

## Section 11.1

## Chapter 11 Field extensions

Recall (Section 3.1)

Field is commutative ring  $R$  with identity  $1_R \neq 0_R$   
such that for every  $a \in R, a \neq 0_R$  the equation  
 $ax = 1_R$  has a solution in  $R$ .

Field is a set  $F$  with two operations (addition and multiplication)  
which satisfy  $a(b+c) = ab + ac$  for every  $a, b, c \in F$

such that  $F$  is an abelian group with respect to the addition  
with the neutral element  $0_F$

$F \setminus \{0_F\} = F^*$  is an abelian group with respect to the multiplication  
with the neutral element  $1_F$

Examples:  $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$ ,  $p$  is a prime

Minimalistic example -  $\mathbb{Z}_2$  - a field out of two elements

Field extension  $F \subseteq K$ , both fields  $0_F = 0_K$

$$1_F = 1_K$$

$K$  is an extension of  $F$

$F$  is a subfield of  $K$

Section 11.1 If  $F \subseteq K$  is a field extension, then  $K$  is a vector space over  $F$

Recall from Linear Algebra

Def Vector space  $V$  over a field  $F$  is an abelian group, and multiplication by scalars (elements of  $F$ ) is defined and satisfies

$$a(v_1 + v_2) = av_1 + av_2 \quad a \in F, v_1, v_2 \in V$$

$$(a_1 + a_2)v = a_1v + a_2v \quad a_1, a_2 \in F, v \in V$$

$$a_1(a_2v) = (a_1a_2)v \quad a_1, a_2 \in F \quad v \in V$$

$$1_F v = v \quad v \in V$$

Notions to review: dimension, basis

If  $v_1, \dots, v_n \in V$ , then  $a_1v_1 + \dots + a_nv_n$  with  $a_i \in F$  is called a linear combination of vectors  $v_1, \dots, v_n$ .

$v_1, \dots, v_n$  is a spanning set for  $V$

if every element of  $V$  can be written as a linear combination of  $v_1, \dots, v_n$

$v_1, \dots, v_n$  are linearly independent if

$$c_1v_1 + \dots + c_nv_n = 0_V \text{ implies } c_1 = \dots = c_n = 0_F$$

Example  
 $C$  is a 2-dimensional vector space over  $\mathbb{R}$   
basis:  $\{1, i\}$   
 $z = a \cdot 1 + b i$   
 $z \in C \quad a, b \in \mathbb{R}$

$$c_i \in F \quad v_i \in V$$

Basis of  $V$  (vector space) over  $F$  is a spanning set which linearly indep.

A vector space is called finite-dimensional if it admits a finite spanning set

Every finite spanning set contains (can be reduced to) a basis.

Lemma II.1  $u_1, \dots, u_n \in V$  is linearly dependent iff

there is  $u_k$  which is a linear combination of preceding vectors  $(u_1, \dots, u_{k-1})$ .

Lemma II.2 If  $v_1, \dots, v_n$  span  $V$  and  $v_1, \dots, v_m$  are linearly independent, then  $m \leq n$

Th II.3 Every two bases for a vector space  $V$  have same numbers of elements

Def dimension of a finite-dimensional vector space is the number of elements in any basis of  $V$

For a field extension  $F \subseteq K$ , the dimension of  $K$  as a vector space over  $F$  is denoted by  $[K:F]$ .  
 (in all cases under our consideration the dimension is finite)

Easy to check:

$[K:F]=1$  means  $K=F$

Infinite-dimensional:

$$\mathbb{Q} \subset \mathbb{C}$$

Th 11.4  $F \subseteq K \subseteq L$

If  $[K:F]$  and  $[L:K]$  are finite, then so is  $[L:F]$ .

$$\text{Moreover } [L:F] = [L:K][K:F].$$

Pf Let  $v_1, \dots, v_n$  be a basis for  $L$  over  $K$

$$u_1, \dots, u_m \longrightarrow \longrightarrow K \rightarrow F$$

Claim  $u_i v_j$  form a basis of  $L$  over  $F$

} implies  $[L:F] = nm$

$$i=1 \dots m$$

$$u_i v_j \in L$$

$$j=1 \dots n$$

Th 11.5 Let  $K \supseteq F$  and  $L \supseteq F$  be two field extensions (finite-dim'l)

Let  $f: K \rightarrow L$  be a field isomorphism such that  $\{f\}_F = \text{id}$

$f(c) = c$  for every  $c \in F$

Then  $[L:F] = [K:F]$

Pf  $f$  takes a basis to a basis:

Let  $u_1, \dots, u_n$  be a basis of  $K$  over  $F$ .

Wanted:  $f(u_1), \dots, f(u_n)$  is a basis of  $L$  over  $F$

① Spans  $v \in L$

Since  $f$  is an isomorphism,  $f$  is surjective  $v = f(u)$ ,  $u \in K$

$$u = c_1 u_1 + \dots + c_n u_n \quad c_i \in F \subseteq K$$

$$\begin{aligned} v &= f(u) = f(c_1 u_1) + \dots + f(c_n u_n) = f(c_1) f(u_1) + \dots + f(c_n) f(u_n) \\ &= c_1 f(u_1) + \dots + c_n f(u_n) \end{aligned}$$

② Linearly independent

$$\text{Let } c_1 f(u_1) + \dots + c_n f(u_n) = 0$$

Wanted:  $c_1 = \dots = c_n = 0$

$$f(c_1 u_1 + \dots + c_n u_n) = 0$$

Since  $f$  is an isomorphism,  $f$  is injective

$c_1u_1 + \dots + c_nu_n = 0$  implies  $c_1 = \dots = c_n = 0$   
because  $u_1, \dots, u_n$  is a basis  
of  $K$  over  $F$ , therefore  
linearly independent.