Zariski 的定理

要證明 Hilbert's Nullstellensatz 一般是用 Zariski 的定理處理. 要了解這個定理的證明, 需要充分地了解所謂 algebraic element 和 integral element 之間的關係, 以及 vector space 和 module 之間的關係. 由於一般同學可能對 integral element 和 module 不是很清楚, 我們將利用這個機會介紹相關的性質.

Zariski 的定理是說, 假設 K 是一個 field, L 是 K 的一個 field extension. 若 $\alpha_1,\ldots,\alpha_n \in L$ 使得 $K[\alpha_1,\ldots,\alpha_n]$ 是一個 field, 則 $\alpha_1,\ldots,\alpha_n$ 皆 algebraic over K.

這裡 L/K 是 field extension 對這個定理來說並不是重要的, 我們特別提及主要是要確保 K 的元素以及 $\alpha_1,\ldots,\alpha_n$ 都在一個共同的 field 之內, 所以才能談這些元素間的運算. $K[\alpha_1,\ldots,\alpha_n]$ 表示在 L 中包含 K 和 $\alpha_1,\ldots,\alpha_n$ 最小的 ring. 也就是說 $K[\alpha_1,\ldots,\alpha_n]$ 中的元素都可以表示成 $f(\alpha_1,\ldots,\alpha_n)$, 其中 $f(x_1,\ldots,x_n) \in K[x_1,\ldots,x_n]$. 一般來說我們也習慣將 L 中包含 K 和 $\alpha_1,\ldots,\alpha_n$ 最小的 field 用 $K(\alpha_1,\ldots,\alpha_n)$ 來表示. 所以這個定理的假設可以簡化成 $K[\alpha_1,\ldots,\alpha_n] = K(\alpha_1,\ldots,\alpha_n)$. 最後定理提及一個元素 α 是 algebraic over K. 這個意思是表示存在不等於 0 的多項式 $f(x) \in K[x]$ 使得 $f(\alpha) = 0$.

這個定理在 $n = 1$ 時很容易證明. 首先若 $\alpha = 0$ 當然就沒甚麼好證, 0 當然是 algebraic over K. 若 $\alpha \neq 0$, 由於 $\alpha^{-1} \in K(\alpha)$ (別忘了 $K(\alpha)$ 是一個包含 α 的 field), 故由假設 $K[\alpha] = K(\alpha)$ 知 $\alpha^{-1} \in K[\alpha]$. 也就是說存在 $f(x) \in K[x]$ 使得 $\alpha^{-1} = f(\alpha)$. 因此若考慮 $g(x) = xf(x) - 1$, 則不但 $g(x) \in K[x]$ 是一個非 0 的多項式且 $g(\alpha) = 0$, 故得證 α 為 algebraic over K.

當我們要把這個證明推廣到 $n = 2$ 的情況時, 就會碰到困難. 首先由定義我們有以下的關係式:

$$K[\alpha,\beta] = K[\alpha][\beta] \subseteq K(\alpha)[\beta] \subseteq K(\alpha,\beta).$$

故由 $K[\alpha,\beta] = K(\alpha,\beta)$ 的假設可得 $K[\alpha,\beta] = K(\alpha)[\beta]$ (再次強調這個等式一般來說不對, 不過因我們假設 $K[\alpha,\beta]$ 是一個 field, 所以成立). 因此由 $K(\alpha)$ 是一個 field 以及歸納法 (前面證的 $n = 1$ 之情形) 知 β 為 algebraic over $K(\alpha)$. 不過我們也只能進行到這裡, 因為由 $K[\alpha,\beta]$ 是 field 的這個假設, 沒有直接的方法讓我們知道是否 $K[\alpha]$ 是否是一個 field. 因此我們不只要了解 β 和 $K(\alpha)$ 的關係, 還必需了解 β 和 $K[\alpha]$ 的關係. 一般來說一個元素和 field 之間我們會談是否 algebraic 的關係, 而一個元素和 ring 之間便是要談所謂 integral 的關係.

Algebraic Element Vs. Integral Element. 當 L/K 是一個 field extension 且 $\alpha \in L$, 前面提過若存在 $f(x) \in K[x]$ 是一個非 0 的多項式使得 $f(\alpha) = 0$, 則稱 α 是 algebraic over K. 我們希望把這關係推廣到 ring, 特別是 integral domain 的情形.

