

# Introduction to Algebra II, Field Theory

AnLei

## Contents

<b>1</b>	<b>Basics</b>	<b>1</b>
1.1	Characteristic . . . . .	1
1.2	Field extensions . . . . .	2
1.3	Prime subfield . . . . .	4
1.4	Simple Extension . . . . .	4
1.5	Algebraic Extension . . . . .	7
1.6	Composite Field . . . . .	8
1.7	Example of Extensions . . . . .	8
1.8	Algebraic Elements . . . . .	8
<b>2</b>	<b>Splitting fields and algebraic closures</b>	<b>8</b>
<b>3</b>	<b>Separable Extensions</b>	<b>8</b>
<b>4</b>	<b>Cyclotomic Polynomials and Extensions</b>	<b>8</b>

## 1 Basics

### 1.1 Characteristic

**Definition 1** (Characteristic). Let  $F$  be a field. The characteristic of  $F$  is defined by

$$\text{char } F := \begin{cases} \min\{n \in \mathbb{N} : n \cdot 1_F = \underbrace{1_F + \cdots + 1_F}_n = 0\} & \text{if such } n \text{ exists} \\ 0 & \text{otherwise} \end{cases}$$

**Proposition 1.**  $\text{char } F$  is either a prime or 0.

*Proof.*

Suppose  $p = \text{char } F = ab$  for some  $a, b \in \mathbb{N}_{\geq 1}$ . Then  $p1_F = (ab)1_F = (a1_F)(b1_F) = 0$ . Since  $F$  is a integral domain,  $(a1_F) = 0$  or  $(b1_F) = 0$ , which contradicts with the minimality of  $p$ .  $\square$

## 1.2 Field extensions

**Definition 2** (Field Extension).  $K$  is a **field extension** of  $F$  if  $K$  is a field containing a subfield  $F$ , denoted by  $K/F$ .

Examples:

1.  $\mathbb{C}/\mathbb{R}/\mathbb{Q}$  ( $\mathbb{C}$  is a field extension of  $\mathbb{R}$  and  $\mathbb{R}$  is a field extension of  $\mathbb{Q}$ )
2. For any squarefree integer  $D \neq 1$ ,  $\mathbb{C}/\mathbb{Q}(\sqrt{D})/\mathbb{Q}$ .

我們有  $\mathbb{C} = \mathbb{R} + \mathbb{R}i$  作為  $\mathbb{R}$  的 field extension。對於任意  $a + bi \in \mathbb{C}$ ，我們可以將其視為以  $a, b \in \mathbb{R}$  作為係數， $\{1, i\}$  作為基底而得到的一個向量。事實上，可以觀察到若  $K/F$ ，則  $(K, F, +, \cdot)$  是一個向量空間，其中加法使用兩個  $K$  的元素，而乘法為  $K$  中元素與  $F$  元素的係數積。

**Definition 3** (Degree). If  $K/F$ , the **degree**  $[K : F]$  is defined by the dimension of  $K$  as an  $F$ -vector space.

$$[K : F] = \dim_F(K)$$

Examples:

1.  $[\mathbb{C} : \mathbb{R}] = 2$  since  $\mathbb{C}/\mathbb{R}$  has a basis  $\{1, i\}$
2.  $[\mathbb{Q}(\sqrt{D}) : \mathbb{Q}] = 2$  since  $\mathbb{Q}(\sqrt{D})/\mathbb{Q}$  has a basis  $\{1, \sqrt{D}\}$
3.  $[\mathbb{R} : \mathbb{Q}] = \infty$ , since  $\dim_{\mathbb{Q}}(\mathbb{R}) = \infty$ .

