**Wednesday, November 28**

**Vector Space**

**Def.** Let $F$ be a field. A vector space over $F$ is:

- an abelian group $V$, written additively, together with
- a function $F \times V \to V$, written $(a, \alpha) \mapsto a\alpha \ (a \in F, \alpha \in V)$

that satisfies:

$V_1: \alpha \in V \quad$ (redundant)

$V_2: a(b\alpha) = (ab)\alpha \quad \forall a, b \in F$

$V_3: (a+b)\alpha = a\alpha + b\alpha \quad \forall \alpha \in V$

$V_4: a(a+b) = a\alpha + a\beta \quad \forall \alpha, \beta \in V$

$V_5: 1\alpha = \alpha$

(Why is $V_5$ needed?) Otherwise we could have $a\alpha = 0 \quad \forall \alpha, a$.  

Here: **Vectors** are the elements of $V$.  

**Scalars** are the elements of $F$.  

and $F \times V \to V$ is scalar multiplication.

**Examples:***

1. $F = \mathbb{R}$, $V = \mathbb{R}^n$
2. $F$ is any field, $V = F^n$
3. $F$ is any field, $V = F[x]$
4. $F = \mathbb{R}$, $V = \{\text{continuous functions} \mid \mathbb{R} \to \mathbb{R}\}$  
5. $F = \mathbb{R}$, $V = \{\text{C}^\infty \text{ functions} \mid \mathbb{R} \to \mathbb{R}\}$  

Important for us -> $0\alpha = 0, \quad 0\alpha = 0$, and $(-a)\alpha = a(-\alpha) = -a\alpha \quad \forall a \in F, \alpha \in V$

These could be $V_6$, $V_7$, and $V_8$, except that they can be proved from $V_5 + V_5$ (Thm. 30.5).

**Def:** Linear combination $a_1\alpha_1 + a_2\alpha_2 + \ldots + a_n\alpha_n$ of $\alpha_1, \ldots, \alpha_n \in V$

(with weights $a_1, \ldots, a_n \in \mathbb{R}$)

- Span (of a subset of $V$),  
- Linear dependence/independence  
- Basis

are all as in Math 54.
Also: Gaussian elimination works.

**Def.** $\dim V$ is as in Math 54:

1. Any two finite bases of a vector space have the same number of elements.
2. If one basis of a given vector space $V$ is finite, then all bases of $V$ are finite.
3. Every vector space has a basis.

**Def.** A vector space $V$ is **finite dimensional** if

- it can be spanned by a finite set, or
- $\dim V < \infty$ (Math 54)

These conditions are equivalent.

**Note (not in book):** A **linear transformation** $T: V \rightarrow W$ of vector spaces over $F$ is a function $T: V \rightarrow W$ such that:

1. $T(\alpha + \beta) = T(\alpha) + T(\beta)$ \hspace{1cm} $\forall \alpha, \beta \in V$ and \hspace{1cm} homomorphism of abelian groups.
2. $T(a\alpha) = aT(\alpha)$ \hspace{1cm} $\forall a \in F$, $\alpha \in V$

This plays the role of homomorphism of vector spaces over $F$:

- it "plays nice" with the algebraic structures of $V$ and $W$.
- An **isomorphism** of $F$-vector spaces is a bijective linear transformation.

**Last time:** Let $E/F$ be a field extension and let $\alpha \in E$.

Assume that $\alpha$ is algebraic over $F$. Let $f = \text{irr}(\alpha, F) \in F[x]$ and let $n = \deg(\alpha, F) = \deg f$.

We showed that every element $\beta \in F(\alpha)$ can be written uniquely in the form

$$\beta = a_n \alpha^n + a_{n-1} \alpha^{n-1} + \cdots + a_1 \alpha + a_0$$

with $a_0, \ldots, a_{n-1} \in F$.

Recall that $E$ is a vector space over $F$.

Then $F(\alpha)$ is a linear subspace of $E$, and
\[ \{1, x, x^2, \ldots, x^{n-1}\} \text{ spans } F(x) \] (by existence of \(a_0, \ldots, a_n\))

and also \(\{1, x, \ldots, x^{n-1}\}\) is linearly independent \(\text{(over } F)\)

(by uniqueness of \(a_0, \ldots, a_n\), specifically for \(\beta = 0\))

\(\{1, x, \ldots, x^{n-1}\}\) is a basis for \(F(x)\).

We've proved:

**Thm**: Let \(E/F\) be a field extension, and let \(x \in E\).

Assume that \(x\) is algebraic over \(F\), and let \(n = \deg(x, F)\).

Then \(F(x)\) is a vector space over \(F\), and \(\{1, x, \ldots, x^{n-1}\}\) is a basis for it.

