Math Introduction

- $\begin{bmatrix} \boxed{\vec{c}_1} & \boxed{\vec{c}_2} & \cdots & \boxed{\vec{c}_n} \end{bmatrix}_{m\times n} \boxed{\vec{x}} = x_1\vec{c}_1 + x_2\vec{c}_2 + \cdots + x_n\vec{c}_n$ where $\vec{c}_j$ is $m\times 1$, $\vec{x}$ is $n\times 1$.
- $\begin{bmatrix} \boxed{\vec{r}_1^{\,T}} \\ \boxed{\vec{r}_2^{\,T}} \\ \vdots \\ \boxed{\vec{r}_m^{\,T}} \end{bmatrix}_{m\times n} \boxed{\vec{x}} = \begin{bmatrix} \vec{r}_1^{\,T}\vec{x} \\ \vec{r}_2^{\,T}\vec{x} \\ \vdots \\ \vec{r}_m^{\,T}\vec{x} \end{bmatrix}$ where $\vec{r}_i$ is $n\times 1$, $\vec{x}$ is $n\times 1$.
- $\underline{x}\begin{bmatrix} \boxed{\underline{c}_1^T} & \boxed{\underline{c}_2^T} & \cdots & \boxed{\underline{c}_n^T} \end{bmatrix}_{m\times n}^{T} = x_1\underline{c}_1 + x_2\underline{c}_2 + \cdots + x_n\underline{c}_n$
- A **set** is an arbitrary collection of object, or elements, without any predefined operations between set elements.
- A **binary operation** operates on two set elements at a time, yielding a third (not necessarily distinct) element.
- The expression "$a|b$" is used to denote that an element *a* divides an element *b* without remainder.

Modular arithmetic

- **Addition modulo *m*** (or mod *m*) is often expressed in the following manner

  $$a + b \equiv c \text{ modulo } m$$

  which read "*a* plus *b* is equivalent to *c* modulo *m*." The result *c* is obtained by summing *a* and *b* using standard integer addition and dividing the result by the modulus *m*; *c* is the positive remainder.
- Two integers *a* and *b* are said to be in the same **equivalence class** modulo *m* if *a* can be written as *a* = *xm* + *b* for some integer *x*.
  - Addition modulo *m* groups the infinite set of integers into *m* distinct equivalence classes.

- Elements in an equivalent class modulo *m* are "equivalent" in the sense that any element in a given class can be substituted for any other element in the same class without changing the outcome of a modulo *m* operation.
  - Equivalence classes of integers are usually labeled with their smallest constituent nonnegative integer.
- **Multiplication modulo *m*** is performed over the integers in much the same manner as modular addition. The result of the integer multiplication operation is divided by the modulus *m* and the positive remainder retained as the result of the modular operation.
- If 0 is in the set, we do not have a group under modulo *m* multiplication. (0 has no inverse.)
- A **zero divisor** is any nonzero number *a* for which there exists nonzero *b* such that $a \cdot b \equiv 0$ modulo *m*.
- If the modulus *m* has factors other than 1 in a given set $\{1, 2, \ldots, m-1\}$, the set will have zero divisors under modulo *m* multiplication. (Say $m = x \times y$, then $x \cdot y \equiv 0$ modulo *m*.)

Group, subgroups, cosets

- A **group** is a set of objects *G* on which a binary operation "$\cdot$" has been defined. $"\cdot": G \times G \to G$ (closure). The operation must also satisfy
  1. Associativity: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
  2. Identity: $\exists e \in G$ such that $\forall a \in G$ $\; a \cdot e = e \cdot a = a$ $\; \exists a \in G$
  3. Inverse: $\forall a \in G$ $\exists$ a unique element $a^{-1} \in G$ such that $a \cdot a^{-1} = a^{-1} \cdot a = e$.
- A group is said to be **commutative** (or abelian) if it also satisfies commutativity: $\forall a, b \in G$, $a \cdot b = b \cdot a$.
  - The group operation for a commutative group is usually represented using the symbol "+", and the group is sometimes said to be "additive."
- Remarks:
  - Identity element *e* in a group is unique.