**Theorem 1** (Degree 的 Chain Rule). If  $L/K/F$ . Then  $[L : F] = [L : K][K : F]$

*Proof.*

Let  $[L : K] = m$ ,  $[K : F] = n$  (both finite) and

$\alpha_1, \dots, \alpha_m$  be basis of  $L/K$

$\beta_1, \dots, \beta_n$  be basis of  $K/F$

這邊就直接猜  $L/F$  的一組基底是

$$C = \bigcup_{i=1}^m \bigcup_{j=1}^n \{\alpha_i \beta_j\}$$

- $C$  span  $L/K$

對於任意  $x \in L$ ，存在  $a_1, \dots, a_m \in K$  使得

$$x = \sum_{i=1}^m a_i \alpha_i$$

而其中的係數  $a_i$  又可以用  $F$  中的係數表示

$$a_i = \sum_{j=1}^n b_{ij} \beta_j \quad b_{ij} \in F$$

所以

$$x = \sum_{i,j} b_{ij} \boxed{\alpha_i \beta_j}$$

- $C$  is linearly independent

若存在  $b_{ij} \in F$  使得

$$\sum_{i,j} b_{ij} \alpha_i \beta_j = 0$$

只要寫成

$$\sum_{i=1}^m \left( \sum_{j=1}^n b_{ij} \beta_j \right) \alpha_i = 0$$

因為  $\alpha_i$  在  $L/K$  中是線性獨立的，所以

$$\left( \sum_{j=1}^n b_{ij} \beta_j \right) = 0 \quad \forall i$$

再一次，因為  $\beta_j$  在  $K/F$  中是線性獨立的，所以：

$$b_{ij} = 0 \quad \forall i, j$$

所以  $C$  是  $L/F$  上的基底，且

$$[L : F] = |C| = mn = [L : K][K : F]$$

無窮的證明暫略.....

□

**Definition 4** (Subfield generated by elements). 假定  $F$  是一個 field， $K/F$ 。並且令：

$$\alpha_1 \dots \alpha_n \in K$$

由於 subfield 的交集還是 subfield，所以若令  $\mathcal{J}$  為  $K$  中「同時包含  $F$  與  $\alpha_1 \dots \alpha_n$  的 subfield 形成的搜集」，也就是：

$$\mathcal{J} = \{J \subseteq K \mid K/J, \text{ and } J/F \text{ and } \alpha_1 \dots \alpha_n \in J\}$$

則所有這樣的 subfield 形成的交集：

$$\bigcap_{J \in \mathcal{J}} J$$

仍然會是一個  $K$  中同時包含  $F$  與  $\alpha_1 \dots \alpha_n$  的 subfield。且這是所有「 $K$  中同時包含  $F$  與  $\alpha_1 \dots \alpha_n$  的 subfield」中最小的 subfield，稱為 subfield generated by  $\alpha_1 \dots \alpha_n$  over  $F$ ，並且記成：

$$F(\alpha_1, \alpha_2 \dots \alpha_n) = \bigcap_{J \in \mathcal{J}} J$$

如果只有一個  $\alpha$ ，則  $F(\alpha)$  成為一個 simple extension， $\alpha$  為一個 primitive element。

現在我們來看這個 extension  $E = F(\alpha_1, \alpha_2 \dots \alpha_n)$  實際上長什麼樣子。因為  $\alpha_1, \dots, \alpha_n \in E$  而  $E$  有加法和乘法的封閉性，所以任何以  $F$  中元素為係數的  $\alpha_1, \dots, \alpha_n$  的多項式都在  $E$  裡面。而  $E$  也有除法的封閉性 (因為乘法有逆)，所以應該包含所有這些多項式的分式：

$$F(\alpha_1, \dots, \alpha_n) \supseteq \left\{ \frac{f(\alpha_1, \dots, \alpha_n)}{g(\alpha_1, \dots, \alpha_n)} : f, g \in F[\alpha_1, \dots, \alpha_n], g \neq 0 \right\}$$

可以驗證由這些多項式分式的蒐集應該也是一個 field，所以也是  $\mathcal{J}$  中的元素，但  $E$  又是其中最小的，所以“ $\subseteq$ ”也成立，於是等號成立。

### 1.3 Prime subfield

**Definition 5** (Prime Subfield). The prime subfield  $P$  of a field  $F$  is the minimal subfield of  $F$  containing  $1_F$ :

$$P = \bigcap_{\substack{F/S \\ 1_F \in S}} S$$

i.e. the subfield generated by  $1_F$ .