當 R 是一個 integral domain 時, 若 R' 是一個包含 R 的 ring 且 $\alpha \in R'$, 我們當然可考慮是否存在係數在 R 且不為 0 的多項式 $f(x) \in R[x]$ 使得 $f(\alpha) = 0$. 不過這樣的關係和 α 是 algebraic over R 的 quotient field F 沒什麼兩樣. 這是因為若 α 是 algebraic over F 且 $g(x) = a_n x^n + \cdots a_1 x + a_0 \in F[x]$ 是一個非 0 的多項式使得 $g(\alpha) = 0$, 則由於 $a_i \in F$ 且 F

是 R 的 quotient field, 故對任意 $0 \le i \le n$ 皆存在 $c_i, d_i \in R$ 且 $d_i \neq 0$ 使得 $a_i = c_i/d_i$. 因此若令 $f(x) = d_n \cdots d_0 \cdot g(x)$, 則 $f(x) \in R[x]$ 是一個非 0 的多項式且 $f(\alpha) = 0$. 換言之對任意 algebraic over F 的元素 α 都可以找到一個非 0 的多項式 $f(x) \in R[x]$ 使得 $f(\alpha) = 0$. 所以限制多項式的係數在 R 實際上並沒有增加限制, 不過若我們把多項式限制多一點, 要求係數在 R 且最高次項係數為 1, 那麼一般的 algebraic element 就不一定符合了. 我們有以下的定義.

Definition 1. 假設 R, R' 是 integral domain 滿足 $R \subseteq R'$. 對於 $\alpha \in R'$, 若存在一個係數在 R 且最高次項係數為 1 的多項式 $g(x)$ (即 $g(x) \in R$ 是一個 monic polynomial) 使得 $g(\alpha) = 0$, 則稱 α 為 integral over R.

一般來說若 F 是 R 的 quotient field, 那麼若 α 為 integral over R 當然便是 algebraic over F, 但是反過來就不一定對. 例如 $\sqrt{2}$ 滿足 $x^2 - 2 = 0$ 故為 integral over $\mathbb{Z}$, 但 $\sqrt{2}/2$ 雖為 algebraic over $\mathbb{Q}$ (滿足 $2x^2 - 1 = 0$) 但不是 integral over $\mathbb{Z}$ (這點需加以證明). 當然了若 R 本身是一個 field, 此時 $R = F$ 所以自然 algebraic element 就會是 integral element. 事實上每一個係數在 F 的非 0 多項式我們都可以除掉其最高次項係數得到一個係數仍在 F (因 F 為 field) 的 monic polynomial. 所以任何的 algebraic over F 的元素都會是某一個係數在 F 的 monic polynomial 的根.

底下為了方便, 若 R 是一個 integral domain, 我們都用 F 來表示其 quotient field, 不再另行強調. 另外我們討論的元素都會在一個固定包含 F (或 R) 的 field L (或 ring R') 中所以我們不再強調這個 L (或 R').

假設 α 為 algebraic over F, 且 $f(x) = x^n + a_{n-1}x^{n-1} \cdots + a_1 x + a_0 \in F[x]$ 使得 $f(\alpha) = 0$. 由於對任意 $0 \le i \le n-1$, 皆存在 $c_i, d_i \in R$ 且 $d_i \neq 0$ 使得 $a_i = c_i/d_i$. 若令 $b = d_{n-1} \cdots d_1 \cdot d_0$, 則由於

$$f(\alpha) = \alpha^n + d_{n-1}^{-1} c_{n-1} \alpha^{n-1} + \cdots + d_1^{-1} c_1 \alpha + d_0^{-1} c_0 = 0$$

我們有

$$b^n \cdot f(\alpha) = (b\alpha)^n + b d_{n-1}^{-1} c_{n-1} (b\alpha)^{n-1} + \cdots + b^{n-1} d_1^{-1} c_1 (b\alpha) + b^n d_0^{-1} c_0 = 0.$$

若令 $g(x) = x^n + \sum_{i=0}^{n-1} b^{n-i} d_i^{-1} c_i x^i$, 則由於 $b^{n-i} d_i^{-1} \in R$ (因 $i \le n-1$), 故知 $g(x) \in R[x]$ 且是一個 monic polynomial, 又因為 $g(b\alpha) = 0$ 我們知 $b\alpha$ 為 integral over R. 要注意這裡由於 R 是 integral domain, 故由 $d_i \neq 0$ 知 $b = d_{n-1} \cdots d_1 \cdot d_0 \neq 0$. 依此我們有以下之結論.

