查看: 21 | 回复: 11

**[数论] $x^{p^d}-x$在$\mathbb{F}_p$完全分解为一次因式，当且仅当$d \mid k$** [复制链接]

---

**hbghlyj**

2423 主题 5768 回帖 4万 积分
只看该作者
发消息

发表于 2023-10-29 21:16 1# 电梯直达

正整数$d,k$，素数$p$. 证明$x^{p^d}-x$在$\mathbb{F}_{p^k}$完全分解为一次因式，当且仅当$d \mid k$.
例如$f(x)=x^{2^2}-x$

在$\mathbb{F}_2$上

$$f(x)=x(x+1)(x^2+x+1)$$

不能完全分解为一次因式，因为$x^2+x+1$不可约。

在$\mathbb{F}_3$上

$$f(x)=x(x+1)(x^2+x+1)$$

不能完全分解为一次因式，因为$x^2+x+1$不可约。

在$\mathbb{F}_2$上完全分解为一次因式

$$f(x)=x(x+1)(x+a)(x+a+1)$$

其中$a^2+a+1=0$.

在$\mathbb{F}_3$上完全分解为一次因式

$$f(x)=x(x+1)(x+a^3+a^2)(x+a^3+a^2+1)$$

其中$a^4+a^3+a^2+a+1=0$.

有限域

收藏 淘帖

**相关帖子**

- $x^n-a$不可约$\Leftrightarrow a$不是$n$的约数次幂,且不为$-4b^4$若$4|n$
- Constructing Finite Fields
- 证明$f(x)=x^p-x+a\in\mathbb{F}_p[x]$ 不可约
- 大小为 $q$ 的有限域问题
- 同余方程组（？）
- 怎么证明一个多项式对所有的素数p都可约 模p

回复 举报

---

**业余的业余**

43 主题 291 回帖 2318 积分
只看该作者
发消息

发表于 2023-10-29 21:44 2#

定理

> Let $p$ be a prime and let $m \in \mathbb{N}$. Then $x^{p^m}-x$ is the product of all monic irreducible polynomials in $\mathbb{F}_p[x]$ of degree dividing $n$.
>
> 令 $p$ 为质数，令$m \in \mathbb{N}$,那么 $x^{p^n}-x$ 是 $\mathbb{F}_p[x]$ 中度数整除 $n$ 的所有首一不可约多项式的乘积.

例 $p=2$ 时，我们有

$$x^4-x=x(x+1)(x^2+x+1)$$
$$x^8-x=x(x+1)(x^3+x^2+1)(x^3+x+1)$$

该定理有如下推论

> Let $p$ be a prime and let $n \in \mathbb{N}$. Let $f(x),g(x) \in \mathbb{F}_p[x]$ be two irreducible polynomials of degree $n$. Then $\mathbb{F}_p[x]/(f(x)) \cong \mathbb{F}_p[x]/(g(x))$.
>
> 令 $p$ 为质数，令 $n \in \mathbb{N}$. 如果$f(x),g(x) \in \mathbb{F}_p[x]$ 是两个度数为 $n$ 的不可约多项式，那么 $\mathbb{F}_p[x]/(f(x)) \cong \mathbb{F}_p[x]/(g(x))$.

又有如下推论的推论

> Every irreducible polynomial in $\mathbb{F}_p$ of degree dividing $n$ splits completely in $\mathbb{F}_{p^n}$.

回复 1 举报

---

**业余的业余**

43 主题 291 回帖 2318 积分
只看该作者
发消息

发表于 2023-10-29 21:50 3#

还是这个推论更接近些

> Let $F$ be a finite field and let $q=|F|$. Then
>
> $$x^q-x=\prod_{\alpha\in F}(x-\alpha) \qquad (1)$$

回复 举报

---

**hbghlyj**

2423 主题 5768 回帖 4万 积分
只看该作者
发消息

楼主 | 发表于 2023-10-29 21:54 4#

当$d \mid k$时$p^d-1 \mid p^k-1$，故$x^{p^d-1}-1 \mid x^{p^k-1}-1$，故$x^{p^d}-x \mid x^{p^k}-x$.
由(1)，$x^{p^k}-x$在$\mathbb{F}_{p^k}$分解为一次因式（它的根是$\mathbb{F}_{p^k}$中所有元素），故$x^{p^d}-x$分解为一次因式。
当$d \nmid k$时，如何证明不能完全分解为一次因式？

回复 举报

---

**业余的业余**

43 主题 291 回帖 2318 积分
只看该作者
发消息

发表于 2023-10-29 22:07 5#

> hbghlyj 发表于 2023-10-29 21:54
>
> 当$d \mid k$时$p^d-1 \mid p^k-1$，故$x^{p^d-1}-1 \mid x^{p^k-1}-1$，故$x^{p^d}-x \mid x^{p^k}-x$.
> 由(1)，$x^{p^k}-x$在$\mathbb{F}_{p^k}$分解为一次因式（它的根是$\mathbb{F}_{p^k}$中所有元素），故$x^{p^d}-x$分解为一次因式。
> 当$d \nmid k$时，如何证明不能完全分解为一次因式？

加这个定理够不够

> The field $\mathbb{F}_{p^d}$ has a subring isomorphic to $\mathbb{F}_{p^d}$ if and only if $d \mid n$, in which case, the subring is unique and we say $\mathbb{F}_{p^d}$ is a subfield of $\mathbb{F}_{p^n}$.

