ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 29, Number 3, Fall 1999

# A NOTE ON CYCLOTOMIC POLYNOMIALS

MING-CHANG KANG

ABSTRACT. Let $R$ be a Dedekind domain and $n$ a square-free positive integer, $\Lambda := R[T]/T^n - 1$. The fact that $\Lambda$ is a Dedekind-like ring will make possible the classification of integral representations of the cyclic group of order $n$ over $R$ [**7**]. We shall prove that $\Lambda$ is a Dedekind-like ring for a fairly large class of Dedekind domains $R$. The proof is facilitated by an identity among cyclotomic polynomials [**2**]. Some other applications of the same identity will be presented also.

**1. Introduction.** Let $\Phi_n(X)$ be the $n$th cyclotomic polynomial. Then the formula

$$X^n - 1 = \prod_{d|n} \Phi_d(X) \tag{1}$$

is well known. There are other identities among cyclotomic polynomials, which are not so well known, for example, identities of Beeger and Schinzel [**12, 1**]. Recently a new factorization identity was proved by Cheng, McKay and Wang [**2**], namely,

**Theorem 1.1** [**2**, Lemma 1][**10**, p. 105] [**5**, p. 394]. *Let $m, n, k$ be positive integers so that g.c.d. $\{m, n\} = 1$ and $m$ is divisible by every prime factor of $k$. Then*

$$\Phi_m(X^{nk}) = \prod_{d|n} \Phi_{mkd}(X). \tag{2}$$

In particular, we find that

$$\Phi_m(X^n) = \prod_{d|n} \Phi_{md}(X), \text{if g.c.d. } \{m, n\} = 1; \tag{3}$$

Received by the editors on June 5, 1996, and in revised form on October 7, 1997.
1991 AMS *Mathematics Subject Classification.* Primary 12E10, Secondary 13C10, 20C10.
*Key words and phrases.* Cyclotomic polynomials, integral group rings.
Partially supported by the National Science Council, Republic of China.

$$\Phi_{p^r}(X) = \Phi_p(X^{p^{r-1}}) = \Phi_{p^{r-1}}(X^p), \qquad (4)$$
$$\text{if } p \text{ is a prime number and } r \geq 2.$$

The purpose of this note is to provide several applications of formulae (2) and (3). Before proceeding to these applications, let us state a result which seems not well known.

**Theorem 1.2.** *Let $d$ and $e$ be distinct positive integers and $\langle \Phi_d(X), \Phi_e(X) \rangle$ the ideal generated by $\Phi_d(X)$ and $\Phi_e(X)$ in $\mathbf{Z}[X]$. Then*

$$\langle \Phi_d(X), \Phi_e(X) \rangle \cap \mathbf{Z} = \begin{cases} \mathbf{Z} & \text{if } e/d \text{ is not a prime power,} \\ p\mathbf{Z} & \text{if } (e/d) = p^l \text{ for some prime number } p. \end{cases}$$

In the second case if $e > d$ and we write $e = dp^l$ for some prime number $p$ and some integer $l \geq 1$, then

$$\mathbf{Z}[X]/\langle \Phi_d(X), \Phi_e(X) \rangle \simeq \mathbf{Z}[X]/\langle p, \Phi_d(X) \rangle.$$

Theorem 1.2 is equivalent to the computation of $\mathrm{Ext}_\Lambda(\Lambda/\Phi_d(X), \Lambda/\Phi_e(X))$ where $\Lambda := \mathbf{Z}[X]/X^n - 1$ with $d \mid n$ and $e \mid n$.

We shall give three applications of the above two theorems:

**Application 1.** Let $n$ be any positive integer. In high-school algebra it is known that (i) $X^n - 1$ is always divisible by $X - 1$ and (ii) $X^n + 1$ is divisible by $X + 1$ if and only if $n$ is an odd integer. Consider the question: If $f(X)$ is any nonzero polynomial with integer coefficients and $f(X^n)$ is divisible by $f(X)$, what will the polynomial $f(X)$ look like?

**Application 2.** In view of the particular form of formula (3), one might ask the question: If $f_1(X), f_2(X), \ldots, f_m(X), \ldots$ is a sequence of nonzero polynomials with integer coefficients so that

$$f_m(X^n) = \prod_{d \mid n} f_{md}(X)$$

whenever g.c.d.$\{m, n\} = 1$, what can we say about these polynomials $f_m(X)$'s?

