Exam 1 - Definitions and Basic Theorems

One of the difficuliies in preparing for an exam where there will be a lot of proof problems is knowing what you're allowed to cite and what you actually have to demonstrate. Below I'll try to summarize the most basic notions underlying what we've studied so far. These notions you will be allowed to cite in the course of carrying out your proofs. Furthermore, I'll split these notions into two categories: *basic definitions* and *basic theorems*.

The *basic definitions* should be committed to memory. In so doing be sure to commit **my** definitions to memory, retaining exactly the same wording. For example, I defined the rank of a matrix as the dimension of its column space. We later proved that the rank of a matrix is equal to number of pivots in a row echelon form of the matrix. If you try to use "the rank of a matrix is the number of pivots in a row echelon form of the matrix" as the definition of rank on an exam problem, you will lose points.

The *basic theorems* will be a subset of the theorems, propositions, lemmas, corollaries that we have proved in class. These will be statements that you can cite without proof in your solutions to exam problems. You need not memorize these statements as I will list them on the final page of the exam and you can cite them by number in your solutions. In your preparations for the exam you should try to see how you carry out proof problems using only these statements (rather than other results in the text or lecture).

1. Basic Definitions

Definition 1.1. *A **field** is a set $\mathbb{F}$ with two operations defined; **addition** and **multiplication**, which we shall denote, respectively,by $\oplus$ and $\otimes$ (just so you resist the temptation to think purely in terms of the real numbers). These two operations are required to satisfy*

(1) $\alpha \otimes \beta = \beta \otimes \alpha$ *for all* $\alpha, \beta \in \mathbb{F}$ *(commutativity of multiplication);*
(2) $\alpha \oplus (\beta \oplus \gamma) = (\alpha \oplus \beta) \oplus \gamma$ *for all* $\alpha, \beta, \gamma \in \mathbb{F}$ *(associativity of addition);*
(3) $\alpha \otimes \beta = \beta \otimes \alpha$ *for all* $\alpha, \beta \in \mathbb{F}$ *(commutativity of multiplication)*
(4) $\alpha \otimes (\beta \otimes \gamma) = (\alpha \otimes \beta) \otimes \gamma$ *for all* $\alpha, \beta, \gamma \in \mathbb{F}$ *(associativity of multiplication);*
(5) $\alpha \otimes (\beta \oplus \gamma) = (\alpha \otimes \beta) \oplus (\alpha \otimes \gamma)$ *for all* $\alpha, \beta, \gamma \in \mathbb{F}$ *(distributivity of multiplication over addition);*
(6) *There exists an element* 0_F *of* F *such that* $\alpha + 0_F = \alpha$ *for all* $\alpha \in \mathbb{F}$ *(additive identity element);*
(7) *For each element* $\alpha \in \mathbb{F}$ *there is an element* $-\alpha \in \mathbb{F}$ *such that* $\alpha \oplus (-\alpha) = 0_{\mathbb{F}}$ *(existence of additive inverses);*
(8) *There exists an element* $1_{\mathbb{F}} \in \mathbb{F}$ *such that* $1 \otimes \alpha = \alpha$ *for all* $\alpha \in \mathbb{F}$ *(multiplicative identity element);*
(9) *For each* $\alpha \neq 0_F$ *in* $\mathbb{F}$ *there is an element* $\alpha^{-1} \in \mathbb{F}$ *such that* $\alpha \otimes \alpha^{-1} = 1_{\mathbb{F}}$.

Definition 1.2. *Let* $\mathbb{F}$ *be a field, and let* V *be a set upon which two operations are defined*

(i) ***vector addition**: a rule for combining two elements of* V *to get another element of* V;
(ii) ***scalar multiplication:** a rule for taking an element of* $\mathbb{F}$ *and an element of* V *and producing an element of* V.