    Proof. Let e_1 and e_2 be identity. Then $e_1 \overset{e_1 \text{ is an identity}}{=} e_1 \cdot e_2 \overset{e_2 \text{ is an identity}}{=} e_2$.
  - Inverse a^{-1} of an element *a* in a group is unique.

    Proof. Let $v \cdot v_1 = e$, and $v \cdot v_2 = e$. Then, $v_1 \cdot v \cdot v_2 = (v_1 \cdot v) \cdot v_2 = e \cdot v_2 = v_2$.

    Also, $v_1 \cdot v \cdot v_2 = v_1 \cdot (v \cdot v_2) = v_1 \cdot e = v_1$.
  - $a \oplus b = c \oplus b \;\Rightarrow\; a = c$. (Proof: add –*b* to the right of both sides) Note that this work because *b* has inverse.
    - $a \neq c \Rightarrow a + b \neq c + b$.
  - $(b^{-1})^{-1} = b$

Proof. For any $b \in G$, there exists $b^{-1} \in G$ such that $b \cdot b^{-1} = b^{-1} \cdot b = e$. Let $x = b^{-1}$. Then, we have $b \cdot x = x \cdot b = e$. Hence, $b = x^{-1}$ (from uniqueness of inverse). Therefore, $x^{-1} = \left(b^{-1}\right)^{-1} = b$.

  - $a \neq b \Rightarrow a * x \neq b * x$

    Proof. Suppose $a * x = b * x$, then $a * x * x^{-1} = b * x * x^{-1}$, which implies $a = b$.

- The **order** of a group is defined to be the cardinality of the group.
  - Order of a group alone is not sufficient to completely specify the group unless we restrict ourselves to a particular operation.
- Ex. group
  - The set of integers form an infinite commutative group under integer addition, but not under integer multiplication.
  - The set of ($n \times n$) matrices with real elements forms a commutative group under matrix addition.
  - The equivalence classes {0, 1, 2, 3, …, m -1} form a commutative group of order m under modulo m integer addition for any positive integer m.
- $S = \{1, 2, \ldots, p-1\}$ forms a commutative group of order (p-1) under modulo p multiplication if and only if p is a prime integer.
  - If p is not prime, then there exists $m, n \in S$ such that $1 < m, n < p$ and $mn \equiv 0$ modulo p; closure is not satisfied.
    - If 0 is included in the set, we still do not have a group because
      - 0 does not have a multiplicative inverse.
      - n does not have a multiplicative inverse. Suppose it has, then $m \equiv m\left(n \cdot n^{-1}\right) \equiv (mn)n^{-1} \equiv 0$.
  - Given an element $x \in S$, the products $\{x \cdot 1, x \cdot 2, \ldots, x \cdot (p-1)\}$ are distinct, otherwise $x \cdot y = x \cdot z$ implies $x \cdot (y - z) \equiv 0$.
  - Since the (p-1) products are distinct, one must equal the multiplicative identity, assuring existence of inverses for all $x \in S$.
- For convenience, define $g^m = \underbrace{g \cdot g \cdot \cdots \cdot g}_{m \text{ times}}$.
- **Order of a group element**:

  Let g be an element in the group G with group operation "$\cdot$" and identity element e.

  The order of g = $\operatorname{ord}(g) = \min_{m \in \mathbb{N}} \{m : g^m = e\}$
- Let S be a subset of the group G. If for all a and b in S, $c = a \cdot b^{-1}$ is also in S, then S is said to be a **subgroup** of G.
  - A subset of G is a subgroup if it exhibits closure and contains the necessary inverses.

- A subgroup is itself a group.

  Proof. 1) Associativity follows from the fact that $S \subset G$.

  2) Need only to show that identity in *G* is also in *S*. To do this, let *b* be any element in *S*, then by definition, we have $b \cdot b^{-1} \in S$. But *b* is also in *G*, hence, $b \cdot b^{-1} = e$. Therefore, $\boxed{e \in S}$.

  3) Inverse: Need only to show that inverse in *G* is also in *S*. First, we'd already proved that $e \in S$. Now, $\forall b \in S$ we must have $e \cdot b^{-1} \in S$.

