

Definition 5.6. A field extension  $F \subseteq E$  is called finitely generated if  $\exists \alpha_1, \dots, \alpha_n \in E$  such that  $E = F(\alpha_1, \dots, \alpha_n)$ .

Clearly a finite extension is finitely generated. The opposite is not true.

Example 5.7. Let  $t \in \mathbb{R}$  be a transcendental number (e.g.  $t = \pi$  or  $t = e$ ). Then  $\mathbb{Q} \subseteq \mathbb{Q}(t)$  is a finitely generated field extension, but is not finite since  $t$  is not algebraic.

However, we have the following.

Theorem 5.8. Let  $F \subseteq E = F(\alpha_1, \dots, \alpha_n)$  be a finitely generated field extension such that  $\alpha_i$  is algebraic over  $F$  for  $1 \leq i \leq n$ . Then it is a finite and, by Theorem 5.3, an algebraic extension.

Proof. We have

$$F \subseteq F(\alpha_1) \subseteq F(\alpha_1, \alpha_2) \subseteq \dots \subseteq F(\alpha_1, \dots, \alpha_n) = E.$$

Moreover,  $\alpha_i$  algebraic over  $F \Rightarrow \alpha_i$  algebraic over  $F(\alpha_1, \dots, \alpha_{i-1})$ .

Hence  $[F(\alpha_1, \dots, \alpha_i) : F(\alpha_1, \dots, \alpha_{i-1})] < \infty$  if  $1 \leq i \leq n$ . By Theorem 4.2

we obtain

$$[E : F] = [F(\alpha_1, \dots, \alpha_n) : F(\alpha_1, \dots, \alpha_{n-1})] \cdot \dots \cdot [F(\alpha_1) : F] < \infty,$$

as required.  $\square$

Corollary 5.9. Let  $F \subseteq E$  be a field extension. The set

$$K = \{\alpha \in E \mid \alpha \text{ algebraic over } F\}$$

is a subfield of  $E$  and an algebraic extension of  $F$ , called the algebraic closure of  $F$  in  $E$ .

Proof. It is enough to show that  $K$  is a subfield of  $E$ . If  $\alpha, \beta \in K$ ,

then  $F \cong F(\alpha, \beta)$  is algebraic by Theorem 5.8. and so  $F(\alpha, \beta) \subseteq K$ .  
 But then  $-\alpha, \alpha^{-1}, \alpha + \beta, \alpha - \beta \in K$  and so  $K$  is a subfield of  $E$ .  $\square$

Example 5.10. Algebraic closure of  $\mathbb{Q}$  in  $\mathbb{C}$ :  $\mathbb{C} = \{ \alpha \in \mathbb{C} \mid \exists f(x) \in \mathbb{Q}[x] \text{ with } f(\alpha) = 0 \}$   
 $= \{ \alpha \in \mathbb{C} \mid \exists f(x) \in \mathbb{Z}[x] \text{ with } f(\alpha) = 0 \}$   
 $= \{ \text{algebraic numbers} \}$

Definition 5.11. Let  $F \subseteq K, F \subseteq L$  be field extensions.  
 A field embedding  $\sigma: K \rightarrow L$  (i.e. nonzero ring homomorphism) is called an  $F$ -homomorphism or an embedding over  $F$  if  $\sigma|_F = \text{id}_F$  that is,  $\sigma(\alpha) = \alpha \quad \forall \alpha \in F$ .

Theorem 5.12. Let  $F \subseteq E$  be an algebraic field extension and  $\sigma: E \rightarrow E$  an  $F$ -homomorphism. Then  $\sigma$  is onto and hence an isomorphism.

Proof. Let  $\alpha \in E$  and let  $p(x) = a_0 + a_1x + \dots + a_{n-1}x^{n-1} + x^n$  be the minimal polynomial of  $\alpha$  over  $F$ . Let  $S = \{ r \in E \mid p(r) = 0 \}$ .  
 Since  $\sigma$  is an  $F$ -homomorphism, for every  $r \in S$  we have  

$$p(\sigma(r)) = a_0 + a_1\sigma(r) + \dots + a_{n-1}\sigma(r)^{n-1} + \sigma(r)^n = \sigma(a_0) + \sigma(a_1)\sigma(r) + \dots + \sigma(a_{n-1})\sigma(r)^{n-1} + \sigma(r)^n$$

$$= \sigma(a_0 + a_1r + \dots + a_{n-1}r^{n-1} + r^n) = \sigma(p(r)) = \sigma(0) = 0.$$

Hence  $\sigma$  maps  $S$  to  $S$ . Since  $\sigma$  is injective and  $S$  is a finite set,  $\sigma|_S: S \rightarrow S$  is a bijection. The claim follows since  $\alpha \in S$ .  $\square$

Example 5.13. Theorem 5.12 hints at a connection between algebraic extensions  $F \subseteq E$  and  $F$ -homomorphisms. We have  $\mathbb{R} \subseteq \mathbb{R}(i) = \mathbb{C}$  and  $[\mathbb{C}:\mathbb{R}] = \deg(x^2+1) = 2$ . An  $\mathbb{R}$ -homomorphism  $\sigma: \mathbb{C} \rightarrow \mathbb{C}$  satisfies

$$\sigma(i)^2 = \sigma(i^2) = \sigma(-1) = -1$$

and so  $\sigma(i) \in \{-i, i\}$ . On the other hand, we have

$$\sigma(a+bi) = \sigma(a) + \sigma(b)\sigma(i) = a + b\sigma(i)$$

and so there exist exactly two  $\mathbb{R}$ -homomorphisms of  $\mathbb{C}$ :

$$\sigma(a+bi) = a+bi \quad \text{and} \quad \sigma(a+bi) = a-bi (= \overline{a+bi}).$$

These correspond to the roots  $i, -i$  of the minimal polynomial  $x^2+1$  of  $i$  over  $\mathbb{R}$ .