Section 30 - Vector spaces

Let $F \leq E$ be field extension, $\alpha \in E$ algebraic over F.

Recall $irr(\alpha, F) \in F[x]$ is the unique monic irreducible polynomial s.t. $f(\alpha) = 0$.

If $\phi_\alpha : F[x] \longrightarrow E$ is the evaluation homomorphism,

$$\text{Ker } \phi_\alpha = \langle irr(\alpha, F) \rangle.$$

~~Simple extensions~~

~~Let $F \leq E$ be field extension, $\alpha \in E$.~~

Example $i \in \mathbb{C} \geq \mathbb{Q}$. $x^2+1 \in \mathbb{Q}[x]$ is monic & irreducible, and $(i)^2+1 = 0$, so $irr(i, \mathbb{Q}) = x^2+1$, $\text{Ker } \phi_i = \langle x^2+1 \rangle \subset \mathbb{Q}[x]$.

Simple extensions

Let $F \leq E$ be field extension, $\alpha \in E$. Define new field $F(\alpha) \leq E$ by

- If α algebraic: $\phi_\alpha : F[x] \longrightarrow E$ evaluation homomorphism.

  $\phi_\alpha[F[x]] \leq E$ subring

  $\phi_\alpha[F[x]] \simeq F[x]/\text{Ker } \phi_\alpha = F[x]/\langle irr(\alpha, F) \rangle$.

  $irr(\alpha, F)$ irreducible $\Rightarrow \langle irr(\alpha, F) \rangle$ maximal $\Rightarrow F[x]/\langle irr(\alpha, F) \rangle$ a field

  $\Longrightarrow \phi_\alpha[F[x]]$ a field.

- If α transcendental: $\text{Ker } \phi_\alpha = \{0\} \Rightarrow \phi_\alpha$ injective

  $\Rightarrow F[x] \simeq \phi_\alpha[F[x]]$.

  Set $F[\alpha] = \phi_\alpha[F[x]]$, $F(\alpha) \leq E$, $F(\alpha)$ fraction field of $F[\alpha]$.

Examples • $i \in \mathbb{C} > \mathbb{Q}$, $\mathbb{Q}(i) \leq \mathbb{C}$

$$\mathbb{Q}(i) = \phi_i[\mathbb{Q}[x]] = \{ f(i) \mid f(x) \in \mathbb{Q}[x] \}$$

$$= \{ a_n i^n + a_{n-1} i^{n-1} + \cdots + a_0 \mid n \geq 0,\ a_i \in \mathbb{Q} \} < \mathbb{C}.$$

• $e \in \mathbb{R} > \mathbb{Q}$, e is transcendental.

$$\mathbb{Q}[e] = \phi_e[\mathbb{Q}[x]] = \{ f(e) \mid f(x) \in \mathbb{Q}[x] \} \in \mathbb{R}$$

$$\mathbb{Q}(e) = \left\{ \frac{f(e)}{g(e)} \mid f(x), g(x) \in \mathbb{Q}[x],\ g(e) \neq 0 \right\} < \mathbb{R}.$$

$$\mathbb{Q}[e] \simeq \mathbb{Q}[x] \Rightarrow \mathbb{Q}(e) \simeq \mathbb{Q}(x).$$

Def If $E = F(\alpha)$ for some $\alpha \in E$, say E is a simple extension of F.

Thm Let $F \leq E$ be field extension, $\alpha \in E$, $E = F(\alpha)$. Assume α algebraic & $\deg(\alpha, F) = n$. Then every $\beta \in E$ can be written uniquely as

$$\beta = b_0 + b_1 \alpha + \cdots + b_{n-1} \alpha^{n-1} \qquad b_i \in F.$$

Proof $\beta \in F(\alpha) = \phi_\alpha[F[x]] = \{ \phi_\alpha(f(x)) \mid f(x) \in F[x] \} = \{ f(\alpha) \mid f(x) \in F[x] \}$

Hence there is an $f(x) = c_0 + \cdots + c_m x^m$, $c_i \in F$, s.t.

$$\beta = f(\alpha) = c_0 + c_1 \alpha + \cdots c_m \alpha^m.$$

If $m \leq n-1$, we are done.

