Vector Spaces

A vector space \( V \) over a field \( K \) is an abelian group with operation + and an additional operation, called scalar multiplication, that combines an element of \( K \) and an element of \( V \). These operations satisfy, for \( k, l, m \) in \( K \) and \( v, w \) in \( V \),

\[
(k + l)v = kv + lv;
klv = (kl)v; \text{ and }

k(v + w) = kv + kw.
\]

Any expression \( \Sigma k_i v_i \), where the \( k_i \) are in \( K \) and the \( v_i \) are in \( V \), is a linear combination. A set of vectors \( \{v_1, \ldots, v_m\} \) such that every \( V \) is a linear combination of the \( v_i \)s is said to span \( V \), and such a set is linearly independent if whenever a linear combination \( \Sigma k_i v_i \) is zero then all of the coefficients \( k_i \) are zero. A spanning set of independent vectors is called a basis for \( V \), and its cardinality is the dimension of \( V \). All vector spaces in cryptography are finite dimensional.

For example, the set of \( n \)-tuples from \( K \) forms a vector space using component-wise addition and scalar product \( k \cdot (v_1, \ldots, v_n) = (kv_1, \ldots, kv_n) \).

For a more interesting example, let \( K \) be the field of order 2, and consider the set \( V = \{0, 1, \alpha, \alpha + 1\} \). This is a vector space with basis \( \{1, \alpha\} \). It is isomorphic to the set of 2-tuples from \( K \), via, e.g., the map \( (1, 0) \mapsto 1 \) and \( (0, 1) \mapsto \alpha \).

In fact, \( V \) is itself a field. Much of the multiplication table is obvious \( (1 \cdot \alpha = \alpha, \text{ etc.}) \), except for \( \alpha^2 \). The only choice that works to make a field is to define \( \alpha^2 = \alpha + 1 \). This means that \( (\alpha + 1)^2 = \alpha^2 + 2\alpha + 1 = \alpha \).

If \( \alpha^2 = \alpha + 1 \), then \( \alpha \) is a root of the polynomial \( p(x) = x^2 + x + 1 \). It is easy to check that this polynomial has no roots in \( K \), which makes it irreducible. In fact, its two roots are \( \alpha \) and \( \alpha + 1 \).

Every vector space of dimension \( n \) is isomorphic to the vector space of \( n \)-tuples.

Linear Algebra

You should note that linear algebra, that is, matrix arithmetic, is exactly the same in a finite field. In particular, a linear transformation from a vector space of dimension \( n \) to itself is given by an \( n \times n \) matrix, and its values everywhere are determined by its values on a basis.

Rijndael uses several linear transformations.
Finite Fields, again

Every finite field is a vector space over the prime field, because the vector space operations are, in fact, field operations. Suppose that $K \subset L$ are finite fields, where $K$ has prime order, and let $\alpha$ be an element of $L$ not in $K$. Construct the sequence $\alpha, \alpha^2, \alpha^3, \ldots$. Since $L$ is finite, this sequence must repeat, so there is an $n$ such that $\alpha^n = 1$. Then $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ forms a basis for $L$ as a vector space over $K$. But, $\alpha^n$ is in $L$, so there are coefficients $k_i$ such that $\alpha^n = \Sigma k_i \alpha^i$. This leads to a polynomial $\alpha^n - k_{n-1} \alpha^{n-1} - \cdots - k_1 \alpha - k_0$.

In the example when $L$ had order 4, the polynomial was $x^2 + x + 1$. Rijndael uses the polynomial $R(x) = x^8 + x^4 + x^3 + x + 1$, implying that $x^8 = x^4 + x^3 + x + 1$. (keep in mind that in $GF(2)$ $x + y$ is the same as $x - y$.)

A good example is the product $(x^5 + x^4 + x)(x^4 + x^2 + 1)$ in the Rijndael Field. First, use ordinary algebra to get

$$
(x^9 + x^7 + x^5) + (x^8 + x^6 + x^4) + (x^5 + x^3 + x) = x^9 + x^8 + x^7 + x^6 + x^4 + x^3 + x
$$

$$
= (x^5 + x^4 + x^2 + x) + (x^4 + x^3 + x + 1) + x^7 + x^6 + x^4 + x^3 + x
$$

$$
= x^7 + x^6 + x^4 + x^2 + x + 1
$$

The arithmetic here is taken mod $R(x)$, in the same sense that arithmetic in $\mathbb{Z}/p\mathbb{Z}$ is taken mod $p$.

The field is a vector space of $GF(2)$ with basis $1, \theta, \theta^2, \ldots, \theta^7$, where $R(\theta) = 0$. It is called the Rijndael element.

