

## Introduction

Quadratics (Babylonians):

$$\begin{aligned} X^2 + bX + c &= (X + \frac{1}{2}b)^2 + c - \frac{b^2}{4} \\ &= (X - x_1)(X - x_2) \implies x_1x_2 = c, x_1 + x_2 = -b \\ x_1 &= \frac{1}{2} [(x_1 + x_2) + (x_1 - x_2)] = \frac{1}{2} [-b + \sqrt{b^2 - 4c}] \end{aligned}$$

Cubics (Italy, 16th Century):

$$\begin{aligned} X^3 + aX^2 + bX + c &= (X - x_1)(X - x_2)(X - x_3) \\ \implies x_1 + x_2 + x_3 &= -a, x_1x_2 + x_1x_3 + x_2x_3 = b, x_1x_2x_3 = -c \end{aligned}$$

WLOG  $X \rightarrow X - a/3$  and  $a = 0$

$$x_1 = \frac{1}{3} \left[ (x_1 + x_2 + x_3) + \underbrace{(x_1 + \omega x_2 + \omega^2 x_3)}_{=u} + \underbrace{(x_1 + \omega^2 x_2 + \omega x_3)}_{=v} \right]$$

where  $\omega = e^{2\pi i/3}$  so  $\omega^2 + \omega + 1 = 0$ . Cyclic permutation of  $x_1, x_2, x_3$  gives  $u \rightarrow \omega u \rightarrow \omega^2 u$  and  $v \rightarrow \omega v \rightarrow \omega^2 v$  which implies  $u^3$  and  $v^3$  are invariant under cyclic permutations of the roots.

Also  $u \leftrightarrow v$  under  $x_2 \leftrightarrow x_3$ . So  $u^3 + v^3, u^3v^3$  are invariant under permutations of roots.

In fact,

$$\begin{aligned} u^3 + v^3 &= 27x_1x_2x_3 = -27c \\ u^3v^3 &= -27b^2 \end{aligned}$$

So  $u^3, v^3$  are roots of  $Y^2 + 27cY - 27b^2$ . This gives a formula for  $x_1$  (Cardano's formula).

Can follow a similar method for quartics - auxilliary cubic equation. Unfortunately it doesn't work for quintics - the reason being group theory.

## 1 Polynomials

In this course, all rings are commutative and non-zero. Let  $R$  be a ring, then  $R[X]$  denotes the ring of polynomials  $\sum_{i=0}^n a_i X^i$ ,  $a_i \in R$ . A polynomial  $f \in R[X]$  determines a function  $R \rightarrow R$ ,  $r \mapsto f(r)$ .

The polynomial is not in general determined by this function, e.g let  $R = \mathbb{Z}/p\mathbb{Z}$  ( $p$  prime). Then for all  $a \in R$ ,  $a^p = a$  so the polynomials  $X^p$  and  $X$  represent the same function.

In the case when  $R = K$  (a field),  $K[X]$  is a Euclidean domain. The “division algorithm” says that if  $f, g \in K[X]$ ,  $g \neq 0$  then there exists unique  $q, r \in K[X]$  such that  $f = gq + r$  and  $\deg r < \deg g$  (define  $\deg(0) = -\infty$ ).

In particular, if  $g = X - a$  is linear then  $f = (X - a)q + f(a)$  (“remainder theorem”). So  $K[X]$  is also a PID and a UFD - every polynomial is a product of irreducible polynomials, and there are GCD’s, computable via Euclid’s algorithm in the usual way.

**Proposition 1.1.** *If  $K$  is a field,  $0 \neq f \in K[X]$ , then  $f$  has at most  $\deg f$  roots in  $K$ .*

*Proof.* If  $f$  has no roots then we are done. Otherwise, suppose  $f(a) = 0$  for  $a \in K$ . Then

$$f = (X - a)g$$

for some  $g \in K[X]$  and  $\deg g = \deg f - 1$ . If  $b \in K$  is a root of  $f$  then either  $b = a$  or  $g(b) = 0$  so the number of roots of  $f$  is at most one more than the number of roots of  $g$ . Now done by induction.  $\square$

## 2 Symmetric polynomials

Let  $R$  be a ring, consider  $R[X_1, \dots, X_n]$  for  $n \geq 1$ .

