第七章 习题

1. 设 E 是 F 的 p 次扩域， p 是素数， $\alpha \in E$， $\alpha \notin F$ ，证明： $E = F(\alpha)$ 。

证明： E 是 F 的有限扩张，因此是 F 的代数扩张，所以 E 中的任意元素都是 F 中的代数元。$\alpha \in E, \alpha \notin F$，所以$E \supseteq F(\alpha) \supseteq F$，即有$[E:F] = [E:F(\alpha)][F(\alpha):F] = p$。$p$是素数，所以$[F(\alpha):F] = p$或 1，又$\alpha \notin F$，所以$[F(\alpha):F] \neq 1$，即$[F(\alpha):F] = p$。因此$E = F(\alpha)$。

2. 若 E 是 F 的一个 n 次扩域， $\alpha \in E$ ，且在 F 上的次数为 m ，证明： $m \mid n$.

证明： $\alpha \in E, \alpha \notin F$，且在 F 上的次数为 m，所以$E \supseteq F(\alpha) \supseteq F$，而且$[F(\alpha):F] = m$。由定理 7.1.3 可知，$[E:F] = [E:F(\alpha)][F(\alpha):F]$，因此有$m|n$。

3. 若 E 是 F 的扩域， $u \in E$ 在 F 上的次数为奇数，证明： u^2 在 F 上的次数也是奇数且 $F(u) = F(u^2)$.

证明： 因为$u^2 \in F(u)$，故

$$F \subseteq F(u^2) \subseteq F(u)$$

从而有

$$[F(u):F] = [F(u):F(u^2)][F(u^2):F]$$

由于u在F上的次数为奇数，故$[F(u):F]$是奇数，因此$[F(u^2):F]$也是奇数，即u^2在F上的次数也是奇数。

又由于

$$F(u) = F(u^2, u) = F(u^2)(u)$$

即$F(u)$也是域$F(u^2)$上的单扩域。设u在域$F(u^2)$上的极小多项式为$q(x)$，次数为m，则m必为奇数。

又因为u是多项式

$$x^2 - u^2 \in F(u^2)[x]$$

的根，故$q(x) | x^2 - u^2$，从而$m < 2$，但由于m是奇数，故只能有$m = 1$，即

$$[F(u):F(u^2)] = 1$$

因此，$F(u) = F(u^2)$。

4. 若 E 是 F 的一个代数扩张， α 是 E 上的代数元，证明： α 也是 F 上的代数元.

证明： α是 E 上的代数元，不妨设α满足 E 上的多项式$f(x) = \sum_{i=0}^{n} a_i x^i$。又 E 是 F 的一个代数扩张，所以$a_i$ $(0 \leq i \leq n)$都是 F 上的代数元，则 E 的子域

$$E' = F(a_0, a_1, \ldots, a_n)$$

是 F 上的一个有限扩域。显然，由于α满足多项式$f(x) = \sum_{i=0}^{n} a_i x^i$，所以$\alpha$是 E′上的一个代数元。所以$E'(\alpha)$是 E′上的一个有限扩张，因而也是 F 上的一个有限扩张。这样

$$E'(\alpha) == F(a_0, a_1, \ldots, a_n, \alpha)$$

是 F 上的一个代数扩域。因此，α是 F 上的代数元

5. 设 E, F, K 是域，$F \subset K \subset E$ ，若$[E:K]$ m ，$\alpha \in E$ 在 F 上的次数为 n ，且 $(n, m) = 1$.

证明： α 在 K 上的次数也是 n .

证明：

6. 若 $x^n-\alpha\in F[x]$ 不可约，证明：任意正整数 m，当 $m\mid n$ 时，x^m-a 在 $F[x]$ 中也不可约.

7. 确定 $f(x)=x^3-2x-2$ 和 $g(x)=x^3-3x-1$ 在有理数域 $\mathbf{Q}$ 上的分裂域.

8. 证明：$\mathbf{Q}$ 上的多项式 x^4+1 在 $\mathbf{Q}$ 上的分裂域是一个单扩张 $\mathbf{Q}(\alpha)$，α 是 x^4+1 的一个根.

