线性代数

王丹阳

2020/7/22

目录

第一章 线性方程组

线性方程组是高等代数研究问题的起点

1.1 一些概念

由对 n 元线性方程组的高斯消元法求解引入矩阵及其相关基本概念

$$\begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + \cdots + a_{2n}x_n = b_2 \\ \cdots \\ a_{s1}x_1 + \cdots + a_{sn}x_n = b_s \end{cases}$$

求解过程中不难发现方程组的解只与系数和常数项有关。为此我们从中抽象出一个数学模型，把它叫矩阵。

定义 1.1.1 由 $s \cdot n$ 个数排成 s 行，n 列的一张数表称为一个 $s \times n$ 矩阵，矩阵常用大写字母 A, B, C 表示. 若令 $A = (a_{ij})_{s\times n}$，则其第 i 行，第 j 列个元素可表示为 $A(i;j)$ 或 a_{ij}

定义 1.1.2 线性方程组系数所组成的矩阵称为系数矩阵，带上常数项后称为增广矩阵

易知，高斯消元法中所用到的变换不改变方程组的解，因此引入矩阵初等行变换的概念

定义 1.1.3 称以下三种变换为矩阵的初等行变换:

- 用一个非零数乘以一行
- 交换两行
- 用一行的倍数加到另一行

由最后的求解又引入了行阶梯型矩阵和行最简型矩阵、主元。主元反映到线性方程组中又产生了主变量和自由变量的概念。

定义 1.1.4 (行阶梯形矩阵) 一个矩阵是行阶梯型矩阵，当且仅当它满足:

- 若有零行，零行在最下方

- 对于非零行，从左到右第一个非零元称为主元，主元的列指标随着行指标的增大严格增大

定义 1.1.5 (行最简型矩阵) 一个矩阵是行最简型矩阵，当且仅当它满足：

- 是行阶梯型矩阵
- 主元都是 *1*
- 主元所在列的其它元素都是 *0*

定义 1.1.6 (主变量) 以主元为系数的便量称为主变量，其它变量称为自由变量

1.2　线性方程组的解的情形及判别准则

根据一些例子不难猜想出线性方程组的解有三种情形：

1. 当方程出现不相容时，无解
2. 有唯一解
3. 有无穷多解

现予以说明：首先将对应的增广矩阵化为行阶梯型，设变量有 n 个，此时有 r 个非零行。

- 若某行出现"$0 = d(d \neq 0)$" 时，显然无解
- 由主元的定义知有 r 个主元，故 $r \leq n$
  - 当 $r = n$ 时，继续将行阶梯型化为行最简型，可直接得到此时有唯一解
  - 当 $r < n$ 时，存在自由变量，此时有无穷多解

定理 1.2.1 (线性方程组解的情况及判定准则) n 元线性方程组的解的情形只有三种：

- 无解 $\Longleftrightarrow$ 出现"$0 = d(d \neq 0)$"
- 有唯一解 $\Longleftrightarrow$ 增广矩阵化行阶梯型非零行行数 $r = n$
- 有无穷多解 $\Longleftrightarrow$ 增广矩阵化行阶梯型非零行行数 $r < n$

推论 1 n 元齐次线性方程组的解的情形有两种：

- 有唯一零解 $\Longleftrightarrow$ 系数矩阵化行阶梯型非零行行数 $r = n$
- 有无穷多解 $\Longleftrightarrow$ 系数矩阵化行阶梯型非零行行数 $r < n$