**Definition.** A polynomial  $f \in R[X_1, \dots, X_n]$  is *symmetric* if for every  $\sigma \in S_n$ ,  $f(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = f$ .

The set of symmetric polynomials is a subring of  $R[X_1, \dots, X_n]$ .

**Example.**  $X_1 + \dots + X_n$ , or more generally,  $p_k = X_1^k + \dots + X_n^k = \sum_{i=1}^n X_i^k$ .

Alternative definition: if  $f \in R[X_1, \dots, X_n]$ , define  $f\sigma = f(X_{\sigma(1)}, \dots, X_{\sigma(n)})$ . This is an action (on the right) of  $S_n$  on  $R[X_1, \dots, X_n]$ . A polynomial  $f$  is symmetric if and only if it is fixed by this action.

**Definition.** *The elementary symmetric polynomials are*

$$s_r(X_1, \dots, X_n) = \sum_{1 \leq i_1 < \dots < i_r \leq n} X_{i_1} X_{i_2} \dots X_{i_r}$$

**Example.** When  $n = 3$  we have

$$s_1 = X_1 + X_2 + X_3$$

$$s_2 = X_1 X_2 + X_1 X_3 + X_2 X_3$$

$$s_3 = X_1 X_2 X_3$$

**Theorem 2.1.**

- (i) *Every symmetric polynomial over  $R$  can be expressed as a polynomial in  $\{s_r : 1 \leq r \leq n\}$ , with coefficients in  $R$ .*
- (ii) *There are no non-trivial relations between  $s_1, \dots, s_n$ .*

**Remark:**

(a) Consider the ring homomorphism

$$\theta : R[Y_1, \dots, Y_n] \rightarrow R[X_1, \dots, X_n], \quad Y_r \mapsto s_r$$

then (i) says the image of  $\theta$  is the set of symmetric polynomials. (ii) says that  $\theta$  is injective.

(b) Equivalent definition of the  $s_r$ 's is

$$\prod_{i=1}^n (T + X_i) = T^n + s_1 T^{n-1} + \dots + s_{n-1} T + s_n$$

If we need to specify the number of variables, write  $s_{r,n}$  instead of  $s_r$ .

*Proof.* Terminology:

- A *monomial* is some  $X_I = X_1^{i_1} \dots X_n^{i_n}$  for  $I \in \mathbb{N}^n = \{0, 1, 2, \dots\}^n$ . Its (total) degree is  $\sum_{\alpha} i_{\alpha}$ .
- A *term* is some  $cX_I$ , for  $0 \neq c \in R$ . So a polynomial is uniquely a sum of terms.
- *Total degree* of  $f$  is the maximum degree over its terms

Lexicographical ordering on monomials  $X_I$ : write  $X_I > X_J$  if either  $i_1 > j_1$  or, for some  $1 \leq r < n$ ,  $i_1 = j_1, \dots, i_r = j_r$  and  $i_{r+1} > j_{r+1}$ .

This is a total ordering: for each pair  $I \neq J$ , exactly one of  $X_I > X_J$  or  $X_J > X_I$  holds.

First we prove (ii):

Let  $d$  be the total degree of some symmetric polynomial  $f$ , and let  $X_I$  be the largest (in lexicographical order) monomial which occurs in  $f$ , with coefficient  $c \in R$ . As  $f$  is symmetric, we must have  $i_1 \geq i_2 \geq \dots \geq i_n$  (otherwise we could exchange variables to get a larger monomial).

So

$$X_I = X_1^{i_1-i_2} (X_1 X_2)^{i_2-i_3} \dots (X_1, \dots, X_n)^{i_n}$$

consider

$$g = s_1^{i_1-i_2} s_2^{i_2-i_3} \dots s_{n-1}^{i_{n-1}-i_n} s_n^{i_n}$$

the leading monomial (i.e largest in lexicographical order) of  $g$  is  $X_I$ , and  $g$  is symmetric. So  $f - cg$  is symmetric of total degree  $\leq d$ , and its leading monomial term is smaller (lexicographical) than  $X_I$ . As the set of monomials of degree at most  $d$  is finite, this process terminates.

