KTH Teknikvetenskap

SF2729 GROUPS AND RINGS LECTURE NOTES 2010-05-06

SANDRA DI ROCCO

CONTENTS

1. VECTOR SPACES OVER A FIELD

This is a notion that you have studied in linear algebra when the fields considered were only $\mathbb{R}$ or $\mathbb{C}$. All the important results on vectors, basis and dimension generalize to all fields. The scalars are no longer just real or complex numbers, but the elements of a field.

Definition 1.1. Let F be a fileld. A vector space over F consists of an abelian group $(V, +)$ endowed with a "scalar multiplication", i.e a function

$$F \times V \to V,\ (a, v) \mapsto av \in V,$$

such that:

(1) $(ab)v = a(bv)$,
(2) $(a + b)v = av + bv$,
(3) $a(v + w) = av + aw$,
(4) $1_F v = v$.

Example 1.2. $\mathbb{R}^n, F^n, M_{m,n}(\mathbb{C})$. For all fields F, $F[x]$ is a vector space over F.

Example 1.3. Let K be a subfield of F. Then F is a vector space over K with scalar multiplication given by the operation of multiplication.

Definition 1.4. $W \subset V$ is a subvector space if it is a subgroup and the scalar multiplication restricts to a scalar multiplication on W.

Definition 1.5.
- A vector v is a linear combination on vectors $(v_1, \dots, v_l)$ if there are elements $a_1, \dots a_l$ such that $v = \sum_1^l a_i v_i$.
- Elements $v_1, \dots, v_k$ are linearly independent if:
$$a_1 v_1 + \dots + a_k v_k = 0_V \Rightarrow a_1 = \dots = a_k = 0_F.$$
Elements $v_1, \dots, v_k$ are linearly dependent if there are $a_1, \dots, a_k$ (at least one of which non zero) such that $a_1 v_1 + \dots + a_k v_k = v$.
- Let $I = \{v_i\}$ be a set of vectors in V (possibly infinite). By $Span(I)$ we denote the subvectorspace of all possible finite linear combinations of vectors in I.
- V is said to be *finitely generated* if there is a finite number $v_1, \dots, v_k$, such that $V = Span(v_1, \dots, v_k)$.
- A subset $B = \{v_1, \dots, v_k\} \subset V$ is a basis of V is $V = Span(v_1, \dots, v_k)$ and $v_1, \dots, v_k$ are linearly independent.

Example 1.6. Consider $\mathbb{Q}[\sqrt{2}]$. It is a vector space over $\mathbb{Q}$ with scalar product:
$$(q, a + b\sqrt{2}) \mapsto (qa) + (qb)\sqrt{2}.$$
One sees that the vectors $(1, \sqrt{2})$ are linearly independent and generate the whole space.

Similarly to what showed in linear algebra one proves that two basis must have the same number of vectors and thus defines:

$$\dim(V) = n \text{ is there is a basis consisting of } n \text{ vectors.}$$

otherwise one says that V is infinite dimensional.

Example 1.7. The polynomials $F[x]$ is an infinite dimensional vector space over F. If one looks at only polynomial up to degree k, $F_k[x]$ then this is a vector space over F of dimension $k + 1$. The vector space $\mathbb{Q}[\sqrt{2}]$ has dimension 2 over $\mathbb{Q}$.

2. Field extensions

Definition 2.1. We say that a field L is an extension of a field K if K is a subfield of L.

Example 2.2. $\mathbb{R}$ and $\mathbb{C}$ are extensions of $\mathbb{Q}$. The field $\mathbb{Z}_3[x]/x^2 + 1$ is an extension of $\mathbb{Z}_3$.

Definition 2.3. Let L be an extension of K. The degree of the extension is:
$$[L : K] = \dim_K(F)$$
If the dimension if finite then the extension is said to be a finite extension.

Example 2.4. Notice that $\mathbb{C} = Span_{\mathbb{R}}(1, i)$, it is then a finite extension with degree $[\mathbb{C}, \mathbb{R}] = 2$.