**Application 3.** In the study of all finitely generated modules over the integral group ring of a cyclic group of square-free order, a crucial step is to show that the integral group ring $\Lambda := R[X]/X^n - 1$ is a Dedekind-like ring in Levy's sense [**7**] where $R$ is a Dedekind domain and $n$ is a square-free positive integer. Indeed, Levy was able to show that it was the case when $R = \mathbf{Z}$ or $\mathbf{Z}[\zeta_q]$ if $qn$ is square-free [**8**, Theorem 1.2, Corollary 1.8]. Using Theorem 1.2 we can prove the following theorem which generalizes Levy's result, and therefore $\Lambda$ becomes a Dedekind-like ring when $R$ satisfies some mild conditions, see Example 3.10.

**Theorem 1.3.** *Let $n$ be a square-free positive integer, $\Lambda := R[X]/X^n - 1$ where $R$ is a Dedekind domain satisfying both the conditions* (R1) *and* (R2).

(R1) *$R[X]/\Phi_d(X)$ is a Dedekind domain for every integer $d$ with $d \mid n$;*

(R2) *The ideal $nR$ is not zero in $R$ and is an intersection of maximal ideals.*

*Then $\Lambda$ is a Dedekind-like ring.*

*Standing notations.* All the polynomials in this note are polynomials of one variable. $\Phi_n(X)$ will be the $n$th cyclotomic polynomial [**6**, pp. 263–267]. $\mu(n)$ is the Möbius function defined by

$$\mu(n) := \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n \text{ has a square factor}, \\ (-1)^r & \text{if } n \text{ is square-free and has precisely } r \text{ prime factors} \end{cases}$$

[**6**, p. 145]. $\varphi(n)$ is the Euler-$\varphi$ function, which is equal to the number of positive integers $\leq n$ which are relatively prime to $n$ [**6**, p. 47]. If $a, b \in A$, a commutative ring, then $\langle a, b\rangle$ will denote the ideal generated by $a$ and $b$.

## 2. Polynomials with integer coefficients.

**Lemma 2.1.** *Let $m$ and $n$ be any positive integers. Then $\Phi_m(X^n)$ is divisible by $\Phi_m(X)$ if and only if g.c.d.$\{m, n\} = 1$.*

*Remark.* When $m = 1$ and 2, the above are just the formulae of high school algebra mentioned in Application 1 of Section 1.

*Proof.* The proof follows from formula (3) of Theorem 1.1 because $\Phi_r(X)$ and $\Phi_s(X)$ are relatively prime if $r \neq s$ [**6**, p. 264]. (Note that $\mathbf{Z}[X]$ is a unique factorization domain [**6**, p. 147].)

**Theorem 2.2** [4] [**3**, pp. 550–554]. *Let $d$ and $e$ be distinct positive integers. Then*

$$\langle \phi_d(X), \Phi_e(X)\rangle \cap \mathbf{Z} = \begin{cases} \mathbf{Z} & \text{if } (e/d) \text{ is not a prime power,} \\ p\mathbf{Z} & \text{if } (e/d) = p^l \text{ for some prime number } p. \end{cases}$$

*In the second case if $e > d$ and we write $e = dp^l$ for some prime number $p$ and some integer $l \geq 1$, then*

$$\mathbf{Z}[X]/\langle \Phi_d(X), \Phi_e(X)\rangle \simeq \mathbf{Z}[X]/\langle p, \Phi_d(X)\rangle.$$

**Theorem 2.3.** *Let $n$ be any positive integer with $n \geq 2$, $f(X)$ a nonzero polynomial with integer coefficients. Then $f(X^n)$ is divisible by $f(X)$ if and only if*

$$f(X) = aX^{\alpha}\{\Phi_1(X)\}^{\alpha_0}\{\Phi_{m_1}(X)\}^{\alpha_1} \cdots \{\Phi_{m_k}(X)\}^{\alpha_k}\{\Phi_{d_1}(X)\}^{\beta_1} \cdots \{\Phi_{d_l}(X)\}^{\beta_l}$$

*where g.c.d.$\{n, m_i\} = 1$ and $m_i \geq 2$ for any $1 \leq i \leq k$, $d_1, \dots, d_l$ are distinct divisors of $n$ with $d_j \geq 2$ for any $1 \leq j \leq l$, $\alpha$, $\alpha_0$, $\alpha_1, \dots \alpha_k$, $\beta_1, \dots, \beta_l$ are nonnegative integers with $\beta_j \leq \alpha_0$ for $1 \leq j \leq l$, and $a$ a nonzero integer.*

*Proof.* $\Leftarrow$. By Theorem 1.1.

