Luc TARTAR, University Professor of Mathematics, Wean Hall 6212, tartar@cmu.edu

28- Wednesday November 9, 2011.

Definition 28.1: A *vector space* over a field F (or an F*-vector space*) is an Abelian group for addition $+$ (with identity 0 and inverse of x denoted $-x$), and a *scalar multiplication* (since the elements of F are called *scalars*), which is a mapping from $F\times V$ into V, with the image of (λ, v) denoted $\lambda\, v$, satisfying

$\lambda\,(v_1+v_2)=\lambda\, v_1+\lambda\, v_2$ for all $\lambda\in F$ and all $v_1,v_2\in V$,

$(\lambda_1+\lambda_2)\, v=\lambda_1 v+\lambda_2 v$ for all $\lambda_1,\lambda_2\in F$ and all $v\in V$,

$\lambda_1(\lambda_2 v)=(\lambda_1\lambda_2)\, v$ for all $\lambda_1,\lambda_2\in F$ and all $v\in V$,

$1\, v=v$ for all $v\in V$,

which imply $\lambda\, 0=0$ for all $\lambda\in F$, and $0\, v=0$ for all $v\in V$.

A *linear mapping* from an F-vector space V_1 into an F-vector space V_2 is a mapping L from V_1 into V_2 such that

$L(v+w)=L(v)+L(w)$ for all $v,w\in V_1$,

$L(\lambda\, v)=\lambda\, L(v)$ for all $\lambda\in F$ and all $v\in V_1$,

and the set $L(V_1;V_2)$ of all linear mappings from V_1 into V_2 is an F-vector space.[1] The *kernel* of a linear mapping L is $L^{-1}(\{0\})=\{v_1\in V_1\mid L(v_1)=0\}\subset V_1$, and the *range* of L is the image $\{L(v_1)\mid v_1\in V_1\}\subset V_2$. For an F-vector space V, the *general linear group* $GL(V)$ is the multiplicative group of all *invertible linear mappings* from V into itself.[2]

A *bilinear mapping* B from $V_1\times V_2$ into V_3, where V_1,V_2,V_3 are F-vector spaces, is a mapping such that $v_1\mapsto B(v_1,v_2)$ is linear (from V_1 into V_3) for all $v_2\in V_2$ and $v_2\mapsto B(v_1,v_2)$ is linear (from V_2 into V_3) for all $v_1\in V_1$.

Examples 28.2: If I is non-empty and for each $i\in I$ one is given an F-vector space V_i, then the product $\prod_{i\in I}V_i$ has a natural structure of F-vector space.[3] A particular case is when all V_i are equal to an F-vector space W, which corresponds to considering the (F-vector space of) mappings from I into W; this example is encountered with $W=F$ and $I=\mathbb{N}$ in the case of the ring of formal power series $F[[x]]$. Other F-vector spaces already encountered are the ring of polynomials $F[x]$, the ring of formal Laurent series $F((x))$, as well as any quotient ring $F[x]/(P_0)$ for some $P_0\in F[x]$.

In the case P_0 is an irreducible polynomial of degree n, then $K=F[x]/(P_0)$ is a field, and as an F-vector space it is isomorphic to F^n, since each coset $P+(P_0)$ corresponds to $r+(P_0)$ where $r=a_0+\ldots+a_{n-1}x^{n-1}$ is the remainder in the Euclidean division of P by P_0, and $a_0,\ldots,a_{n-1}$ may be chosen independently in F.

$F[x]$, $F[x]/(P_0)$, $F[[x]]$, and $F((x))$ also have a multiplication, and they are particular cases of an F-vector space V having a product given by a bilinear mapping from $V\times V$ into V, in which case V is called an *algebra* over F.

Remark 28.3: If R is a ring but not a field, one has a similar notion of R-module, or more precisely of left R-module and right R-module in the case where R is not commutative, and the structure of modules is not as simple of that of vector spaces, in particular because one cannot define a notion of dimension, or use a basis as for a vector space. However, if D is a division ring, then the properties of a D-module are exactly similar to that of a vector space.