1.3　数域

之前我们对线性方程组默认是系数对加减乘除都封闭，但是有些方程组在整数范围内不一定有解，例如:

$$\begin{cases} x+y=1 \\ x-y=0 \end{cases}$$

这种情形对我们的求解造成了额外的困扰。因此，要使我们所做的初等变换是合理的，我们引入数域的概念。

定义 1.3.1 (数域) 设集合 K 是复数集的一个子集，如果 K 满足：

1. $0,1\in K$
2. K 对加减乘除运算封闭

则称 K 是一个数域

推论 2 根据定义容易验证最小的数域是有理数域，最大的数域是复数域

第二章　行列式

为了直接从线性方程组的系数出发探究线性方程组的解的情况。我们先从解剖“麻雀”—2 个未知数，2 个线性方程的方程组开始。对方程组：

$$\begin{cases} a_{11}x_1 + a_{12}x_2 = b_1 \\ a_{21}x_1 + a_{22}x_2 = b_2 \end{cases}$$

a_{11}, a_{21} 不全为 0，不妨设 $a_{11} \neq 0$, 对其增广矩阵化行阶梯型有：

$$\begin{bmatrix} a_{11} & a_{12} & b_1 \\ 0 & a_{22} - a_{12}\frac{a_{21}}{a_{11}} & b_2 - b_1\frac{a_{21}}{a_{11}} \end{bmatrix}$$

不难得出以下结论：

- $a_{22} - a_{12}\frac{a_{21}}{a_{11}} \neq 0$

  $$\Longleftrightarrow$$

  原方程有唯一解

- $a_{22} - a_{12}\frac{a_{21}}{a_{11}} = 0$

  $$\Longleftrightarrow$$

  原方程无解或有无穷多解

由此我们给出二阶行列式的定义

定义 2.0.1 设 2 阶方阵

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$$

, 则其行列式为

$$detA = |A| = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{12}a_{21}$$

注 1 2 阶行列式有 2! 项，每一项的元素都取自不同行不同列，每一项的正负由行指标按顺序排列后，列指标排列的逆序对个数决定

有上面的分析, 容易得到以下定理：

定理 2.0.1 对于两个方程的二元一次方程组：

- 有唯一解 $\Leftrightarrow$ 系数矩阵的行列式不等于零
- 无解或无穷多解 $\Leftrightarrow$ 系数矩阵的行列式等于零

对于 n 个方程的 n 元线性方程组，能否用所谓的 n 阶行列式反应其解的情况呢？实际上是可以的。

注 2 n 阶行列式的定义方式并不自然，暂时也只能这样了。

2.1　n 元排列

由二阶行列式的定义与列指标排列的逆序对个数有关，为了给出 n 阶行列式的每一项的符号，我们需要先研究一个 n 元排列的奇偶性

定义 2.1.1 n 个不同整数的一个全排列称为一个 n 元排列

定义 2.1.2 一个 n 元排列中任意取两个数，若大的在前，小的在后，则这两个元素形成了一个逆序对。

定义 2.1.3 对一个 n 元排列，若逆序对个数为奇数个，则称其为奇排列，反之称为偶排列。

定理 2.1.1 相邻两个元素交换改变排列的奇偶性

不难推出：

定理 2.1.2 任意两个元素交换改变排列的奇偶性，即*:*

$$(-1)^{\tau(p_1p_2\cdots p_{i-1}\boldsymbol{p_i}p_{i+1}\cdots p_{j-1}\boldsymbol{p_j}p_{j+1}\cdots p_n)} = (-1)\times(-1)^{\tau(p_1p_2\cdots p_{i-1}\boldsymbol{p_j}p_{i+1}\cdots p_{j-1}\boldsymbol{p_i}p_{j+1}\cdots p_n)}$$

2.2　n 阶行列式的定义

2.2.1　行指标有序的定义方式

仿照 2 阶行列式，n 阶行列式的每一项都是 n 个不同行不同列的元素的乘积，共有 $n!$ 项，每一项的正负由行指标按顺序排列后，列指标排列的逆序对个数决定，因而对 n 阶行列式定义如下：

定义 2.2.1 设 n 阶方阵

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}$$

定义其行列式

$$detA = |A| = \sum_{j_1j_2\cdots j_n} (-1)^{\tau(j_1j_2\cdots j_n)} a_{1j_1}a_{2j_2}\cdots a_{nj_n}$$