Another example of fine extension is $\mathbb{Z}_3[x]/x^2 + 1$. Every element is a combination of $1 + (x^2 + 1)$ and $x + (x^2 + 1)$. This two elements are linearly independent and thus:
$$\dim_{\mathbb{Z}}(\mathbb{Z}_3[x]/x^2 + 1) = [\mathbb{Z}_3[x]/x^2 + 1 : \mathbb{Z}_3] = 2.$$

Proposition 2.5. *Assume that L is am extension of K and K is an extension of F. Then*
$$[L : F] = [L : K][K : F].$$

Proof. Notice that if L is an infinite extension of K it will be an infinite extension of F. Viceversa if K is an infinite extension of F then L will certainly be an infinite extension of F. We may assume that the extensions are finite. Let $[L : K] = m, [K : F] = n$. Let $a_1, \dots a_n$ a basis of K over F and let $b_1, \dots, b_m$ a basis of L over K. We shal prove that $\{a_i b_j\}$ for a basis of L over F. They certainly generate L as for every element $a \in L, a = \sum \beta_i b_i$ and for every $\beta_i \in K, \beta_i = \sum \alpha_{ij} a_j$. Now assume that

$$\sum_{i=1}^{m} \sum_{j=1}^{n} \gamma_{ij} a_i b_j = 0_L.$$

Then $\sum_1^n \gamma_{ij} a_i = 0_K$ for $j = 1, \dots m$. But then we have that $\gamma_{ij} = 0_F$ for all $i = 1 \dots n$. □

EXERCISE Prove that if L is an extension of K then $L = K$ if and only if $[L : K] = 1$.

Observe that one can define an extension by "adding" certain elements. Let S be a set of elements of a field L and let K be a subfields of L. one can define $K(S)$ to be the smallest subfield of L containing K and S. This is an extension of K. For example $\mathbb{R}(i) = \mathbb{C}$. If $S = \{a\}$ the extension $K(a)$ is said to be a *simple extension*.

EXERCISE Show that $F[a] = Im(ev_a : K[x] \to L) \subseteq F(a)$ and that $F[a] = F(a)$ if and only if $F[a]$ is a field.

3. Algebraic Extensions

Definition 3.1. Let L be an extension of K. An element $\alpha \in L$ is said to be *algebraic over* F if there is a $0 \neq f(x) \in F[x]$ such that $f(\alpha) = 0_L$, i.e. $f \in Ker(ev_\alpha)$.

Example 3.2. The elements $\sqrt{2}, i$ are algebraic over $\mathbb{Q}$ because they are roots of $x^2 - 2, x^2 + 1$.

Definition 3.3. An extension L over K is said to be an *algebraic extension* if every element $\alpha \in L$ is algebraic over K. An extension which is not algebraic is said to be *trascendental*.

Example 3.4. $\mathbb{C}$ is an algebraic extension of $\mathbb{R}$ and $\mathbb{R}$ is an algebraic extension of $\mathbb{Q}$.

Proposition 3.5. *Every finite extension is algebraic.*

Proof. Let L be an extension of K with $[L : K] = n$. Let $\alpha \in L$. The elements $1, \alpha, \alpha^2, \dots, \alpha^n$ must be linearly independent over K which means that there are $a_0, \dots, a_n \in K$ such that $a_0 + a_1\alpha + \dots + a_n\alpha^n = 0$. Obviously α is the root of the polynomial $f(x) = \sum a_i x^i \in K[x]$. □

As observed above, if $a \in L$ and L is an extension of K the we have that

$$K[a] \cong K[x]/Ker(ev_a).$$

Because $F[x]$ is a PID there is a polynomial $f_a \in K[x]$ such that $Ker(ev_a) = (f_a)$. Recall that f_a is uniquely defined up to a non vanishing constant. In particular there is ONLY one generator which is monic, i.e. with leading coefficient equal to one.

The monic generator is called the *minimal polynomial of* a *over* K.