V *is a **vector space over*** $\mathbb{F}$ *if the following 8 properties are satisfied:*

(1) $u + v = v + u$ *for all elements* $u, v \in \mathbb{V}$ *(commutativity of vector addition);*
(2) $(u + v) + w = u + (v + w)$ *for all elements* $u, v, w \in V$ *(associativity of vector addition);*
(3) *There exists a vector* 0_V *such that* $v + 0_V = v$ *for all* $v \in V$;
(4) *For each vector* v, *there exists a vector* $-v$ *with the property that* $v + (-v) = 0_V$;
(5) $\alpha (\beta v) = (\alpha\beta) \cdot v$ *for all* $\alpha, \beta \in \mathbb{F}$ *and all* $v \in V$ *(associativity of scalar multiplication)*
(6) $(\alpha + \beta) v = (\alpha v) + (\beta v)$ *for all* $\alpha, \beta \in \mathbb{F}$ *and all* $v \in V$ *(distributivity of scalar addition w.r.t. scalar multiplication)*

(7) $\alpha(u+v) = (\alpha u + \beta v)$ *for all* $\alpha \in \mathbb{F}$ *and for all* $u, v \in V$ *(distributivity of vector addition w.r.t. scalar multiplications);*

(8) $1_{\mathbb{F}} \cdot v = v$ *for all vectors* $v \in V$ *(scalar mulitplication by* 1 *is trivial).*

Definition 1.3. *We say that a set* S *is* ***closed under an operation*** $*$ *if the outcome of applying the operation* $*$ *to elements of* S *is another element of* S*.*

Definition 1.4. *Let* V *be a vector space over a field* $\mathbb{F}$ *and let* U *be a subset of the elements of* V*. We say that* U *is a* ***subspace*** *of* V *if* U *is closed under the operations of scalar multiplicaition and vector addition: In other words,* U *is a subspace if*

$$(u \in U \quad \text{and} \quad \alpha \in \mathbb{F}) \quad \Rightarrow \quad \alpha u \in U \tag{1}$$

$$u_1, u_2 \in U \quad \Rightarrow \quad u_1 + u_2 \in U \tag{2}$$

Definition 1.5. *Let* $\{v_1, \ldots, v_k\}$ *be a set of vectors in a vector space* V*. Then the set*

$$span_{\mathbb{F}}(v_1, \ldots, v_k) := \{\alpha_1 v_1 + \cdots + \alpha_k v_k \mid \alpha_1, \ldots, \alpha_k \in \mathbb{F}\}$$

(where the coefficients $\alpha_1, \ldots, \alpha_k$ *vary over all possible element of* $\mathbb{F}$*) is called the* ***span*** *of the vectors* $\{v_1, \ldots, v_n\}$*.*

Definition 1.6. *The subspace* $span_{\mathbb{F}}(v_1, \ldots, v_k)$ *is the* ***subspace generated by vectors*** $v_1, \ldots, v_k$*. A subspace* S *is said to be* ***finitely generated*** *whenever there exists a finite set of vectors* $\{v_1, \ldots, v_k\}$ *such that* $S = span_{\mathbb{F}}(v_1, \ldots, v_k)$*.*

Definition 1.7. *A set of vectors* $v_1, \ldots, v_k$ *is said to be* ***linearly dependent*** *if the vectors satisfy an equation of the form*

$$\alpha_1 v_1 + \cdots + \alpha_k v_k = \mathbf{0} \tag{1}$$

with at least one coefficient $\alpha_i \neq 0$*. An equation of the form (1) (with at least one non-zero coefficient) is a called a* ***dependence relation*** *(amongst the vectors* $v_1, \ldots, v_k$*).*

Definition 1.8. *A set of vectors* $v_1, \ldots, v_k$ *is said to be* ***linearly independent*** *if the only way of satisfying*

$$\alpha_1 v_1 + \cdots + \alpha_k v_k = \mathbf{0}$$

is to take all the coefficients $a_1, \ldots, a_k$ *equal to* 0_F*.*

Definition 1.9. *The common cardinality of any linearly independent set of generators for a subspace* S *is called the* ***dimension*** *of* S*.*

Definition 1.10. *A* ***basis*** *for a subspace* S *is a linearly independent set of generators for* S*.*