$\Rightarrow$. Write

$$f(X^n) = g(X) \cdot f(X) \tag{5}$$

where $g(X)$ is some nonzero polynomial with integer coefficients.

If $\xi$ is any root of $f(X) = 0$ such that $\xi \neq 0, 1$, then $\xi^n$ is also a root of $f(X) = 0$ by (5). Thus $|\xi| = 1$; otherwise, $f(X) = 0$ would have infinitely many roots.

Write $\xi = \exp(2\pi\sqrt{-1}\eta)$ for some real number $\eta$. Again $\eta$ should be a rational number; otherwise, $\{\xi, \xi^n, \xi^{n^2}, \dots\}$ would be an infinite set of roots of $f(X) = 0$. Write

$$\eta = \frac{r}{sm}$$

where $r, s, m$ are nonzero integers so that

(i) $s > 0$, $m > 0$,

(ii) g.c.d.$\{r, sm\} = 1$

(iii) g.c.d.$\{s, m\} = 1$, g.c.d.$\{m, n\} = 1$ and every prime factor of $s$, if any, should divide $n$.

It is clear that $\xi^{n^l}$ will be a primitive $m$th root of 1 if $l$ is an integer large enough. Thus, if $m \geq 2$, then $f(X)$ will be divisible by $\Phi_m(X)$ since $\Phi_m(X)$ is irreducible [**6**, p. 264]. On the other hand, if $m = 1$ and $s \geq 2$, choose nonnegative integer $a$ such that $\eta \cdot n^a \notin \mathbf{Z}$ but $\eta n^{a+1} \in \mathbf{Z}$. Write

$$\eta n^a = \frac{e}{d}$$

where $d \geq 2$ and g.c.d.$\{d, e\} = 1$. Then $f(X)$ is divisible by $\Phi_d(X)$ with $d \mid n$. Thus we may write $f(X) = x^\alpha \cdot \{\Phi_1(X)\}^\beta \{\Phi_{m'}(X)\}^\gamma \cdot h(X)$ where either g.c.d.$\{m', n\} = 1$ or $m' \mid n$.

In either case, if $\deg h(X) = 0$, then $h(X)$ is a nonzero integer. If $\deg h(X) \geq 1$, we can also extract a factor $\{\Phi_{m'}(X)\}^\gamma$ from $h(X)$ where either g.c.d.$\{m', n\} = 1$ or $m' \mid n$. Proceeding as before, we can prove that every factor of degree $\geq 1$ of $f(X)$ is of the form

$$X, \quad X - 1, \quad \Phi_m(X), \Phi_d(X)$$

where $m, d \geq 2$, g.c.d.$\{n, m\} = 1$ and $d \mid n$.

Suppose that $d_1, \ldots, d_l$ are those distinct divisors of $n$ such that $\Phi_{d_j}(X)$ is a factor of $f(X)$ and $d_j \geq 2$. Write

$$n = n_j k_j$$

where $d_j$ and $k_j$ have the same set of prime factors and g.c.d.$\{d_j, n_j\} = 1$. Apply formula (2) and note that $\Phi_{d_j}(X)$ is relatively prime to

$$\prod_{i=1}^{l} \Phi_{d_i}(X^n) = \prod_{i=1}^{l} \prod_{d|n_i} \Phi_{d_i k_i d}(X)$$

because $d_j \mid n$ and, for each $1 \leq i \leq l$, there is a prime $p$ such that the exponent of $p$ in $d_i k_i$ exceeds that of $p$ in $n$, and therefore $d_j \neq d_i k_i d$. Clearly $\Phi_{d_j}(X)$ is also relatively prime to

$$\Phi_m(X^n) = \prod_{d|n} \Phi_{md}(X), \quad \text{if g.c.d.}\{m, n\} = 1,$$

because $d_j \mid n$ and $md$ contains a prime factor not appearing in the factorization of $n$ provided that $m \geq 2$, and therefore $d_j \neq md$.