回复 举报

---

**hbghlyj**

2423 主题 5768 回帖 4万 积分
只看该作者
发消息

楼主 | 发表于 2023-10-29 22:17 6#

> 业余的业余 发表于 2023-10-29 15:07
>
> The field $\mathbb{F}_{p^d}$ has a subring isomorphic to $\mathbb{F}_{p^d}$

我有一点不懂：
这个subring就是$x^{p^d}-x$在$\mathbb{F}_{p^d}$的所有根组成的吗？

回复 举报

---

**业余的业余**

43 主题 291 回帖 2318 积分
只看该作者
发消息

发表于 2023-10-29 22:18 7#

$\mathbb{F}_{p^d}$ 是最小能使之完全分解的有限域，当且仅当 $d \mid k$ 时，$\mathbb{F}_{p^k}$ 有一个和 $\mathbb{F}_{p^d}$ isomorphic 的子域。归根结底，$f(x)=x^{p^d}-x=0$ 的根都在 $\mathbb{F}_{p^k}$ 内。你是想说存在某个根不在 $\mathbb{F}_{p^k}$ 的可能吗？

回复 举报

---

**业余的业余**

43 主题 291 回帖 2318 积分
只看该作者
发消息

发表于 2023-10-29 22:19 8#

> hbghlyj 发表于 2023-10-29 22:17
>
> 我有一点不懂：
> 这个subring就是$x^{p^d}-x$在$\mathbb{F}_{p^d}$的所有根组成的吗？

这些根都在 $\mathbb{F}_{p^k}$ 中。但组成这个域的元素显然还有很多其他的。

回复 举报

---

**业余的业余**

43 主题 291 回帖 2318 积分
只看该作者
发消息

发表于 2023-10-29 22:24 9#

> 业余的业余 发表于 2023-10-29 21:50
>
> 还是这个推论更接近些

就是三楼的这个推论。所有的根都在 $F$ 内。

回复 举报

---

**业余的业余**

43 主题 291 回帖 2318 积分
只看该作者
发消息

发表于 2023-10-29 22:27 10#

后面两个推论是这个推论

> Let $p$ be a prime and let $n \in \mathbb{N}$. Let $f(x),g(x) \in \mathbb{F}_p[x]$ be two irreducible polynomials of degree $n$. Then $\mathbb{F}_p[x]/(f(x)) \cong \mathbb{F}_p[x]/(g(x))$.
>
> 令 $p$ 为质数，令 $n \in \mathbb{N}$. 如果$f(x),g(x) \in \mathbb{F}_p[x]$ 是两个度数为 $n$ 的不可约多项式，那么 $\mathbb{F}_p[x]/(f(x)) \cong \mathbb{F}_p[x]/(g(x))$.

的证明过程中出现的副产品。它们都是紧关联的。我不知道怎么证明，但有它的证明。现在施脚不来，等有空了再回头消化理解

回复 1 举报

---

**hbghlyj**

2423 主题 5768 回帖 4万 积分
只看该作者
发消息

楼主 | 发表于 2023-10-29 22:36 11#

> 业余的业余 发表于 2023-10-29 15:27
>
> 如果$f(x),g(x) \in \mathbb{F}_p[x]$ 是两个度数为 $n$ 的不可约多项式，那么 $\mathbb{F}_p[x]/(f(x)) \cong \mathbb{F}_p[x]/(g(x))$.

我知道这个定理的证明：首先$\mathbb{F}_p[x]/(f(x))$和$\mathbb{F}_p[x]/(g(x))$的元素个数都是$p^n$，
$\mathbb{F}_p[x]/(f(x))$中的元素都是$x^{p^n}-x$的根，因此$\mathbb{F}_p[x]/(f(x)) \cong \mathbb{F}_p[x]/(g(x))$，它们都是$x^{p^n}-x$的分裂域.

回复 举报

---

**业余的业余**

43 主题 291 回帖 2318 积分
只看该作者
发消息

发表于 2023-10-29 22:38 12#

> hbghlyj 发表于 2023-10-29 22:36
>
> 我知道这个定理的证明：首先$\mathbb{F}_p[x]/(f(x))$和$\mathbb{F}_p[x]/(g(x))$的元素个数都是$p^n$，
> ...

回复 举报

发新帖 返回列表

在此处输入 LaTeX 代码及文字，右边即时预览。
大家可以用来打草稿或者调试代码。
详尽的代码列表及输入说明请见置顶帖。

暂停预览 清空 示例 撤销一下 加入编辑框
行内公式 行间公式 分式 d分式 √ ⁿ√ ≥ ≤ × · … ≈
≡ (mod) $\lim_{x\to}$ ∞ ∫ dx log ln sin cos tan α β γ θ
λ ε φ ω $\Delta$(阿丽代) △(三角形) ⊙ ∠ ° ⊥ // ~ ≌ $\{a_n\}$
箭头向量 粗体向量
align* gather* cases ☺