To prove (ii): induct on  $n$ . Suppose we have  $G \in R[Y_1, \dots, Y_n]$  with  $G(s_{n,1}, \dots, s_{n,n}) = 0$ . We want to show  $G = 0$ . If  $n = 1$ , this is trivial ( $s_{1,1} = X_1$ ). If  $G = Y_n^k H$ , with  $Y_n \nmid H$ , then  $s_{n,n}^k H(s_{n,1}, \dots, s_{n,n}) = 0$ . As  $s_{n,n} = X_1 \dots X_n$ ,  $s_{n,n}$  is not a zero divisor in  $R[X_1, \dots, X_n]$  so  $H(s_{n,1}, \dots, s_{n,n}) = 0$ .

So we may assume  $G$  is not divisible by  $Y_n$ . Replace  $X_n$  by 0. Then

$$s_{n,r}(X_1, \dots, X_{n-1}, 0) = \begin{cases} s_{n-1,r}(X_1, \dots, X_{n-1}) & \text{if } r < n \\ 0 & \text{if } r = n \end{cases}$$

and so  $G(s_{n-1,1}, \dots, s_{n-1,n-1}, 0) = 0$ . So by induction,  $G(Y_1, \dots, Y_{n-1}, 0) = 0$ , i.e.  $Y_n \mid G$ , a contradiction.  $\square$

**Example.**  $f = \sum_{i \neq j} X_i^2 X_j$  for  $n \geq 3$ . The leading term is  $X_1^2 X_2 = X_1(X_1 X_2)$ . Then compute

$$s_1 s_2 = \sum_i \sum_{j < k} X_i X_j X_k = \sum_{i \neq j} X_i^2 X_j + 3 \sum_{i < j < k} X_i X_j X_k$$

so  $f = s_1 s_2 - 3 s_3$ .

Computing say  $\sum X_i^5$  by hand is tedious. But there are alternative formulae.

Recall  $p_k = \sum_{i=1}^n X_i^k$  for  $k \geq 1$ .

**Theorem 2.2** (Newton's formulae). *Let  $n \geq 1$ . Then for all  $k \geq 1$*

$$p_k - s_1 p_{k-1} + \dots + (-1)^{k-1} s_{k-1} p_1 + (-1)^k k s_k = 0$$

by convention,  $s_0 = 1$ , and  $s_r = 0$  if  $r > n$ .

*Proof.* We may assume  $R = \mathbb{Z}$  (or  $\mathbb{R}$ ). Generating function

$$F(T) = \prod_{i=1}^n (1 - X_i T) = \sum_{r=0}^n (-1)^r s_r T^r$$

Take logarithmic derivative with respect to  $T$ :

$$\frac{F'(T)}{F(T)} = \sum_{i=1}^n \frac{-X_i}{1 - X_i T} = -\frac{1}{T} \sum_{i=1}^n \sum_{r=1}^{\infty} X_i^r T^r = -\frac{1}{T} \sum_{r=1}^{\infty} p_r T^r$$

So

$$\begin{aligned} -TF'(T) &= s_1 T - 2s_2 T^2 + \dots + (-1)^{n-1} n s_n T^n \\ &= F(T) \sum_{r=1}^{\infty} p_r T^r = (s_0 - s_1 T + \dots + (-1)^n s_n T^n) (p_1 T + p_2 T^2 + \dots) \end{aligned}$$

comparing coefficients of  $T^k$  gives the result.  $\square$

**Definition.** The *discriminant polynomial* is

$$D(X_1, \dots, X_n) = \Delta(X_1, \dots, X_n)^2$$

where  $\Delta = \prod_{i < j} (X_i - X_j)$ . (Recall from IA Groups that applying  $\sigma \in S_n$  to  $\Delta$  multiplies  $\Delta$  by  $\text{sgn}(\sigma)$ , so  $D$  is symmetric.)

So  $D(X_1, \dots, X_n) = d(s_1, \dots, s_n)$  for some polynomial  $d$  ( $\mathbb{Z}$ -coefficients). For example, when  $n = 2$ ,  $D = (X_1 - X_2)^2 = s_1^2 - 4s_2$ .