2.2.2　更一般的定义方式

上面每一项的行指标都是有序排列的，但每一项的 n 个元素的乘积可以按任意次序相乘。即若将每一项的行指标混排，其符号该如何确定呢？
对 $a_{1j_1}a_{2j_2}\cdots a_{nj_n}$ 这一项，假设经过 s 次对换变为排列 $a_{k_1p_1}a_{k_2p_2}\cdots a_{k_np_n}$, 则对于行指标排列的奇偶性和列指标排列的奇偶性分别有：

$$\begin{cases}(-1)^s(-1)^{\tau(12\cdots n)}=(-1)^{\tau(k_1k_2\cdots k_n)}\\(-1)^s(-1)^{\tau(p_1p_2\cdots p_n)}=(-1)^{\tau(j_1j_2\cdots j_n)}\end{cases}$$

故有

$$(-1)^{\tau(k_1k_2\cdots k_n)+\tau(p_1p_2\cdots p_n)}=(-1)^{\tau(j_1j_2\cdots j_n)}$$

和

$$(-1)^{\tau(k_1k_2\cdots k_n)+\tau(p_1p_2\cdots p_n)}a_{k_1p_1}a_{k_2p_2}\cdots a_{k_np_n}=(-1)^{\tau(j_1j_2\cdots j_n)}a_{1j_1}a_{2j_2}\cdots a_{nj_n}$$

由上面的分析，容易导出以下两条性质：

定理 2.2.1 (行列式的一般定义) 给定行指标的一个排列 $k_1k_2\cdots k_n$, n 级矩阵 A 的行列式

$$|A|=\sum_{p_1p_2\cdots p_n}(-1)^{\tau(k_1k_2\cdots k_n)+\tau(p_1p_2\cdots p_n)}a_{k_1p_1}a_{k_2p_2}\cdots a_{k_np_n}$$

若每一项按照列指标自然序排好位置，那么

定理 2.2.2

$$|A|=\sum_{i_1i_2\cdots i_n}(-1)^{\tau(i_1i_2\cdots i_n)}a_{i_11}a_{i_22}\cdots a_{i_nn}$$

注 3 上面这条定理其实已经说明行列式的行和列具有相同的地位

2.3　行列式的性质

从探究系数矩阵 A 的初等变换会对它的行列式产生什么样的影响这个问题出发我们容易探究出关于行列式的一系列性质：

1. $|A|=|A^T|$ 这一条由定义可以直接导出，说明了对行成立的性质对列也成立，故下面只注明行的性质

2. 一行的公因子可以提出

3. 互换两行行列式变号

4. 若某一行是两组数的和，则行列式可以拆成两个行列式的和，他们的这一样分别是上述两组数，其它行不变

5. 有两行相同，则行列式的值为 0

6. 行列式中有两行成比例，则行列式的值为 0

7. 把一行的倍数加到另一行上，行列式的值不变

以上性质全都可以由定义为出发点推导得来

2.4　行列式按一行/列展开

注意这样一句话：行列式的每一项都是不同行不同列的元素的乘积，因而在取定一个元素 a_{ij} 后，d 第 i 行，第 j 列的元素都不能取了。

由于 n 阶行列式可以按一行一直分解至 n 个行列式的和，不难得出行列式按一行（列）展开的定理

先铺垫如下概念：

定义 2.4.1 (（代数）余子式) n 阶行列式 $|A|$ 中，取定一个元素 a_{ij}，则划去该元素所在的第 i 行，第 j 列，剩下的元素按原来次序组成的 $n-1$ 阶行列式称为元素 a_{ij} 的余子式，记为 M_{ij},$(-1)^{i+j}M_{ij}$ 称为元素 a_{ij} 的代数余子式，记为 A_{ij}

