynomial with coefficient in a field D/Q and an unit in $D/Q[x]$. Hence $a_i + Q = Q$ for every $i \geqq 1$ and $a_0 + Q$ are a unit in D/Q, which means that

$$a_i \in Q \;=\; \langle p\rangle \;\Leftrightarrow\; p \mid a_i, \quad \forall i \geqq 1, \quad \text{and}$$

$$p \nmid a_0,$$

which complete the proof. □

Theorem 42. *Let D be a principal ideal domain. Then the following statements are equivalent.*

(a) *Every maximal ideal of $D[x]$ has height 2.*

(b) *D has infinitely many irreducible elements.*

Proof. Let M be a maximal ideal in $D[x]$. Recall that, by Remark 10(3), M is a prime ideal in $D[x]$.

Let $\wp = M \cap D$, then $\wp$ is a prime ideal of D. In fact, if $ab \in \wp$ and $a, b \in D$, then $ab \in M$, and so $a \in M$ or $b \in M$. Hence $a \in \wp = M \cap D$ or $b \in \wp = M \bigcap D$.

Suppose $\wp = \bigcap_{p \in \mathrm{Spec}(D)} p = \sqrt{0} = 0$. We shall show that the height of M is 1. Note that $M \neq \{0\}$ since $D[x]$ is not a field. Then there exists an element $g(x) \in M$ of the least degree. Then $\deg g(x) > 0$. If $\deg g(x) = 0$, then $g(x) \in D$, that is, $g(x) \in \wp = M \cap D = \{0\}$, a contradiction.

Let $g(x) = (c)h(x)$ where c is the content of $g(x)$ and $h(x)$ is a primitive polynomial. Since M is a prime ideal of $D[x]$ and $c \notin M$, we have $h(x) \in M$. In other words, we may assume that $g(x)$ is a primitive polynomial.

Now assume $g(x) = s(x)t(x)$ where $s(x)$ and $t(x)$ are primitive polynomials of $D[x]$ (see Lemma 45.25, [ ]) with

$$0 < \deg s(x), \deg t(x) < \deg g(x).$$

Then, since M is a prime ideal. We can see that $s(x) \in M$ or $t(x) \in M$, which is a contradiction, since $g(x)$ has the least degree among all nonzero element in M. Hence we can assume $g(x)$ is a primitive irreducible polynomial in M.

Let k be the quotient field of D, and $q(x)$, $r(x)$, $q_1(x)$, $r_1(x)$ are polynimials in $D[x]$.

Since $q_1(x)$ and $r_1(x)$ are polynomails of $k[x]$ and D is a PID, that is, UFD, by Remark 39(d) $q(x) = \alpha q_1(x)$ and $r(x) = \alpha r_1(x)$ is polynomials in $D[x]$ for some $\alpha \in D$. Hence we can write

$$\begin{aligned} f(x) &= g(x)q_1(x) + r_1(x) \\ &= g(x)\frac{q(x)}{\alpha} + \frac{r(x)}{\alpha}, \end{aligned}$$

and hence

$$\alpha f(x) = g(x)q(x) + r(x),$$

which means that

$$r(x) = \alpha f(x) - g(x)q(x) \in M \quad (\because f(x), g(x) \in M)$$

If $r(x) \neq 0$, then $\deg r(x) = \deg r_1(x) < \deg g(x)$, which is a contradiction since $g(x)$ has the least degree among all elements in M. In other words, $r(x) = 0$. Recall that, by Remark 39(c), $D[x]$ is a UFD.

Since $g(x) \mid g(x)q(x) = \alpha f(x)$ and $g(x)$ are a irreducible of $D[x]$, and hence a prime element $g(x)$ of $D[x]$, by Lemma 33, has to divide $f(x)$.

Thus $f(x) \in \langle g(x) \rangle \subseteq M \subseteq \langle g(x) \rangle$, which follows that $M = \langle g(x) \rangle$, and hence the height of M is 1. Therefore, $\wp = M \cap D \neq \{0\}$.

