Lecture 16: Vector space over a field

Sunday, March 17, 2019 4:25 PM

In your linear algebra courses, you have learned about vector spaces over $\mathbb{R}$ or $\mathbb{C}$. One can define and study vector spaces over a field F.

<u>Def.</u> We say V is a vector space over a field F if

(1) $(V,+)$ is an abelian group

(2) There is a scalar multiplication

$$\forall c\in F,\ \forall v\in V,\ c\cdot v\in V \quad \text{s.t.}$$

$$(c_1+c_2)\cdot v = c_1\cdot v + c_2\cdot v$$

$$c\cdot(v_1+v_2) = c\cdot v_1 + c\cdot v_2$$

$$c_1\cdot(c_2\cdot v) = \underbrace{(c_1c_2)}_{\text{multiplication in } F}\cdot v$$

Here is an important example: if F is a subfield of a ring A, then A can be viewed as an F-vector space. Here scalar multiplication $c\cdot a = ca$ is just multiplication in A.

Lecture 16: Dimension of Q[a] over Q

Sunday, March 17, 2019 4:34 PM

Theorem. Suppose $\alpha \in \mathbb{C}$ is an algebraic number. Suppose $d = \deg m_\alpha$ where $m_\alpha(x) \in \mathbb{Q}[x]$ is the minimal polynomial of α over $\mathbb{Q}$. Then $\{1, \alpha, \ldots, \alpha^{d-1}\}$ is a $\mathbb{Q}$-basis of $\mathbb{Q}[\alpha]$; and so $\dim_{\mathbb{Q}} \mathbb{Q}[\alpha] = \deg m_\alpha$.

Pf. We have to show that the $\mathbb{Q}$-span of $\{1, \alpha, \ldots, \alpha^{d-1}\}$ is $\mathbb{Q}[\alpha]$. Recall that

$\forall \beta \in \mathbb{Q}[\alpha]$, $\beta = h(\alpha)$ for some $h(x) \in \mathbb{Q}[x]$. By long division $\exists\, q(x), r(x) \in \mathbb{Q}[x]$, $h(x) = q(x)\, m_\alpha(x) + r(x)$ and

$$\deg r < \deg m_\alpha = d.$$

$$\Rightarrow \beta = h(\alpha) = q(\alpha) \underbrace{m_\alpha(\alpha)}_{0} + r(\alpha).$$

Since $\deg r < d$, $r(x) = a_0 + a_1 x + \cdots + a_{d-1} x^{d-1}$ for some $a_i \in \mathbb{Q}$. Therefore $\beta = a_0 + a_1 \alpha + \cdots + a_{d-1} \alpha^{d-1}$; and so β is a $\mathbb{Q}$-linear combination of $1, \alpha, \ldots, \alpha^{d-1}$. Thus $\mathbb{Q}[\alpha]$ is the $\mathbb{Q}$-span of $\{1, \alpha, \ldots, \alpha^{d-1}\}$. Next we have to show that $1, \alpha, \ldots, \alpha^{d-1}$ are $\mathbb{Q}$-linearly independent.

Lecture 16: Dimension of Q[a] over Q

Sunday, March 17, 2019 4:46 PM

Suppose $c_0 + c_1\alpha + \cdots + c_{d-1}\alpha^{d-1} = 0$ for some $c_i \in \mathbb{Q}$.

Then α is a zero of $g(x) = c_0 + c_1 x + \cdots + c_{d-1} x^{d-1}$. Hence

$g(x) \in \ker \phi_\alpha = m_\alpha(x)\,\mathbb{Q}[x]$; this means

$$g(x) = m_\alpha(x)\,h(x) \quad \text{for some } h(x) \in \mathbb{Q}[x].$$

$$\left.\begin{array}{l} \Rightarrow \deg g = \deg m_\alpha + \deg h \\ \deg g \le d-1 < \deg m_\alpha \end{array}\right\} \Rightarrow \deg h < 0$$

$$\Rightarrow h(x) = 0$$

$$\Rightarrow g(x) = 0$$

$$\Rightarrow c_0 + c_1 x + \cdots + c_{d-1} x^{d-1} = 0$$

$$\Rightarrow c_0 = c_1 = \cdots = c_{d-1} = 0. \quad \blacksquare$$

Lecture 16: Finding a zero of a polynomial

Sunday, March 17, 2019 3:41 PM

As it was mentioned at the beginning of the course, algebra was developed in order to understand zeros of polynomials.

A polynomial in $\mathbb{C}[x]$ by the fundamental theorem of algebra (that has a very nice proof using complex analysis) has a zero in $\mathbb{C}$. What happens if $f(x) \in F[x]$ and F is not a subfield of $\mathbb{C}$, e.g. $F = \mathbb{Z}_p$?

We will show later that any polynomial $f(x) \in F[x] \setminus F$ can be written as a product of irreducibles (essentially) in a unique way. Having

$$f(x) = f_1(x) \cdot f_2(x) \cdot \dots \cdot f_m(x)$$

where $f_i(x)$ are irreducible in $F[x]$, it is enough to find a zero of $f_1(x)$ in order to get a zero of $f(x)$. So we would like to study zeros of an irreducible polynomial $p(x) \in F[x]$ in a possibly larger field E, and the question is if there is such a field E.

