向量空间的基本性质

给定F为域，X为F上的向量空间，n为自然数，$v_1, v_2, \ldots, v_n \in X$.

1. 称$v_1, v_2, \ldots, v_n$在F上**线性无关**，如果
$$\forall a_1, a_2, \ldots, a_n \in F, \sum_{i=1}^{n} a_i v_i = 0 \implies a_1 = a_2 = \ldots a_n = 0.$$
反之，则称$v_1, v_2, \ldots, v_n$在F上线性相关。
2. 称X可由$v_1, v_2, \ldots, v_n$**生成**，如果
$$\forall w \in X, \text{存在} a_1, a_2, \ldots, a_n \in F, \text{ 使得} w = \sum_{i=1}^{n} a_i v_i.$$
3. 若$v_1, v_2, \ldots v_n$在F上线性无关，且X由$v_1, v_2, \ldots, v_n$生成，则称$v_1, v_2, \ldots v_n$是X的一组**基**。

最典型的例子还是F^n, 一组基是

$$\begin{aligned}
e_1 &= (1, 0, 0, \ldots, 0) \\
e_2 &= (0, 1, 0, \ldots, 0) \\
e_3 &= (0, 0, 1, \ldots, 0) \\
&\cdots\cdots\cdots\cdots\cdots\cdots \\
e_n &= (0, 0, 0, \ldots, 1)
\end{aligned}$$

4. 若$v_1, v_2, \ldots v_n$是${}_F X$(这个符号表示F上的线性空间X)的一组基，则称${}_F X$是n维的向量空间。记作$\dim_F X = n$. 若不存在n使得$\dim_F X = n$，则称${}_F X$是无穷维的向量空间。

定义4本身并不保证“维数”的**唯一性**。这个**唯一性**由下面的命题保证。

命题 1

设X中的元素$w_1, w_2, \ldots, w_n, w_{n+1}$每个都可由$u_1, u_2, \ldots, u_n$线性表出，则$w_1, w_2, \ldots w_{n+1}$在$F$上线性相关。
上述命题可以由**归纳法**证明，此处从略。

一个无穷维向量空间的例子是$\mathbb{R}$，作为$\mathbb{Q}$上的向量空间。证明是容易的，假设$\dim_{\mathbb{Q}} \mathbb{R} = n$, 则$\mathbb{R}$与$\mathbb{Q}^n$一一对应。由$\mathbb{Q}$可列，知$\mathbb{R}$可列，矛盾。(《集合与图论》课程的结论：可列集的有限笛卡尔基可列）

命题 2

设K为域，F是K的子域，$\alpha \in K$，则α是K上的代数元当且仅当$F(\alpha)$作为F上的向量空间是有限维的。（前面结论的直接推论）（）（）（）

证明

设$f \in F[x], f \neq 0$是α在F上的极小多项式，$\deg f = n$，则$\dim_F F(\alpha) = n$，一组基是$1, \alpha, \ldots, \alpha^{n-1}$.

命题 3

设$\dim_F X = n, U$是X上的一个$F-$子空间（回顾定义：满足加法和数乘的封闭性即可），则$_F U$也是有限维的，且$\dim_F U \leq n$，并且

$$\dim_F U = \dim_F X \iff U = X$$

对于这个结论，**域**的性质也是必要的。在环上未必有如此性质。该命题可由命题1证明。

命题 4

设K为域，E为K的子域，$\dim_E K = n$，F为E的子域，$\dim_F E = m$. 则有

$$\dim_F K = mn = \dim_F E \cdot \dim_E K$$

证明

由$\dim_E K = n$，存在$v_1, \ldots v_n$是$_E K$上的一组基，同理存在$u_1, \ldots, u_m$是$_F E$上的一组基。我们断言

$$\{u_i v_j \mid 1 \leq i \leq m, 1 \leq j \leq n\}$$

是$_F K$上的一组基。
为此，首先说明K中任意元素都可由$u_i v_j$按F上的系数线性表出：任取$y \in K$, 则存在$b_1, \ldots, b_n \in E$，使得

$$y = \sum_{i=1}^{n} b_i v_i$$

又对于每个b_i，都存在$a_{1i}, a_{2i}, \ldots, a_{mi} \in F$，使得

$$b_i = \sum_{j=1}^{m} a_{ji} u_j$$

于是有

$$\begin{aligned} y &= \sum_{i=1}^{n} (\sum_{j=1}^{m} a_{ji} u_j) v_i \\ &= \sum_{i=1}^{n} \sum_{j=1}^{m} a_{ji} (u_j v_i) \end{aligned}$$

这就是线性表出。

另一方面，要证明$(u_i v_j)$在F上线性无关。对于满足

$$\sum_{i=1}^{n}\sum_{j=1}^{m} a_{ji}u_j v_i = 0$$

的一组元素$(a_{ji}) \in F$. 则有

$$0 = \sum_{i=1}^{n}\sum_{j=1}^{m} a_{ji}u_j v_i = 0 = \sum_{i=1}^{n}(\sum_{j=1}^{m} a_{ji}u_j)v_i$$

则由$v_1, \dots, v_n$线性无关知

$$\sum_{j=1}^{m} a_{ji}u_j = 0,\ \ i = 1, 2, \dots, n$$

于是最后由$u_1, \dots, u_m$线性无关，知$a_{1i} = a_{2i} = \dots a_{mi} = 0, i = 1, 2, \dots, n$. 综上可知原命题成立。

$\mathbb{F}_2$上的可逆矩阵

定义

$$M_n(\mathbb{F}_2) := \{A \mid A\text{是}\mathbb{F}_2\text{上的}n\text{阶方阵}\}$$

以及

$$GL_n(\mathbb{F}_2) := \{\mathbb{F}_2\text{上的所有}n\text{阶可逆矩阵}\}$$

我们试图对$GL_n(\mathbb{F}_2)$计数。先来看二阶的情形：考虑$\mathbb{F}_2$上的二阶方阵

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

若不加限制，则每行有2^2种选择。可逆矩阵不允许出现零行，故每行最多有2^2-1种选择；第二行不可由第一行线性表出，于是取定第一行后，第二行至多有2^2-2种选择。于是有

$$\mid GL_2(\mathbb{F}_2) \mid = (2^2-1)(2^2-2)$$

对于三阶方阵，前两行的情形与二阶方阵的情形类似，共有$(2^3-1)(2^3-2)$种取法；对于第三行，我们要求它不能有**前两行**线性表出。取定前两行的情况下，**已知前两行线性无关**，那么前两行一共可以线性表出2^2个元素（我们有两个系数可以选取，每个系数有两个取值，并且由于**线性无关**，每种系数选取对应不同的表出结果），于是第三行共有2^3-2^2种取法。于是有

$$\mid GL_3(\mathbb{F}_2) \mid = (2^3-1)(2^3-2)(2^3-2^2)$$

事实上，我们从这里也可以看出，不可能再找“第四行”了，因为如果有，那么它的取法是2^3-2^3种。

从这两种简单的情况已经可以看出一般情形的计算方法了，我们略去。容易看出

$$|\ GL_n(\mathbb{F}_2)\ |=\prod_{i=0}^{n}(2^n-2^{i-1})$$

并且容易计算$v_2(|\ GL_n(\mathbb{F}_2)\ |)=0+1+\ldots+n-1=\frac{n(n-1)}{2}$.