**Definition.** Let  $f = T^n + \sum_{i=0}^{n-1} a_{n-i} T^i \in R[T]$ . Its *discriminant* is  $\text{Disc}(f) = d(-a_1, a_2, -a_3, \dots, (-1)^n a_n) \in R$ .

Observe that if  $f = \prod_{i=1}^n (T - x_i)$ ,  $x_i \in R$ , then  $a_r = (-1)^r s_r(x_1, \dots, x_n)$ , so

$$\text{Disc}(f) = \prod_{i < j} (x_i - x_j)^2 = D(x_1, \dots, x_n)$$

If moreover  $R = K$  is a field, then  $\text{Disc}(f) = 0$  iff  $f$  has a repeated root (i.e.  $x_i = x_j$  for some  $i \neq j$ ). E.g. when  $n = 2$ ,  $\text{Disc}(T^2 + bT + c) = b^2 - 4c$ .

### 3 Fields

Recall:

**Definition.** A *field* is a ring  $K$  (commutative with a 1) in which every non-zero element has a multiplicative inverse. The set of non-zero elements of  $K$  is a group under multiplication, written  $K^\times$  or  $K^*$ , called the *multiplicative group* of  $K$ .

**Definition.** The *characteristic* of a field  $K$  is the least positive integer  $p$  (if it exists) such that  $p \cdot 1_K = 0_K$ , or is said to be 0 if no such  $p$  exists.

**Example.**  $\mathbb{Q}$  has characteristic 0 and  $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$  has characteristic  $p$  ( $p$  prime).

The characteristic  $\text{char}(K)$  of  $K$  is either 0 or a prime. Inside  $K$ , there is a smaller subfield, called the *prime subfield* of  $K$ . It is either isomorphic to  $\mathbb{Q}$  (if characteristic is 0), or to  $\mathbb{F}_p$  (if  $\text{char}(K) = p$ ).

**Proposition 3.1.** Let  $\varphi : K \rightarrow L$  be a homomorphism of fields. Then  $\varphi$  is an injection.

*Proof.*  $\varphi(1_K) = 1_L \neq 0$ , so  $\text{Ker}(\varphi) \subsetneq K$  is a proper ideal of  $K$ , so  $\text{Ker}(\varphi) = (0)$   $\square$

**Definition.** Let  $K \subseteq L$  be fields (where the field operations on  $K$  are the same as those on  $L$ ). We say  $K$  is a *subfield* of  $L$ , and  $L$  is an *extension* of  $K$ , denoted  $L/K$ .

**Remarks:**

- (i) The notation  $L/K$  has nothing to do with the quotient (some write  $L \mid K$ )
- (ii) It is useful to be more general - if  $i : K \rightarrow L$  is a homomorphism of fields, then Proposition 3.1 says that  $K$  is isomorphic to its image  $i(K) \subseteq L$ . In this situation, also say  $L$  is an extension of  $K$ .

**Example.** Some extensions include

- $\mathbb{C}/\mathbb{R}$
- $\mathbb{R}/\mathbb{Q}$
- $\mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}/\mathbb{Q}$

**Definition.**  $K \subseteq L$ ,  $x \in L$ . Define  $K[x] = \{p(x) : p \in K[T]\}$  (a subring of  $L$ ). Define  $K(x) = \{\frac{p(x)}{q(x)} : p, q \in K[T], q(x) \neq 0\}$  (a subfield of  $L$ ) “ $K$  adjoin  $x$ ”. For  $x_1, \dots, x_n \in L$ , define

$$K(x_1, \dots, x_n) = \left\{ \frac{p(x_1, \dots, x_n)}{q(x_1, \dots, x_n)} : p, q \in K[T_1, \dots, T_n], q(x_1, \dots, x_n) \neq 0 \right\}$$

(Easy to check  $K(x_1, \dots, x_{n-1})(x_n) = K(x_1, \dots, x_n)$ ). Likewise  $K[x_1, \dots, x_n]$  is defined analogously.

