NOTES FOR 8 AUG (THURSDAY)

1. Recap

(1) Defined row reduced and row echelon forms. Proved that every matrix can be brought to the (unique) row echelon form.
(2) Proved that $AX = 0$ has a non-trivial solution if $m < n$. If $m = n$ it has a non-trivial solution iff it cannot be row equivalent to the identity matrix.
(3) Defined matrix multiplication and proved that it is associative. Proved that if $E = e(I)$ then $e(A) = EA$.

2. Matrix multiplication and invertible matrices

(1) As a corollary, A is row equivalent to B iff $B = PA$ where P is a product of $m \times m$ elementary matrices. Indeed, inductively, if after k elementary row operations, $B' = P'A$, then after one more, $B = E(P'A) = (EP')A = PA$.
(2) The transpose A^T of an $m \times n$ matrix A is an $n \times m$ matrix defined as $(A^T)_{ij} = A_{ji}$. Note that $(AB)^T = B^T A^T$. If X, Y are row vectors, then $XA = Y$ iff $A^T X^T = Y^T$. So we have a parallel theory of elementary column operations, column echelon forms, and a column rank.

Def : Let A be an $n \times n$ matrix over a field. An $n \times n$ matrix B satisfying $BA = I$ is called a left inverse of A. Likewise, if $AB = I$, it is called a right inverse. If it satisfies both, it is called an inverse of A and A is said to be invertible.
It is easy to prove that if A is invertible, then its inverse is unique. Indeed, if $B_1 A = I$ and $B_2 A = I$, then $B_1 = B_1 A B_2 = B_2$. Moreover, A^{-1} is invertible with inverse A. If B is also invertible, then so is AB and $(AB)^{-1} = B^{-1}A^{-1}$. Hence, a product of invertible matrices is invertible (by induction). Since elementary row operations are invertible, so are elementary matrices.
Here is a theorem : If A is an $n \times n$ matrix, TFAE :

(1) A is left invertible.
(2) A is row equivalent to the identity matrix.
(3) A is a product of elementary matrices.

Proof. $2 \Rightarrow 3$: $PA = I$ and hence $A = P^{-1} = (E_1 E_2 \ldots)^{-1} = \ldots E_2^{-1} E_1^{-1}$. $3 \Rightarrow 1$: A product of invertible matrices is invertible. Also easy to see $3 \Rightarrow 2$. Indeed, $A = E_1 \ldots E_k$ and hence $E_k^{-1} \ldots A = I$.
$1 \Rightarrow 2$: If A is left invertible, then $AX = 0$ implies that $0 = BAX = IX = X$ and hence the row echelon form of A is the identity. Therefore, $I = PA$. □

The proof above shows that if A is left invertible, then $A = P^{-1}$ and hence A is actually right invertible and $A^{-1} = P$ (where P is a left inverse of A) and hence A is invertible ! Likewise, if A is right invertible, i.e., there exists a B so that $AB = I$, then B is left invertible with left inverse A. Hence, B is right invertible with right inverse also equal to A. Therefore, $BA = I$ and $B = A^{-1}$.
As a consequence, if A is invertible and if $e(A) = I$, then $e(I) = A^{-1}$. Also, if A, B are $m \times n$ matrices, then B is row equivalent to A iff $B = CA$ where C is an invertible $m \times m$ matrix.
A similar theorem is : A is invertible iff $AX = 0$ has only the trivial solution iff $AX = Y$ has a solution for every Y. If $AX = 0$ has only the trivial solution, A is row equivalent to identity. If A is invertible,

then $AX = 0$ implies that $X = 0$. Likewise, if A is invertible, $AX = Y$ implies that $X = A^{-1}Y$. If $AX = Y$ has a solution for every Y, then choose Y_i to be the ith column of I. Then $AX_i = Y_i$ and hence $A[X_1 \ldots X_n] = I$. (Indeed, matrix multiplication acts column by column.) This means that A is right invertible and hence A is actually invertible.
As a last corollary, if $A = A_1 A_2 \ldots A_k$, then A is invertible iff each A_i is so. Indeed, if each of them is so, we are done. In the other direction, let us induct on k. If A is invertible, then firstly A_k is invertible. Indeed, if not, there exists an $X \neq 0$ such that $A_k X = 0$. Hence $AX = 0$ - a contradiction. Now, $AA_k^{-1} = A_1 \ldots A_{k-1}$. By induction we are done.

3. Vector spaces

Here is a question from earlier : Let $c_1, c_2, \ldots, c_n$ be real numbers such that $f(x) = c_1 + c_2 e^{ix} + c_3 e^{2ix} + \ldots = 0$ for all $x \in \mathbb{R}$. Then $c_i = 0$ for all i.

Proof. There are several ways to prove this statement. One cute way is as follows : Note that $\int_0^{2\pi} e^{ikx} e^{-lx} = \delta_{kl} 2\pi$. Hence, $\int_0^{2\pi} f(x) e^{-ilx} dx = 0 = c_l 2\pi \ \forall \ l$. This way should be reminiscent of proving a vector is zero by taking dot products with the standard unit vectors in the x, y, z directions. □

Here is another observation : If you look at $y'' + P(x)y' + Q(x)y = R(x)$, it behaves exactly like $AX = Y$, in that if you find one solution, you can get all the other solutions by solving a homogeneous problem.

The above examples suggest that the geometrical intuition of vectors carries over to any set where one has a natural notion of taking linear combinations. Motivated by this, we make the following definition :
A vector space $(V, 0, \mathbb{F}, +, .)$ over a field $\mathbb{F}$ is a set V equipped with functions $+ : V \times V \to V$ and $. : \mathbb{F} \times V \to V$ and an element $0 \in V$ such that

(1) $(V, +, 0)$ is an Abelian group.
(2) $a.(v + w) = a.v + a.w$
(3) $1.v = v$.
(4) $a(b.v) = (ab).v$
(5) $(a + b).v = a.v + b.v$

Just using these axioms,

(1) $0.v = 0 : 0.v = (0 + 0).v = 0.v + 0.v$.
(2) $c.0 = 0 : c.(0 + 0) = c.0 + c.0$.
(3) If $c.v = 0$ for $c \neq 0$, then $c^{-1}c.v = 1.v = v = 0$.
(4) $-v = (-1).v$ because $(-1).v + 1.v = (-1 + 1).v = 0.v = 0$.