Vector Spaces §30

Ex $\mathbb{R}[x]/\langle x^2+1\rangle$ is a simple extension of $\mathbb{R}$.

Let $\alpha = x + \langle x^2+1\rangle \in \mathbb{R}[x]/\langle x^2+1\rangle$.

$\mathrm{irr}(\alpha,\mathbb{R}) = x^2+1$

$\deg(\alpha,\mathbb{R}) = 2$

By Thm 29.18 $\forall\ \beta \in \mathbb{R}(\alpha) = E$ is written uniquely as $a + b\alpha \quad a,b \in \mathbb{R}$

$\alpha^2 + 1 = 0$ in E $\qquad \alpha^2 = -1$ in E

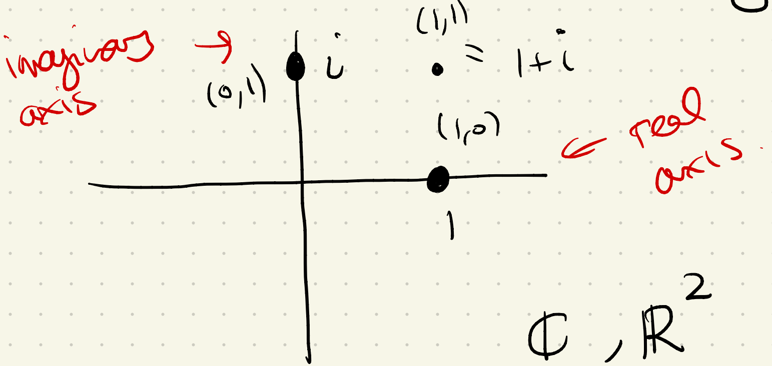
$$(a+b\alpha)(c+d\alpha)$$
$$= (ac - bd) + (bc+ad)\alpha$$

Try: $(a+bi)(c+di)$
$$= (ac-bd) + (bc+ad)i$$
in $\mathbb{C}$

Addition $(a+b\alpha) + (c+d\alpha)$
$$= (a+c) + (b+d)\alpha$$

$\Rightarrow \mathbb{R}(\alpha) \cong \dfrac{\mathbb{R}[x]}{\langle x^2+1\rangle}$ is isomorphic to $\mathbb{C}$

We are used to drawing $\mathbb{C}$ as a vector space $/\mathbb{R}$



$\cong \mathbb{R}(\alpha) = \mathbb{R}(i)$

$\{1, i\}$

$\mathbb{C}, \mathbb{R}^2$

We will generalise this for all simple extensions

<u>Goal</u> View $F(\alpha)$ as a "vector space" over F.

Recall $\forall$ element $\beta \in F(\alpha)$ can be uniquely written as

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

when $\deg(\alpha, F) = n$.

Book keeping Keep track of coefficients b_i as entries of a vector: $(b_0, b_1, \dots, b_{n-1}) \in F^n$

$\quad 1 \quad 2 \quad \dots \quad n$

If $F = \mathbb{R}, \mathbb{Q}, \mathbb{C}$, we know we can add vectors, multiply by scalars, $\Rightarrow$ linear combinations, independence, bases.

Main Example of a vector space

over F

F a field, $V = F^n$ is a vector space of dim n

$\alpha = (b_0, \ldots, b_{n-1})$

$\beta = (c_0, \ldots, c_{n-1})$

$b_i, c_i \in F$

$a \in F$

$\alpha + \beta = (b_0 + c_0, \ldots, b_{n-1} + c_{n-1})$

$a\alpha = (ab_0, \ldots, ab_{n-1})$ "scalar multipli"

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

Def 30.1. A vector space V over F is an abelian group with an operation of scalar multiplication satisfying 5 axioms See Def 30.1.