我們能夠定義一個 natural ring homomorphism。如果  $\text{char } F = p > 0$ ，考慮  $\phi : \mathbb{Z} \rightarrow F, \phi(a) = a1_F \circ \phi$  的 kernel 是

$$\ker \phi = \{a \in \mathbb{Z} : \phi(a) = a \cdot 1_F = 0_F\} = \{a \in \mathbb{Z} : p|a\} = p\mathbb{Z}$$

$\phi$  的 image 就是  $F$  的 prime subfield。所以由 1st theorem of isomorphism 我們有  $P \cong \mathbb{Z}/p\mathbb{Z}$ 。

如果  $\text{char } F = 0$ ，考慮  $\phi : \mathbb{Q} \rightarrow F, \phi(a/b) = (a1_F)(b1_F)^{-1}$ 。因為  $b \neq 0$  所以  $(b1_F) \neq 0_F$ ， $\phi$  是 well-defined。  $\phi$  是可逆的：

$$\phi^{-1}((a1_F)(b1_F)^{-1}) = \frac{a}{b}$$

所以  $\phi$  是一個 ring isomorphism， $P \cong \mathbb{Q}$ 。可以總結如下

**Proposition 2.** Let  $P$  be prime subfield of a field  $F$ .

- If  $\text{char } F > 0$ , then  $P \cong \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$
- If  $\text{char } F = 0$ , then  $P \cong \mathbb{Q}$

### 1.4 Simple Extension

**Definition 6** (Simple Extension). If  $K/F$ , we say that  $K$  is a simple extension if  $K = F(\alpha)$  for some  $\alpha \in K$ .

一個 extension 是否 simple 並不顯然，即使我們使用兩個以上的元素 extent 也可能得到一個 simple extension，比如  $\mathbb{Q}[\sqrt{2}, \sqrt{3}] = \mathbb{Q}[\sqrt{2} + \sqrt{3}]$  (作業題)。

**Definition 7** (algebraic/transcendental). Let  $K/F$  be a field extension. An element  $\alpha \in K$  is said to be **algebraic over**  $F$  if  $\alpha$  is a root of some nonzero polynomial over  $F$ . If no such polynomials exist, then we say  $\alpha$  is **transcendental** over  $F$ . If every element of  $K$  is algebraic over  $F$ , then we say  $K$  is an **algebraic extension** of  $F$ .

**Theorem 2.** Let  $p(x)$  be an irreducible polynomial in  $F[x]$ . Then there is an extension field  $K$  s.t.  $p(x)$  has a root in  $K$ .

*Proof.*

Let  $K = F[x]/(p(x))$ . By Prop 15 of Chapter 9,  $K$  is a field. It contains  $F$  as a subfield. (To be more rigorous,  $K$  contains a subfield  $\{a + (p(x)) : a \in F\}$  which is isomorphic to  $F$ .) It's clear  $\alpha = x + (p(x)) \in K$  is a root of  $p(x)$ . ( $p(\alpha) = p(x) + (p(\alpha)) = 0 + (p(x))$ )  $\square$

**Proposition 3** (Minimal Polynomial: 以特定元素為根的多項式存在唯一的最小元素). Assume  $\alpha$  is algebraic over  $F$ . Then  $\exists!$  monic irreducible polynomial  $m_{\alpha,F}(x) \in F[x]$  s.t.

$$\begin{cases} \alpha \text{ is a root of } m_{\alpha,F}(x) \\ \text{a polynomial } f(x) \text{ has } \alpha \text{ as a root} \Leftrightarrow m_{\alpha,F}(x) | f(x) \end{cases}$$

The polynomial  $m_{\alpha,F}(x)$  is called the **minimal polynomial** of  $\alpha$  over  $F$ . We define the **degree** of  $\alpha$  over  $F$  to be  $\deg(m_{\alpha,F}(x))$ .

*Proof.*

Let  $I_\alpha := \{f(x) \in F[x], f(\alpha) = 0\}$ . It's straightforward to check that  $I$  is an ideal of  $F[x]$ . By the assumption that  $\alpha$  is algebraic over  $F$ ,  $I_\alpha \neq \{0\}$ . Let  $p(x)$  be a polynomial s.t.  $I_\alpha = (p(x))$ . Check  $p(x)$  is irreducible. Assume  $p(x) = a(x)b(x)$ ,  $a(x), b(x) \in F[x]$ . We want to show that one of  $a(x), b(x)$  is a unit, i.e. one of  $a(x), b(x)$  is a nonzero constant polynomial. Now we have

$$a(\alpha)b(\alpha) = p(\alpha) = 0$$

$$\Rightarrow a(\alpha) = 0 \text{ or } b(\alpha) = 0$$

If  $a(\alpha) = 0$ , then  $a(x) \in I_\alpha = (p(x))$

$$\Rightarrow p(x) | a(x)$$

$$\deg(a(x)) \geq \deg(p(x)) \geq \deg(a(x))$$

$$\Rightarrow \deg(a(x)) = \deg(p(x)) = \deg(b(x)) = 0$$

$\Rightarrow b(x)$  is a nonzero constant polynomial, i.e.  $b(x) \in F[x]^\times$ . Likewise, if  $b(\alpha) = 0$ , then  $a(x) \in F[x]^\times$ . This proves that  $p(x)$  is irreducible. Set

$$m_{\alpha,F}(x) = \frac{1}{(\text{leading coefficients of } p(x))} p(x)$$

Then  $m_{\alpha,F}(x)$  is the polynomial with the claimed properties.  $\square$