Lecture 16: Field extension

Sunday, March 17, 2019 3:58 PM

<u>Theorem</u>. Let F be a field, and $p(x)$ be an irreducible polynomial in $F[x]$. Then, there are a field E, an embedding $i: F \hookrightarrow E$, and $\alpha \in E$ such that

$$i(p)(\alpha) = 0,$$

where $i\left(\sum_{j=0}^{\infty} c_j x^j\right) = \sum_{j=0}^{\infty} i(c_j) x^j$.

(we often simply write $p(\alpha) = 0$ with an understanding that we are viewing F as a subfield of E).

(Embedding means an injective (ring) homomorphism.)

<u>Idea of the proof</u>.

Suppose we have found such (E, α). Let $\phi_\alpha : F[x] \to E$ be the evaluation at α. Then $\exists$ an irreducible polynomial $m_\alpha(x) \in F[x]$ such that $\ker \phi_\alpha = m_\alpha(x) F[x]$; and

$F[x]/m_\alpha(x)F[x] \simeq F[\alpha]$, where $F[\alpha] = \operatorname{im} \phi_\alpha$ is a field.

Since $p(\alpha) = 0$, we get $p(x) \in \ker \phi_\alpha$; which implies

Lecture 16: Field extension

Saturday, September 2, 2017 3:12 AM

$p(x) = m_\alpha(x)\, q(x)$ for some $q(x) \in F[x]$. Since p is irreducible, either m_α is a unit or q is a unit (in $F[x]$). Since m_α is irreducible, it is not a unit. Therefore $q(x) \in F[x]^\times$ and so $q \in F^\times$; which implies $m_\alpha(x) = q^{-1} p(x)$; and so $\ker \phi_\alpha = p(x) F[x]$. So we should let $E = F[x]/p(x)F[x]$, and the poly. which under the evaluation at α is mapped to α is the polynomial x. So we should let $\alpha = x + p(x)F[x]$

Proof. Since $p(x)$ is irreducible and $F[x]$ is a PID, we have $I := p(x)F[x]$ is a maximal ideal. Therefore $E = F[x]/I$ is a field. Let $i: F \to E$ be $i(c) := c + I$.

<u>i is a ring homomorphism</u>

$$i(c_1+c_2) = (c_1+c_2)+I = (c_1+I)+(c_2+I)$$
$$= i(c_1)+i(c_2).$$

$$i(c_1c_2) = c_1c_2 + I = (c_1+I)(c_2+I)$$
$$= i(c_1)\, i(c_2).$$

<u>Injective.</u> Suppose $i(c) = 0$. Then $c + I = I$

Then $c \in I$. Since I is a proper ideal,

$$I \cap F[x]^{\times} = \emptyset.$$

So $I \cap F^{\times} = \emptyset$. On the other hand, $c \in I \cap F$. Therefore $c=0$.

$\alpha = x + I$ is a zero of $i(p)(x)$.

Suppose $p(x) = \sum^{n} c_i x^i$. We have to show

$$i(c_0) + i(c_1)\alpha + \cdots + i(c_n)\alpha^n = 0$$

in $E = F[x]/I$.

$$i(c_0) + i(c_1)\alpha + \cdots + i(c_n)\alpha^n =$$

$$(c_0 + I) + (c_1 + I)(x + I) + \cdots + (c_n + I)(x+I)^n =$$

$$(c_0 + c_1 x + \cdots + c_n x^n) + I = p(x) + I \underset{\boxed{p(x) \in I}}{=} 0 + I,$$

which is the 0 in $E := F[x]/I$. ■

We say E is a field extension of F, which has a zero of $p(x)$.

In the next lecture we will show that $F[x]$ is a

Unique Factorization Domain (UFD).

Def. An integral domain D is called a Unique Factorization

Lecture 16: UFD

Sunday, March 17, 2019 4:56 PM

Domain if

(Existence) $\forall\, d \in D \setminus (D^\times \cup \{0\})$, there are $p_i \in D$ s.t.

p_i's are irreducible in D and

$$d = p_1 \cdot p_2 \cdot \cdots \cdot p_m .$$

(Any non-zero non-unit element can be written as a product of irreducibles.)

(Uniqueness) Suppose p_i's and q_j's are irreducible in D, and $p_1 \cdot p_2 \cdot \cdots \cdot p_m = q_1 \cdot q_2 \cdot \cdots \cdot q_n$. Then $m = n$,

$p_1 = u_1 q_{i_1}$, $p_2 = u_2 q_{i_2}$, $\ldots$, $p_m = u_m q_{i_m}$ for some $u_i \in D^\times$ and a reordering $i_1, i_2, \ldots, i_m$ of $1, 2, \ldots, m$.

(Up to a reordering and multiplication by units a non-zero non-unit element can be <u>uniquely</u> written as a product of irreducibles.)