定理 2.4.1 行列式的一行（列）展开对 n 阶行列式 $|A|$，

- 按第 i 行展开有：
$$|A| = \sum_{j=1}^{n} a_{ij}A_{ij}$$

- 按第 j 列展开有：
$$|A| = \sum_{i=1}^{n} a_{ij}A_{ij}$$

容易从行列式的分解性质和交换行的性质得到，先给出按一行展开的形式化的证明

证明 1 对 n 阶行列式 $|A|$，取定第 i 行，并把每一项的元素 a_{ij} 放到第一个位置，其余 $n-1$

个元素按自然序排好位置，根据列指标 $j=1,2,\cdots,n$ 将 $|A|$ 的 $n!$ 项分成 n 组，则有：

$$\begin{aligned}
|A| &= \sum_{jk_1\cdots k_{i-1}k_{i+1}\cdots k_n} (-1)^{\tau(i1\cdots,i-1,i+1,\cdots n)+\tau(jk_1\cdots k_{i-1}k_{i+1}\cdots k_n)} a_{ij}a_{1k_1}\cdots a_{i-1,k_{i-1}}a_{i+1,k_{i+1}}\cdots a_{nk_n} \\
&= \sum_{jk_1\cdots k_{i-1}k_{i+1}\cdots k_n} (-1)^{i-1+j-1+\tau(k_1\cdots k_{i-1}k_{i+1}\cdots k_n)} a_{ij}a_{1k_1}\cdots a_{i-1,k_{i-1}}a_{i+1,k_{i+1}}\cdots a_{nk_n} \\
&= \sum_{jk_1\cdots k_{i-1}k_{i+1}\cdots k_n} (-1)^{i+j}a_{ij}\cdot(-1)^{\tau(k_1\cdots k_{i-1}k_{i+1}\cdots k_n)} a_{1k_1}\cdots a_{i-1,k_{i-1}}a_{i+1,k_{i+1}}\cdots a_{nk_n} \\
&= \sum_{j=1}^{n}(-1)^{i+j}a_{ij}\left[\sum_{k_1\cdots k_{i-1}k_{i+1}\cdots k_n} (-1)^{\tau(k_1\cdots k_{i-1}k_{i+1}\cdots k_n)} a_{1k_1}\cdots a_{i-1,k_{i-1}}a_{i+1,k_{i+1}}\cdots a_{nk_n}\right] \\
&= \sum_{j=1}^{n}(-1)^{i+j}a_{ij}M_{ij}(\text{根据定义}) \\
&= \sum_{j=1}^{n} a_{ij}A_{ij}
\end{aligned}$$

证毕

2.5　行列式按 k 行/列展开

定义 2.5.1 (k 阶子式) 对 n 级矩阵 A, 任取 k 行 $i_1,\cdots,i_k$, 其中 $1\le i_1<\cdots<i_k\le n$, k 列 $j_1,\cdots,j_k$, 其中 $1\le j_1<\cdots<j_k\le n$, 这 k 行 k 列交叉处按原来的次序形成的行列式称为 A 的 k 阶子式，记为

$$A\begin{pmatrix} i_1 & \cdots & i_k \\ j_1 & \cdots & j_k \end{pmatrix}$$

定义 2.5.2 (（代数）余子式) 令 $\{i_1',\cdots,i_{n-k}'\}=\{1,2,\cdots,n\}\backslash\{i_1,\cdots,i_k\}$, 其中 $1\le i_1'\le\cdots\le i_{n-k}'$；$\{j_1',\cdots,j_{n-k}'\}=\{1,2,\cdots,n\}\backslash\{j_1,\cdots,j_k\}$, 其中 $1\le j_1'\le\cdots\le j_{n-k}'$, 则称

$$A\begin{pmatrix} i_1' & \cdots & i_{n-k}' \\ j_1' & \cdots & j_{n-k}' \end{pmatrix}$$

为上述 k 阶子式的余子式称

$$(-1)^{(i_1+\cdots+i_k)+(j_1+\cdots+j_k)}A\begin{pmatrix} i_1' & \cdots & i_{n-k}' \\ j_1' & \cdots & j_{n-k}' \end{pmatrix}$$