**Theorem 3.** Given a simple extension  $F(\alpha)$  of  $F$ , where  $\alpha$  is algebraic over  $F$  with minimal polynomial  $m(x)$ . Then

$$F(\alpha) \cong F[x]/(m(x))$$

*Proof.*

Consider the surjective ring homomorphism (evaluation at  $\alpha$ )  $\psi : F[x] \rightarrow F(\alpha)$ ,  $p(x) \mapsto p(\alpha)$ . The kernel is the set of polynomials having  $\alpha$  as a root, which is simply the ideal  $(m(x))$  of multiples of  $m$ . By the first isomorphism theorem

$$F(\alpha) \cong F[x]/(m(x))$$

□

**Corollary 1** (Extension as a vector space). If  $\alpha$  is algebraic over  $F$ , then

- $[F(\alpha), F] = \deg m_{\alpha, F} =: n$
- $\{1, \alpha, \dots, \alpha^{n-1}\}$  is a basis of  $F(\alpha)$  over  $F$
- $F(\alpha) = F[\alpha]$

*Proof.*

Let  $n = \deg m$ , then the coset representatives are the remainders in the division by  $m(x)$ ,

$$F[x]/(m(x)) = \{a_0 + a_1x + \dots + a_{n-1}x^{n-1} : a_i \in F\}$$

Equivalently, this says that the set  $1, \bar{x}, \dots, \bar{x}^{n-1}$  forms an  $F$ -basis for  $F(x)/(m(x))$ . Applying the isomorphism to  $F(\alpha)$  shows that the set  $\{1, \dots, \alpha^{n-1}\}$  is an  $F$ -basis for  $F(\alpha)$ . Therefore, we have  $[F(\alpha) : F] = n$ . Furthermore, we see immediately that  $F(\alpha) = F[\alpha]$ . □

Thus, for example, if  $K$  is a finite extension of  $\mathbb{F}_p$ . Let  $n = [K : \mathbb{F}_p]$  and  $\{\alpha_1, \dots, \alpha_n\}$  be a basis of  $K/\mathbb{F}_p$ , then

$$K = \{a_1\alpha_1 + \dots + a_n\alpha_n : a_j \in \mathbb{F}_p\}$$

so  $|K| = p^n$ . Since every finite field  $F$  has a prime subfield  $P$  isomorphic to  $\mathbb{F}_p$ , the cardinality of a finite field must be a prime power.

**Corollary 2.** (Algebraic Equivalence) If  $\alpha$  and  $\beta$  are two elements in  $K/F$  have the same minimal polynomials, then the fields  $F(\alpha)$  and  $F(\beta)$  are isomorphic as fields. Explicitly, there is an isomorphism  $\phi : F(\alpha) \rightarrow F(\beta)$  that fixes  $F$  (i.e. sends every element in  $F$  to itself) and sends  $\alpha$  to  $\beta$

*Proof.*

Let  $m(x)$  be the common minimal polynomials.  $F(\alpha)$  and  $F(\beta)$  are both isomorphic to  $F[x]/(m(x))$ . Thus  $F(\alpha)$  and  $F(\beta)$  are isomorphic. □

**Proposition 4** (Algebraic iff Finite Degree).  $\alpha$  is algebraic over  $F \Leftrightarrow [F(\alpha) : F] < \infty$

*Proof.*

" $\Rightarrow$ " is clear. Conversely, suppose that  $[F(\alpha) : F] = n < \infty$ . Consider  $1, \alpha, \dots, \alpha^n$ , the former  $n - 1$  terms form a basis of  $F(\alpha)$  over  $F$ . So  $\alpha^n = a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1}$  for some  $a_i \in F$ . So  $a_0 + a_1\alpha + \dots - a_{n-1}\alpha^{n-1} - \alpha^n = 0$ . Thus  $\alpha$  is algebraic over  $F$  □