Definition 28.4: If V is an F-vector space, a *linear combination* of elements of a non-empty subset $A\subset V$ is any element of the form $\sum_{i=1}^n\lambda_i a_i$ with $a_1,\ldots,a_n\in A$ and $\lambda_1,\ldots,\lambda_n\in F$; $span(A)=\{\sum_{i=1}^n\lambda_i a_i\mid n\in\mathbb{N}^\times, a_1,\ldots,a_n\in A,\lambda_1,\ldots,\lambda_n\in F\}$ is the vector *subspace generated by* A. Distinct elements $a_1,\ldots,a_n\in V$ are *linearly dependent* if $\sum_{i=1}^n\lambda_i a_i=0$ and not all λ_i are equal to 0; a non-empty subset $A\subset V$ is *linearly*

[1] If $L_1,L_2\in L(V_1;V_2)$, then L_1+L_2 is the mapping $v\mapsto L_1(v)+L_2(v)$ for all $v\in V_1$, and for $\lambda\in F$, $\lambda\, L_1$ is the mapping $v\mapsto\lambda\, L_1(v)$ for all $v\in V_1$.

[2] Notice that $GL(V)$ is not a vector space. It is a pointed cone in the vector space $L(V;V)$, i.e. one can multiply an element $A\in GL(V)$ by $\lambda\in F^*$, but 0 is not allowed.

[3] If $a=(a_i,i\in I),b=(b_i,i\in I)\in\prod_{i\in I}V_i$, and $\lambda\in F$, then $c=a+b$ and $d=\lambda\, a$ are the elements of $\prod_{i\in I}V_i$ defined by $c_i=a_i+b_i$, $d_i=\lambda\, a_i$ for all $i\in I$.

independent if no non-empty finite subset of A is linearly dependent, i.e. if $n \geq 1$ and $\sum_{i=1}^n \lambda_i a_i = 0$ for distinct elements $a_1, \ldots, a_n \in A$ imply $\lambda_i = 0$ for $i = 1, \ldots, n$. A *basis* of an F-vector space V is a linearly independent set which spans V.

Lemma 28.5: If V is an F-vector space, and $v_1, \ldots, v_n \in V$ for $n \geq 1$, then any $n+1$ (or more) vectors in $span(v_1, \ldots, v_n)$ are linearly dependent.
Proof: One first checks the case $n = 1$, i.e. one considers two vectors, $w_1 = \alpha\, v_1, w_2 = \beta\, v_1$ for some $\alpha, \beta \in F$: since $\beta\, w_1 - \alpha\, w_2 = 0$, it proves linear dependence if α or β is non-zero, but if $\alpha = \beta = 0$ then $w_1 = w_2 = 0$ and any of the two vectors is linearly dependent (since $1\, w_j = w_j = 0$).

One proves the general case by induction on n: one assumes that $n \geq 2$ and that the result is proved for a number of vectors $\leq n-1$, and one chooses $w_1, \ldots, w_{n+1}$ which are linear combinations of $v_1, \ldots, v_n$, i.e. one writes $w_j = \sum_{i=1}^n \lambda_{j,i} v_i$ for some $\lambda_{j,i} \in F, i = 1, \ldots, n, j = 1, \ldots, n+1$; if all $\lambda_{j,n}$ are 0, then $span(v_1, \ldots, v_n) = span(v_1, \ldots, v_{n-1})$, and the induction hypothesis applies; if $\lambda_{j_0,n} \neq 0$, then for $j \neq j_0$ one considers the vectors $z_j = w_j - \lambda_{j_0,n}^{-1} \lambda_{j,n} w_{j_0}$ for $j \neq j_0$, which are linear combinations of $v_1, \ldots, v_{n-1}$, hence the induction hypothesis applies and there exist $\mu_j \in F$ for $j \neq j_0$, not all equal to 0, and such that $\sum_{j \neq j_0} \mu_j z_j = 0$, so that it means $\sum_j \mu_j w_j = 0$ if one defines $\mu_{j_0} = -\sum_{j \neq j_0} \lambda_{j_0,n}^{-1} \lambda_{j,n} \mu_j$, and since not all μ_j are 0 the w_j are linearly dependent.

