Rings

*Definition*: A ring is a set $R$ with binary operations, $+$ and $\cdot$, that satisfy the following axioms:

1. $(R, +)$ is a commutative group (five axioms)
2. Associative law for multiplication: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
3. Distributive laws:
   
   $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$, \hspace{10pt} (Two distributive laws are needed if multiplication is not commutative.)
   
   $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$

Here is an example of an “obvious” property that holds for all rings.

*Proposition*: In any ring, $0 \cdot a = 0$.

*Proof*: By the distributive law,

$$0 \cdot a = (0 + 0) \cdot a = (0 \cdot a) + (0 \cdot a)$$

Subtracting $0 \cdot a$ from both sides of equation yields $0 = 0 \cdot a$. 

EE 387, October 5, 2015
Important rings

Several rings will be used in this course:

- integers \( \mathbb{Z} = \{\ldots, -3, -2, -1, 0, +1, +2, +3, \ldots\} \)
- integers modulo \( m \): \( \mathbb{Z}_m = \{0, 1, \ldots, m - 1\} \)
- polynomials with coefficients from a field:
  \[
  F[x] = \{ f_0 + f_1 x + \cdots + f_n x^n : n \geq 0, f_i \in F \}
  \]
- polynomials over a field modulo a prime polynomial \( p(x) \) of degree \( m \)
- the \( n \times n \) matrices with coefficients from a field

Similarities and differences between the rings of integers and of binary polynomials.

Similarities:

- Elements can be represented by bit strings
- Multiplication by shift-and-add algorithms

Differences:

- Arithmetic for polynomials does not require carries
- Factoring binary polynomials is easy but factoring integers seems hard.
Rings with additional properties

By adding more requirements to rings, we ultimately arrive at fields.

- **Commutative ring**: \(a \cdot b = b \cdot a\).

  The \(2 \times 2\) matrices are a familiar example of a *noncommutative* ring:
  \[
  \begin{bmatrix}
  0 & 0 \\
  1 & 0
  \end{bmatrix}
  \begin{bmatrix}
  0 & 1 \\
  0 & 0
  \end{bmatrix}
  =
  \begin{bmatrix}
  0 & 0 \\
  0 & 1
  \end{bmatrix}
  \neq
  \begin{bmatrix}
  1 & 0 \\
  0 & 0
  \end{bmatrix}
  =
  \begin{bmatrix}
  0 & 1 \\
  0 & 0
  \end{bmatrix}
  \begin{bmatrix}
  0 & 0 \\
  1 & 0
  \end{bmatrix}
  \]

  Some *subrings* of \(2 \times 2\) matrices are commutative. E.g., complex numbers:
  \[
  \begin{bmatrix}
  a & -b \\
  b & a
  \end{bmatrix}
  \begin{bmatrix}
  c & -d \\
  d & c
  \end{bmatrix}
  =
  \begin{bmatrix}
  ac - bd & -ad - bc \\
  ad + bc & ac - bd
  \end{bmatrix}
  =
  \begin{bmatrix}
  c & -d \\
  d & c
  \end{bmatrix}
  \begin{bmatrix}
  a & -b \\
  b & a
  \end{bmatrix}
  \]

- **Ring with identity**: there is an element 1 such that \(1 \cdot a = a \cdot 1 = a\).

  Ring without identity: even integers \(2\mathbb{Z} = \{\ldots, -4, -2, 0, +2, +4, \ldots\}\).

  Fact: if an identity exists, the identity is unique.

  *Proof*: \(1_1 = 1_1 \cdot 1_2 = 1_2\). (Same as proof for groups.)
Inverses and divisors

- **Inverse or reciprocal** of \( a \): an element \( a^{-1} \) with \( a \cdot a^{-1} = a^{-1} \cdot a = 1 \). If it exists, an inverse is unique.

- An element with an inverse is called a **unit**. Units in familiar rings:
  - integers: \( \pm 1 \).
  - polynomials over a field: nonzero constants.
  - matrices over a field: matrices with nonzero determinant
  - matrices with integer coefficients: units are ?