**Corollary 3** (Finite-degree Extensions are Algebraic). If  $K/F$  is a finite extension, then  $K/F$  is an algebraic extension. (The converse is not true in general)

## 1.5 Algebraic Extension

**Theorem 4** (Finite Algebraic Extensions). If  $K/F$  is a field extension with  $K = F(\alpha_1, \dots, \alpha_n)$ , then

$$K/F \text{ is algebraic} \iff \text{each of the } \alpha_i \text{ are algebraic over } F$$

In this case,

$$[K : F] \leq \prod_{i=1}^n [F(\alpha_i) : F]$$

and every element of  $K$  is a polynomial with coefficients from  $F$  in the  $\alpha_i$

*Proof.*

(" $\Rightarrow$ "): Prove the negation. If any of the  $\alpha_i$  is transcendental over  $F$  then  $K$  is not algebraic over  $F$ .

(" $\Leftarrow$ "): Suppose the  $\alpha_i$  are algebraic. For each  $i$  we have  $F(\alpha_1, \dots, \alpha_i) = F(\alpha_1, \dots, \alpha_{i-1})(\alpha_i)$ . Since a simple extension is algebraic if and only if it has finite degree. By the chain rule we have

$$[K : F] = \prod_{i=1}^n [F(\alpha_1, \dots, \alpha_i) : F(\alpha_1, \dots, \alpha_{i-1})]$$

So  $[K : F]$  is also finite,  $K/F$  is algebraic.

Now, consider the minimal polynomial  $m(x)$  of  $\alpha_i$  over  $F$  and the minimal polynomial  $m'(x)$  of  $\alpha_i$  over  $F(\alpha_1, \dots, \alpha_{i-1})$ . Since  $m(x)$  is also a polynomial in  $F(\alpha_1, \dots, \alpha_{i-1})$  having  $\alpha_i$  as a root, by properties of minimal polynomials we see that  $m'(x) | m(x)$ , so

$$[F(\alpha_1, \dots, \alpha_i) : F(\alpha_1, \dots, \alpha_{i-1})] = \deg m' \leq \deg m = [F(\alpha_i) : F]$$

Taking the product from  $i = 1$  to  $n$  yields

$$[K : F] = \prod_{i=1}^n [F(\alpha_i) : F]$$

□

More explicitly, every element of  $K = F(\alpha_1, \dots, \alpha_n)$  is an  $F$ -linear combination of elements of the form  $\alpha_1^{c_1} \dots \alpha_n^{c_n}$ , where each  $c_i$  is an integer with  $0 \leq c_i \leq [F(\alpha_i) : F]$

$$F(\alpha_1, \dots, \alpha_n) = \{b_{1\dots n} \alpha_1^{c_1} \dots \alpha_n^{c_n} : b_{1\dots n} \in F, c_i \in \mathbb{Z}, 0 \leq c_i \leq [F(\alpha_i) : F]\}$$

**Theorem 5** (Towers of Algebraic Extensions). If  $L/K$  is an algebraic extension, and  $K/F$  is an algebraic extension, then  $L/F$  is an algebraic extension.

*Proof.*

These results are obvious if the extensions have finite degree. the content is when one of the extensions has infinite degree (but is still algebraic).

Consider any  $\alpha \in L$ . Since  $L/K$  is algebraic,  $\alpha$  is algebraic over  $K$  and is the root of some polynomial  $p(x) = a_0 + a_1x + \dots + a_nx^n \in K[x]$ . Since  $K/F$  is also algebraic, each of the  $a_i$  are algebraic over  $F$ , so the extension  $E = F(a_0, \dots, a_n)$  has finite degree over  $F$ .

Furthermore,  $|E(\alpha) : E| < \infty$  because  $\alpha$  is the root of a nonzero polynomial in  $E[x]$ . Thus, since  $|E(\alpha) : E|$  and  $|E/F|$  are both finite, so does  $|E(\alpha) : F|$ . So  $\alpha$  is a root of a polynomial of finite degree over  $F$ , so  $\alpha$  is algebraic over  $F$ . This holds for all  $\alpha \in L$ , so  $L$  is algebraic over  $F$ .  $\square$

## 1.6 Composite Field

### 1.7 Example of Extensions

By using our results on simple and composite extensions, along with the chain rule of field degrees, we can often say a great deal about extensions of small degree. First, we can characterize quadratic extensions:

**Proposition 5** (Quadratic Extensions).  $F$ : field with  $\text{char} \neq 2$ ;  $K/F$ : a quadratic extension (i.e.  $[K : F] = 2$ ). Then  $K = F(\alpha)$  for any  $\alpha \in K \setminus F$ .