Thus, if $f(X) \mid f(X^n)$ and $\Phi_{d_j}(X)$ divides $f(X)$, then $X^n - 1$ should be the multiple of $\Phi_{d_j}(X)$ in $f(X^n)$ and the multiplicity of $\Phi_{d_j}(X)$ in $f(X)$ is not greater than that of $X - 1$ in $f(X)$. Hence the result.

Before we start to solve the second question, consider the following lemma, which is the Möbius inversion formula in some special context [**6**, p. 145].

**Lemma 2.4.** *Let $f_1(X), f_2(X), \ldots, f_n(X), \ldots$ be a sequence of nonzero polynomials so that*

$$f_m(X^n) = \prod_{d|n} f_{md}(X)$$

*whenever* g.c.d.$\{m, n\} = 1$. *Then*

$$f_{mn}(X) = \prod_{d|n} \{f_m(X^d)\}^{\mu(n/d)} \tag{6}$$

*provided that* g.c.d.$\{m,n\}=1$. *In particular,*

$$\Phi_{mn}(X)=\prod_{d|n}\{\Phi_m(X^d)\}^{\mu(n/d)}$$

*whenever g.c.d.*$\{m,n\}=1$.

*Proof.* We shall prove formula (6).

Induction on $n$. Consider

$$\begin{aligned}
\prod_{d|n}\Big\{\prod_{e|d} f_m(X^e)^{\mu(d/e)}\Big\} &= \prod_{\substack{e|d\\ d|n}} f_m(X^e)^{\mu(d/e)} = \prod_{e|n}\Big\{\prod_{ef|n} f_m(X^e)^{\mu(f)}\Big\} \\
&\quad \text{(by writing } d=ef) \\
&= \prod_{e|n}\Big\{f_m(X^e)^{\sum_{f|n/e}\mu(f)}\Big\} \\
&= f_m(X^n) \quad \Big(\sum_{f|m'}\mu(f)=0 \quad \text{if } m'\geq 2\Big) \\
&= \prod_{d|n} f_{md}(X) = f_{mn}(X)\cdot\prod_{\substack{d|n\\ d<n}} f_{md}(X) \\
&= f_{mn}(X)\cdot\prod_{\substack{d|n\\ d<n}}\Big\{\prod_{e|d} f(X^e)^{\mu(d/e)}\Big\} \\
&\quad \text{(by induction).}
\end{aligned}$$

Hence the result.

*Remark.* It is unnecessary to assume that $f_m(X)$ has integer coefficients in the above lemma.

**Theorem 2.5.** *Let* $f_1(X), f_2(X), \ldots, f_m(X), \ldots$ *be a sequence of nonzero polynomials with integer coefficients. Then this sequence of polynomials satisfies the following property*

$$f_m(X^n)=\prod_{d|n} f_{md}(X)$$

*whenever g.c.d.*$\{m,n\}=1$ *if and only if there exist nonnegative integers* $\alpha$ *and* $\beta$, *a nonzero integer* $a$, *so that*

$$f_1(X) = aX^{\alpha}(X-1)^{\beta}; \tag{7}$$

*and*

$$f_m(X) = X^{\alpha\varphi(m)}\Phi_m(X)^{\beta}, \quad \text{if } m \geq 2. \tag{8}$$

*Proof.* $\Leftarrow$. By Theorem 1.1 and the formulae

$$n = \sum_{d|n} \varphi(d),$$
$$\varphi(mn) = \varphi(m)\varphi(d) \quad \text{if g.c.d.}\{m,d\} = 1$$

[**6**, p. 107].

$\Rightarrow$. Since

$$f_1(X^n) = \prod_{d|n} f_d(X)$$

for any positive integer $n$, it follows that $f_1(X^n)$ is divisible by $f_1(X)$ for any $n$. Using Theorem 2.3 and after some computation, we find that

$$f_1(X) = aX^{\alpha}(X-1)^{\beta}$$

for some nonnegative integers $\alpha$ and $\beta$, $a \neq 0$.