**Examples**:

- \(\mathbb{Q}(\sqrt{1 + \sqrt{3}})\) \quad \text{irr}(\sqrt{1 + \sqrt{3}}, \mathbb{Q}) = 2

- \(\mathbb{Q}(\sqrt{3})\) \quad \text{irr}(\sqrt{3}, \mathbb{Q}) = x^2 - 3 \quad \text{(because } x^2 - 3 \text{ is irreducible)}

Also \(\mathbb{Q}(\sqrt{1 + \sqrt{3}}) \supseteq \mathbb{Q}(\sqrt{3})\) because \(\mathbb{Q}(\sqrt{1 + \sqrt{3}}) \supseteq \mathbb{Q}(\sqrt{3})\) and \(\sqrt{1 + \sqrt{3}}\)

and \(\mathbb{Q}(\sqrt{3})(\sqrt{1 + \sqrt{3}}) = \mathbb{Q}(\sqrt{1 + \sqrt{3}}, \sqrt{3}) \quad \text{(true)}.

and \(\deg(\sqrt{1 + \sqrt{3}}, \mathbb{Q}(\sqrt{3})) = 2 \quad \text{because } \sqrt{1 + \sqrt{3}} \in \mathbb{Q}(\sqrt{3})\).

Also \(\deg(\sqrt{1 + \sqrt{3}}, \mathbb{Q}(\sqrt{3})) = 2 \quad \text{because } \sqrt{1 + \sqrt{3}} \in \mathbb{Q}(\sqrt{3})\).

\(\text{def:}\) Let \(E/F\) be a field extension.

Then the degree \((d)\) is finite dimensional \((\text{as a vector space over } F)\) \(\text{degree of } E \text{ over } F \text{ is } d\).

\(\deg(\sqrt{1 + \sqrt{3}}, \mathbb{Q}(\sqrt{3})) = 2 \quad \text{because } \sqrt{1 + \sqrt{3}} \in \mathbb{Q}(\sqrt{3})\).

\(\deg(\sqrt{1 + \sqrt{3}}, \mathbb{Q}(\sqrt{3})) = 2 \quad \text{by definition of degree.}\)
Example: \[ [F(x):F] = n \quad \text{if } \deg x \text{ is algebraic over } F \] and \( \deg (\alpha_1 F) = n \).

\[ [C:R] = 2 \quad C = R(i), \]
\[ [R:Q] = \infty \quad (I \text{ won't prove}) \]

Notes: \( [E:F] = 1 \quad \Rightarrow \quad E = F \quad (E/F \text{ is a field extension}). \)

\( \leq \quad \Rightarrow \quad \{i\} \text{ is a basis.} \)

\( \Rightarrow \quad \{i\} \text{ is linearly independent, } \Rightarrow \text{so it's a basis,} \)

Previous examples:

\[ \mathbb{Q}(j) \]
\[ \mathbb{Q}((-\sqrt{3}) \]
\[ \mathbb{Q}(\sqrt{3}) \]
\[ \mathbb{Q}(\sqrt{5}) \]

Definition: A field extension \( E/F \) is:

- algebraic if all \( \alpha \in E \) are algebraic over \( F \), and
- finite if \( [E:F] < \infty \).

Theorem: If \( E/F \) is algebraic, then it's finite. (as a v.s.)

Proof: Assume \( E/F \) is finite. Let \( n = [E:F] = \dim_E \) over \( F \)

Let \( \alpha \in E \). Then \( 1, \alpha, \alpha^2, \ldots, \alpha^n \) are \( n+1 \) elements of \( E \), so they must be linearly dependent:

\[ a_n \alpha^n + a_{n-1} \alpha^{n-1} + \ldots + a_0 = 0 \]

with \( a_i \in F \forall i \), not all \( a_i = 0 \).

Then \( a_n \alpha^n + a_{n-1} \alpha^{n-1} + \ldots + a_0 \in F[x] \) is a nonzero polynomial that vanishes at \( \alpha = \alpha \). So \( \alpha \) is algebraic over \( F \).

(This also shows: \( \deg (\alpha_1 F) \leq n \))

(We know this, because \( \deg (\alpha F) = \dim F(\alpha) \leq \dim E = n \))

\( F(\alpha) \text{ is a subspace of } E \).
Theorem. Let $K/E/F$ be a tower of field extensions. Then

$$[K:F] = [K:E][E:F]$$

(in the sense that if the RHS is finite, then so is the LHS, and conversely).

Proof. Assume that the RHS is finite. Let $\alpha_1, \ldots, \alpha_n$ be a basis for $E$ over $F$ and $\beta_1, \ldots, \beta_m$ a basis for $K$ over $E$. Let $S = \{\alpha_i \beta_j : i=1, \ldots, n; j=1, \ldots, m\}$, note $|S| = mn < \infty$.

Claim: $S$ spans $K$ (as a v.s. over $F$).