Assume that every maximal ideal M in $D[x]$ has height 2. By the above argument, $M \cap D \neq \{0\}$ follows that every such M must contain some nonzero constant, say, $c \in M$. Note that c is not a unit in D, since M is a maximal ideal of $D[x]$.

Suppose now that there are only finitely many irreducible elements $p_1, \ldots, p_s$ of D. Then, by Remark 39(d), D is a PID, that is, a UFD, thus $c = q_1 \cdots q_r$ where q_i are all irreducible elements of D.

Note that $c = q_1 \cdots q_r$ is a multiple of $p_1 \cdots p_s$. Hence $p_1 \cdots p_s \in M$, for every maximal ideal M in $\Omega(R)$. Hence

$$p_1 \cdots p_s \in \bigcap_{M \in \Omega(R)} M = \sqrt{0} = \{0\} \quad (\because \text{Lemma 40})$$

which is a contradiction. Because D is a domain, $\bigcap_{M \in \Omega(R)} M = \sqrt{0} = \{0\}$, a contradiction. Therefore, D has infinitely many irreducible elements.

Let M again be an arbitray maximal ideal of $D[x]$. We want to show M has height 2.

If $\wp = M \cap D = \bigcap_{P \in \mathrm{Spec}(D)} P = \sqrt{0} = \{0\}$, then we have already seen that $M = \langle g(x) \rangle$ for some irreducible $g(x) \in D[x]$. Since M is a maximal ideal, for every irreducible $p \in D$ we must have $\langle g(x), p \rangle = D[x]$, that is, $D[x]/\langle g(x), p \rangle = 0$, and therefore $\varphi(\bar{g}(x))$ must be a constant in $(D/\langle p \rangle)[x]$ for each such p,where φ is an isomorphism in Lemma 40, and $\bar{g}(x) = g(x) + P$ with $P = \{pf(x) \mid f(x) \in D[x]\}$.

In other words, every coefficient of $g(x)$ other than the constant term is divisible by every irreducible element p of D, by Lemma 41. This is a contradiction, since we are assuming that there are infinitely many irreducible elements of D.

Hence $\wp = M \cap D \neq \sqrt{0}$, so $\wp = \langle p \rangle$ for some irreducible element $p \in D$, since D is a PID. Moreover, M is not principal.

Indeed, if M is principal, then

$$M = \langle p \rangle = \{pf(x) \mid f(x) \in D[x]\}.$$

Hence $D[x]/M = D[x]/\langle P \rangle \simeq (D/Q)[x]$, by Lemma 40, where

$$Q = \{pc \mid c \in D\},$$

which is a contradiction, since $D[x]/M$ is a field, but $(D/Q)[x]$ is not a field.

Hence M strictly contains the prime ideal $P = \langle p \rangle$, that is, $\{0\} \subsetneq \langle p \rangle \subsetneq M$.

So it's height is at least 2. But

$$\dim D[x] = \dim D + 1 = 2.$$

Thus, the height of M is exactly 2, as we wished. □

Example 43. (a) Consider a ring $\mathbb{Z}$ of integers and a field F. Then, by Remark 39(a),(b), a ring $\mathbb{Z}$ of integers and the polynomial ring $F[x]$ over a field F are principal ideal domains. The chief result is that every Euclidean domain is a

principal ideal domain and every principal ideal domain is an unique factorization domain.

i) By Lemma 35, a ring of integers $\mathbb{Z}$ has infinitely many primes, that is, irreducibles of $\mathbb{Z}$ by Lemma 33. Hence, by Theorem 42, any maximal ideal M of a polynomial ring $\mathbb{Z}[x]$ has height 2.

(b) Let F be a field and $F[x]$ be a polynomial ring over a field F.

i) $F[x]$ has infinitely many irreducible polynomials.