- **Divisor**: if \( c = a \cdot b \) then \( a \) and \( b \) are *divisors* of \( c \).
  - The units in a ring are the divisors of 1.
  - A nonunit \( c \) is *irreducible* if whenever \( c = a \cdot b \) then either \( a \) or \( b \) is a unit.

- **Zero divisor**: if \( a \cdot b = 0 \) but \( a \neq 0 \) and \( b \neq 0 \) then \( a \) and \( b \) are zero divisors.
  - The integers and the polynomials over a field have no zero divisors.
  - A zero divisor does not have an inverse and is therefore not a unit.
Integral domain, division ring, field

- **Integral domain**: a commutative ring without zero divisors. Integral domains have many properties in common with the integers. The integers are a subring of the field of rational numbers:

\[ \mathbb{Q} = \left\{ \frac{p}{q} : p, q \in \mathbb{Z}, q \neq 0 \right\} \]

Similarly, the polynomials are subring of the field of rational functions:

\[ F(x) = \left\{ \frac{p(x)}{q(x)} : p(x), q(x) \in F[x], q(x) \neq 0 \right\} \]

Fact: quotients of elements from any integral domain form a field.

- **Division ring or skew field**: noncommutative ring in which every nonzero element has a multiplicative inverse.

Most famous skew field: Sir William Hamilton’s *quaternions*. These extend the complex numbers obtained by adding imaginary elements, \( j \) and \( k \), such that

\[ i^2 = j^2 = k^2 = ijk = -1. \]

- **Field**: a commutative division ring.
Fields, polynomials, and vector spaces

A field is a set \( F \) with associative and commutative operators + and \( \cdot \) that satisfy the following axioms.

1. \((F, +)\) is a commutative group
2. \((F - \{0\}, \cdot)\) is a commutative group
3. Distributive law: \( a \cdot (b + c) = (a \cdot b) + (a \cdot c) = ab + ac \)

Fields have the 4 basic arithmetic operations: +, \( \times \), and inverses −, \( \div \).

Infinite fields: rational numbers \( \mathbb{Q} \), algebraic numbers, real numbers \( \mathbb{R} \), complex numbers \( \mathbb{C} \), rational functions.

Finite fields (all possible):

- \( \text{GF}(p) = \) integers with arithmetic modulo a prime number \( p \)
- \( \text{GF}(p^m) = \) polynomials over \( \text{GF}(p) \) with arithmetic modulo a prime polynomial of degree \( m \)

An algebraic number is any zero of polynomial with integer coefficients; e.g., \( \sqrt[3]{3} \) or \( (1 + \sqrt{5})/2 \).
The finite field $\mathbf{GF}(p)$

If $p$ is prime, there is one and only one field with $p$ elements:

$$Z_p = \{ 0, 1, 1+1, \ldots, 1+\cdots+1 \} = \{ 0, 1, \ldots, p-1 \}$$

with addition and multiplication mod $p$. This field is named $\mathbf{GF}(p)$.

Associativity and commutativity of addition and multiplication mod $p$ follow from the corresponding properties for integer arithmetic.

The only field axiom that remains to be verified is the existence of multiplicative inverses.

Recall that if $p$ is a prime number and $0 < r < p$, then $\gcd(r, p) = 1$. Since $\gcd(r, p) = ar + bp$ for some integers $a$ and $b$,

$$1 = \gcd(r, p) = ar + bp \implies ar = 1 - bp \equiv 1 \text{ mod } p$$

Thus the reciprocal of $r$ in $\mathbf{GF}(p)$ is $a$ mod $p$. 
Polynomials

The *polynomials over* a field $F$ are $F[x]$, the expressions of the form

$$f_0 + f_1 x + f_2 x^2 + \cdots + f_n x^n, \quad n \in \mathbb{N}, \ f_i \in F$$

$F[x]$ is a commutative ring with identity and no zero divisors, i.e., an integral domain.