  0) Closure: Let $a, b \in S$. We already know that $b^{-1} \in S$. Then, $a \cdot b = a \cdot \left(b^{-1}\right)^{-1} \in S$.

- A subgroup *S* is said to be a **proper subgroup** of *G* if $S \subset G$ but $S \neq G$.
- Properties of subgroup
  - $e \in S$
  - If $a \in S$, then $\forall m \quad a^m \in S$.

    Proof. $a \in S \Rightarrow a^{-1} \in S \Rightarrow a \cdot \left(a^{-1}\right)^{-1} = a \cdot a \in S \Rightarrow (a \cdot a) \cdot \left(a^{-1}\right)^{-1} = a^3 \in S$ etc.

  - If $a, b \in S$, then $\exists c \in S$ such that $c \cdot b = a$

    Proof. Let $c = a \cdot b^{-1}$. By definition of subgroup, $c \in S$. $c \cdot b = a \cdot b^{-1} \cdot b = a$.
- Example:
  - Let $a \in G$, $\left\{e, a, a^2, \ldots, a^{\operatorname{ord}(a)-1}\right\} = \left\{a, a^2, \ldots, a^{\operatorname{ord}(a)}\right\}$ is a subgroup of *G*.
- **Cosets**
  - Let *S* be a subgroup of *G* with operation "+".

    A **left coset** of *S* in *G* : $x + S = \{x + s, s \in S\} \subset G$.

    A **right coset** of *S* in *G*: $S + x = \{s + x, s \in S\} \subset G$.

  - If *G* is commutative, every left coset $x + S$ is identical to every right coset $S + x$.
- Properties of cosets
  - A coset of *S* in *G* may not be a subgroup. In fact, only when $S + x = S$ that the coset is a subgroup.

    Proof. They don't contain *e*.

  - The distinct cosets of a subgroup *S* in a group *G* are disjoint.

    Proof. Let $(S + x) \cap (S + y) \neq \varnothing$. Then, $\exists b \in (S + x) \cap (S + y)$. Hence, $b = b' + x = b'' + y$ for some $b', b'' \in S$. So, we have $y = -b'' + b' + x$. Now consider any $c \in S + y$. By definition, $c = c' + y$ for some $c' \in S$. Hence, $c = c' + y = \underbrace{c' + (-b'') + b'}_{\in S} + x \in S + x$. Therefore, we have $S + y \subset S + x$. Similarly, we can show that $S + x \subset S + y$. So,

$S+x=S+y$. Hence, we have proved that $(S+x)\cap(S+y)\neq\varnothing\Rightarrow$ $S+x=S+y$.

- All coset of *S* in *G* have the same cardinality = $|S|$.

  Proof. Distinct elements in *S* give distinct elements in $S+x$.

- If $x\in S$, then $S+x=S$.

  Proof. $\forall y\in S\ \ y+x\in S$. In particular, $e\in S\Rightarrow x=e+x\in S+x$. So, $x\in S\cap(S+x)$. Distinct cosets are disjoint. Because $S\cap(S+x)\neq\varnothing$, they are identical.

- A subgroup *S* of a group *G* defines a partitioning of *G* into distinct, disjoint cosets. This partitioning of *G* is called the **coset decomposition** of *G* induced by *S*.
- If $v_2-v_1\in S$, then v_2,v_1 are in the same coset.

  Proof. Assume $v_1\in S+x$. Then, $v_1=s+x$ for some $s\in S$. From $v_2-v_1\in S$, we have $\exists s''\in S\ \ v_2=s''+v_1=\underbrace{s''+s}_{\in S}+x\in S+x$.

- **Lagrange's Theorem**: If *S* is a subgroup of *G*, then $\operatorname{ord}(S)|\operatorname{ord}(G)$.

  Proof. A subgroup *S* of a group *G* defines a partitioning of *G* into distinct, disjoint cosets, all with size $|S|$. Hence, $|G|=|S|\times(\#\text{ distinct cosets})$.