Proposition 3.6. *Let L be an extension of K and let $a \in L$. Let $p(x) \in K[x]$ be a monic polynomial. The following statements are equivalent:*

(1) *$p(x)$ if the minimal polynomial of a over K.*
(2) *$p(x)$ is irreducible and $p(a) = 0$.*
(3) *$p(x)$ is the minimal polynomial (w.r.t degree) in $Ker(ev_a)$.*

Proof. $(1) Rightarrow (2)$ Let $p(x)$ be the minimal polynomial of a over K. then clearly $p(a) = 0$. If $p(x) = g(x)h(x)$ then $g(a) = 0$ or $f(a) = 0$. Assume $g(a) = 0$ then $g \in Ker(ev_a)$ and this p/g. But we are assuming that g/p which is a contradiction.

$(2) \Rightarrow (1)$ Because $p(a) = 0$ then f_a/p and because p is irreducible it is $p = \alpha f_a$ for a constant $\alpha \in K^*$. But f_a and p are monic which implies $\alpha = 1$.

$(1) \Rightarrow (3)$ Obvious. $(3) \Rightarrow (1)$. Such p is certainly a generator of $Ker(ev_a)$. □

We conclude that $K[x]/(f_a) \cong K[a]$. Because f_a is irreducible the ideal (f_a) is a maximal ideal and therefore $F[a]$ is a field and it follows that:

$$K[a] = K(a).$$

If $\deg(f_a) = n$, we have that

$$F[a] = \{\sum_0^{n-1} a_i x^i + (f_a)\}.$$

It follows that the elements $1 + (f_a), x + (f_a), \ldots, x^{n-1} + (f_a)$ for a basis for $K[x]/(f_a)$ and thus using the isomorphism:

$$K[x]/(f_a) \cong K[a] \text{ via } p(x) + (f_a) \mapsto p(a)$$

we see that $1, a, \ldots, a^{n-1}$ is a basis of $K(a)$ and that

$$[F(a) : F] = n.$$

Example 3.7. the polynomial $x^2 - 2$ is the minimal polynomial for $\sqrt{2}$ over $\mathbb{Q}$. we have then that:

$$\mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}[\sqrt{2}] \cong \mathbb{Q}[x]/(x^2 - 1)$$

Similarly $\mathbb{C} \cong \mathbb{R}(i) \cong \mathbb{R}[i] \cong \mathbb{R}[x]/(x^2 + 1)$.

We can then conclude that:

α is algebraic over K if and only if $K(\alpha) = K[\alpha]$ is a finite extension of K and moreover $[K(\alpha) : K]$ is equal to the degree of the minimal polynomial of α over K.

EXERCISE Let L be a field extension of K. Show that the set of the elements in L which are algebraic over K is a subfield of L containing K.

Definition 3.8. This subfield is said to be the algebraic closure of K in L. If the algebraic closure of a field K is the flied K itself then K is said to be algebraically closed.

Example 3.9. The field $\mathbb{Q}$ is not algebraically closed in $\mathbb{R}$, we know that $\sqrt{2} \notin \mathbb{Q}$. Observe that for every $n \geq 1$ then $[Q(\sqrt[n]{2}) : Q] = n$ since $x^n - 2$ is the minimal polynomial. It follows that if $\overline{\mathbb{Q}}$ is the algebraic closure of $\mathbb{Q}$ is $\mathbb{R}$ then:

$$[\overline{\mathbb{Q}} : Q] \geq [Q(\sqrt[n]{2}) : Q] = n \text{ for all } n \geq 1$$

which implies that $\overline{\mathbb{Q}}$ is not a finite extension. This shows that Proposition 3.5 cannot be inverted.

EXERCISE Let F be a subfield of L. Show that the algebraic closure of F in L is algebraically closed.

Recommended excercises

- VI-29 29, 30, 31, 36, 37.
- VI-30 21, 22, 24.
- VI-31 22, 23, 24, 25, 28