Definition 28.6: An F-vector space V is *finite-dimensional* if it is generated by finitely many elements, and its *dimension* is the number of elements in a basis (indeed independent of the basis by Lemma 28.5).

Remark 28.7: Every F-vector space V has a basis, because a basis is a maximal family of linearly independent vectors $\{e_i \mid i \in I\}$, since if $W = span(e_i, i \in I)$ was different from V, adding to the family $e_i, i \in I$ any element in $V \setminus W$ would contradict the maximality; then such a maximal family exists by a simple application of "Zorn's lemma". If $f_j, j \in J$ is another basis, then I and J have the same cardinal, even in the case where I (and then J by Lemma 28.5) is infinite: for $i \in I$, e_i can be expressed as a linear combination of the f_j, with non-zero coefficient for $j \in A(i)$, but since $i' \neq i$ could have $A(i') = A(i)$, one puts a total order on I (for example a well order by Zermelo's theorem), and one denotes $\alpha(i)$ the order of i in the set $A^{-1}\big(A(i)\big)$ of indices i' having the same image than i (noticing that this set is finite and has a number of element at most that of $A(i)$ by Lemma 28.5); then the mapping $i \mapsto \big(\alpha(i), A(i)\big)$ is injective from I into $\mathbb{N} \times \mathcal{P}_{finite}(J)$, where $\mathcal{P}_{finite}(J)$ denotes the set of finite subsets of J, and since for J infinite $\mathcal{P}_{finite}(J)$ has the same cardinal than J, and $\mathbb{N} \times J$ has the same cardinal than J, one deduces that $cardinal(I) \leq cardinal(J)$; reversing the roles gives $cardinal(J) \leq cardinal(I)$, hence $cardinal(J) = cardinal(I)$ by the Schröder–Bernstein theorem.[4,5]

Definition 28.8: The *prime subfield* F_0 of a field F is the subfield generated by 0 and 1. If F has *characteristic* 0, the prime subfield is isomorphic to $\mathbb{Q}$, and if F has finite characteristic, necessarily a prime p, then the prime subfield is isomorphic to $\mathbb{Z}_p$.

If E is a subfield of F, one says that F is an *extension field* of E, or that F/E is a *field extension*. F is an E-vector space, whose dimension is denoted $[F\!:\!E]$, and F is called a *finite-dimensional extension* (or a *finite extension*) if $[F\!:\!E] < \infty$, and an *infinite-dimensional extension* (or *infinite extension*), if $[F\!:\!E] = \infty$.

Lemma 28.9: If F is a finite field, then $|F| = p^k$ for a prime p (the characteristic of F) and a positive integer k.
Proof: Let F_0 be the prime subfield of F, isomorphic to $\mathbb{Z}_p$ for the characteristic p of F. Then F is an F_0-vector space, necessarily of finite dimension k, so that F is isomorphic to F_0^k as F_0-vector spaces.

Remark 28.10: It can be shown that, for each prime p and each $k \geq 1$, there is only one finite field with $q = p^k$ elements, up to isomorphism (as fields), and one denotes it F_q.

---

[4] Friedrich Wilhelm Karl Ernst Schröder, German mathematician, 1841–1902. He worked in Darmstadt, and in Karlsruhe, Germany. The Schröder–Bernstein theorem is partly named after him (Cantor stated it without giving a proof, which Bernstein provided in 1898, and Schröder obtained it independently the same year).

[5] Felix Bernstein, German mathematician, 1878–1956. He worked at Georg-August-Universität, Göttingen, Germany. The Schröder–Bernstein theorem is partly named after him (Cantor stated it without giving a proof, which Bernstein provided in 1898, and Schröder obtained it independently the same year).