Ring

- A **ring** is a collection of elements *R* with two binary operations "+" and "$\cdot$" such that
  1. *R* forms a commutative group under "+".
     The additive identity element is labeled "0"
  2. The operation "$\cdot$" is associative: $(a\cdot b)\cdot c=a\cdot(b\cdot c)$ for all *a, b, c* ∈ *R*.
  3. The operation "$\cdot$" distributes over "+": $a\cdot(b+c)=(a\cdot b)+(a\cdot c)$.

  A ring is said to be a **commutative ring** if the operation "$\cdot$" commutes (i.e., $a\cdot b=b\cdot a$)

  A ring is said to be **a ring with identity** if the operation "$\cdot$" has an identity element, which is labeled "1".

  A ring that is both a commutative ring and a ring with identity is said to be a **commutative ring with identity**.

- Examples
  - Matrices with integer elements form a ring with identity under standard matrix addition and multiplication.
  - The integers under modulo *m* addition and multiplication form a commutative ring with identity.

  - The set of all polynomials with binary coefficients forms a commutative ring with identity under standard polynomial addition and multiplication. This ring is usually denote $F_2[x]$ or $\mathrm{GF}(2)[x]$.

- Any element in a ring *R* that has its multiplicative inverse in *R* is called a **unit**.

Field

- Let *F* be a set of objects on which two operations "+" and "$\cdot$" are defined. *F* is said to be a **field** if and only if
  1. *F* forms a commutative group under +. The additive identity element is labeled "0“.
  2. *F* – {0} forms a commutative group under $\cdot$. The multiplicative identity element is labeled "1".
  3. The operation "+" and "$\cdot$" distribute: $a\cdot(b+c)=(a\cdot b)+(a\cdot c)$.

- A field can also be defined as a commutative ring with identity in which every element has a multiplicative inverse.
- All of the field elements form an additive commutative group, while the nonzero elements form a multiplicative commutative group.
- $\boxed{0\cdot c=0}$

  Proof. $0\cdot c=(0+0)\cdot c=0\cdot c+0\cdot c$. Add $-(0\cdot c)$ to both side, then we have $0=0\cdot c$.

- $-c=(-e)c$

  Proof. $0=0\cdot c=(e\oplus -e)\cdot c=e\cdot c\oplus(-e)\cdot c=c\oplus(-e)\cdot c$. Also, $0=c\oplus -c$. Hence, $c\oplus(-e)\cdot c=c\oplus -c$.

- $a\cdot b=0$ iff *a* = 0 or *b* = 0.

  Proof. "$\Leftarrow$" trivial because $0\cdot x=0$. "$\Rightarrow$" Assume $a\cdot b=0$, and $a,b\neq 0$. Then, $\exists b^{-1}$, and hence, $a=a\cdot b\cdot b^{-1}=0\cdot b^{-1}=0$. Contradiction.

- $a\neq 0, b_1\neq b_2\Rightarrow a\cdot b_1\neq a\cdot b_2$

  Proof. If $a\cdot b_1=a\cdot b_2$, then multiplying both side by a^{-1} gives $b_1=b_2$.

- The integers {0, 1, 2, …, *p*-1}, where *p* is a prime, form the field GF(*p*) under modulo *p* addition and multiplication.
- Cannot construct $\mathrm{GF}(p^m)$ using modular arithmetic.

  Proof. $p\cdot p^{m-1}\equiv p^m\equiv 0$. $1<p<p^{m-1}<p$. *p* has no inverse. Suppose it has then $p^{m-1}\equiv p^{m-1}\cdot(p\cdot p^{-1})\equiv(p^{m-1}\cdot p)\cdot p^{-1}\equiv 0\cdot p^{-1}\equiv 0$.

Vector spaces

- Let *V* be a set of elements call **vectors** and *F* a field of elements called **scalars**.

Two operations are introduced in addition to the two already defined between the field elements.

Let "+" be a binary additive operation, henceforth called vector addition, that maps pairs of vectors $\underline{v}_1, \underline{v}_2 \in V$ onto a vector $\underline{v} = \underline{v}_1 + \underline{v}_2$ in *V*.