9. 设 x^3-a 是 $\mathbf{Q}$ 上的不可约多项式，α 是 x^3-a 的一个根，证明：$\mathbf{Q}(\alpha)$ 不是 x^3-a 在 $\mathbf{Q}$ 上的分裂域.

10. 设 P 是一个特征为素数 p 的域，$F=P(\alpha)$ 是 P 的一个单扩张，α 是 $x^p-a\in P[x]$ 的根.

    问 $P(\alpha)$ 是不是 x^p-a 在 P 上的分裂域？

11. 给出商环 $\mathbf{Z}_2[x]/(x^2+x+1)$ 上的加法和乘法表，问此商环是否为域？

解：$\mathbb{Z}_2/\langle x^2+x+1\rangle=\{0,1,x,x+1\}$
可构造其乘法表和加法表，如下所示

+	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

*	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

此商环是域，由乘法表可知其非零元对于乘法构成交换群。

12. 证明：　x^2+1 及 x^2+x+4 在 $\mathbf{Z}_{11}$ 上不可约. 并证明：

$$\mathbf{Z}_{11}[x]/(x^2+1)\cong\mathbf{Z}_{11}[x]/(x^2+x+4).$$

证明：将{0,1,2，……，10}分别代入多项式x^2+1和x^2+x+4，可得

	0	1	2	3	4	5	6	7	8	9	10
x^2+1	1	2	5	10	6	4	4	6	10	5	2
x^2+x+4	4	6	10	5	2	1	2	5	10	6	4

因此，x^2+1和x^2+x+4在$\mathbb{Z}_{11}$上不可约。
设α是x^2+1的根，β是x^2+x+4的根，则
$\mathbb{Z}_{11}[x]/(x^2+1)\cong\mathbb{Z}_{11}(\alpha)=\{a\alpha+b|a,b\in\mathbb{Z}_{11}\}$
$\mathbb{Z}_{11}[x]/(x^2+x+4)\cong\mathbb{Z}_{11}(\beta)=\{a\beta+b|a,b\in\mathbb{Z}_{11}\}$
在$\mathbb{Z}_{11}(\alpha)$中找多项式x^2+x+4的根，来构造同构映射。
设$\alpha+b$是多项式x^2+x+4的根，则

$$(\alpha+b)^2+\alpha+b+4=0$$

解之得$b=5$，即$\alpha+5$是多项式x^2+x+4的根。
构建映射$\varphi:\mathbb{Z}_{11}(\beta)\to\mathbb{Z}_{11}(\alpha)$为

$$\varphi(a\beta+b)=a(\alpha+5)+b$$

容易验证该映射为一一映射，而且$\forall\ a_1\beta+b_1,a_2\beta+b_2\in\mathbb{Z}_{11}(\beta)$有

$$\begin{aligned}\varphi(a_1\beta+b_1+a_2\beta+b_2) &= \varphi((a_1+a_2)\beta+b_1+b_2)\\ &= (a_1+a_2)(\alpha+5)+b_1+b_2\\ &= a_1(\alpha+5)+b_1+a_2(\alpha+5)+b_2\\ &= \varphi(a_1\beta+b_1)+\varphi(a_2\beta+b_2)\end{aligned}$$

$$\begin{aligned}\varphi((a_1\beta+b_1)(a_2\beta+b_2)) &= \varphi((a_1b_2+a_2b_1-a_1a_2)\beta+b_1b_2-4a_1a_2)\\ &= (a_1b_2+a_2b_1-a_1a_2)(\alpha+5)+b_1b_2-4a_1a_2\\ &= (a_1b_2+a_2b_1+10a_1a_2)\alpha+2a_1a_2+5a_1b_2+5a_2b_1+b_1b_2\end{aligned}$$

$$\begin{aligned}\varphi(a_1\beta+b_1)\varphi(a_2\beta+b_2) &= [a_1(\alpha+5)+b_1][a_2(\alpha+5)+b_2]\\ &= a_1a_2(\alpha+5)^2+a_1b_2(\alpha+5)+a_2b_1(\alpha+5)+b_1b_2\\ &= (a_1b_2+a_2b_1+10a_1a_2)\alpha+2a_1a_2+5a_1b_2+5a_2b_1+b_1b_2\end{aligned}$$