By Lemma 2.4, we find that, for any $n \geq 2$,

$$\begin{aligned} f_n(X) &= \prod_{d|n} \{f_1(X^d)\}^{\mu(n/d)} \\ &= \prod_{d|n} \{\alpha^{\mu(n/d)} \cdot X^{\alpha\mu(n/d)d} \cdot (X^d-1)^{\beta\cdot\mu(n/d)}\} \\ &= a^{\sum_{d|n}\mu(n/d)} \cdot X^{\alpha\cdot\sum_{d|n}\mu(n/d)d} \cdot \left\{\prod_{d|n}(X^d-1)^{\mu(n/d)}\right\}^{\beta} \\ &= X^{\alpha\cdot\varphi(n)}\Phi_n(X)^{\beta}. \end{aligned}$$

*Remark.* If $f_1(X), f_2(X), \dots$ are defined by (7) and (8), clearly this sequence satisfies the property

$$f_m(X^{nk}) = \prod_{d|n} f_{mkd}(X)$$

whenever g.c.d.$\{m, n\} = 1$ and $m$ is divisible by every prime factor of $k$.

**3. Integral group rings.** Throughout this section, except in Theorem 3.9 and Example 3.10, we shall assume that $n := p_1 p_2 \cdots p_r$ is a square-free positive integer and $R$ is a Dedekind domain satisfying the following two conditions.

(R1) $R[X]/\Phi_d(X)$ is a Dedekind domain for any integer $d$ with $d \mid n$,

(R2) The ideal $nR$ is not zero in $R$ and is an intersection of maximal ideals.

Note that $\operatorname{char} R = 0$ because of the condition (R2).

**Definition 3.1.** Define $S_1$ and $S_2$ by

$$S_1 := \{d \in \mathbf{N} : d \mid n \text{ and } \mu(d) = 1\}$$
$$S_2 := \{d \in \mathbf{N} : d \mid n \text{ and } \mu(d) = -1\}.$$

**Definition 3.2.** Define $f_1(X), f_2(X) \in \mathbf{Z}[X] (\subset R[X])$ by

$$f_1(X) := \prod_{d \in S_1} \Phi_d(X), \qquad f_2(X) := \prod_{d \in S_2} \Phi_d(X).$$

**Definition 3.3.** Define $\Lambda$, $A_0$, $A_1$ and $A_2$ by

$$\Lambda := R[X]/X^n - 1, \qquad A_0 := R[X]/\langle f_1(X), f_2(X)\rangle,$$
$$A_1 := R[X]/f_1(X), \qquad A_2 := R[X]/f_2(X).$$

Let $\pi_i : A_i \to A_0$, $\phi_i : \Lambda \to A_i$ be the canonical projections for $1 \le i \le 2$. Note that $\Lambda$ is the integral group ring of the cyclic group of order $n$ over $R$.

**Lemma 3.4.** *Let $d \in S_1$, $e \in S_2$. Then*

$$n \in \langle \Phi_d(X), f_2(X) \rangle \cap \langle f_1(X), \Phi_e(X) \rangle.$$

*Proof.* We shall prove $n \in \langle \Phi_d(X), f_2(X) \rangle$. The proof of $n \in \langle f_1(X), \Phi_e(X) \rangle$ is similar.

For any $e \in S_2$, if $(e/d) \neq p_i^{\pm 1}$ for some $i$, $1 \leq i \leq r$, then

$$1 \in \langle \Phi_d(X), \Phi_e(X) \rangle \tag{9}$$

by Theorem 2.2.

If $p_i \mid d$, then $(d/p_i) \in S_2$ and

$$p_i \in \langle \Phi_d(X), \Phi_{d/p_i}(X) \rangle \tag{10}$$

again by Theorem 2.2.

If $p_i \nmid d$, then $dp_i \in S_2$ and

$$p_i \in \langle \Phi_d(X), \Phi_{dpi}(X) \rangle. \tag{11}$$

From (9), (10) and (11) we obtain

$$n = p_1 p_2 \cdots p_r \in \langle \Phi_d(X), f_2(X) \rangle.$$

**Lemma 3.5.**

$$A_1 \simeq \bigoplus_{d \in S_1} R[X]/\Phi_d(X), \qquad A_2 \simeq \bigoplus_{e \in S_2} R[X]/\Phi_e(X).$$

*Proof.* For any $d, d' \in S_1$, if $d \neq d'$, then $1 \in \langle \Phi_d(X), \Phi_{d'}(X) \rangle$ by Theorem 2.2. Hence the decomposition of $A_1$ (or $A_2$) follows from the Chinese Remainder Theorem.

