第七章 有限域

任课教师：胡丽琴
网络空间安全学院

有限域

定义

- 设F是具有加法和乘法运算的非空集合。如果F对于加法构成一个交换群，$F^*=F\backslash\{0\}$对于乘法也构成一个交换群，且加法和乘法之间满足分配律，则F称为**域**。

01

有限域

- 当域的元素个数有限时，称为**有限域**或伽罗瓦(Galois)域

- 最常见的有限域例子：$\mathbf{F}_2=\{0,1\}$。
- 事实上，对于所有的素数p，$\mathbf{F}_p$对于模p加法和模p乘法都构成有限域。

有限域

除了$\mathbf{F}_p$以外，还有哪些有限域呢？

有限域一般含有多少个元素？

两个元素个数相同的有限域一定同构

定义

扩域

- **定义7.1.1** 设F是一个域。如果K是F的子域，则称F是K的扩域。

有限域

例 实数域**R**和复数域**C**是有理数域**Q**的扩域。

例 $\mathbf{F}_{2^3}=\mathbf{F}_2[x]/(x^3+x+1)$是$\mathbf{F}_2$的扩域。

如果**F**是**K**的扩域，则$1_{\mathbf{F}}=1_{\mathbf{K}}$

若**F**是**K**的扩域，则**F**可作为**K**上的线性空间

有限域

若F是K的扩域，用[F:K]表示F作为K上的线性空间的维数

[C: R]=？

[R: Q]=？

F为K的有限扩张，如果[F:K]有限，否则称为无限扩张

有限域

例 $\mathbf{F}_2$和$\mathbf{F}_2[x]/(x^3+x+1)$

都是有限域。

有限域构造

- 事实上，给定素数p和正整数n，有限域$\mathbf{F}_{p^n}$都存在。那么，如何得到这个有限域呢？

- 设**K**是一个有限域，则其特征必为素数，记为p。
  - **K**是$\mathbf{F}_p$的扩域，设$[\mathbf{K}: \mathbf{F}_p]=n$
  - 则**K**是元素个数为p^n的有限域，在同构意义下可记作$\mathbf{F}_{p^n}$

有限域的构造

定义

- 例 构造有限域$\mathbf{F}_{24}$。
- 有限域$\mathbf{F}_{24}$的特征为2，因此素域是$\mathbf{F}_2$.
- 寻找$\mathbf{F}_2$上的4次不可约多项式$p(x)$，得到的商环

$\mathbf{F}_2[x]/(p(x))$即是有限域$\mathbf{F}_{24}$

有限域

02

$\sqrt{2}\in\mathbf{R}$是$\mathbf{Q}$上的代数数

$e^{2\pi i/n}\in\mathbf{C}$是$\mathbf{Q}$上的代数数

01

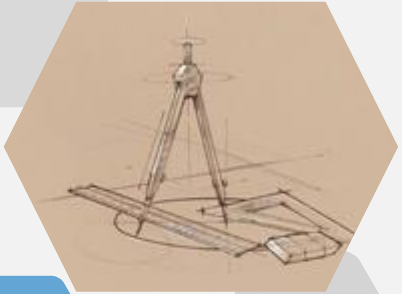
设$\mathbf{F}$是$\mathbf{K}$的一个扩域。$\mathbf{F}$中的一个元素u称为$\mathbf{K}$上的代数数，如果存在一个非零多项式$f(x)\in\mathbf{K}[x]$使得$f(u)=0$。

有限域

F中的一个元素v称为**K**上的超越数，如果不存在任何非零多项式$f(x)\in\mathbf{K}[x]$使得$f(v)=0$

- $\pi=3.1415926\ldots\in\mathbf{R}$是$\mathbf{Q}$上的超越数
- $e=2.718281828\ldots\in\mathbf{R}$是$\mathbf{Q}$上的超越数

有限域



- 所有超越数构成的集是一个不可数集。可是，现今发现的超越数极少，因为要证明一个数是超越数是十分困难的。
- 已被证明是超越数的只有π和e
- 超越数的证明，使得几千年来数学上的难题——尺规作图三大问题，即倍立方问题、三等分任意角问题和化圆为方问题无法用尺规作图解决得到了证明。