**Definition.** Suppose  $L/K$  is a field extension. Then  $L$  is naturally a vector space over its subfield  $K$  (forget multiplication by elements of  $L$ ). We can ask if it is a finite-dimensional vector space, if so we say that  $L/K$  is a *finite extension* and write  $[L : K] = \dim_K(L)$  for the dimension. The dimension is called the *degree of the extension  $L$  over  $K$* . If the dimension is infinite write  $[L : K] = \infty$ .

$\dim_K$  denotes the dimension as a  $K$ -vector space. Of course  $L$  has dimension 1 over itself. As a  $K$ -vector space,  $L \cong K^{[L:K]}$ .

**Example.**

- (i)  $\mathbb{C}/\mathbb{R}$ ,  $[\mathbb{C} : \mathbb{R}] = 2$
- (ii) For any field  $K$ ,  $K(X)$  = field of rational functions in  $X$  = field of fractions of polynomial ring  $K[X] = \{\frac{p}{q} : p, q \in K[X], q \neq 0\}$ . Then  $[K(X) : K] = \infty$  since  $1, X, X^2, \dots$  are linearly independent.
- (iii)  $\mathbb{R}/\mathbb{Q}$ ,  $[\mathbb{R} : \mathbb{Q}] = \infty$ . This follows from countability - every finite dimensional vector space over  $\mathbb{Q}$  is countable.

This course is largely about properties (and symmetries) of finite extensions of fields.

**Definition.** We say an extension  $L/K$  is *quadratic* (*cubic*, ...) if  $[L : K] = 2$  ( $3$ , ...)

**Proposition 3.2.** Suppose  $K$  is a finite field (necessarily of characteristic  $p > 0$ ). Then  $|K|$  is a power of  $p$ .

*Proof.* Certainly  $K/\mathbb{F}_p$  is finite, so  $K \cong (\mathbb{F}_p)^n$  (as a vector space), where  $n = [K : \mathbb{F}_p]$ , so  $|K| = p^n$ .  $\square$

Later on we will see that every prime power  $q = p^n$  admits a field  $\mathbb{F}_q$  with  $q$  elements.

Here is a simple but powerful fact:

**Theorem 3.3** (“Tower Law”). Suppose  $M/L$  and  $L/K$  are field extensions. Then  $M/K$  is a finite extension if and only if both  $M/L$  and  $L/K$  are finite. If so, then  $[M : K] = [M : L][L : K]$ .

In fact, a slightly more general statement holds:

**Theorem 3.4.** Let  $L/K$  be an extension,  $V$  an  $L$ -vector space. Then  $\dim_K(V) = [L : K] \dim_L(V)$  (and obvious conclusions if any quantities are infinite).

**Example.** If  $V = \mathbb{C}^n$  then  $V \cong \mathbb{R}^{2n}$ .



*Proof.* Let  $\dim_L(V) = d < \infty$ . Then  $V \cong L \oplus \dots \oplus L = L^d$  as an  $L$ -vector space, so also as a  $K$ -vector space. If  $[L : K] = n < \infty$ , then  $L \cong K^n$  as a  $K$ -vector space, so

$$V \cong \underbrace{K^n \oplus \dots \oplus K^n}_{d \text{ times}} = K^{nd}$$

so  $\dim_K(V) = [L : K] \dim_L(V)$ . If  $V$  is finite-dimensional over  $K$ , then a  $K$ -basis for  $V$  certainly spans  $V$  over  $L$ . So if  $\dim_L(V) = \infty$  then  $\dim_K(V) = \infty$ . Likewise, if  $[L : K] = \infty$  and  $V \neq \{0\}$ , then  $V$  has an infinite linearly independent subset, so  $\dim_K(V) = \infty$ .  $\square$

Another important fact:

**Proposition 3.5.**

- (i) Let  $K$  be a field,  $G \subseteq K^\times$  a finite subgroup. Then  $G$  is cyclic
- (ii) If  $K$  is finite, then  $K^\times$  is cyclic