Let "$\cdot$" be a binary multiplicative operation, henceforth called scalar multiplication, that maps a scalar $a \in F$ and a vector $\underline{v} \in V$ on to a vector $\underline{w} = a \cdot \underline{v} \in V$.

V forms a vector space over *F* if the following conditions are satisfied:

1. *V* forms a commutative group under the operation "+".
2. For any element $a \in F$, and $\underline{v} \in V$, $a \cdot \underline{v} = \underline{u} \in V$.
3. The operation "+" and "$\cdot$" distribute:

   $a \cdot (\underline{u} + \underline{v}) = a \cdot \underline{u} + a \cdot \underline{v}$, and $(a+b) \cdot \underline{v} = a \cdot \underline{v} + b \cdot \underline{v}$.
4. Associativity: For all $a, b \in F$ and all $\underline{v} \in V$, $(a \cdot b) \cdot \underline{v} = a \cdot (b \cdot \underline{v})$.
5. The multiplicative identity 1 in *F* acts as a multiplicative identity in scalar multiplication: for all $\underline{v} \in V$, $1 \cdot \underline{v} = \underline{v}$.

- *F* is commonly called the "scalar field" or the "ground field" of the vector space *V*.
- The *n*-tuple $\underline{v} = (v_0, v_1, \ldots, v_{n-1})$ of elements $\{v_i\}$ from the ground field *F* s a type of vectors. Such vectors allow for a convenient definition for vector addition and scalar multiplication.

  Let $\underline{v} = (v_0, v_1, \ldots, v_{n-1})$ and $\underline{u} = (u_0, u_1, \ldots, u_{n-1})$, with the $\{v_i\}$ and $\{u_i\}$ $\subseteq$ *F*.

  vector addition: $\underline{u} + \underline{v} = (u_0 + v_0, u_1 + v_1, \ldots, u_{n-1} + v_{n-1})$.

  scalar multiplication: $a \cdot \underline{v} = (av_0, av_1, \ldots, av_{n-1})$.
- Let $\underline{v}_1, \underline{v}_2, \ldots, \underline{v}_n$ be vectors in *V* and let $a_1, a_2, \ldots, a_n$ be scalars in *F*. Since *V* forms a commutative group under +, the **linear combination** $\underline{v} = a_1 \cdot \underline{v}_1 + a_2 \cdot \underline{v}_2, \ldots, a_n \cdot \underline{v}_n$ is a vector in *V*.
- A collection of vectors $G = \{\underline{v}_1, \underline{v}_2, \ldots, \underline{v}_n\}$, the linear combinations of which include all vectors in a vector space *V*, is said to be a **spanning set** for *V* or to **span** *V*.
- A set of vectors is said to be **linearly independent** when one or more of the vectors can be expressed as a linear combination of the others.
- A spanning set for *V* that has minimal cardinality is called a **basis** for *V*.
- The elements of a basis must be linearly independent.
- All bases of a vector space have the same cardinality.
- If a basis for a vector space *V* has *k* elements, then the vector space is said to have **dimension** *k*, written $\dim(V) = k$.

- Let $\{\underline{v}_i\}$ be a basis for a vector space *V*. For every vector $\underline{v}$ in *V*, there is a representation $\underline{v} = a_0 \cdot \underline{v}_0 + a_1 \cdot \underline{v}_1, \ldots, a_{k-1} \cdot \underline{v}_{k-1}$. This representation is unique.

- Let $\underline{v}_1$ and $\underline{v}_2$ be an arbitrary pair of vectors in the subset *S* of the vector space *V* over *F*. *S* is a **vector subspace** of *V* if and only if any linear combination of $\underline{v}_1$ and $\underline{v}_2$ (i.e., $a \cdot \underline{v}_1 + b \cdot \underline{v}_2$, $a, b \in F$) is also in *S*.

Proof. "⇒" *S* is a vector space hence *S* is closed under linear combinations. "⇐" The closure properties for vector addition and scalar multiplication are satisfied for *S*. Since *S* is closed under scalar multiplication, all additive inverses $(-1) \cdot \underline{v}$ for any element $\underline{v} \in S$ are also in *S*. Then, additive identity must also be in *S*. (Use $\underline{v} - \underline{v}$ for any $\underline{v} \in S$). The remainder of the vector-space properties follow by noting that since *V* is a vector space, the various properties for operations (Associativity and commutativity) that hold in *V* must also hold in $S \subset V$.

