Math 4030-001/Foundations of Algebra/Fall 2017

Linear Algebra at the Foundations: Number Fields

Definition 12.1 A **vector space** consists of the following:

(i) A field F of scalars (e.g. $F = \mathbb{R}$ or $\mathbb{Q}$)

(ii) A set V of vectors with vector addition and scalar multiplication:

$$v + w \in V \text{ and } cv \in V \text{ for } v, w \in V \text{ and } c \in F$$

satisfying the following rules:

• Vector addition is commutative and associative, with an additive identity vector 0 and additive inverses $-v$ of each v.

• Scalar multiplication distributes with vector addition:

$$c(v + w) = cv + cw \text{ and } (c + d)v = cv + dv$$

• Scalar multiplication satisfies:

$$1 \cdot v = v \text{ and } c(dv) = (c\dot{d})v \text{ for all } c, d \in F$$

Examples. (a) The set of ordered n-tuples $(c_1, ..., c_n)$ of elements of a field F with coordinate addition and scalar multiplication:

$$(c_1, ..., c_n) + (d_1, ..., d_n) = (c_1 + d_1, ..., c_n + d_n)$$

$$c(d_1, ..., d_n) = (cd_1, ..., cd_n)$$

is the vector space F^n.

(b) The polynomials with coefficients in F:

$$F[x] = \{f(x) = c_d x^d + \cdots + c_0\}$$

are a vector space with scalar field F.

Definition 12.2. Vectors $v_1, ..., v_n \in V$ in a vector space:

• are **linearly independent** if:

$$c_1 v_1 + \cdots + c_n v_n = 0 \ \Leftrightarrow 0 = c_1 = c_2 = \cdots = c_n \in F$$

• **span** V if $(\forall v \in V)(\exists c_1, ..., c_n \in F)\ c_1 v_1 + \cdots c_n v_n = v$.

i.e. every vector in V is a linear combination of $v_1, ..., v_n$.

• are a **basis** if they are both linearly independent and span V .

Observation. If $v_1, ..., v_n$ are a basis and $v \in V$, then if:

$$c_1 v_1 + \cdots c_n v_n = v = d_1 v_1 + \cdots d_n v_n$$

it follows that $(c_1 - d_1)v_1 + \cdots + (c_n - d_n)v_n = 0$ so $c_i = d_i$ for all i. Thus $v_1, ..., v_n \in V$ is a basis if and only if each $v \in V$ is a **unique** linear combination of $v_1, ..., v_n$.

Theorem/Definition 12.3. Any two bases of a vector space have the same number of elements. This number is the **dimension** of V.

Proof. If $w_1, ..., w_m$ and $v_1, ..., v_n$ are bases of V and $m < n$, then:

$$c_{1,1}w_1 + \cdots + c_{1,m}w_m = v_1$$

$$\vdots$$

$$c_{m,1}w_1 + \cdots + c_{m,m}w_m = v_m$$

This is a system of m independent equations (because the vectors $v_1, ..., v_m$ are linearly independent), so it can be inverted, to solve:

$$d_{1,1}v_1 + \cdots + d_{1,m}v_m = w_1$$

$$\vdots$$

$$d_{m,1}v_1 + \cdots + d_{m,m}v_m = w_m$$

and then, as a result, v_{m+1} is a linear combination of $w_1, ..., w_m$ (because $w_1, ..., w_m$ span), hence v_{m+1} is a linear combination of $v_1, ..., v_m$, which is a contradiction. So $m \geq n$ and also $n \geq m$ by the same argument. $\square$

Example. The vectors $e_1 = (1, 0, ..., 0), e_2 = (0, 1, ..., 0)$, etc are the *standard* basis for the vector space F^n.

Main Example. Declare that r is to be a root of a prime polynomial $p(x) = x^d + ... + c_1x + c_0 \in \mathbb{Q}[x]$. Then:

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

is the vector space of polynomials evaluated at r.