*Proof.* We prove (i) ((ii) follows immediately): (recall from IB GRM) we can write

$$G \cong \frac{\mathbb{Z}}{m_1\mathbb{Z}} \oplus \dots \oplus \frac{\mathbb{Z}}{m_k\mathbb{Z}}$$

where  $1 < m_1 \mid m_2 \mid \dots \mid m_k = m$ . So for all  $x \in G$ ,  $x^m = 1$ . As  $K$  is a field, the polynomial  $T^m - 1$  has at most  $m$  roots. So  $|G| < m$ . Hence  $k = 1$  and  $G$  is cyclic.  $\square$

**Remark:** Let  $K = F = \mathbb{Z}/p\mathbb{Z}$ . The above says there exists  $a \in \{1, \dots, p-1\}$  such that  $\mathbb{Z}/p\mathbb{Z} = \{0\} \cup \{a, a^2, \dots, a^{p-1}\}$ .  $a$  is called a primitive root modulo  $p$ .

**Proposition 3.6.** *Let  $R$  be a ring,  $p$  a prime such that  $p \cdot 1_R = 0_R$  (e.g.  $R$  a field of characteristic  $p$ ). Then the map*

$$\varphi_p : R \rightarrow R, \varphi_p(x) = x^p$$

*is a homomorphism from  $R$  to itself (called the Frobenius endomorphism of  $R$ ).*

*Proof.* Have to show:

- $\varphi_p(1) = 1$
- $\varphi_p(xy) = \varphi_p(x)\varphi_p(y)$
- $\varphi_p(x+y) = \varphi_p(x) + \varphi_p(y)$

The first two are obvious. For the last one,

$$\begin{aligned} \varphi_p(x+y) &= x^p + \sum_{i=1}^{p-1} \underbrace{\binom{p}{i}}_{\equiv 0 \pmod{p}} x^i y^{p-i} + y^p \\ &= \varphi_p(x) + \varphi_p(y) \end{aligned}$$

□

**Example.** This gives another proof of Fermat's Little Theorem:  $x^p \equiv x \pmod{p}$  (induction on  $x$ :  $(x+1)^p = x^p + 1$ ).

## 4 Algebraic elements and extensions

**Definition.** Have  $L/K$  an extension,  $x \in L$ . We say  $x$  is *algebraic over  $K$*  if there exists a non-zero polynomial  $f \in K[T]$  such that  $f(x) = 0$ . Otherwise we say  $x$  is *transcendental over  $K$* .

Suppose  $f \in K[T]$ ; evaluation  $f(x) \in L$ . This gives a map  $\text{ev}_x : K[T] \rightarrow L$ ,  $f \mapsto f(x)$ . This is obviously a homomorphism of rings.

$I = \text{Ker}(\text{ev}_x) \subseteq K[T]$  is an ideal (the set of polynomials which vanish at  $x$ ). As  $\text{Im}(\text{ev}_x)$  is a subring of  $L$ , it is an integral domain. So  $I$  is a prime ideal. Two possibilities:

- (i)  $I = \{0\}$ . Then the only  $f$  with  $f(x) = 0$  is  $f = 0$ . Hence  $x$  is transcendental over  $K$ .
- (ii)  $I \neq \{0\}$ . As  $K[T]$  is a PID, there exists a unique monic irreducible  $g \in K[T]$  such that  $I = (g)$ . So  $f(x) = 0$  if and only if  $f$  is a multiple of  $g$ . So  $x$  is algebraic over  $K$ ; we call  $g$  the *minimal polynomial* of  $x$  over  $K$ . It is the unique monic irreducible polynomial such that  $x$  is a root (and the monic polynomial of least degree with this property). [Depends on  $K$  as well as  $x$ ]

**Example.**

- $x \in K$ ,  $m_{x,K} = T - x$
- $p$  prime,  $d \geq 1$ . Then  $T^d - p \in \mathbb{Q}[T]$  is irreducible (Eisenstein's criterion) so it is the minimal polynomial of  $\sqrt[d]{p} = x \in \mathbb{R}$  over  $\mathbb{Q}$ .
- $z = e^{2\pi i/p}$  ( $p$  prime) is a root of  $T^p - 1$  and of  $\frac{T^p - 1}{T - 1} = g(T) = T^{p-1} + \dots + T + 1 \in \mathbb{Q}[T]$ . As

$$g(T + 1) = \frac{(T + 1)^p - 1}{T} = T^{p-1} + \binom{p}{1}T^{p-2} + \dots + \binom{p}{2}T + \binom{p}{1}$$

which is irreducible by Eisenstein, so  $g$  is irreducible and  $g$  is the minimal polynomial of  $z$  over  $\mathbb{Q}$ .