*Proof.*

If  $\alpha \in K \setminus F$ , then the set  $\{1, \alpha\}$  is basis for  $K/F$  since  $[K : F] = 2$ . Thus  $K = F(\alpha)$   $\square$

Determine the degree of  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$  over  $\mathbb{Q}$

### 1.8 Algebraic Elements

## 2 Splitting fields and algebraic closures

## 3 Separable Extensions

## 4 Cyclotomic Polynomials and Extensions

**Definition 8** ( $n$ th root of unity). Let  $\zeta_n = e^{2\pi i/n}$  and  $\mu_n$  denote the group of  $n$ th root of unity over  $\mathbb{Q}$ .

$$\mu_n = \{1, \zeta_n, \dots, \zeta_n^{n-1}\}$$

這些元素就是  $x^n - 1 \in \mathbb{Q}[x]$  的所有根。 $\zeta \notin \mathbb{Q}$ ，可以用他 extent 出  $x^n - 1$  的 splitting field  $E = \mathbb{Q}(\xi)$ 。

**Definition 9** (Primitive).  $\zeta \in \mu_n$  is primitive if  $\langle \zeta \rangle = \mu_n$ , i.e. if  $\zeta = \zeta_n^k$  where  $(k, n) = 1$ .

**Remark 1.** 可以 recall 一些 group theory 的東西:

- $\mathbb{Z}/n\mathbb{Z}$  和  $\mu_n$  之間有一個 isomorphism:  $a \mapsto \zeta_n^a$ ，且  $\mu_n$  中有  $\varphi(n)$  個 primitive 的元素。
- $|\zeta_n^i| = n/(n, i)$



**Definition 10** (Cyclotomic Polynomial). Define the  $n$ th cyclotomic polynomial  $\Phi_n(x)$  to be the polynomial whose roots are the primitive  $n$ th roots of unity:

$$\Phi_n(x) := \prod_{\zeta \text{ primitive } \in \mu_n} (x - \zeta) = \prod_{\substack{1 \leq k < n \\ (k, n) = 1}} (x - \zeta_n^k) \in E[x]$$

so  $\deg \Phi_n = \varphi(n)$

現在我們來看一個包含完整的 root of unity 的  $x^n - 1$  如何拆分成 Cyclotomic Polynomials: 如果  $n = p$  是質數, 則

$$x^p - 1 = (x - 1)(x^{p-1} + x^{p-2} + \cdots + 1) = (x - 1)\Phi_p(x)$$

如果  $n$  不是質數, 比如

$$x^4 - 1 = (x - 1)(x + 1)(x^2 + 1)$$

$$x^6 - 1 = (x^3 - 1)(x^3 + 1) = (x - 1)(x + 1)(x^2 + x + 1)(x^2 - x + 1)$$

$$x^n - 1 = \prod_{\zeta \in \mu_n} (x - \zeta)$$

可以將  $\mu_n$  中的元素以它們的 order  $d$  (為  $n$  的因數) 分類:

$$x^n - 1 = \prod_{d|n} \prod_{\substack{\zeta \in \mu_n \\ |\zeta| = d}} (x - \zeta)$$

因為  $\mu_d = \{1, \zeta_d, \dots, \zeta_d^{d-1}\}$  中元素的 order 為  $|\zeta_d^i| = d/(d, i)$ 。所以第二個連乘相當於把  $\mu_d$  中的 primitive 元素收集起來:

$$x^n - 1 = \prod_{d|n} \prod_{\substack{1 \leq k < d \\ (k, d) = 1}} (x - \zeta_d^k) = \prod_{d|n} \Phi_d(x)$$

在 Definition 10 中我們是在  $E[X]$  中定義的, 現在我們證明他實際上在  $\mathbb{Z}[X]$  中而且是 monic。

**Lemma 1.**  $\Phi_n(x) \in \mathbb{Z}[x]$  and is monic.

*Proof.*

We already have

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

We now prove by induction on  $n$ .

$$n - 1 \Rightarrow \Phi_1(x) = x - 1$$

Assume the statement holds until  $n - 1$ . Now

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{d|n, d \neq n} \Phi_d(x)} \in \mathbb{Z}[x]$$

where the above fraction polynomial is in  $\mathbb{Z}[x]$  because both the numerator and the denominator are monic.  $\square$