By definition, $r^d + c_{d-1}r^{d-1} + \cdots + c_0 = 0$ which gives:

$$r^d = -c_{d-1}r^{d-1} - \cdots - c_0$$

and so every occurance of r^d in each $f(r)$ can be replaced with lower powers of r until finally $f(r)$ is a linear combination of $1, r, r^2, ..., r^{d-1}$. Thus these vectors span $\mathbb{Q}[r]$. If

$$a_0 \cdot 1 + a_1 \cdot r + \cdots a_{d-1}r^{d-1} = 0$$

for some $a_0, ..., a_{d-1} \in \mathbb{Q}$, then r is also a root of the polynomial:

$$f(x) = a_{d-1}x^{d-1} + \cdots + a_0$$

and then $\gcd(f(x), p(x)) \neq 1$, which can only happen if $f(x) = 0$, since otherwise $p(x)$ is prime and $f(x)$ is a polynomial of smaller degree sharing a common factor. Thus the $1, r, ..., r^d$ are linearly independent. So they are a basis of $\mathbb{Q}[r]$.

Examples. (a) $\mathbb{Q}[i]$ is the vector space of Gaussian rational numbers. Each $f(i)$ is a linear combination of 1 and i since:

$$i^2 = -1,\ i^3 = -i,\ i^4 = 1, \text{etc.}$$

(b) The vector space $\mathbb{Q}[\sqrt[3]{2}]$ has basis $1, \sqrt[3]{2}, \sqrt[3]{4}$. Each $f(\sqrt[3]{2})$ is a linear combination of these vectors since:

$$(\sqrt[3]{2})^3 = 2,\ (\sqrt[3]{2})^4 = 2\sqrt[3]{2},\ (\sqrt[3]{2})^5 = 2\sqrt[3]{4},\ \text{etc.}$$

Let r be a root of a prime polynomial $p(x) \in \mathbb{Q}[x]$ of degree d. Then:

Proposition 12.3. $\mathbb{Q}[r]$ is a field. These are the **number fields**.

Proof. Multiply elements of $\mathbb{Q}[r]$ as polynomials:

$$f(r) \cdot g(r) = (f \cdot g)(r)$$

Since $\mathbb{Q}[x]$ is a commutative ring, the same product (and sum) makes $\mathbb{Q}[r]$ also a commutative ring, so it satisfies all the properties of a field except for the existence of multiplicative inverses of nonzero elements. Let $v = a_{d-1}r^{d-1} + \cdots + a_0$ and set $f(x) = a_{d-1}x^{d-1} + \cdots + a_0$. Because $\gcd(f(x), p(x)) = 1$, it follows that $a(x)f(x) + b(x)p(x) = 1$ can be solved with Euclid's algorithm, and:

$$a(r)f(r) + b(r)p(r) = 1$$

But $p(r) = 0$ by assumption, so $a(r)f(r) = 1$. Thus $a(r) = 1/v$. □

Multiplication Tables. We can create multiplication tables for the products of basis vectors in $\mathbb{Q}[r]$. This is all the information we need to compute all products of elements of $\mathbb{Q}[r]$ by the distributive law.

Examples. (a) $p(x) = x^2 + 1$ and i is the imaginary declared root.

$\cdot$	1	i
1	1	i
i	i	-1

$$(a + bi)(c + di) = ac + bci + adi + bd(-1) = (ac - bd) + (bc + ad)i$$

(b) $p(x) = x^2 - x - 1$ and r is the declared root.

$\cdot$	1	r
1	1	r
r	r	$r + 1$

$$\begin{aligned}(a + br)(c + dr) &= ac + bcr + adr + bd(r + 1)\\ &= (ac + bd) + (bc + ad + bd)r\end{aligned}$$

(c) $p(x) = x^3 - x^2 - 1$ and r is the declared root.

