习题课讲义：有限域与线性方程组

1. 有限域的性质

设 F 为域，若 $|F|<+\infty$，则称 F 为有限域。

则 F 的素域一定同构于 $\mathbb{Z}_p$，其中 p 为 F 的特征。
记 F_p 为 F 的素域，则 $|F_p|=p$，因为 $F_p\cong\mathbb{Z}_p$.
Freshmen's dream

$$\forall x,y\in F,\quad (x+y)^p=x^p+y^p.$$

下面我们可以做如下对照：

$$\mathbb{R}^n \longrightarrow \mathbb{R}$$

$$F \longrightarrow F_p$$

我们已经学过了如何在一个 $\mathbb{R}^n$ 的线性闭集中找出一组极大线性无关集。下面我们可以类似地将 F 看成 F_p 上的线性空间：我们需要定义线性运算。

加法：$\forall x,y\in F$，$x+y$ 即为域中加法。

数乘：因为 $F_p\subseteq F$，则可以定义乘法：$\forall r\in F_p$，
$a\in F$，$r\cdot a\in F$.

由此可以定义线性相关与线性无关：

$\forall a_1,\cdots,a_n\in F$，若存在 $c_1,c_2,\cdots,c_n\in F_p$，不全为零，使得

$$c_1a_1+c_2a_2+\cdots+c_na_n=0$$

则称 $a_1,\cdots,a_n$ 线性相关。否则线性无关。

命题1：$|F|=p^n$，其中n为非负整数.

证明：下面我们先构造F中一组线性无关组.

若$F=\{0\}$，则取$n=0$即可，否则存在$a_1\in F$且$a_1\neq 0$，可以由定义得$\{a_1\}$是线性无关的.

令$\langle a_1\rangle=\{ra_1 \mid r\in \mathbb{F}_p\}$，$\langle a_1\rangle$为一个线性闭集.

若$F=\langle a_1\rangle$，则构造终止. 否则存在$a_2\in F$且$a_2\notin\langle a_1\rangle$，即$\{a_1,a_2\}$线性无关. 则考虑

$$\langle a_1,a_2\rangle=\{r_1a_1+r_2a_2 \mid r_1,r_2\in \mathbb{F}_p\}$$

也仍为线性闭的. 若$F=\langle a_1,a_2\rangle$，则构造终止.

继续上述过程，因为$|F|<+\infty$，则该过程在有限步内终止. 则得到$\{a_1,a_2,\cdots,a_n\}\subset F$为$F$的一组极大线性无关集合. 满足：$\forall x\in F$，存在唯一的$c_1,\cdots,c_n\in \mathbb{F}_p$使得

$$x=c_1a_1+c_2a_2+\cdots+c_na_n.$$

即F的元素与向量$(c_1\cdots c_n)$ 1-1对应. 对于每个c_i有p种选取方式，所以有p^n个这样的向量，于是有$|F|=p^n$.

$\boxtimes$

有限域上方程求解：

我们曾经说过在$\mathbb{R}^n$中如果一个线性闭集的维数大于(
则包含有无穷多个元素，因为$\mathbb{R}$中有无穷多个元素。这样我们
得出若一个线性方程组是相容的且解不确定，则在$\mathbb{R}^n$中
的解全体是一个无穷集合。当我们考虑解在有限域中时
情况就不一样了，但是高斯消去法还是保持不变的。

例1. 设 $F=\mathbb{Z}_5$，求解方程（解在$F\times F$中）

$$\begin{cases} \bar{2}x+\bar{4}y=\bar{3} & ① \\ \bar{3}x+\bar{1}y=\bar{2} & ② \end{cases} \quad (*)$$

$$\xrightarrow{\bar{3}\cdot ①} \begin{cases} \bar{1}\cdot x+\bar{2}y=\bar{4} & ①' \\ \bar{3}x+\bar{1}y=\bar{2} & ② \end{cases}$$

$$\xrightarrow{② - \bar{3}\cdot ①'} \begin{cases} \bar{1}\cdot x+\bar{2}y=\bar{4} & ①' \\ 0=0 & ②' \end{cases}$$

所以解为： $x=\bar{4}-\bar{2}y$，则(*)有5个解！