**Definition 3.6.** For $1 \le i \le r$, define

$$n_i := \frac{n}{p_i}.$$

Since $p_i \nmid n_i$, $X^{n_i} - 1$ is a separable polynomial in $\mathbf{Z}/p_i\mathbf{Z}[X]$. Moreover, $p_i R$ is an intersection of maximal ideals in $R$ by the condition (R2). Write

$$R/p_i R = \mathbf{F}_{i,1} \times \mathbf{F}_{i,2} \times \cdots \times \mathbf{F}_{i,l_i}$$

where each $\mathbf{F}_{i,j}$ is a field of characteristics $p_i > 0$.

In $\mathbf{F}_{i,j}[X]$, $X^{n_i} - 1$ is a separable polynomial. Write

$$X^{n_i} - 1 = \prod_{1 \le k \le m(i,j)} g(i,j,k)$$

where each $g(i,j,k)$ is a monic irreducible polynomial in $\mathbf{F}_{i,j}[X]$ and $m(i,j)$ is a positive integer.

Let $S_0$ be the set of these triples $(i,j,k)$, i.e.,

$$S_0 := \{(i,j,k) \in \mathbf{N}^3 : 1 \le i \le r, 1 \le j \le l_i, 1 \le k \le m(i,j)\}.$$

**Lemma 3.7.**

$$A_0 \simeq \bigoplus_{(i,j,k) \in S_0} \mathbf{F}_{i,j}[X]/g(i,j,k)$$

*where $\mathbf{F}_{i,j}[X]/g(i,j,k)$ is a field of characteristic $p_i > 0$.*

*Proof.*

$$\begin{aligned} A_0 &= R[X]/\langle f_1(X), f_2(X)\rangle \\ &\simeq R[X]/f_1(X) \underset{\Lambda}{\otimes} R[X]/f_2(X) \\ &\simeq \Big(\bigoplus_{d \in S_1} R[X]/\Phi_d(X)\Big) \underset{\Lambda}{\otimes} R[X]/f_2(X) \\ &\simeq \bigoplus_{d \in S_1} R[X]/\langle \Phi_d(X), f_2(X)\rangle \end{aligned}$$

$$
\begin{aligned}
&= \bigoplus_{d\in S_1} R[X]/\langle n, \Phi_d(X), f_2(X)\rangle \quad \text{(by Lemma 3.4)}\\
&\simeq \bigoplus_{1\le i\le r}\bigoplus_{d\in S_1} R[X]/\langle p_i, \Phi_d(X), f_2(X)\rangle\\
&\simeq \bigoplus_{1\le i\le r}\bigoplus_{1\le j\le l_i}\bigoplus_{d\in S_1} \mathbf{F}_{i,j}[X]/\langle \Phi_d(X), f_2(X)\rangle\\
&\simeq \bigoplus_{1\le i\le r}\bigoplus_{1\le j\le l_i}\left\{\bigoplus_{\substack{d\in S_1\\ p_i\mid d}} \mathbf{F}_{i,j}[X]/\langle \Phi_d(X), \Phi_{d/p_i}(X)\rangle\right.\\
&\qquad\qquad\qquad\qquad\left.\times \bigoplus_{\substack{d\in S_1\\ p_i\nmid d}} \mathbf{F}_{i,j}[X]/\langle \Phi_d(X), \Phi_{dp_i}(X)\rangle\right\}\\
&\simeq \bigoplus_{1\le i\le r}\bigoplus_{1\le j\le l_i}\left\{\bigoplus_{\substack{d\in S_1\\ p_i\mid d}} \mathbf{F}_{i,j}[X]/\Phi_{d/p_i}(X) \times \bigoplus_{\substack{d\in S_1\\ p_i\nmid d}} \mathbf{F}_{i,j}[X]/\Phi_d(X)\right\}\\
&\simeq \bigoplus_{1\le i\le r}\bigoplus_{1\le j\le l_i}\bigoplus_{\substack{m\mid n\\ p_i\nmid m}} \mathbf{F}_{i,j}[X]/\Phi_m(X)\\
&\simeq \bigoplus_{1\le i\le r}\bigoplus_{1\le j\le l_i} \mathbf{F}_{i,j}[X]/X^{n_i}-1\\
&\simeq \bigoplus_{(i,j,k)\in S_0} \mathbf{F}_{i,j}[X]/g(i,j,k).
\end{aligned}
$$