Lemma 2. 假設 R 是 *integral domain* 且 F 為其 *quotient field.* 若 α 為 *algebraic over* F, 則存在 $b \in R$ 且 $b \neq 0$ 使得 $b\alpha$ 為 *integral over* R.

由於以後我們要討論的 R 為 $K[x]$ 這樣的多項式環, 大家都知道 $K[x]$ 是一個 UFD (unique factorization domain), 底下我們將討論 integral over UFD 的特殊性質.

Lemma 3. 假設 R 是一個 *unique factorization domain* 且 F 是 R 的 *quotient field.* 若 $\alpha \in F$ 為 *integral over* R, 則 $\alpha \in R$.

Proof. 因 $\alpha \in F$ 所以可將 α 寫成 ab^{-1}, 其中 $a,b \in R$. 又因為 R 為 UFD, 所以我們可假設 a,b 沒有共同的 divisor. 又因為 α 為 integral over R 故存在 monic polynomial $f(x) \in R[x]$ 使得 $f(\alpha) = 0$. 假設 $f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0$, 故得

$$a^n = -b(c_{n-1}a^{n-1} + \cdots + c_1 ab^{n-2} + c_0 b^{n-1}).$$

若 b 不是 unit, 必存在一個 irreducible element p 且 $p|b$. 此時 $p|a^n$ 因 p 為 prime 故得 $p|a$. 此和 a,b 沒有共同 divisor 矛盾. 故知 b 必為一個 unit, 得證 $\alpha = ab^{-1} \in R$. □

有時可以直接用定義處理一些 algebraic 的性質, 例如若 $K \subseteq K'$ 且 α 為 algebraic over K, 則 α 為 algebraic over K'. 同樣的方法我們有以下之結果

Lemma 4. *若 $R \subseteq R'$ 且 α 為 integral over R, 則 α 必為 integral over R'.*

Proof. 若 $f(x) \in R[x]$ 為 monic polynomial 且 $f(\alpha) = 0$, 則 $f(x)$ 仍可看成是 over R' 的 monic polynomial, 所以 α 為 integral over R'. □

然而在一般情形直接用定義處理 algebraic 的情形可能會有困難, 例如若 α, β 皆 algebraic over K, 要證明 $\alpha + \beta$ 及 $\alpha\beta$ 為 algebraic over K 就必需引進 vector space 的概念來處理. 相同的要證明兩個 integral over R 的元素相加及相乘為 integral over R 就必需引進 module 的概念.

Vector Space Vs. Module. 給定一個 field K 所謂 V 為 vector space over K, 表示 V 本身加法是一個 abelian group, 另外對 K 和 V 之間有乘法運算並要求對任意 $c \in K$ 且 $v \in V$ 皆有 $cv \in V$. 這之間加法乘法需滿足分配率的性質. 依此, 若 K 是一個 field, 且 L/K 是 field extension, 則可將 L 看成是 K 的 vector space.

相對的給定一個 integral domain R, 若 M 本身加法是一個 abelian group 且 R 和 M 之間有乘法運算滿足對任意 $r \in R$ 且 $m \in M$ 皆有 $rm \in M$, 再加上加法乘法之間滿足分配率的性質. 我們稱 M 為一個 R-module. 簡言之, module 就如 vector space 只是乘上的係數不要求是 field 只要是個 ring 即可. 依此, 若 R, R' 是 integral domain 且 $R \subseteq R'$, 則可將 R' 視為一個 R-module.

Vector space 和 module 最大的不同便是, 由於 vector space 係數是一個 field, 我們可定義其 dimension. 特別是 vector space 有所謂的 basis, 當一個 vector space V over K 可找到一組 basis $v_1, \ldots, v_n$ 展成 V 時, 這個 basis 組成份子的個數是固定的, 就是其 dimension. 對於 R-module 這就不一定對了. 可能有一個 R-module 你可以找到有限多元素展成此 module 但另一方面你又可找到無窮多個元素是 linearly independent over R. 關於 module 的這些相關問題我們不深談, 目前僅討論以下的情形.

Definition 5. 假設 M 是一個 R-module. 若存在 $m_1 \ldots, m_t \in M$ 使得對任意 $m \in M$ 皆有 $r_1, \ldots, r_t \in R$ 使得 $m = r_1 m_1 + \cdots + r_t m_t$, 則稱 M 是一個 *finitely generated* R-module.

Finitely generated R module 就好像 finite dimension vector space 一樣可由有限多個元素展成.