为上述 k 阶子式的代数余子式

定理 2.5.1 (Laplace 定理) 取定行列式 $|A|$ 的 k 行，则这 k 行形成的 k 阶子式与其对应的代数余子式乘积之和就是行列式的值, 即

$$|A|=\sum_{1\le j_1<\cdots<j_k\le n} A\begin{pmatrix} i_1 & \cdots & i_k \\ j_1 & \cdots & j_k \end{pmatrix}(-1)^{(i_1+\cdots+i_k)+(j_1+\cdots+j_k)}A\begin{pmatrix} i_1' & \cdots & i_{n-k}' \\ j_1' & \cdots & j_{n-k}' \end{pmatrix}$$

证明 2 取定 $|A|$ 的 k 行，将这 k 行形成的 $\mathbf{C}_n^k$ 个 k 阶子式分组，并把这 k 行的 k 个元素排在最前面，则：

$$|A| = \sum_{u_1\cdots u_k v_1\cdots v_{n-k}} (-1)^{i_1+\cdots+i_k-\frac{k(k+1)}{2}\tau(u_1\cdots u_k v_1\cdots v_k)} a_{i_1u_1}\cdots a_{i_ku_k}a_{i_1'v_1}\cdots a_{i_{n-k}'v_{n-k}}$$

其中 $u_1\cdots u_k$ 是 $j_1,\cdots,j_k$ 的一个 k 元排列；$v_1\cdots v_{n-k}$ 是 $j_1',\cdots,j_{n-k}'$ 的一个 $n-k$ 元排列；分组思路为：

1. 先从 n 列中任取 k 列：$j_1,\cdots,j_k$

2. $u_1\cdots u_k$ 是列指标 $j_1,\cdots,j_k$ 的一个全排列

3. $v_1\cdots v_{n-k}$ 是剩下的列指标 $j_1',\cdots,j_{n-k}'$ 的一个全排列

另外，假设排列 $u_1\cdots u_k$ 经过 s 次对换变为 $j_1\cdots j_k$ 则:

$$(-1)^{\tau(u_1\cdots u_k)} = (-1)^s(-1)^{\tau(j_1,\cdots,j_k)} = (-1)^s$$

从而：

$$\begin{aligned}
&(-1)^{\tau(u_1\cdots u_k v_1\cdots v_{n-k})}\\
&=(-1)^s(-1)^{\tau(j_1\cdots j_k v_1\cdots v_{n-k})}\\
&=(-1)^{\tau(u_1\cdots u_k)}(-1)^{j_1+\cdots+j_k-\frac{k(k+1)}{2}+\tau(v_1\cdots v_{n-k})}\\
&=(-1)^{j_1+\cdots+j_k-\frac{k(k+1)}{2}}(-1)^{\tau(u_1\cdots u_k)+\tau(v_1\cdots v_{n-k})}
\end{aligned}$$

于是有：

$$\begin{aligned}
|A| &= \sum_{u_1\cdots u_k v_1\cdots v_{n-k}} (-1)^{\tau(i_1\cdots i_k i_1'\cdots i_{n-k}')+\tau(u_1\cdots u_k v_1\cdots v_k)} a_{i_1u_1}\cdots a_{i_ku_k}a_{i_1'v_1}\cdots a_{i_{n-k}'v_{n-k}}\\
&= \sum_{u_1\cdots u_k v_1\cdots v_{n-k}} (-1)^{i_1+\cdots+i_k-\frac{k(k+1)}{2}+\tau(u_1\cdots u_k v_1\cdots v_k)} a_{i_1u_1}\cdots a_{i_ku_k}a_{i_1'v_1}\cdots a_{i_{n-k}'v_{n-k}}\\
&= \sum_{1\le j_1<\cdots<j_k}\sum_{u_1\cdots u_k}\sum_{v_1\cdots v_{n-k}} (-1)^{i_1+\cdots+i_k-\frac{k(k+1)}{2}+j_1+\cdots+j_k-\frac{k(k+1)}{2}}(-1)^{\tau(u_1\cdots u_k)+\tau(v_1\cdots v_{n-k})}.\\
&\quad a_{i_1u_1}\cdots a_{i_ku_k}a_{i_1'v_1}\cdots a_{i_{n-k}'v_{n-k}}\\
&= \sum_{1\le j_1<\cdots<j_k} (-1)^{(i_1+\cdots+i_k)+(j_1+\cdots+j_k)} \sum_{u_1\cdots u_k}(-1)^{\tau(u_1\cdots u_k)}a_{i_1u_1}\cdots a_{i_ku_k}\sum_{v_1\cdots v_{n-k}}(-1)^{\tau(v_1\cdots v_k)}a_{i_1'v_1}\cdots a_{i_{n-k}'v_{n-k}}\\
&= \sum_{1\le j_1<\cdots<j_k\le n} A\begin{pmatrix} i_1 & \cdots & i_k\\ j_1 & \cdots & j_k\end{pmatrix}(-1)^{(i_1+\cdots+i_k)+(j_1+\cdots+j_k)}A\begin{pmatrix} i_1' & \cdots & i_{n-k}'\\ j_1' & \cdots & j_{n-k}'\end{pmatrix} \text{(根据定义)}
\end{aligned}$$