Different views of polynomial $f(x)$ with coefficients from a field $F$:

- **Function:** $x \mapsto f_0 + f_1 x + \cdots + f_n x^n$ where $x, f_0, \ldots, f_n$ belong to $F$
- **Finite power series:** $f_0 + f_1 x + \cdots + f_{n-1} x^{n-1} + f_n x^n + 0 x^{n+1} + \cdots$
- **Finite sequence:** $(f_0, f_1, \ldots, f_{n-1}, f_n)$ with coefficients from $F$
- **Infinite sequence, finitely many nonzero terms:** $(f_0, f_1, \ldots, f_n, 0, 0, \ldots)$

The functional view is not adequate for finite fields; there are infinitely many binary polynomials but only $2^2 = 4$ functions from $\{0, 1\}$ to $\{0, 1\}$.

*Example:* nonzero polynomial $x^2 + x$ over $\text{GF}(2)$ evaluates to 0 for $x = 0, 1$, which are the only two elements of $\text{GF}(2)$. 

EE 387, October 5, 2015
Facts about polynomials

Definition: The degree of a polynomial is the exponent of the term with the highest power of the indeterminant.

Well known facts about degrees of polynomials:

► \( \deg(f(x) \pm g(x)) \leq \max(\deg f(x), \deg g(x)) \)

► \( \deg f(x)g(x) = \deg f(x) + \deg g(x) \), since
\[
(f_n x^n + \cdots + f_0)(g_m x^m + \cdots + g_0) = f_n g_m x^{n+m} + \cdots + f_0 g_0
\]

► \( \deg f(x)/g(x) = \deg f(x) - \deg g(x) \) if \( g(x) \neq 0 \)

Because of the convention \( \deg 0 = -\infty \),

\[
\deg f(x)g(x) = \deg f(x) + \deg g(x)
\]

is true even when one of the factors is 0.

By convention, the degree of 0 is \(-\infty\).
Prime polynomials

Definition: A **monic** polynomial is a polynomial with leading coefficient 1.

Example: $x^3 + 2x^2 + 3x + 4$ is monic, $2x^3 + 4x^2 + 6x + 8$ is not.

Every monic polynomial is nonzero.

All nonzero polynomials over GF(2) are monic.

Definition: An **irreducible polynomial** is a polynomial that has no proper divisors (divisors of smaller degree).

Definition: A **prime polynomial** is a monic irreducible polynomial.

Example:

- Over the real numbers, $2x^2 + 1$ is irreducible, but $x^2 + \frac{1}{2}$ is prime.
- Over the complex numbers, $x^2 + \frac{1}{2} = \left(x + \frac{i}{\sqrt{2}}\right)\left(x - \frac{i}{\sqrt{2}}\right)$ is not prime.

Note: irreducibility depends on what coefficients are allowed in the factors.
Divison algorithm for polynomials

For every dividend \( a(x) \in F[x] \) and nonzero divisor \( d(x) \in F[x] \) there is a unique quotient \( q(x) \) and remainder \( r(x) \) such that
\[
a(x) = q(x)d(x) + r(x), \quad \text{where } \deg r(x) < \deg d(x)
\]
Multiples and divisors are defined for polynomials just as for integers.

The greatest common divisor \( \gcd(r(x), s(x)) \) is the monic polynomial

- of largest degree that is a common divisor
- of smallest degree of the form \( a(x)r(x) + b(x)s(x) \)

If \( p(x) \) is prime and \( 0 \leq \deg r(x) < \deg p(x) \), then \( \gcd(r(x), p(x)) = 1 \).
\[
a(x)r(x) + b(x)p(x) = 1 \implies a(x)r(x) \mod p(x) = 1
\]
\[
\implies a(x) = r(x)^{-1} \mod p(x).
\]

Thus \( r(x) \) has a reciprocal.

Polynomials over \( F \) of degree \(< m \) with arithmetic \( \mod p(x) \) form a field.
If \( F \) is \( \text{GF}(p) \), this finite field \( \text{GF}(p^m) \) consists of \( m \)-tuples from \( \text{GF}(p) \).
Finite field $\mathbb{GF}(2^4)$

Over $\mathbb{GF}(2)$, is $x^4 + x + 1$ is prime of degree 4.