對於 algebraic over K 的元素 α 我們有一個等價的條件就是存在一個 field K' 滿足 $\alpha \in K'$ 且 K' 是一個 finite dimensional vector space over K. 簡單來說假設 $\dim_K(K') = n$, 則由 vector space 中 basis 的性質知 $1, \alpha, \cdots, \alpha^n$ 必為 linearly dependent over K, 於是我們便找到一個 α 所需符合的多項式了. 對於 integral over R 的元素我們也有相對應的性質. 不過由於 R-module 一般來說沒有 basis, 所以我們需用另外的方式處理.

Proposition 6. 假設 R 是一個 *integral domain* 則 α 為 *integral over* R 若且唯若存在一個 *integral domain* R' 滿足 $R \subseteq R'$, $\alpha \in R'$ 且 R' 是一個 *finitely generated* R*-module.*

Proof. 首先說明若 α 為 integral over R, 則令 $R' = R[\alpha]$ 即為所求. 假設 $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in R[x]$ 滿足 $f(\alpha) = 0$. 對任意 $\beta \in R[\alpha]$, 依定義即存在 $g(x) \in R[x]$ 使得 $\beta = g(\alpha)$. 由於 $f(x)$ 的最高次項係數為 1, 存在 $h(x), l(x) \in R[x]$ 使得 $g(x) = f(x)h(x) + l(x)$, 其中 $l(x) = 0$ 或 $\deg(l(x)) \leq n-1$. 故得 $\beta = g(\alpha) = l(\alpha)$. 換言之, $R[\alpha]$ 中的元素皆可表成 $c_{n-1}\alpha^{n-1} + \cdots + c_1\alpha + c_0$. 也就是說 $R[\alpha]$ 是由 $1, \alpha, \ldots, \alpha^{n-1}$ 展成的 finitely generated R-module. (大家應注意這個證明中 $f(x)$ 是 monic 的重要性.)

反之, 假設 R' 是一個 integral domain 滿足 $R \subseteq R'$ 以及 $\alpha \in R'$ 且 R' 是一個 finitely generated R-module. 令 $\alpha_1, \ldots, \alpha_n \in R'$ 展成 R'. 由於 R' 是一個 ring 且 $\alpha \in R$, 我們知對任意 $1 \leq i \leq n$ 皆有 $\alpha\alpha_i \in R'$, 亦即存在 $c_{i1}, \ldots, c_{in} \in R$ 使得 $\alpha\alpha_i = c_{i1}\alpha_1 + \cdots + c_{in}\alpha_n$. 移項得 $x_1 = \alpha_1, \ldots, x_n = \alpha_n$ 滿足聯立方程組

$$\begin{cases} (c_{11} - \alpha)x_1 + & c_{12}x_2 + & \cdots & + c_{1n}x_n = 0 \\ c_{21}x_1 + & (c_{22} - \alpha)x_2 + & \cdots & + c_{2n}x_n = 0 \\ \vdots & \vdots & \vdots & \vdots \\ c_{n1}x_1 + & c_{n2}x_2 + & \cdots & + (c_{nn} - \alpha)x_n = 0 \end{cases}$$

將這些方程組的係數看成在 R' 的 quotient field 中, 由此方程組有一組不全為 0 的解, 得

$$\det \begin{pmatrix} c_{11} - \alpha & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} - \alpha & \cdots & c_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ c_{n1} & c_{n2} & \cdots & c_{nn} - \alpha \end{pmatrix} = 0$$

亦即 α 滿足一個次數為 n 係數在 R 的 monic polynomial, 故得 α 為 integral over R. □

有了 Proposition 6, 我們便能如同證明 algebraic elements 相加相乘依然為 algebraic 的方法證明以下的性質.

Proposition 7. 若 α, β 為 *integral over* R, 則 $\alpha + \beta$ 和 $\alpha\beta$ 皆為 *integral over* R.

Proof. 因 α 為 integral over R 故由 Proposition 6 知存在一 integral domain R' 滿足 $\alpha \in R'$, $R \subseteq R'$ 且 R' 為 finitely generated R-module. 又因 β 為 integral over R 且 $R \subseteq R'$ 故知 β 為 integral over R'. 再由 Proposition 6 知存在 integral domain R'' 滿足 $\beta \in R''$ 以及 $R' \subseteq R''$ 且 R'' 為 finitely generated R'-module.

我們欲證明 R'' 為 finitely generated R-module. 若得證, 此時因 $\alpha,\beta \in R''$ 且 R'' 為一個 ring, 可得 $\alpha+\beta \in R''$ 且 $\alpha\beta \in R''$. 故再利用 Proposition 6 可得 $\alpha+\beta$ 和 $\alpha\beta$ 皆為 integral over R.