Definition 1.11. *Let* $\mathbb{F}$ *be a field. An* $n \times m$ ***matrix*** *over* $\mathbb{F}$ *is an ordered list of* n *elements of* $\mathbb{F}^m$*.*

Definition 1.12. *The* ***row space*** $RowSp(\mathbf{A})$ *of an* $n \times m$ *matrix* $\mathbf{A} \in Mat_{n,m}(\mathbb{F})$ *is the subspace of* $\mathbb{F}^m$ *that is generated by the* n *(row-) vectors of the matrix. The* ***column space*** $ColSp(\mathbf{A})$ *of an* $n \times m$ *matrix* $\mathbf{A}$ *is the subspace of* $\mathbb{F}^n$ *generated by the column vectors of* $\mathbf{A}$*.*

Definition 1.13. $v = [\alpha_1, \ldots, \alpha_n]$ *be an element of* $\mathbb{F}$*. The* ***pivot*** *of* v *is the first (following the natural ordering of the list entries)* α_i *that is not equal to* $0_{\mathbb{F}}$*. If* α_i *is the pivot of* $v = [\alpha_1, \ldots, \alpha_i, \ldots, \alpha_n]$*. then* i *is the* ***pivot position*** *of* v*.*

Definition 1.14. *A matrix* $\mathbf{A} = [v_1, \ldots, v_n]$ *is in* ***row echelon form****, if the pivot position of* v_i *is less than the pivot position of* v_j *whenever* $i < j$*.*

Definition 1.15. *Let* $B = [v_1, \ldots, v_m]$ *be a basis for a vector space* V *and let* $v \in V$*. The* ***coordinate vector*** $\mathbf{v}_B$ ***of*** v ***with respect to*** B *is the ordered list of coefficients* $[a_1, \ldots, a_m]$ *corresponding to the expansion of* v *with respect to the basis* B *:*

$$v = a_1 v_1 + \cdots + a_m v_m \qquad \Longleftrightarrow \qquad \mathbf{v}_B = [a_1, \ldots, a_m] \in \mathbb{F}^n \quad .$$

Definition 1.16. *Let* $B = [v_1, \ldots, v_m]$ *be a basis for a vector space* V *over a field* $\mathbb{F}$ *and let* $[u_1, u_2, \ldots, u_n]$ *be an ordered list of* n *vectors in* V*. To this data we can attach an* $n \times m$ *matrix* $\mathbf{A}$ *with entries in* $\mathbb{F}$*. The entries of the* i^{th} *row of this matrix* $(1 \leq i \leq n)$ *are taken to coincide with the entries of coordinate vector of the the* i^{th} *vector* u_i *with respect to the basis* B*.*

Definition 1.17. *The **rank** of a linear system (or of its associated coefficient matrix) is the dimension of the column space of its coefficient matrix.*[1]

Definition 1.18. *Let* $\mathbf{A}$ *is the coefficient matrix for a* $n \times m$ *linear system*

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1m}x_m &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2m}x_m &= b_2 \\ &\vdots \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nm}x_m &= b_n \end{aligned}$$

and let $\mathbf{b}$ *is the inhomogeneous part of the same system. The **augmented matrix** for this system is the* $n \times (m+1)$ *matrix*

$$[\mathbf{A} \mid \mathbf{b}] \equiv \begin{bmatrix} a_{11} & \cdots & a_{1m} & b_1 \\ \vdots & \ddots & \vdots & \vdots \\ a_{n1} & \cdots & a_{nm} & b_n \end{bmatrix}$$

Definition 1.19. *Let* $\mathbf{p}_0$ *be an element of a vector space* V *and let* S *be subspace of* V*. The **hyperplane through*** $\mathbf{p}_0$ ***generated by*** S *is the set*

$$H_{\mathbf{p}_0,S} = \{\mathbf{v} \in V \mid v = \mathbf{p}_0 + \mathbf{s} \quad ; \quad \mathbf{s} \in S\}$$

