

Proof of items (a), (b), (d) of the following proposition. Item (c) will be addressed later.

**Proposition.** (Milne, Prop.2.4) *For every polynomial  $f \in \mathbf{F}[x]$ , there exists a field extension  $\mathbf{F} \subset \mathbf{K}$  with the property that*

- (a)  *$f$ , as a polynomial in  $\mathbf{K}[x]$ , decomposes as  $f(x) = c(x - \alpha_1) \dots (x - \alpha_m)$ , with  $\alpha_i \in \mathbf{K}, c \in \mathbf{K}$ ;*
- (b)  *$\mathbf{F}(\alpha_1, \dots, \alpha_m) = \mathbf{K}$ .*

In addition,

- (c) *the field  $\mathbf{K}$  is unique up to  $\mathbf{F}$ -isomorphism;*
- (d) *If  $\deg(f) = n$ , then  $[\mathbf{K} : \mathbf{F}] \leq n!$ .*

**Definition.** An algebraically closed field is a field  $\mathbf{F}$  with the property that every polynomial  $f \in \mathbf{F}[x]$  splits as  $f(x) = c(x - \alpha_1) \dots (x - \alpha_m)$ , with  $\alpha_i, c \in \mathbf{F}$ .

In other words, “all zeroes of every polynomial  $f \in \mathbf{F}[x]$  are in  $\mathbf{F}$ ”.

**Example.** The field of complex numbers  $\mathbf{C}$  is algebraically closed: by the Fundamental of Algebra, every non-constant polynomial in  $\mathbf{C}[x]$  has a zero in  $\mathbf{C}$ . This implies that every  $f \in \mathbf{C}[x]$  splits as  $f(x) = c(x - \alpha_1) \dots (x - \alpha_m)$  in  $\mathbf{C}[x]$ .

**Example.** The fields  $\mathbf{Q}$  and  $\mathbf{R}$  are not algebraically closed: for example the polynomial  $f(x) = x^2 + 1$  has no zero in  $\mathbf{Q}$ , nor in  $\mathbf{R}$ .

Equivalent characterizations of an algebraically closed field (Milne, Prop.1.4.2 & Def. 1.4.3(a)).

**Definition.** An algebraic closure of a field  $\mathbf{F}$  is an extension  $\overline{\mathbf{F}}$  of  $\mathbf{F}$  which is algebraically closed over  $\mathbf{F}$  and consists of algebraic elements over  $\mathbf{F}$ .

**Fact.** (Milne Chapter 6) For every field  $\mathbf{F}$  there exists an extension  $\mathbf{F} \subset \mathbf{L}$  which is algebraically closed.

**Proposition.** (Milne, Prop. 1.45) *Every field  $\mathbf{F}$  admits an algebraic closure  $\overline{\mathbf{F}}$ .*

$\overline{\mathbf{F}}$  is unique, but *only* up to isomorphism and the isomorphism is generally not unique. Colloquially we often speak of “the” algebraic closure of a given field, but it is not correct.

Let  $\mathbf{L}$  be an algebraically closed extension of  $\mathbf{F}$ . Then one defines

$$\overline{\mathbf{F}} = \{x \in \Omega \mid x \text{ is algebraic over } \mathbf{F}\}.$$

The proof that  $\overline{\mathbf{F}}$  satisfies the required properties, i.e. is a field and it is algebraically closed, is based on the following two facts:

- (1)  $\mathbf{F} \subset \mathbf{K}$  fields,  $\alpha \in \mathbf{K}$ . Then  $\alpha$  is algebraic over  $\mathbf{F}$  if and only if there exists a finite extension  $\mathbf{E}$  of  $\mathbf{F}$  such that  $\mathbf{F} \subset \mathbf{E} \subset \mathbf{K}$ .
- (2)  $\mathbf{F} \subset \mathbf{K} \subset \mathbf{L}$  fields. If  $\mathbf{K}$  is algebraic over  $\mathbf{F}$  and  $\mathbf{L}$  is algebraic over  $\mathbf{K}$ , then  $\mathbf{L}$  is algebraic over  $\mathbf{F}$ .

**Example.**  $\overline{\mathbf{R}} \cong \mathbf{C}$ ;

In  $\mathbf{C}$  there is an algebraic closure  $\overline{\mathbf{Q}}$  of  $\mathbf{Q}$ : it consists of the complex numbers which are algebraic over  $\mathbf{Q}$ . It is a proper subset of  $\mathbf{C}$  because it is countable: for example it does not contain  $\pi$ .