**Theorem 3.8.** *The following is a pull-back diagram*

$$
\begin{array}{ccc}
\Lambda & \xrightarrow{\phi_1} & A_1\\
{\scriptstyle\phi_2}\downarrow & & \downarrow{\scriptstyle\pi_1}\\
A_2 & \xrightarrow[\pi_2]{} & A_0
\end{array}
$$

*i.e., the map* $\Lambda \to \{(a_1,a_2)\in A_1\oplus A_2 : \pi_1(a_1)=\pi_2(a_2)\}$ *by sending* $a\in\Lambda$ *to* $(\phi_1(a),\phi_2(a))$ *is an isomorphism. Moreover,* $\Lambda$ *is a Dedekind-like ring in the sense of Levy* [**8**, p. 355].

*Proof.* To prove the above diagram is a pull-back diagram is equivalent to proving that the following is a short exact sequence

$$0 \to \Lambda \overset{(\phi_1,\phi_2)}{\longrightarrow} A_1 \oplus A_2 \to A_0 \to 0$$
$$(a_1, a_2) \mapsto \pi_1(a_1) - \pi_2(a_2).$$

However it is clear that the above is a short exact sequence by definitions of $\Lambda$, $A_1$, $A_2$ and $A_0$.

It remains to prove that $\Lambda$ is a Dedekind-like ring in Levy's sense. Define $q_i : A_1 \oplus A_2 \to A_0$ by $q_1(a_1, a_2) = \pi_1(a_1)$, $q_2(a_1, a_2) = \pi_2(a_2)$. It is easy to verify that $(a_1, a_2) \mapsto (q_1(a_1, a_2), q_2(a_1, a_2))$ of $A_1 \oplus A_2 \to A_0 \oplus A_0$ is onto and $\Lambda \simeq \{(a_1, a_2) \in A_1 \oplus A_2 : q_1(a_1, a_2) = q_2(a_1, a_2)\}$. Note that $\operatorname{Ker} q_1 \supset A_2$, $\operatorname{Ker} q_2 \supset A_1$; thus, the independence condition [**8**, p. 355] is satisfied. Since $A_1 \oplus A_2$ is a finite direct sum of Dedekind domains (but not fields) by Lemma 3.5 and $A_0$ is a finite direct sum of fields by Lemma 3.7, hence $\Lambda$ is a Dedekind-like ring.

**Theorem 3.9.** *Let $R$ be the ring of integers of some algebraic number field $K$, and let $n$ be a square-free positive integer. Assuming that* (*i*) *$K$ and the cyclotomic field* $\mathbf{Q}(\exp(2\pi\sqrt{-1}/n))$ *are linearly disjoint over* $\mathbf{Q}$, *and* (*ii*) *$nR$ is unramified in $R$. Then $R$ satisfies both conditions* (R1) *and* (R2). *Therefore,* $\Lambda := R[X]/X^n - 1$ *is a Dedekind-like ring.*

*Proof.* Let $\zeta_d := \exp(2\pi\sqrt{-1}/d)$ for any $d \mid n$. Note that $K$ and $\mathbf{Q}(\zeta_d)$ are linearly disjoint over $\mathbf{Q}$, because of [**9**, p. 50] and the assumption (i). Hence $R[\zeta_d] \simeq R \otimes_{\mathbf{Z}} \mathbf{Z}[X]/\Phi_d(X) \simeq R[X]/\Phi_d(X)$ by [**9**, p. 49]. Moreover, the only prime numbers $p$ ramified in $\mathbf{Q}(\zeta_d)$ are the odd prime numbers $p$ with $p \mid d$ by [**11**, p. 92]. Thus the ring of integers in $K(\zeta_d)$ is $R[\zeta_d]$ by [**11**, p. 91], thanks to the assumption (ii). Hence $R[X]/\Phi_d(X)$ is a Dedekind domain. It follows that both the conditions (R1) and (R2) are satisfied.

**Example 3.10.** Let $\zeta_k := \exp(2\pi\sqrt{-1}/k)$ and $n$ be a square-free positive integer.

For any positive integer $m$ with g.c.d.$\{m, n\} = 1$, $\mathbf{Q}(\zeta_m)$ and $\mathbf{Q}(\zeta_n)$ are linearly disjoint over $\mathbf{Q}$. (Note that $[\mathbf{Q}(\zeta_m) \otimes_{\mathbf{Q}} \mathbf{Q}(\zeta_n) : \mathbf{Q}] = \varphi(mn) = [\mathbf{Q}(\zeta_{mn}) : \mathbf{Q}] = [\mathbf{Q}(\zeta_m)\mathbf{Q}(\zeta_n) : \mathbf{Q}]$. Then apply [**9**, p. 49].