假設 R' 看成為 R-module 可由 $a_1,\ldots,a_m \in R'$ 展成 (即任意 R' 中的元素皆可寫成 $c_1a_1+\cdots+c_ma_m$, 其中 $c_i \in R$ 的形式). 再假設 R'' 看成為 R'-module 可由 $b_1,\ldots,b_n \in R''$ 展成. 我們可證得 R'' 看成為 R-module 可由 $\{a_ib_j \mid 1 \le i \le m, 1 \le j \le n\}$ 展成. 這是因為對任意 $\lambda \in R''$ 可寫成 $\lambda = \sum_{j=1}^{n} d_jb_j$ 其中 $d_j \in R'$. 再由 $d_j \in R'$ 知存在 $c_{1j},\ldots,c_{mj} \in R$ 使得 $d_j = \sum_{i=1}^{m} c_{ij}a_i$. 故可得 $\lambda = \sum_{j=1}^{n}(\sum_{i=1}^{m} c_{ij}a_ib_j)$. □

Remark 8. 當 $R = F$ 是一個 field 時, 也可由 Proposition 7 知若 α,β 為 algebraic over F, 則 $\alpha+\beta$ 和 $\alpha\beta$ 也為 algebraic over F.

$K[\alpha]$ Vs. $K(\alpha)$. 接下來我們來談論 $K[\alpha]$ 這個 ring 和 $K(\alpha)$ 這個 field 之間的關係. $K[\alpha]$ 和 $K(\alpha)$ 若相等時, 前面已知 α 必為 algebraic over K, 因而若 α 不是 algebraic over K, 則 $K[\alpha]$ 不等於 $K(\alpha)$. 這裡我們便是要探討何時 $K(\alpha)$ 和 $K[\alpha]$ 相等. 事實上當 $K[\alpha]$ 是一個 ring 不是 field 時, α 為 transcendental over K (即不是 algebraic over K) 此時 $K[x]$ 和 $K[\alpha]$ 是 isomorphic (考慮 $f(x) \mapsto f(\alpha)$), 所以我們僅需探討 $K[x]$ 的情形.

由於 $K[x]$ 是 UFD, 我們可以仿照 Euler 證明整數中有無窮多個質數的方法來證明 $K[x]$ 中有無窮多個 non-associate irreducible polynomial. 也就是說 $K[x]$ 中有無窮多個 monic irreducible polynomial. 因此我們有以下的結果.

Lemma 9. 不可能存在 $q(x) \in K[x]$ 使得對任意 $r(x) \in K(x)$ 皆存在 $n \in \mathbb{N}$ 使得 $q(x)^n r(x) \in K[x]$.

Proof. 假設存在這樣的 $q(x)$, 由於在 $K[x]$ 中有無窮多個 monic irreducible polynomial, 我們可找到 $p(x) \in K[x]$ 是 irreducible polynomial 且 $p(x) \nmid q(x)$. 然而 $1/p(x) \in K(x)$ 且對任意 $n \in \mathbb{N}$, $p(x)$ 在 $K[x]$ 中皆不能整除 $q(x)^n$ (利用 $K[x]$ 是 UFD), 故知 $q(x)^n/p(x)$ 不在 $K[x]$ 中, 此與假設矛盾故得證. □

若 $K[\alpha] = K(\alpha)$ 則當然對任意 $r(\alpha) \in K(\alpha)$ 皆有 $r(\alpha) \in K[\alpha]$. 所以此時我們只要取 $q(\alpha) = 1$ 就可得 $q(\alpha)r(\alpha) \in K[\alpha]$. 因此 Lemma 9 可以說是一種判別 $K[\alpha]$ 是否等於 $K(\alpha)$ 的方法.

一般來說當 $r(x) \in K(x)$, 若無法判定是否 $r(x) \in K[x]$, 由於 $K[x]$ 是 UFD, 我們可以利用 Lemma 3 放寬標準考慮 $r(x)$ 是否 integral over $K[x]$ 即可. 因此套用若 α 不是 algebraic over K, 則 $K[\alpha] \simeq K[x]$ 以及 Lemma 9, 我們有以下之結果.

Corollary 10. 若存在 $q(\alpha) \in K[\alpha]$ 使得對任意 $\beta \in K(\alpha)$ 皆存在 $n \in \mathbb{N}$ 使得 $q(\alpha)^n\beta$ 為 *integral over* $K[\alpha]$, 則 α 為 *algebraic over* K.