2.6　范德蒙（Vandermonde）行列式

数学归纳法易证：

$$\begin{vmatrix} 1 & 1 & \cdots & 1 \\ x_1 & x_2 & \cdots & x_n \\ x_1^2 & x_2^2 & \cdots & x_n^2 \\ \vdots & \vdots & & \vdots \\ x_1^{n-1} & x_2^{n-1} & \cdots & x_n^{n-1} \end{vmatrix} = \prod_{1\le j<i\le n}(x_i - x_j)$$

2.7　Cramer 法则及其补充

定理 2.7.1 (n **个方程的** n **元线性方程组解的行列式判定准则)** 对含 n 个方程的 n 元线性方程组，设其系数矩阵为 A, 增广矩阵为 $\widetilde{A}$, 对应的行阶梯型矩阵分别为 J,$\widetilde{J}$, 则 $|J| = \lambda|A|(\lambda \neq 0)$. 且有如下判定定理:

- 无解 $\iff$ $\widetilde{J}$ 中出现"$0 = d(d \neq 0)$" $\overset{\text{左箭头可由}}{\underset{\text{反证法得到}}{\iff}}$ J 中的有零行 $\iff |J| = 0 \iff |A| = 0$
- 有唯一解 $\iff$ 增广矩阵化行阶梯型非零行行数 $r = n \iff J$ 中有 n 个主元 $\iff |J| \neq 0 \iff |A| \neq 0$
- 有无穷多解 $\iff$ 增广矩阵化行阶梯型非零行行数 $r < n \iff J$ 中的有零行 $\iff |J| = 0 \iff |A| = 0$

推论 3 n 元齐次线性方程组的解的情形有两种：

- 有唯一零解 $\iff$ 系数矩阵化行阶梯型非零行行数 $r = n \iff |A| \neq 0$
- 有非零解/有无穷多解 $\iff$ 系数矩阵化行阶梯型非零行行数 $r < n \iff |A| = 0$

TODO: Cramer 法则后面会利用矩阵证明

第三章　向量空间

3.1　预备知识-域

运算说白了就由运算对象按照一定的运算法则生成运算结果。这样就很容易用映射来给出运算的数学定义

定义 3.1.1 对于非空集合 X,Y，我们称映射 $\varphi: X \to Y$ 为从 X 到 Y 的一元运算，当 $X = Y$ 时，称 φ 是定义在 X 上的一元（代数）运算

定义 3.1.2 对于非空集合 X,Y,Z，我们称映射 $\varphi: X \times Y \to Z$ 为从 $X \times Y$ 到 Z 的二元运算，当 $X = Y = Z$ 时，称 φ 是定义在 X 上的二元（代数）运算