即$\varphi((a_1\beta+b_1)(a_2\beta+b_2))=\varphi(a_1\beta+b_1)\varphi(a_2\beta+b_2)$

因此，映射$\varphi:\mathbb{Z}_{11}(\beta)\to\mathbb{Z}_{11}(\alpha)$是同构映射，即有

$$\mathbb{Z}_{11}[x]/(x^2+1)\cong\mathbb{Z}_{11}[x]/(x^2+x+4)$$

13. 给出有限域F_9，F_{17}的所有元素，并找出其本原元。

解：F_9可以看成是F_3通过添加一个二次不可约多项式的根α得到的 2 次扩张。

$f(x)=x^2+1$是F_3上一个不可约多项式，设α是$f(x)$的一个根，即$f(\alpha)=\alpha^2+1=0$，

则$1,\alpha$是F_9在F_3上的一组基，从而，F_9中的元素可以表示成F_3上α的次数小于 2 的多项式，即$F_9=\{0,1,2,\alpha,1+\alpha,2+\alpha,2\alpha,1+2\alpha,2+2\alpha\}$。$\xi=1+\alpha$是$F_9$的本原元，因为$\xi=1+\alpha$，$\xi^2=2\alpha$，$\xi^3=1+2\alpha$，$\xi^4=2$，$\xi^5=2+2\alpha$，$\xi^6=\alpha$，$\xi^7=2+\alpha$，$\xi^8=1$。

其所有的本原元为ξ,ξ^3,ξ^5,ξ^7。

$F_{17}=\mathbb{Z}_{17}=\{0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16\}$，由于

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
2^i	2	4	8	16	15	13	9	1								
3^i	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1

所以 3 是F_{17}的本原元，其所有本原元为 3,10,5,11,14,7,12,6。

14. 设F_q是有限域，$q\neq 2$，证明：F_q中所有元素之和为 0。

证明：

15. 将F_{25}的元素表示成F_5上一组基的线性组合。

16. 给出F_2上所有 3 次和 4 次不可约多项式。

解：F_2上的 3 次不可约多项式的形式为$x^3+a_2x^2+a_1x+a_0,\ a_i\in F_2$。若三次多项式可约则至少存在一个一次因式，也就是说在F_2中有一个根。所以要三次多项式不可约，则要求 0,1 都不是多项式的根，所以三次不可约多项式只能是x^3+x^2+1,x^3+x+1。

F_2上的 4 次不可约多项式的形式为$x^4+a_3x^3+a_2x^2+a_1x+a_0,\ a_i\in F_2$。首先，不可约多项式没有根，所以$a_0=1$，而且多项式的项数应该是奇数。经验证，$x^4+x^3+1,x^4+x+1,x^4+x^3+x^2+x+1$是$F_2$上全部 4 次不可约多项式。

17. 设 k 是一个正整数，$a \in F_q^*$，$d = \gcd(q-1, k)$。证明：a 是 F_q 中某个元素的 k 次方幂当且仅当 $a^{(q-1)/d} = 1$。

18. 对任何特征为素数 p 的有限域 F_q，证明：F_q 中任一元素恰好存在一个 p 次方根。

19. 证明：F_q 中任一元素是 F_q 中某个元素的 k 次方幂当且仅当 $\gcd(q-1, k) = 1$。

20. 设 $f(x) = x^3 + x + 1 \in GF(2)[x]$，试证明模 $f(x)$ 的剩余类环 $GF(2)[x]/(f(x))$ 是域，并给出域中所有非零元的逆元。

21. 使用 F_2 上不可约多项式 $f(x) = x^3 + x + 1$ 给出有限域 F_8 的矩阵表示。

22. 设 F 是域，证明：若 F_q^* 是循环群，那么 F 一定是有限域。

23. 用 F_2 上不可约多项式 $f(x) = x^4 + x + 1$ 构造 F_{16}，并找出一个本原元，给出 F_{16} 的指数对数表。