In fact, assume $p_1(x), \ldots, p_s(x)$ are all irreducible polynomial in $F[x]$. Let

$$q(x) = p_1 \cdots p_s(x) + 1 \in F[x].$$

Since $F[x]$ is a PID, that is, a UFD, $q(x)$ must be divided by some irreducible polynomial $p_i(x)$.

Then

$$p_i(x) \mid p_1(x) \cdots p_s(x) \text{ and } p_i(x) \mid q(x),$$

and hence

$$p_i(x) \mid (q - p_i \cdots p_s(x)) = 1,$$

a contradiction.

ii) By Theorem 42 and i), every maximal ideal of $F[x, y]$ has height 2. In other words, every maximal ideal has at least two generators, that is, $F[x, y]$ is not a principal ideal domain.

Theorem 44. *$\mathbb{Z}[x]$ is not a PID. In particular, every maximal ideal of $\mathbb{Z}[x]$ is not principal.*

Proof. A ring $\mathbb{Z}$ of integers has infinitely many primes, and so, by Lemma 33, $\mathbb{Z}$ has infinitely many irreducibles. Hence, by Theorem 42, any maximal ideal M of a polynomial ring $\mathbb{Z}[x]$ has height 2. Moreover, every maximal ideal M in $\mathbb{Z}[x]$ is not a principal ideal. In fact, let $M = \langle f(x)\rangle$ for some polynomial $f(x)$ in $\mathbb{Z}[x]$. Then, by the same argument as in the proof of Theorem 42, $f(x)$ is an irreducible polynimial of $\mathbb{Z}[x]$.

In other words, if $M = \langle f(x)\rangle$ for some $f(x) \in \mathbb{Z}[x]$, then $f(x)$ is an irriducible polynomial in $\mathbb{Z}[x]$.

Now assume that some there is a nonzero prime ideal $\wp$ of $\mathbb{Z}[x]$ such that $\{0\} \lneqq \wp \leqq M = \langle f(x)\rangle$.

Since $\mathbb{Z}[x]$ is a UFD, we may assume that every minimal generator $p(x)$ in $\wp$ has to be an irreducible in $\mathbb{Z}[x]$. Then

$$p(x) \in \langle p(x)\rangle \leqq \wp \leqq M = \langle f(x)\rangle,$$

and so $p(x) = f(x)g(x)$ for some $g(x) \in \mathbb{Z}[x]$. I.e., $f(x)$ is a unit or $g(x)$ is a unit in $\mathbb{Z}[x]$. Since $f(x)$ is not a unit, $g(x)$ has to be a unit in $\mathbb{Z}[x]$.

Thus

$$\langle f(x)\rangle = \langle p(x)\rangle = M = \langle f(x)\rangle,$$

that is, $\wp = M$ has a height 1, a contradiction.

Therefore, every maximal ideal M in $\mathbb{Z}[x]$ is not principal, and hence $\mathbb{Z}[x]$ is not a PID, as we wished. $\square$

References

[1] M.F Atiyah, and I.G. Macdonald., *Introduction to Commutative Algebra*, *Addison-Wesley* (1969).

[2] John B. Fraleigh., *A First Course In Abstract Algebra*, Seventh Edition *Addison-Wesley* (2003).

[3] Thomas W. Hungerford. *Algebra*, *Springer Verlag* (1980).

[4] Fabrizio Zanello, When are there infinitely many irreducible elements in a principal ideal domain?, The American Mathematical Monthly **111** (2004), pp. 150–152.

ABSTRACT

Polynomial ring of krull dimension 2

So-young, Ann
Major in Mathematics Education
Graduate School of Education
Sungshin Womem's University
Supervised by Professor Shin Yong su Ph.D.

F.Zanello proved that D in a PID has infinitely many irreducible if and only if every maximal ideal of D[x] has height 2.

In this thesis, we review F.Zanello's result adding precise details. Moreover, we also give some examples. In Section 2, we give some preliminaries notations and known results. In section 3, for precise proofs, we introduce known results with proofs for readers.