类似地可定义 n 元代数运算

强调几个点：

- φ 只是一个抽象的运算符号，可以是任何东西，但数学中常用 $+, \cdot, *$ 等表示二元运算符
- 运算符的位置有前缀、中缀、后缀三种。常用的是中缀，例如将 $\circ(x,y)$ 写成 $\circ xy, x \circ y, xy\circ$
- 对于定义在非空集合 X 上的一个运算 $*$, 其封闭性显然已蕴含在定义中

在集合之上定义了运算之后，这种运算就赋予了集合元素之间一种代数结构，例如在 $\mathbb{N}$ 之上定义了加法之后，就有 $1 + 3 = 4$，这就在这三个元素之间形成了结构

定义 3.1.3 设 $*$ 是定义在非空集合 S 上的一个运算，则称二元组 $(S,*)$ 为一个（有一个代数运算的）代数系

类似的，可以定义含更多个运算的代数系

对于含一个二元代数运算的代数系，我们关注该运算的交换律和结合律

定义 3.1.4 (交换律、结合律) 设 $(X,*)$ 是一个代数系，$*$ 是二元运算

- 若 $\forall a,b \in X$，恒有 $a * b = b * a$, 则称 $*$ 满足结合律
- 若 $\forall a,b,c \in X$，恒有 $(a * b) * c = a * (b * c)$, 则称 $*$ 满足结合律

同样的，二元代数运算的单位元素，以及由此引入的逆元素的概念同样很重要

定义 3.1.5 (单位元素、逆元素) 设 $(S,*)$ 是一个代数系，$*$ 是二元运算

- 若 $\exists e\in S$，使得 $\forall a\in S$, 恒成立 $e*a=a*e=a$, 则称 e 为 $*$ 的单位元素（也叫幺元，其中幺有数目中的一的含义）。类似地可以定义左单位元素和右单位元素的概念。
- 若 $\forall a\in S\ \exists b\in S$，使得 $a*b=b*a=e$ 则称 b 是 a 在运算 e 下的逆元。

当一个代数系有两个二元代数运算时，这两个运算的交互能否满足分配律是我们关注的

定义 3.1.6 设 $(S,*,+)$ 是一个代数系，$*,+$ 是二元运算，若 $\forall a,b,c\in S$，恒有 $a*(b+c)=a*b+a*c$, 则称 $*$ 对 $+$ 满足左分配律，类似地可以定义右分配律，左右分配律都满足则称 $*$ 对 $+$ 满足分配律

有了上面的准备，我们可以着手定义**域**

定义 3.1.7 设 $(S,+,\cdot)$ 是一个代数系统，$+,\cdot$ 是二元运算（不妨分别称之为加法和乘法），则 $(S,+,\cdot)$ 是一个域当且仅当满足以下五个条件:

1. $+,\cdot$ 满足交换律
2. $+,\cdot$ 满足结合律
3. $+,\cdot$ 有单位元（不妨分别记作 0，1）
4. $\forall x\in S$, 存在加法逆元；$x\neq 0$ 时，存在乘法逆元
5. $\cdot$ 对 $+$ 有分配律

进一步地，不妨将 a 的加法逆元记为 $-a$, 乘法逆元记为 a^{-1}，将减法 $-$ 和除法 $\div$ 分别定义为

$$a-b=a+(-b);a\div b=a\cdot b^{-1}$$

定理 3.1.1 由 a 是 $-a$ 的加法逆元，是 a^{-1} 的乘法逆元立即可得

- $a=-(-a)$
- $a=(a^{-1})^{-1}$

定理 3.1.2 (消去律) $(F,+,\cdot)$ 是一个域，$\forall a,b\in F$，有

- 若 $a+b=a+c$，则 $b=c$
- 若 $a\cdot b=a\cdot c$ 且 $a\neq 0$，则 $b=c$

推论 4 域中的单位元、逆元都唯一

定理 3.1.3 $(F,+,\cdot)$ 是一个域，$\forall a,b\in F$，有

- $a \cdot 0 = 0$
- $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$
- $(-a) \cdot (-b) = a \cdot b$

推论 5 域中的加法单位元没有乘法逆元