$\cdot$	1	r	r^2
1	1	r	r^2
r	r	r^2	r^2+1
r^2	r^2	r^2+1	r^2+r+1

Linear algebra comes into play when we regard multiplication by v:

$$A(w) = v \cdot w$$

as a linear map from $\mathbb{Q}[r]$ to itself. This means it has a matrix, and the **inverse matrix** will give multiplication by the inverse vector, since:

$$\frac{1}{v} \cdot (v \cdot w) = w \text{ and } A^{-1}(A(w)) = w$$

Recall that the columns of A are:

$$v \cdot 1, v \cdot r, v \cdot r^2, ...$$

so in particular, the first column of A^{-1} will be the inverse vector $1/v$. Let's work this out in the examples:

(a) $p(x) = x^2 + 1$ and $v = a + bi$. (This should look familiar!)

$$A = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}, \ A^{-1} = \frac{1}{a^2+b^2}\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$$

$$\frac{1}{v} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i$$

(b) $p(x) = x^2 - x - 1$ and $v = a + br$.

$$A = \begin{bmatrix} a & b \\ b & a+b \end{bmatrix}, \ A^{-1} = \frac{1}{a^2+ab-b^2}\begin{bmatrix} a+b & -b \\ -b & a \end{bmatrix}$$

$$\frac{1}{v} = \frac{a+b}{a^2+ab-b^2} - \frac{b}{a^2+ab-b^2}r$$

As an example, apply the formula to

$$v = -1 + 2r \ \text{ to get } \ \frac{1}{v} = -\frac{1}{5} + \frac{2}{5}r = \frac{v}{5}$$

In other words, $v^2 = 5$ and $v = \pm\sqrt{5}$. This checks with the quadratic formula applied to $p(x)$, which gives:

$$r = \frac{1 \pm \sqrt{5}}{2}$$

(c) $p(x) = x^3 - x^2 - 1$ and $v = a + br + cr^2$.

$$A = \begin{bmatrix} a & c & b+c \\ b & a & c \\ c & b+c & a+b+c \end{bmatrix}$$

(d) If $p(x) = x^d + c_{d-1}x^{d-1} + ... + c_0$ and $v = r$, then:

$$A = \begin{bmatrix} 0 & 0 & \cdots & 0 & -c_0 \\ 1 & 0 & \cdots & 0 & -c_1 \\ 0 & 1 & \cdots & 0 & -c_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -c_{d-1} \end{bmatrix}$$

The Characteristic Polynomial of a matrix A is the determinant:

$$f(x) = \det(xI - A); \ I = \text{ identity matrix}$$

The roots of $f(x)$ are the *eigenvalues* of A.

This is significant since the determinant of a square matrix B is zero if and only if the columns of B are linearly dependent, if and only if there is a non-zero vector $w \in V$ such that:

$$B(w) = 0$$

But if $B = \lambda I - A$ and $\det(B) = 0$, then $B(w) = 0$ gives $A(w) = \lambda w$. Thus the roots of the characteristic polynomial of A are the values of λ for which there is an (eigen)vector $w \in V$ with $A(w) = \lambda w$, and the "stretch factor" λ is the **eigenvalue** of the eigenvector w. A consequence of the fundamental theorem of algebra is the fact that every square matrix of complex numbers has a complex eigenvalue.

Examples. (a) $p(x) = x^2 + c_1x + c_0$ and $v = r$.

$$\begin{bmatrix} x & 0 \\ 0 & x \end{bmatrix} - \begin{bmatrix} 0 & -c_1 \\ 1 & -c_1 \end{bmatrix} = \begin{bmatrix} x & c_0 \\ -1 & x + c_1 \end{bmatrix}$$

and the characteristic polynomial is:

$$f(x) = x(x + c_1) + c_0 = x^2 + c_1x + c_0$$

which means that r is an eigenvalue for multiplication by r.

(b) $p(x) = x^2 + 1$ and $v = a + bi$.

$$\begin{bmatrix} x & 0 \\ 0 & x \end{bmatrix} - \begin{bmatrix} a & -b \\ b & a \end{bmatrix} = \begin{bmatrix} x - a & b \\ -b & x - a \end{bmatrix}$$

and the characteristic polynomial is: $f(x) = (x - a)^2 + b^2$ and once again $a + bi$ is an eigenvalue for multiplication by $a + bi$.

For each $v \in \mathbb{Q}[r]$, there is a prime polynomial with v as a root.