用以上 Lemma 的證明方式我們也能遞迴地找出各個 Cyclotomic polynomials:

- $\Phi_1 = x - 1$
- $\Phi_2 = x + 1$
- $x^3 - 1 = \Phi_1 \Phi_3$ , so  $\Phi_3 = x^2 + x + 1$
- $x^4 - 1 = \Phi_1 \Phi_2 \Phi_4$ , so  $\Phi_4 = x^2 + 1$
- $x^6 - 1 = \Phi_1 \Phi_2 \Phi_3 \Phi_6$ , so  $\Phi_6 = x^2 - x + 1$
- $\Phi_8 = x^4 + 1$
- $\Phi_9 = x^6 + x^3 + 1$
- $\Phi_{10} = x^4 - x^3 + x^2 - x + 1$
- $\Phi_{12} = x^4 - x^2 + 1$

更進一步，我們還能發現它們 irreducible

**Theorem 6.**  $\Phi_n(x)$  is irreducible over  $\mathbb{Q}$

*Proof.*

Let  $f(x) = m_{\zeta_n, \mathbb{Q}}(x)$ . Then  $f(x) | \Phi_n(x)$ . We'll show that  $f(x) = \Phi_n(x)$ . This implies  $\Phi_n(x)$  is irreducible over  $\mathbb{Q}$ . Proving " $f(x) = \Phi_n(x)$ "  $\Leftrightarrow$  " $\forall k$  such that  $(k, n) = 1$ ,  $f(\zeta_n^k) = 0$ ". So it suffices to show that  $\forall k, (k, n) = 1$ ,  $f(\zeta_n^k) = 0$ . ( $\forall$  primitive  $n$ th roots  $\zeta$  of unity,  $f(\zeta) = 0$ .)

We first prove the case  $k = p$  is a prime. Write  $\Phi_n(x) = f(x)g(x)$ . (By Gauss's lemma,  $f, g \in \mathbb{Z}[x]$ .) We have

$$\Phi_n(\zeta_n^p) = 0$$

Suppose that  $f(\zeta_n^p) \neq 0$ , then  $g(\zeta_n^p) = 0$ .  $\Rightarrow \zeta_n$  is a root of  $g(x^p)$ .  $\Rightarrow f(x) | g(x^p)$ . Say  $g(x^p) = f(x)h(x)$ . Now consider the reduction modulo  $p$ . Say  $g(x) = a_m x^m + \dots + a_n$ . Since  $\overline{a_m^p} = \overline{a_m}^p \forall a_m \in \mathbb{Z}$ . ( $\overline{a_n}$  = residue class of  $a_n$  modulo  $p$ .) We have

$$\begin{aligned} \overline{g(x^p)} &= \overline{a_m} x^{pm} + \dots + \overline{a_0} \\ &= \overline{a_m} x^{pm} + \dots + \overline{a_0}^p \\ &= (\overline{a_m} x^m + \dots + \overline{a_0})^p = \overline{g(x)}^p \end{aligned}$$

Therefore

$$\overline{g(x)}^p = \overline{f(x)h(x)}$$

Since  $(\mathbb{Z}/p\mathbb{Z})[x]$  is a UFD, this implies that  $\text{GCD}(\overline{f(x)}, \overline{g(x)}) \neq 1$ .  $\Rightarrow \overline{\Phi_n(x)} = \overline{f(x)g(x)}$  has a repeated root. However we can show that  $\overline{\Phi_n(x)}$  has no repeated roots (which will be proved below). This yields a contradiction. Thus we must have  $f(\zeta_n^p) = 0$ .

We will now show the claim. We'll show that  $\overline{x^n - 1}$  has no repeated roots. Then since  $\overline{\Phi_n(x)} | \overline{x^n - 1}$ ,  $\overline{\Phi_n(x)}$  does not have a repeated root either. Here  $D(\overline{x^n - 1}) = \overline{nx^{n-1}}$ . Since  $p \nmid n$ ,  $\bar{n} \neq \bar{0}$ . We have

$$\overline{x^n - 1} = (\overline{n^{-1}x})D(\overline{x^n - 1}) - 1$$

$$\Rightarrow (\overline{x^n - 1}, D(\overline{x^n - 1})) = 1$$

$\Rightarrow \overline{\Phi_n(x)}$  has no repeated roots. □