- Let $\underline{u} = (u_0, u_1, \ldots, u_{n-1})$ and $\underline{v} = (v_0, v_1, \ldots, v_{n-1})$ be vectors in the vector space *V* over the field *F*. The **inner product** $\underline{u} \cdot \underline{v}$ is defined as $\underline{u} \cdot \underline{v} = \sum_{i=0}^{n-1} u_i \cdot v_i$.
  - The following properties can be demonstrated:
    1. Commutativity: $\underline{u} \cdot \underline{v} = \underline{v} \cdot \underline{u}$.
    2. Associativity with scalar multiplication: $a \cdot (\underline{u} \cdot \underline{v}) = (a \cdot \underline{u}) \cdot \underline{v}$.
    3. Distributivity with vector addition: $\underline{u} \cdot (\underline{v} + \underline{w}) = \underline{u} \cdot \underline{v} + \underline{u} \cdot \underline{w}$.

- Let *S* be a *k*-dimensional subspace of a vector space *V*. Let $S^{\perp}$ be the set of all vectors $\underline{v}$ in *V* such that for all $\underline{u} \in S$ and for all $\underline{v} \in S^{\perp}$, $\underline{u} \cdot \underline{v} = 0$.

  $S^{\perp}$ is said to be the **dual space** of *S*.

- The dual space $S^{\perp}$ of a vector subspace $S \subseteq V$ is itself a vector subspace of *V*.

- **The Dimension Theorem**: Let *S* be a finite-dimensional vector subspace of *V* and let $S^{\perp}$ be the corresponding dual space. Then $\dim(S) + \dim(S^{\perp}) = \dim(V)$.

- To find the dimension of the vector space $\mathcal{C}$ spanned by $\{\underline{v}_1, \underline{v}_2, \ldots, \underline{v}_n\}$, row-reduce

$$G = \begin{bmatrix} \underline{v}_1 \\ \boxed{\quad \underline{v}_2 \quad} \\ \vdots \\ \underline{v}_n \end{bmatrix}$$

, and count the pivot positions. $(= \operatorname{rank} G = \dim(\operatorname{Row}(G)))$

- Given $\left\{\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_n\right\}$, to solve for $\sum_{i=1}^{n} \vec{v}_i = \vec{b}$, solve $A\vec{x} = \begin{bmatrix} \vec{v}_1 & \boxed{\vec{v}_2} & \cdots & \vec{v}_n \end{bmatrix} \vec{x} = \vec{b}$,

  i.e., row reduce $\left[A : \vec{b}\right] \to \left[I : \vec{x}\right]$.

- To find a basis (H) to the dual space of the vector space spanned by $\left\{\underline{v}_1, \underline{v}_2, \ldots, \underline{v}_n\right\}$,

  solve for the solution of $\begin{bmatrix} \underline{v}_1 \\ \boxed{\underline{v}_2} \\ \vdots \\ \underline{v}_n \end{bmatrix} \vec{x} = G\vec{x} = \vec{0}$.

  Use row reduction:

  - If can get in the form $\left[I : P\right]$, then the basis for H is the rows of $\left[P^T : I\right]$.
  - If can get into reduced echelon form, then we have free variable x_{n_i}'s where the n_i corresponds to the non-pivot columns. Then we can express other x_j's as linear combination of free variables. Hence, $\vec{x} = \sum_{n_i} \vec{h}_{n_i} x_{n_i}$. The $\vec{h}_{n_i}$'s form the basis for H.