Let $\operatorname{irr}(\alpha, F) = x^n + d_{n-1} x^{n-1} + \cdots + d_0$. Then

$$\alpha^n + d_{n-1} \alpha^{n-1} + \cdots + d_0 = 0$$

$$\Downarrow$$

$$\alpha^n = -d_{n-1} \alpha^{n-1} - \cdots - d_0.$$

If $m \geq n$, rewrite β as

~~$\beta = c_0 + c_1\alpha + \cdots + c_m\alpha^m = c_0 + c_1\alpha + \cdots + c_{m-1}\alpha^{m-1} + c_m\alpha^n\alpha^{m-n}$~~

~~$= c_0 + c_1\alpha + \cdots + c_{m-1}\alpha^{m-1} + c_m(-d_0 - d_1\alpha - \cdots - d_{n-1}\alpha^{n-1})\alpha^{m-n}$~~

~~$= c_0' + c_1'\alpha + \cdots + c_{m-1}'\alpha^{m-1}$, for some $c_i' \in F$.~~

$\beta = c_0 + c_1\alpha + \cdots + c_m\alpha^m = c_0 + c_1\alpha + \cdots + c_{m-1}\alpha^{m-1} + c_m\alpha^n\alpha^{m-n}$

$= c_0 + c_1\alpha + \cdots + c_{m-1}\alpha^{m-1} + c_m(-d_0 - d_1\alpha - \cdots - d_{n-1}\alpha^{n-1})\alpha^{m-n}$

$= c_0' + c_1'\alpha + \cdots + c_{m-1}'\alpha^{m-1}$, for some $c_i' \in F$.

If $m-1 \leq n-1$, we are done. Otherwise, repeat to find

$\beta = c_0'' + c_1''\alpha + \cdots + c_{m-2}''\alpha^{m-2}$, $c_i'' \in F$, and so on,

until we find $\beta = b_0 + \cdots + b_{n-1}\alpha^{n-1}$.

Alternatively: $\beta = f(\alpha) = c_0 + \cdots + c_m\alpha^m$.

Polynomial division $\Rightarrow$ $f(x) = q(x)\,\mathrm{irr}(\alpha, F) + r(x)$, with $q(x), r(x) \in F[x]$, $r(x) = 0$ or $\deg r(x) < \mathrm{irr}(\alpha, F) = n$.

Let $r(x) = b_0 + \cdots + b_{n-1}x^{n-1}$, then

$\beta = f(\alpha) = q(\alpha)\,\mathrm{irr}(\alpha, F)(\alpha) + r(\alpha)$

$= q(\alpha)\,0 + r(\alpha) = r(\alpha) = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}$.

Uniqueness of the b_i: If $\beta = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1} = b_0' + \cdots + b_{n-1}'\alpha^{n-1}$,

Then $(b_0 - b_0') + (b_1 - b_1')\alpha + \cdots + (b_{n-1} - b_{n-1}')\alpha^{n-1} = 0$.

Let $g(x) = b_0 - b_0' + (b_1 - b_1')x + \cdots + (b_{n-1} - b_{n-1}')x^{n-1}$.

Since $g(\alpha) = 0$ & $\deg g(x) < \deg(\alpha, F)$, must have $g(x) = 0$.

This means $b_i - b_i' = 0$ $\forall i$ $\Rightarrow$ $b_i = b_i'$ $\forall i$.

Example: $\mathbb{Q}(\sqrt{2}) = \{b_0 + b_1\sqrt{2} \mid b_0, b_1 \in \mathbb{Q}\} \subset \mathbb{R}$, & every $\beta \in \mathbb{Q}(\sqrt{2})$ equals $\beta = b_0 + b_1\sqrt{2}$ for unique $b_i \in \mathbb{Q}$

- $\mathbb{R}(i) = \{a + bi \mid a, b \in \mathbb{R}\} = \mathbb{C}$.

Note $\mathbb{R}(i) = \phi_i[\mathbb{R}[x]] \simeq \mathbb{R}[x]/\langle 1 + x^2\rangle$. Since $\mathrm{irr}(i, \mathbb{R}) = 1 + x^2$.

Vector spaces

Let F be a field. A vector space over F is an abelian group $(V,+)$ with an operation† $*: F\times V \to V$, written

$$*(a,\alpha) = a\alpha \qquad a\in F,\ \alpha\in V,$$

satisfying, for $a,b\in F$, $\alpha,\beta\in V$

† scalar multiplication

(1) $a(b\alpha) = (ab)\alpha$

(2) $(a+b)\alpha = a\alpha + b\alpha$

(3) $a(\alpha+\beta) = a\alpha + a\beta$

(4) $1\alpha = \alpha$.