Elements of $\mathbb{GF}(2^4)$ can be represented by polynomial expressions or by bit strings (msb first); e.g.,

- $0101 = 1 + x^2$
- $1011 = 1 + x + x^3$
- $1000 = x^3$

Higher powers of $x$ can be reduced using remainder operation:

- $x^4 = x^4 \mod (x^4 + x + 1) = x + 1$
- $x \cdot x^3 = x + 1 \equiv 0010 \cdot 1000 = 0011$

This one equation completely determines multiplication in $\mathbb{GF}(2^4)$ multiplication.

Multiplication table for $\mathbb{GF}(2^4)$

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>A</td>
<td>B</td>
<td>C</td>
<td>D</td>
<td>E</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>6</td>
<td>8</td>
<td>A</td>
<td>C</td>
<td>E</td>
<td>3</td>
<td>1</td>
<td>7</td>
<td>5</td>
<td>B</td>
<td>9</td>
<td>F</td>
<td>D</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>3</td>
<td>6</td>
<td>5</td>
<td>C</td>
<td>F</td>
<td>A</td>
<td>9</td>
<td>B</td>
<td>8</td>
<td>D</td>
<td>E</td>
<td>7</td>
<td>4</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>4</td>
<td>8</td>
<td>C</td>
<td>3</td>
<td>7</td>
<td>B</td>
<td>F</td>
<td>6</td>
<td>2</td>
<td>E</td>
<td>A</td>
<td>5</td>
<td>1</td>
<td>D</td>
<td>9</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>5</td>
<td>A</td>
<td>F</td>
<td>7</td>
<td>2</td>
<td>D</td>
<td>8</td>
<td>E</td>
<td>B</td>
<td>4</td>
<td>1</td>
<td>9</td>
<td>C</td>
<td>3</td>
<td>6</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>6</td>
<td>C</td>
<td>A</td>
<td>B</td>
<td>D</td>
<td>7</td>
<td>1</td>
<td>5</td>
<td>3</td>
<td>9</td>
<td>F</td>
<td>E</td>
<td>8</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>7</td>
<td>0</td>
<td>7</td>
<td>E</td>
<td>9</td>
<td>F</td>
<td>8</td>
<td>1</td>
<td>6</td>
<td>D</td>
<td>A</td>
<td>3</td>
<td>4</td>
<td>2</td>
<td>5</td>
<td>C</td>
<td>B</td>
</tr>
<tr>
<td>8</td>
<td>0</td>
<td>8</td>
<td>3</td>
<td>B</td>
<td>6</td>
<td>E</td>
<td>5</td>
<td>D</td>
<td>C</td>
<td>4</td>
<td>F</td>
<td>7</td>
<td>A</td>
<td>2</td>
<td>9</td>
<td>1</td>
</tr>
<tr>
<td>9</td>
<td>0</td>
<td>9</td>
<td>1</td>
<td>8</td>
<td>2</td>
<td>B</td>
<td>3</td>
<td>A</td>
<td>4</td>
<td>D</td>
<td>5</td>
<td>C</td>
<td>6</td>
<td>F</td>
<td>7</td>
<td>E</td>
</tr>
<tr>
<td>A</td>
<td>0</td>
<td>A</td>
<td>7</td>
<td>D</td>
<td>E</td>
<td>4</td>
<td>9</td>
<td>3</td>
<td>F</td>
<td>5</td>
<td>8</td>
<td>2</td>
<td>1</td>
<td>B</td>
<td>6</td>
<td>C</td>
</tr>
<tr>
<td>B</td>
<td>0</td>
<td>B</td>
<td>5</td>
<td>E</td>
<td>A</td>
<td>1</td>
<td>F</td>
<td>4</td>
<td>7</td>
<td>C</td>
<td>2</td>
<td>9</td>
<td>D</td>
<td>6</td>
<td>8</td>
<td>3</td>
</tr>
<tr>
<td>C</td>
<td>0</td>
<td>C</td>
<td>B</td>
<td>7</td>
<td>5</td>
<td>9</td>
<td>E</td>
<td>2</td>
<td>A</td>
<td>6</td>
<td>1</td>
<td>D</td>
<td>F</td>
<td>3</td>
<td>4</td>
<td>8</td>
</tr>
<tr>
<td>D</td>
<td>0</td>
<td>D</td>
<td>9</td>
<td>4</td>
<td>1</td>
<td>C</td>
<td>8</td>
<td>5</td>
<td>2</td>
<td>F</td>
<td>B</td>
<td>6</td>
<td>3</td>
<td>E</td>
<td>A</td>
<td>7</td>
</tr>
<tr>
<td>E</td>
<td>0</td>
<td>E</td>
<td>F</td>
<td>1</td>
<td>D</td>
<td>3</td>
<td>2</td>
<td>C</td>
<td>9</td>
<td>7</td>
<td>6</td>
<td>8</td>
<td>4</td>
<td>A</td>
<td>B</td>
<td>5</td>
</tr>
<tr>
<td>F</td>
<td>0</td>
<td>F</td>
<td>D</td>
<td>2</td>
<td>9</td>
<td>6</td>
<td>4</td>
<td>B</td>
<td>1</td>
<td>E</td>
<td>C</td>
<td>3</td>
<td>8</td>
<td>7</td>
<td>5</td>
<td>A</td>
</tr>
</tbody>
</table>
Vector spaces