Ex $F = \mathbb{Z}_2$. $\alpha \in V = F^3$

$|V| = 2^3$

$(0,0,0)$

$(1,0,1) + (1,1,0) = (0,1,1)$

$$\underbrace{(1,0,1) + (1,1,0) + (0,1,1)}_{\text{linearly dependent}} = (0,0,0)$$

Main Theorem for vector spaces & field extensions

<u>Thm 30.23</u> Let $E \supseteq F$ and suppose $\alpha \in E$ is alg. $/F$

If $\deg(\alpha, F) = n$ then $F(\alpha)$ is an n-dim'l vector space over F with basis $\{1, \alpha, \ldots, \alpha^{n-1}\}$

Also every elt β of $F(\alpha)$ is algebraic $/F$ and $\deg(\beta, F) \leq \deg(\alpha, F)$.

<u>Recall</u> $\{\beta_1, \ldots, \beta_n\} \subseteq V$ is a basis for V over F if they span V and are linearly independent

$\overset{\parallel}{}$ $V = \{a_1\beta_1 + \cdots + a_n\beta_n \mid a_i \in F\}$

$\overset{\parallel}{}$ If $a_1\beta_1 + \cdots + a_n\beta_n = 0 \Longrightarrow a_i = 0 \ \forall i$

Proof

$$\begin{array}{ccc} F(\alpha) & \ni & b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1} \\ \downarrow & & \downarrow \\ F^n & \ni & (b_0, \ldots, b_{n-1}) \end{array}$$

addition + scalar mult behave as for vectors!

Notice
$1 \mapsto$
$\alpha \mapsto$
$\vdots$
$\alpha^{n-1} \mapsto$

Second statement: $\beta \in F(\alpha)$ consider $1, \beta, \ldots, \beta^n$.

Fact from linear alg: $n+1$ vectors in n-dim'l vector space must be linearly dependent (Thm 30.19)

Exam Problem 2020

$F = \underset{\{0,1,2\}}{\overset{\|}{\mathbb{Z}_3}}$ $\qquad f(x) = x^3 + 2x + 1 \in F[x]$.

a) Explain why $K = F[x]/\langle x^3+2x+1\rangle$ is a field.

$\langle x^3 + 2x + 1\rangle = \{ f(x) \cdot (x^3+2x+1) \mid f(x) \in F[x] \}$.

R/N is a field $\iff$ N is max ideal of R.

R comm ring w/ unity

When $R = F[x]$ $\langle f(x)\rangle$ is maximal
$\iff$ $f(x)$ is irreducible.

Claim: $f(x)$ is irreducible

If not $f(x) = g(x)h(x)$ with $\deg g = 2$ $\deg h = 1$
$g(x), h(x) \in F[x]$

$\Rightarrow$ and $f(x)$ must have a zero in F

<u>Check</u>: $f(0) = 1 \neq 0$ $f(1) = 1+2+1 = 1 \neq 0$
$f(2) = 8+4+1 = 1 \neq 0$.

Since $f(x)$ has no zero in F $f(x)$ is irred.

Therefore K is a field.

b) $K = F(\alpha)$ where $\alpha = x + \langle x^3 + 2x + 1 \rangle$

use α to write a basis of K over F

Express α^6 and α^4 in this basis.

From today's theorem $F(\alpha)$ is a vector space of dim 3 over F with basis $\{1, \alpha, \alpha^2\}$.

$\alpha^3 + 2\alpha + 1 = 0$ in $F(\alpha)$

$\Rightarrow \alpha^3 = \alpha + 2$

$$\alpha^4 = \alpha \cdot \alpha^3 = \alpha(\alpha + 2) = \alpha^2 + 2\alpha$$

$$\alpha^6 = \alpha^3 \cdot \alpha^3 = (\alpha+2)(\alpha+2) = \alpha^2 + 4\alpha + 4 = \alpha^2 + \alpha + 1$$

c) Find a monic polynomial of deg 3 $g(x)$ in $F[x]$ s.t. α^2 is a zero of $g(x)$.

d) Show $f(1+\alpha)=0$ and $f(2+\alpha)=0$

Conclude K is <u>splitting field</u> of K over F.