Definition 1.20. *Let* $\mathbf{A}$ *be an* $n \times m$ *matrix over* $\mathbb{F}$*, thought of as a arrangement of* nm *elements of* $\mathbb{F}$ *into a rectangular array with* n *rows and* m *columns. mathbf*A *is in **reduced row echelon form** if*

(i) $\mathbf{A}$ *is in row echelon form;*
(ii) *Each pivot of* $\mathbf{A}$ *is equal to* $1_{\mathbb{F}}$*;*
(iii) *The entries above and below any pivot are all equal to* $0_{\mathbb{F}}$*.*

[1] The column space of a matrix is, of course, just the span of its column vectors.

2. Basic Theorems

Proposition 2.1. *The zero vector $\mathbf{0}_{\mathbb{V}}$ of a vector space is unique.*

Proposition 2.2. *Let V be a vector space over a field $\mathbb{F}$. Then $0_F \cdot v = \mathbf{0}_V$ for all $v \in V$.*

Proposition 2.3. *If S is a subspace of a vector space V , then $\mathbf{0}_V \in S$.*

Proposition 2.4. *A subset S of a vector space V over a field $\mathbb{F}$ is a subspace if and only if every linear combination of the form $\alpha v + \beta u$ with $\alpha, \beta \in \mathbb{F}$, $v, u \in S$ is in S.*

Proposition 2.5. *$span\,(v_1, \dots v_{k+1}) = span\,(v_1, \dots, v_k)$ if and only $v_{k+1} \in span\,(v_1, \dots, v_k)$.*

Theorem 2.6. *Let S be a subspace of a vector space V over a field $\mathbb{F}$. Suppose S is generated by n vectors $v_1, \dots, v_n$. Let $\{w_1, \dots, w_m\}$ be a set of m vectors in S with $m > n$. Then the vectors $\{w_1, \dots, w_m\}$ are linearly dependent.*

Corollary 2.7. *Suppose $\{v_1, \dots, v_n\}$ and $\{w_1, \dots, w_m\}$ are two bases for a subspace S. Then $n = m$.*

Proposition 2.8. *Let $L = \{v_1, \dots, v_n\}$ be an ordered list of generating vectors for a subspace S of a vector space V over a field $\mathbb{F}$. The following three* elementary operations *on the list L do not change the subspace generated by the vectors in L.*

(i) *replacing a generating vector v_i with a non-zero scalar multiple of itself: $v_i \rightarrow \lambda v_i$*
(ii) *replaciing a generating vector v_j with its sum with a scalar multiple of another generator: $v_j \rightarrow v_j + \lambda v_i$*
(iii) *interchanging two vectors: $v_i \longleftrightarrow v_j$*

Proposition 2.9. *Let $[v_1, \dots, v_n]$ be an $n \times m$ matrix. If an elementary operation (see Corollary 4.2 and Definition 4.3) is applied to this list of vectors, the new list of vectors is matrix that has the same row space. More generally, if $\mathbf{M}$ is a matrix and $\mathbf{M}'$ is a matrix obtained from $\mathbf{M}$ by applying a sequence of elementary row operations to the (row) vectors of $\mathbf{M}$ (and the intermediary matrices). Then*

$$RowSp\,(\mathbf{M}') = RowSp\,(\mathbf{M})$$

Proposition 2.10. *Let $\mathbf{A}$ be an $n \times m$ matrix. Then there exists a sequence of elementary operations that converts $\mathbf{A}$ to a matrix in row echelon form.*

Theorem 2.11. *Let V be an m-dimensional vector space with basis $B = [v_1, \dots, v_m]$ and $\mathbf{A}$ be the coefficient matrix of a set of n non-zero vectors $[u_1, \dots, u_n]$ with respect to B. Suppose that the row vectors $\mathbf{r}_1, \dots, \mathbf{r}_n \in \mathbb{F}^m$ of $\mathbf{A}$ are in row echelon form. Then the vectors $u_1, \dots, u_n$ are linearly independent.*