A vector space \( V \) of vectors over a field \( F \) of scalars is a set with a binary operator \( + \) on \( V \) and a scalar-vector product \( \cdot \) satisfying these axioms:

1. \((V,+)\) is a commutative group
2. Associative law: \((a_1 a_2) \cdot v = a_1 \cdot (a_2 \cdot v)\).
3. Distributive laws:
   \[ a \cdot (v_1 + v_2) = a \cdot v_1 + a \cdot v_2, \quad (a_1 + a_2) \cdot v = a_1 \cdot v + a_2 \cdot v \]
4. Unitary law: \( 1 \cdot v = v \) for every vector \( v \) in \( V \)

Recall definition of field: a set \( F \) with associative and commutative operators \( + \) and \( \cdot \) that satisfy the following axioms.

1. \((F,+)\) is a commutative group
2. \((F - \{0\}, \cdot)\) is a commutative group
3. Distributive law: \( a \cdot (b + c) = (a \cdot b) + (a \cdot c) \)

A field is a vector space over itself of dimension 1.

In general, vector spaces do not have vector-vector multiplication. An algebra is a vector space with an associative, distributive multiplication; e.g., \( n \times n \) matrices over \( F \).
Span, basis, linear independence

**Definition:** The span of a set of vectors \( \{v_1, \ldots, v_n\} \) is the set of all linear combinations of those vectors:

\[
\left\{ a_1 \cdot v_1 + \cdots + a_n \cdot v_n : a_1, \ldots, a_n \in F \right\}.
\]

**Definition:** A set of vectors \( \{v_1, \ldots, v_n\} \) is linearly independent (LI) if no vector in the set is a linear combination of the other vectors; equivalently, there does not exist a set of scalars \( \{a_1, \ldots, a_n\} \), not all zero, such that

\[
a_1 \cdot v_1 + a_2 \cdot v_2 + \cdots + a_n \cdot v_n = 0.
\]

**Definition:** A basis for a vector space is a LI set that spans the vector space.

**Definition:** A vector space is finite dimensional if it has a finite basis.

**Lemma:** The number of vectors in a linearly independent set is \( \leq \) the number of vectors in a spanning set.

**Theorem:** All bases for a finite-dimensional vector space have the same number of elements. Thus the dimension of the vector space is well defined.
Vector coordinates

*Theorem:* Every vector can be expressed as a linear combination of basis vectors in exactly one way.

*Proof:* Suppose that \( \{v_1, \ldots, v_n\} \) is a basis and

\[
a_1 \cdot v_1 + \cdots + a_n \cdot v_n = a'_1 \cdot v_1 + \cdots + a'_n \cdot v_n,
\]

are two possibly different representations of the same vector. Then

\[
(a_1 - a'_1) \cdot v_1 + \cdots + (a_n - a'_n) \cdot v_n = 0.
\]

By linear independence of the basis

\[
a_1 - a'_1 = 0, \ldots , a_n - a'_n = 0 \implies a_1 = a'_1, \ldots , a_n = a'_n.
\]

We say that \( V \) is *isomorphic* to vector space \( F^n = \{(a_1, \ldots, a_n) : a_i \in F\} \) with componentwise addition and scalar multiplication.