Definition 12.4. The **minimal polynomial** of $v \in \mathbb{Q}[r]$ is gotten by:

(i) Considering the powers of v as vectors in V and solving

$$a_0 + a_1 v + a_2 v^2 + \cdots + v^e = 0$$

for the smallest value of e (with non-zero coefficients).

(ii) Replacing the linear combination with the polynomial:

$$g(x) = x^e + a_{e-1}x^{e-1} + \cdots + a_0$$

Example. Consider $r = \sqrt{2} + \sqrt{3}$. Then:

$$(x - (\sqrt{2} + \sqrt{3}))(x + (\sqrt{2} + \sqrt{3})) = x^2 - (\sqrt{2} + \sqrt{3})^2 = x^2 - (5 + 2\sqrt{6})$$

and let

$$p(x) = (x^2 - (5 + 2\sqrt{6}))(x^2 - (5 - 2\sqrt{6})) = x^4 - 10x^2 + 1$$

Then within the (four dimensional) number field $\mathbb{Q}[r]$, we take:

$$v = -5 + r^2 = 2\sqrt{6}$$

which satisfies $-24 + v^2 = 0$, and therefore $g(x) = x^2 - 24$. With some work, the characteristic polynomial of v can also be computed. It is

$$f(x) = (x^2 - 24)^2$$

Proposition 11.5. The characteristic polynomial for multiplication by $v \in \mathbb{Q}[r]$ is always a power of the minimal polynomial.

Proof. If the miminal polynomial $g(x)$ has the same degree as the characteristic polynomial $f(x)$, then they are the same polynomial, since $g(x)$ is prime and they share the factor $x - v$. Otherwise, let:

$$\mathbb{Q}[v] \subset \mathbb{Q}[r]$$

be the sub-field with root v and $p(x) = g(x)$. If:

$$1, v, ..., v^{e-1} \text{ are a basis for } \mathbb{Q}[v]$$

we may find additional vectors $w_1, ..., w_{d/e}$ so that:

$$\{w_i, w_i v, ..., w_i v^{e-1} \mid 1 \leq i \leq d/e\} \text{ is a basis for } \mathbb{Q}[r]$$

and with this basis, the matrix for multiplication by v consists of d/e blocks of the matrix for multiplication by v, giving the result. □

Warning. The "eigenvectors" for multiplication by v in $\mathbb{Q}[r]$ are not actually vectors in $\mathbb{Q}[r]$ because their coefficients use the root r. For example, the eigenvectors for multiplication by $a + bi \in \mathbb{Q}[i]$ are:

$$(1, i) \text{ (eigenvalue } a + bi) \quad \text{and} \quad (1, -i) \text{ (eigenvalue } a - bi)$$

Exercises. 11.1. Prove from the definition of a vector space that:

(a) The zero vector is uniquely determined.

(b) Scalar multiplication by 0 gives the zero vector.

(c) Scalar multiplication by -1 gives the additive inverse vector.

11.2. (a) Find the eigenvalues for the matrix:

$$\begin{bmatrix} \cos(\theta) & \sin(\theta) \\ \sin(\theta) & -\cos(\theta) \end{bmatrix}$$

and conclude that this is the matrix for a reflection of the plane.

(b) Find eigenvectors for this reflection and draw them.

11.3. Let $p(x) = x^2 - 2$. Then:

(a) Find the multiplication table for $\mathbb{Q}[r]$.

(b) Find the matrix for multiplication by $v = a + br$

(c) Find $1/v$.

11.4. Do the same for the prime polynomial $p(x) = x^2 + x + 1$. Also:

(d) Plug $v = 1 + 2r$ into (c) and comment on the result.

11.5. Find the matrix for multiplication by $1/r$ in $\mathbb{Q}[r]$ for:

$$p(x) = x^3 + c_2x^2 + c_1x + c_0$$

without inverting the matrix for multiplication by r.

11.6. Find a prime polynomial of degree 4 with root:

$$r = \sqrt{2} + \sqrt{5}$$

and then inside $\mathbb{Q}[r]$ find the minimal polynomial for the vector:

$$v = -27 + r^2$$