By the above theorem, if $R := \mathbf{Z}[\zeta_m]$, then $\Lambda := R[X]/X^n - 1$ is a Dedekind-like ring. (Thus the condition that $q$ is square-free in [**8**, Corollary 1.8] is unnecessary; only the condition that g.c.d.$\{q, n\} = 1$ will suffice to guarantee that $\Lambda$ is Dedekind-like in this situation.)

Consider the case of quadratic fields. If $m$ is any square-free integer, i.e., $m < 0$ is permitted, and g.c.d.$\{m, n\} = 1$, then $\mathbf{Q}(\sqrt{m})$ and $\mathbf{Q}(\zeta_n)$ are linearly disjoint over $\mathbf{Q}$ because $\mathbf{Q}(\sqrt{m}) \cap \mathbf{Q}(\zeta_n) = \mathbf{Q}$. (Note that, if $K_1$ and $K_2$ are field extensions of a field $F$ and $K_1$ is a finite Galois extension of $F$, then $K_1$ and $K_2$ are linearly disjoint over $F$ if and only if $K_1 \cap K_2 = F$.) Thus, if $R$ is the ring of integers in $\mathbf{Q}(\sqrt{m})$ and $\Lambda := R[X]/X^n - 1$, then $\Lambda$ is a Dedekind-like ring if $m \equiv 1$ or $2 \pmod 4$. Moreover, if $n$ is odd and $m \equiv 3 \pmod 4$, then $\Lambda$ is also a Dedekind-like ring.

On the other hand, if $K$ is any algebraic number field such that g.c.d.$\{\varphi(n), [K : \mathbf{Q}]\} = 1$, then $K$ and $\mathbf{Q}(\zeta_n)$ are linearly disjoint over $\mathbf{Q}$. Hence if we assume furthermore that $n$ is unramified in $K$, then the ring of integers in $K$ also satisfies the conditions (R1) and (R2).

**Acknowledgment.** I should like to thank the referee for pointing out a dubious argument in the proof of Theorem 2.3 of an original version of this note. It led to the present form and the modified proof of Theorem 2.3.

## REFERENCES

**1.** R.P. Brent, *On computing factors of cyclotomic polynomials*, Math. Comp. **61** (1993), 131–149.

**2.** C.C. Cheng, J.H. McKay and S.S. Wang, *Resultants of cyclotomic polynomials*, Proc. Amer. Math. Soc. **123** (1995), 1053–1059.

**3.** C.W. Curtis and I. Reiner, *Methods of representation theory with applications to finite groups and orders*, Volume 1, Wiley-Interscience, New York, 1981.

**4.** F.E. Diederichsen, *Über die Ausreduktion ganzzahliger Gruppendarstellungen bei arithmetisher Äquivalenz*, Abh. Math. Sem. Univ. Hamburg **13** (1940), 357–412.

**5.** P. Erdös and R.C. Vaughan, *Bounds for the r-th coefficients of cyclotomic polynomials*, J. London Math. Soc. **8** (1974), 393–400.

**6.** N. Jacobson, *Basic algebra* I, W.H. Freeman and Company, San Francisco, 1974.

**7.** L.S. Levy, *Modules over Dedekind-like rings*, J. Algebra **93** (1985), 1–116.

**8.** ———, $\mathbf{Z}G_n$*-modules,* $G_n$ *cyclic of square-free order* $n$, J. Algebra **93** (1985), 354–375.

**9.** S. Lang, *Introduction to algebraic geometry*, Interscience Publ., New York, 1958.

**10.** D.H. Lehmer, *Some properties of the cyclotomic polynomials*, J. Math. Anal. Appl. **15** (1966), 105–117.

**11.** R.L. Long, *Algebraic number theory*, Marcel Dekker, Inc., New York, 1977.

**12.** A. Schinzel, *On primitive prime factors of* $a^n - b^n$, Proc. Cambridge Phil. Soc. **58** (1962), 555–562.

Department of Mathematics, National Taiwan University, Taipei, Taiwan, Republic of China
*E-mail address:* kang@math.ntu.edu.tw