Etc. from linear algebra

- Elementary row operations

  1. Replacement: replace one row by the sum of itself and a multiple of another row ≡ Add to one row a multiple of another row
     - $R_i \to R_i + mR_j$

       $R_j \to R_j$ still.
     - Inverse: $R_i \to R_i - mR_j$
  2. Interchange: interchange 2 rows
     - $R_i \leftrightarrow R_j$
     - Inverse: $R_i \leftrightarrow R_j$
  3. Scaling: multiply all entries in a row by a nonzero constant
     - $R_i \to mR_i$
     - Inverse: $R_i \to \frac{1}{m} R_i$

- A rectangular matrix is in echelon form if

  1. all nonzero rows are above any rows of all zeros (or no row of zeros)

2. each leading entry ($\neq 0$) of a row is in a column to the right of the leading entry of the row above it
3. all entries in a column below a leading entry are zero

Ex $\square$ = pivot position

$$\begin{bmatrix} \square & x & x & x \\ 0 & \square & x & x \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & \square & x & x & x & x & x & x & x & x \\ 0 & 0 & 0 & \square & x & x & x & x & x & x \\ 0 & 0 & 0 & 0 & \square & x & x & x & x & x \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \square & x & x \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \square & x \end{bmatrix}$$

- A pivot position in a matrix $A \Rightarrow$ a location in A that corresponds to a leading entry in an echelon form of A.
  - Each nonzero row has one and only one pivot position.
  - All pivot positions are in the first p rows of $A_{m\times n}$ where $p \leq m$, one pivot position per row. The rest of the rows are all zeros.
  - Some columns (any columns) may not have leading entry.
- Pivot column $\Rightarrow$ a column of A that contains a pivot position
- Pivot $\Rightarrow$ a nonzero number in a pivot position that is used as need to create zeros via row operations.
- A rectangular matrix is in reduced echelon form if

1. It is in echelon form
2. The leading entry in each nonzero row is 1
3. Each leading 1 is the only nonzero entry in its column

Ex $$\begin{bmatrix} 1 & 0 & x & x \\ 0 & 1 & x & x \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & x & 0 & 0 & x & x & 0 & 0 & x \\ 0 & 0 & 0 & 1 & 0 & x & x & 0 & 0 & x \\ 0 & 0 & 0 & 0 & 1 & x & x & 0 & 0 & x \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & x \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & x \end{bmatrix}$$

- Row reduced = transformed by elementary row operations
- A matrix may be row reduced into more than one matrix in echelon form, using different sequences of row operations
- Uniqueness of the reduced echelon form: Each matrix is row equivalent to one and only one reduced echelon matrix
- The row reduction algorithm
  - Forward phrase
    1. Begin with the leftmost nonzero column. This is a pivot column. The pivot position is at the top. (Left of this is zeros)
    2. Select a nonzero entry in the pivot column as a pivot. If necessary, interchange rows to move this entry into the pivot position.

3. Use row replacement operations to create zeros in all position below the pivot.
4. Cover (or ignore) the row containing the pivot position and cover all rows, if any, above it.

Apply steps 1-3 to the submatrix that remains.

Repeat the process until there are no more nonzero rows to modify.

We have reached an echelon form

- Backward phrase

to get the reduced echelon form

5. Beginning with the rightmost pivot, and working upward and to the left, create zeros above each pivot.

   If a pivot is not 1, make it 1 by scaling operation

- Free variables ; basic variables

For $A\vec{x} = \vec{b} \to \begin{bmatrix} A & \vec{b} \end{bmatrix} \to$ echelon form

- Basic variable ⇒ variable x_i where i corresponds to a pivot column in the matrix
- Free variable ⇒ other variable ⇒ variable x_i ; column i is not a pivot column ⇒ free to choose any value

- Parametric description of solution sets in which the free variables act as parameters

General solution: $\begin{cases} x_1 = f\left(x_{free_1}, x_{free_2}, \cdots\right) \\ \vdots \\ x_{free_1} \text{ is free} \\ \vdots \end{cases}$

- Using row reduction to solve a linear system

1. Write the augmented matrix of the system
2. Use the row reduction algorithm to obtain an equivalent augmented matrix in echelon form.

   Decide whether the system is inconsistent.

   If there is no solution, stop.

   Otherwise, go to the next step.
3. Continue row reduction to obtain the reduced echelon form.
4. Write the system of equations corresponding to the matrix obtained in step 3.
5. Rewrite each nonzero equation form step 4 so that its one basic variable is expressed in terms of any free variables appearing in the equation.