有限域

- 设F是域K的一个扩域。如果F中的任何一个元素都是K上的代数数，则称F是K上的代数扩张；如果F中的至少有一个元素是K上的超越数，则称F是K上的超越扩张。

有限域

R是Q上的超越扩张

C是R上的代数扩张

引理7.1.1 设F是域K的扩域，$u \in$ F是K上的代数数，则存在唯一的K上的首一不可约多项式$f(x)$使得$f(u)=0$

定理7.1.3 如果F是域K的一个扩域，$u \in$ F中是K上的超越数，则存在一个在K上的恒等映射的域同构K$(u) \cong$ K(x)

有限域

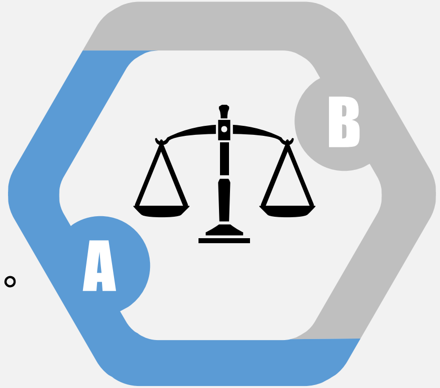
定义7.1.3 设**F**是域**K**的扩域，$u\in\mathbf{F}$是**K**上的代数数。**K**上使得$f(u)=0$的首一不可约多项式$f(x)$称为**u的不可约多项式**(或**极小多项式**)。

$\sqrt{2}$在**Q**上，$i\in\mathbf{C}$在**R**上，的极小多项式是？次数是？共轭根是什么？

u在**K**上的次数是$\deg f$。u的极小多项式的其他根叫做u的**共轭根**

有限域

设$\mathbf{F}$是域$\mathbf{K}$的扩域，$u\in\mathbf{F}$，则$\mathbf{K}(u)=\{f(u)/g(u) \mid f(u), g(u)\in\mathbf{K}[u], g(u)\neq 0\}$也构成一个域，称为$u$在$\mathbf{K}$上的单扩张。



- $\mathbf{K}[u]=?$
- $\mathbf{Q}[\sqrt{2}]=\mathbf{Q}[\sqrt{8}]$

有限域

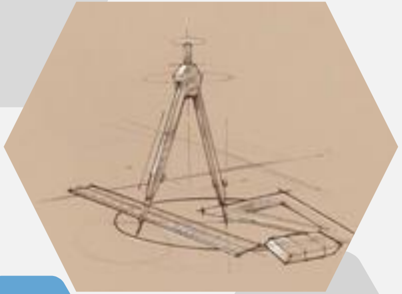
- 设**F**是域**K**的扩域，$u\in\mathbf{F}$是**K**上的代数数，设$f(x)$是u的极小多项式，次数为n，则
  - $\mathbf{K}(u)\cong\mathbf{K}[x]/(f(x))$
  - $[\mathbf{K}(u):\mathbf{K}]=n$
  - $\{1, u, \ldots, u^{n-1}\}$是**K**上向量空间$\mathbf{K}(u)$的基底
  - $\mathbf{K}(u)$的每个元素可唯一地表示为$a_0+a_1u+\ldots+a_{n-1}u^{n-1}$, $a_i\in\mathbf{K}$。

有限域

- 设$\mathbf{F}_{pn}^{*}=\langle g\rangle$，则称$g$为有限域的$\mathbf{F}_{pn}$生成元。
  - 当g为有限域$\mathbf{F}_{pn}$的生成元时，$\mathbf{F}_{pn}=\{0, g^0=1, g, g^2, \ldots, g^{p^n-2}\}$

- **定义7.1.10** 有限域$\mathbf{F}_{pn}$的乘法群$\mathbf{F}_{pn}^{*}=\mathbf{F}_{pn}\backslash\{0\}$是循环群

有限域



- **定理7.1.10** 设g是有限域$\mathbf{F}_{p^n}$中的元素，p^n-1的所有不同素因数是$q_1,\ldots,q_k$，则g是有限域$\mathbf{F}_{p^n}$的一个生成元的充要条件是

$$g^{(p^n-1)/q_i} \neq 1,\ i=1,\ \ldots,\ k.$$