**Definition.** The *degree of  $x$  over  $K$*  ( $x$  algebraic over  $K$ ) is the degree of  $m_{x,K}$ , written  $\deg_K(x)$  or  $\deg(x/K)$ .

Ring/field characterisation of algebraicity:

**Proposition 4.1.** *Let  $L/K$  be a field extension,  $x \in L$ . The following are equivalent*

- (i)  $x$  is algebraic over  $K$
- (ii)  $[K(x) : K] < \infty$
- (iii)  $\dim_K K[x] < \infty$
- (iv)  $K[x] = K(x)$
- (v)  $K[x]$  is a field

If these hold, then  $\deg_K(x) = [K(x) : K]$ .

**Note:** recall  $K[x] = \{p(x)\}$ ,  $K(x) = \left\{ \frac{p(x)}{q(x)} \mid q(x) \neq 0, p, q \in K[T] \right\}$ .

*Proof.* (ii)  $\iff$  (iii), (iv)  $\iff$  (v) are obvious.

Show (iii)  $\Rightarrow$  (v), (iv) and (ii): let  $0 \neq y = g(x) \in K[x]$ . Consider  $K[x] \rightarrow K[x]$ ,  $z \mapsto yz$ . It is a  $K$ -linear transformation, injective as  $y \neq 0$ , and since  $\dim_K K[x] < \infty$ , it is a bijection. So there exists  $z$  such that  $yz = 1$ . So  $K[x]$  is a field, equal to  $K(x)$  and  $[K(x) : K] < \infty$ .

Show (v)  $\Rightarrow$  (i): wlog  $x \neq 0$ , then  $x^{-1} = a_0 + a_1x + \dots + a_nx^n \in K[x]$ . Then  $a_nx^{n-1} + \dots + a_0x - 1 = 0$ , so  $x$  is algebraic over  $K$ .

Show (i)  $\Rightarrow$  (iii) and degree formula: The image of  $\text{ev}_x : K[T] \rightarrow L$  is  $K[x] \subseteq L$ .  $x$  is algebraic over  $K$  so the kernel of this map is  $(m_{x,K})$ , which is a maximal ideal ( $m_{x,K}$  is irreducible). Applying the first isomorphism theorem gives

$\underbrace{K[T]/(m_{x,K})}_{\text{field}} \cong K[x]$ .  $m_{x,K}$  is monic of degree  $d = \deg_K(x)$ . So  $K[T]/(m_{x,K})$  has basis  $1, T, \dots, T^{d-1}$ . So  $\dim_K K[x] = d < \infty$ . Furthermore  $\deg_K(x) = [K(x) : K] = d$ .  $\square$

**Corollary 4.2.**

- (i)  $x_1, \dots, x_n$  are algebraic over  $K$  if and only if  $L = K(x_1, \dots, x_n)$  is a finite extension over  $K$ . If so, every element of  $L$  is algebraic in  $K$
- (ii) If  $x, y$  are algebraic over  $K$ , then so are  $x \pm y, xy$  and  $1/x$  (if  $x \neq 0$ ).
- (iii) Let  $L/K$  any extension. Then  $\{x \in L : x \text{ algebraic over } K\}$  is a subfield of  $L$

*Proof.*

- (i) If  $x_n$  is algebraic over  $K$ , it's certainly algebraic over  $K(x_1, \dots, x_{n-1})$ , so  $[L : K(x_1, \dots, x_{n-1})] < \infty$ . So by induction on  $n$  and the Tower Law,  $[L : K] < \infty$ . Conversely, if  $[L : K] < \infty$ , then the subfield  $K(y)$  is finite over  $K$  for all  $y \in L$ , so  $y$  is algebraic over  $K$  by Proposition 4.1.
- (ii)  $x + y, xy, \frac{1}{x} \in K(x, y)$ . So algebraic by (i).
- (iii) Trivial from (ii).

$\square$