Proof. 利用反證法, 假設 α 不是 algebraic over K, 即 $K[\alpha] \simeq K[x]$. 現由於 $q(\alpha) \in K[\alpha]$ 且 $\beta \in K(\alpha)$ 故知 $q(\alpha)^n\beta \in K(\alpha)$. 因此若 $q(\alpha)^n\beta$ 為 integral over $K[\alpha]$ 則利用 Lemma 3 即

知 $q(\alpha)^n\beta \in K[\alpha]$. 然而由 Lemma 9 知不可能有這樣的 $q(\alpha)$ 存在. 故由此矛盾得證 α 為 algebraic over K. □

再次強調若 α 為 algebraic over K 則對任意 $\beta \in K(\alpha)$ 皆有 $\beta \in K[\alpha]$. 因此 Corollary 10 中的條件可說是 α 為 algebraic over K 的等價條件.

Zariski 的定理.

Theorem 11 (Zariski)**.** 若 $K[\alpha_1,\ldots,\alpha_n]$ 是一個 *field,* 則 $\alpha_1,\ldots,\alpha_n$ 皆 *algebraic over* K.

Proof. 我們對 n 作 induction 處理. 當 $n=1$ 時已知成立. 當 $n \geq 2$ 時, 由於 $K[\alpha_1,\ldots,\alpha_n]$ 是一個 field 故知 $K[\alpha_1,\ldots,\alpha_n] = K(\alpha_1)[\alpha_2,\ldots,\alpha_n]$ 例用 induction 知 $\alpha_2,\ldots,\alpha_n$ 皆 algebraic over $K(\alpha_1)$. 因為 $K(\alpha_1)$ 為 $K[\alpha_1]$ 的 quotient field, 故由 Lemma 2 知對 $2 \leq i \leq n$ 皆存在 $q_i(\alpha) \in K[\alpha]$ 使得 $q_i(\alpha_1)\alpha_i$ 為 integral over $K[\alpha_1]$. 由於 $q_i(\alpha_1) \in K[\alpha_1]$ 本身是 integral over $K[\alpha_1]$ 所以若令 $q(\alpha_1) = q_2(\alpha_1)\cdots q_n(\alpha_1)$, 則由 Proposition 7 知對 $2 \leq i \leq n$ 皆有 $q(\alpha_1)\alpha_i$ 為 integral over $K[\alpha_1]$.

現對任意 $\beta \in K[\alpha_1,\ldots,\alpha_n]$ 知存在 $f(x_1,\ldots,x_n) \in K[x_1,\ldots,x_n]$ 使得 $\beta = f(\alpha_1,\ldots,\alpha_n)$. 若令 m 為 $f(x_1,\ldots,x_n)$ 的最高次, 則由 Proposition 7 知 $q(\alpha_1)^m f(\alpha_1,\ldots,\alpha_n)$ 為 integral over $K[\alpha_1]$, 換言之對任意 $\beta \in K[\alpha_1,\ldots,\alpha_n]$ 皆存在 $m \in \mathbb{N}$ 使得 $q(\alpha_1)^m\beta$ 為 integral over $K[\alpha_1]$. 然而依假設 $K[\alpha_1,\ldots,\alpha_n]$ 是一個 field, 故有 $K(\alpha_1) \subseteq K[\alpha_1,\ldots,\alpha_n]$, 也就是說對任意 $\beta \in K(\alpha_1)$ 皆存在 $m \in \mathbb{N}$ 使得 $q(\alpha_1)^m\beta$ 為 integral over $K[\alpha_1]$. 因此利用 Corollary 10 知 α_1 為 algebraic over K. 既然 $\alpha_2,\ldots,\alpha_n$ 皆 algebraic over $K(\alpha_1)$ 且 α_1 為 algebraic over K, 故知 $\alpha_1,\alpha_2,\ldots,\alpha_n$ 皆 algebraic over K. □

Remark 12. 我們可以很輕易的用 induction 證明若 $\alpha_1,\alpha_2,\ldots,\alpha_n$ 皆 algebraic over K, 則 $K[\alpha_1,\ldots,\alpha_n]$ 是一個 field. 所以 Zariski 的定理可以敘述成:

$K[\alpha_1,\ldots,\alpha_n] = K(\alpha_1,\ldots,\alpha_n)$ 若且唯若 $\alpha_1,\alpha_2,\ldots,\alpha_n$ 皆 algebraic over K.