Examples • $\mathbb{R}^n$ is a vector space over $\mathbb{R}$, via

$$a(b_1,\dots,b_n) = (ab_1,\dots,ab_n)$$

• $F[x]$ is a vector space over F for any field F, via

$$a(b_0+b_1x+\cdots+b_nx^n) = ab_0+ab_1x+\cdots+ab_nx^n.$$

• Key example: Let $F\leq E$ be a field extension. Then E is a vector space over F, where scalar multiplication $a\alpha$ $(a\in F, \alpha\in E)$ is field multiplication in E.

E.g. $\mathbb{C}$ is a vector space over $\mathbb{R}$.

Easy facts: If V is vector space over F, then for $a\in F$, $\alpha\in V$

$$0\alpha = a0 = 0$$
$$(-a)\alpha = a(-\alpha) = -a\alpha$$
$$(-a)(-\alpha) = a\alpha.$$

Spans & (linear) dependence Let V be a vector space over F. Let $\{\alpha_i \mid i\in I\}$ be a set of vectors of V.

The span of $\{\alpha_i \mid i \in I\}$ is the set of $\beta \in V$ which can be written as

$$\beta = a_1 \alpha_{i_1} + \cdots + a_n \alpha_{i_n}$$

for some $n \geq 1$, $a_1, \ldots, a_n \in F$, $i_1, \ldots, i_n \in I$

Write $\operatorname{span}\{\alpha_i\}_{i \in I}$ for this set.

Def If $\operatorname{span}\{\alpha_i\}_{i \in I} = V$, say the α_i span V.

Example: $\mathbb{R}^n$ over $\mathbb{R}$ is spanned by

$$(1, 0, \ldots, 0), (0, 1, 0, \ldots, 0), \ldots, (0, \ldots, 0, 1),$$

since every $(a_1, \ldots, a_n) \in \mathbb{R}^n$ is of the form

$$(a_1, \ldots, a_n) = a_1(1, 0, \ldots, 0) + a_2(0, 1, 0, \ldots, 0) + \cdots + a_n(0, \ldots, 0, 1).$$

- $F[x]$ over F is spanned by $1, x, x^2, \ldots \in F[x]$, since every $f(x) \in F[x]$ is $f(x) = a_0 1 + a_1 x + \cdots + a_n x^n$ for some n, $a_i \in F$.

- Let $E = F(\alpha)$ over F, and assume α is algebraic over F, $\deg(\alpha, F) = n$. Then E is spanned by $1, \alpha, \ldots, \alpha^n$.

Def A vector space V over F is finite-dimensional if there is a finite set $\alpha_1, \ldots, \alpha_n \in V$ spanning V.

Example $\mathbb{R}^n$ over $\mathbb{R}$ & $F(\alpha)$ over F are finite-dimensional $F[x]$ is not finite-dimensional over F.

Linear dependence Let V be a vector space over F. A set of vectors $\{\alpha_i \mid i \in I\}$ is linearly independent if there exist an $n \geq 1$, distinct $i_1, \ldots, i_n \in I$ and non-zero $a_1, \ldots, a_n \in F$ s.t.

$$a_1 \alpha_{i_1} + a_2 \alpha_{i_2} + \cdots + a_n \alpha_{i_n} = 0.$$

Otherwise, say the α_i are linearly independent.

Def A set of vectors $\{\alpha_i \mid i \in I\}$ is a basis of V if

(1) The α_i span V

(2) The α_i are linearly independent.

Example • $(1,0,0,\ldots 0), (0,1,\ldots,0), \ldots (0,\ldots,1)$ is a basis of $\mathbb{R}^n$

• $1, x, x^2, \ldots$ is a basis of $F[x]$

• If $E = F(\alpha)$, α algebraic over F with $\deg(\alpha, F) = n$, then $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ is a basis of E.

Proof: (1) Every $\beta \in E$ can be written $\beta = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$ $a_i \in F$, so the $1, \ldots, \alpha^{n-1}$ span E.

(2) If $a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} = 0$, then must have $a_i = 0$ $\forall i$, so the $1, \alpha, \ldots, \alpha^{n-1}$ are linearly independent.

Dimension theorem: Let V be a finite-dimensional vector space over F. Then

(1) There exists a basis $\beta_1, \ldots, \beta_n$ of V.

(2) If $\beta_1', \ldots, \beta_m'$ is some other basis, $m = n$

(3) If $\alpha_1, \ldots, \alpha_k \in V$ span V, $k \geq n$

(4) If $\alpha_1, \ldots, \alpha_k \in V$ are linearly independent, then $k \leq n$.

Def The number n is the dimension of V.