Inverses

Every non-zero element $k$ of a field $K$ is invertible, that is, there is an element $l \in K$ such that $lk = 1$. Inverses are easy to find in small fields by a search of the multiplication table. For example, in the field $GF(4)$ with 4 elements with basis $1, \alpha$ over $GF(2)$, $\alpha(\alpha + 1) = \alpha^2 + \alpha = 1$, so $\alpha^{-1} = 1 + \alpha$.

There is an easier way to construct an inverse, using the extended Euclidean Algorithm. Recall that in the integer case, the input is two integers $n > m$ and the output is three integers $x, y, d$ such that $d = \gcd (n, m)$ and there are integers $nx + my = d$. The same works with polynomials, except that we consider the degree when making comparisons; it is still the case for polynomials $n(x)$ and $m(x)$ that there are unique $q(x)$ and $r(x)$ such that $n(x) = m(x)q(x) + r(x)$ and the degree of $r$ is less than the degree of $m$.

The first case is in $\mathbb{Z}/p\mathbb{Z}$. If $n \neq 0$ is in $\mathbb{Z}/p\mathbb{Z}$, then $\gcd (n, p) = 1$, and there are integers $x$ and $y$ such that $nx + yp = 1$. This means that $p$ divides $nx - 1$, so $nx - 1 \equiv 0$, i.e., $nx = 1$. 

2
For example, find the inverse of 11 in \( \mathbb{Z}/29\mathbb{Z} \), using the extended Euclidean algorithm. The triples are

\[
(1, 0, 29) \quad \text{and} \quad (0, 1, 11) \quad \text{which become} \\
(0, 1, 11) \quad \text{and} \quad (1, -2, 7) \quad [29 = 2 \cdot 11 + 7] \\
(1, -2, 7) \quad \text{and} \quad (-1, 3, 4) \quad [11 = 1 \cdot 7 + 4] \\
(-1, 3, 4) \quad \text{and} \quad (2, -5, 3) \quad [7 = 1 \cdot 4 + 3] \\
(2, -5, 3) \quad \text{and} \quad (-3, 8, 1) \quad [4 = 1 \cdot 3 + 1] 
\]

Verify that \((-3) \cdot 29 + 8 \cdot 11 = 1\). Thus, \(11^{-1} = 8\) in \( \mathbb{Z}/29\mathbb{Z} \), because \(8 \cdot 11 \equiv 1(29)\).

**Inverting Field Elements**

The same algorithm works to invert elements in \( GF(p^n) \). Consider the field of order 8 defined using arithmetic mod \( x^3 + x^1 \) over \( GF(2) \). The Euclidean algorithm depends on long division.

To find the inverse of \( x \), use triples again as above. The initial pair is \((1, 0, x^3 + x + 1)\) and \((0, 1, x)\). Doing long division, \((x^3 + x + 1)/x\) is \(x^2 + 1\) with remainder 1. The next set of triples is then

\[
(0, 1, x) \quad \text{and} \quad (1, 0x^3 + x + 1) - (x^2 + 1)(0, 1, x) \quad \text{or} \\
(0, 1, x) \quad \text{and} \quad (1, x^2 + 1, 1) 
\]

In other words, \(1 \cdot (x^3 + x + 1) + (x^2 + 1)(x) = 1\), and the inverse of \(x\) is \(x^2 + 1\) (mod \(x^3 + x + 1\)).

It is unusual to have the algorithm terminate after one step; more typical is the case of \((x^2 + x + 1)^{-1}\) in the same field. Long division shows that \(x^3 + x + 1 = x(x^2 + x + 1) + x^2 + 1\). The first few triples are

\[
(1, 0, x^3 + x + 1) \quad \text{and} \quad (0, 1, x^2 + x + 1) \\
(0, 1, x^2 + x + 1) \quad \text{and} \quad (1, x, x^2 + 1) \\
(1, x, x^2 + 1) \quad \text{and} \quad (-1, 1 - x, x) \\
(-1, 1 - x, x) \quad \text{and} \quad (1 + x, x^2, 1) 
\]

This shows that \((1 + x)(x^3 + x + 1) + x^2(x^2 + x + 1) = 1\), and the inverse of \(x^2 + x + 1\) is \(x^2\), as is easily checked.

**Extended Inversion**

Rijndael uses an extended inversion operation \(x^{(-1)}\), which is \(x^{-1}\) when \(x \neq 0\) and 0 when \(x = 0\).

**Exercise**

Find the inverse of 11 in \( \mathbb{Z}/3\mathbb{Z} \). Find the inverse of \(x + 1\) in the field of order 16 with defining polynomial \(x^4 + x + 1\).