Theorem 2.12. *Let $\mathbf{A}$ be the coefficient matrix expressing a list $[u_1, \dots, u_n]$ of vectors in V in terms of their coefficients with respect to a basis $B = [v_1, \dots, v_m]$ of V. Then the following statements hold.*

(i) *There exists a matrix $\mathbf{A}'$ row equivalent to $\mathbf{A}$, such that either $\mathbf{A}' = \mathbf{0}$ or there is a uniquely determined positive integer k (between 1 and n) such that the first k rows of $\mathbf{A}'$ are in row echelon form and the remaining rows are all zero.*
(ii) *The vectors $[w_1, \dots, w_k]$ corresponding to the first k rows of $\mathbf{A}'$ form a basis for $span\,(u_1, \dots, u_n)$.*
(iii) *The original set of vectors are linearly independent if and only if $n = k$.*

Lemma 2.13. *If $\{v_1, \dots, v_m\}$ is a linearly dependent set and if $\{v_1, \dots, v_{m-1}\}$ is a linearly independent set then v_m can be expressed as a linear combination of $v_1, \dots, v_{m-1}$.*

Theorem 2.14. *Every finitely generated vector space has a basis.*

Theorem 2.15. *Let $V = span_{\mathbb{F}}\,(v_1, \dots, v_m)$ be a finitely generated vector space. Then a basis for V can be selected from among the set of generators $\{v_1, \dots, v_m\}$. In other words, any set of generators for a finitely generated vector space V contains a basis for V.*

Lemma 2.16. *Suppose* $\mathbf{A}$ *is an* $n \times m$ *matrix with column vectors* $[\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_m]$ *and* $\mathbf{x}$ *is a* $n \times 1$ *column vector with entries* $\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_m \end{bmatrix}$*. Then*

$$\mathbf{A}\mathbf{x} = x_1\mathbf{c}_1 + x_2\mathbf{c}_2 + \cdots + x_m\mathbf{c}_m \quad .$$

Theorem 2.17. *Consider a* $n \times m$ *linear system with coefficient matrix* $\mathbf{A}$ *and inhomogenous part* $\mathbf{b} \in \mathbb{F}^n$*. For each* i *between* 1 *and* n*, let* $\mathbf{c}_i$ *denote the element of* $\mathbb{F}^n$ *formed by writing the entries in the* i^{th} *column of* $\mathbf{A}$ *in order (from top to bottom). Then the linear system has a solution if and only if either of the following two conditions is satisfied.*

(i) $\mathbf{b} \in span\,(\mathbf{c}_1, \ldots, \mathbf{c}_m)$
(ii) $\dim span\,(\mathbf{c}_1, \ldots, \mathbf{c}_m) = \dim span\,(\mathbf{c}_1, \ldots, \mathbf{c}_m, \mathbf{b})$

Proposition 2.18. *Let* $\mathbf{x}$ *be a solution of an* $n \times m$ *linear system* $S\,(\mathbf{A}, \mathbf{b})$*, and let* S *be the solution set of the corresponding homogeneous linear system* $S\,(\mathbf{A}, \mathbf{0})$*. Then the solution set of* $S\,(\mathbf{A}, \mathbf{b})$ *coincides with the hyperplane through* $\mathbf{x}$ *generated by* S*.*

Theorem 2.19. *The reduced row echelon form of an* $n \times m$ *matrix* $\mathbf{A}$ *is unique.*

Proposition 2.20. *If* $[\mathbf{B} \mid \mathbf{c}]$ *is a matrix in reduced row echelon form obtained from* $[\mathbf{A} \mid \mathbf{b}]$ *by a sequence of elementary row operations, then the solutions to the linear system corresponding to* $[\mathbf{A} \mid \mathbf{b}]$ *will be the same as the solutions to the linear system corresponding to* $[\mathbf{B} \mid \mathbf{c}]$*.*

Theorem 2.21. *Let* $\mathbf{A}$ *be an* $n \times m$ *matrix, then the column rank of* $\mathbf{A}$ *equals its row rank.*