*Theorem:* If \( V \) is a vector space of dimension \( n \) over a field with \( q \) elements, then the number of elements of \( V \) is \( q^n \).

*Proof:* There are \( q^n \) \( n \)-tuples of scalars from \( F \).
Inner product and orthogonal complement

**Definition:** A vector *subspace* of a vector space $V$ is a subset $W$ that is a vector space, i.e., closed under vector addition and scalar multiplication.

**Theorem:** If $W$ is a subspace of $V$ then $\dim W \leq \dim V$.

**Proof:** Any basis $\{w_1, \ldots, w_k\}$ for subspace $W$ can be extended to a basis of $V$ by adding $n-k$ vectors $\{v_{k+1}, \ldots, v_n\}$. Therefore $\dim W \leq \dim V$.

**Definition:** The *inner product* of two $n$-tuples over a field $F$ is
\[
(a_1, \ldots, a_n) \cdot (b_1, \ldots, b_n) = a_1 b_1 + \cdots + a_n b_n.
\]

**Definition:** Two $n$-tuples are *orthogonal* if their inner product is zero.

**Definition:** The *orthogonal complement* of a subspace $W$ of $n$-tuples is the set $W^\perp$ of vectors orthogonal to every vector in $W$; that is,
\[
v \in W^\perp \text{ if and only if } v \cdot w = 0 \text{ for every } w \in W.
\]

**Theorem:** *(Dimension Theorem)* If $\dim W = k$ then $\dim W^\perp = n - k$.

**Theorem:** If $W$ is subspace of finite-dimensional $V$, then $W^{\perp\perp} = W$.

In infinite-dimensional vector spaces, $W$ may be a proper subset of $W^{\perp\perp}$.
Linear transformations and matrix multiplication

**Definition:** A *linear transformation* on a vector space $V$ is a function $T$ that maps vectors in $V$ to vectors in $V$ such that for all vectors $v_1, v_2$ and scalars $a_1, a_2$,

$$T(a_1 v_1 + a_2 v_2) = a_1 T(v_1) + a_2 T(v_2).$$

Every linear transformation $T$ can be described by an $n \times n$ matrix $M$. The coordinates of $T(v_1, \ldots, v_n)$ are the components of the vector-matrix product $(v_1, \ldots, v_n)M$.

Each component of $w = vM$ is inner product of $v$ with a column of $M$:

$$w_j = v_1 m_{1j} + \cdots + v_n m_{nj} = \sum_{i=1}^{n} v_i m_{ij}.$$  

Here is another way to look at $w = vM$. If $m_i$ is $i$-th row of $M$, then

$$(v_1, \ldots, v_n)M = v_1 m_1 + \cdots + v_n m_n.$$  

Thus $vM$ is linear combination of rows of $M$ weighted by coordinates of $v$. As $v$ ranges over $n$-tuples, $vM$ ranges over subspace spanned by rows of $M$. 
Matrix rank

Definition: A square matrix is nonsingular if it has a multiplicative inverse.  
Definition: The determinant of $A = (a_{ij})$ is

$$\det A = \sum_{\sigma} (-1)^\sigma a_{i_1\sigma(i_1)} \cdots a_{i_n\sigma(i_n)},$$

where $\sigma$ is a permutation of $\{1, \ldots, n\}$ and $(-1)^\sigma$ is the sign of $\sigma$.

Theorem: A matrix is nonsingular if and only if its determinant is nonzero.  
Definition: The rank of a matrix is the size of largest nonsingular submatrix.  
The rank of a matrix can be computed efficiently:

1. Use Gaussian elimination to transform matrix to row-reduced echelon form.  
2. The rank is the number of nonzero rows of the row-reduced echelon matrix.  

Theorem: The rank of a matrix is the dimension of the row space, which equals the dimension of the column space.  
Therefore the number of linearly independent rows is the same as the number of linearly independent columns.