近世代数

乐绎华

学号：23363017

2025 年 6 月 1 日

习 题5.1第2， 3， 5， 10， 12， 16题

习 题5.4第2， 4题

Exercice 1

习题1.2. 设 p 为素数，求扩张 $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ 和 $\mathbb{Q}(\zeta_8)/\mathbb{Q}$ 的次数，其中 $\zeta_n = e^{\frac{2\pi i}{n}}$ 为 n 次本原单位根. 对一般的 n，扩张 $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ 的次数是多少？

Consider the cyclotomic polynomial

$$\Phi_n(x) \coloneqq \prod_{a \in \mathbf{Z}_n^\times} (x - \zeta_n^a)$$

Lemma 17.4.3. *We have*

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

Each $\Phi_n(x)$ is a polynomial of degree $\varphi(n)$ with coefficients in $\mathbb{Z}$.

Proof. The first equality is easy:

$$x^n - 1 = \prod_{b \in \mathbf{Z}_n} (x - \zeta_n^b) = \prod_{d|n} \prod_{i \in \mathbf{Z}_d^\times} (x - \zeta_n^{di}) = \prod_{d|n} \Phi_d(x). \tag{17.4.3.1}$$

We will prove that $\Phi_n(x)$ has coefficients in $\mathbb{Z}$ and its coefficients have gcd $= 1$. Assume that this has been proved for smaller n. Then (17.4.3.1) and Gauss' lemma implies that $\Phi_n(x)$ has coefficients in $\mathbb{Z}$ and has coefficients' gcd $= 1$. □

Theorem 17.4.4. *The polynomial $\Phi_n(x)$ is irreducible in $\mathbb{Q}[x]$. So $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$.*

Proof. It suffices to show that $\Phi_n(x)$ is irreducible in $\mathbb{Z}[x]$. Let ζ be a primitive nth root of unity in a splitting field of $\Phi_n(x)$. (We deliberately do not specify one here.)

We need to show that the minimal polynomial $f(x) := m_{\zeta,\mathbb{Q}}(x)$ of ζ over $\mathbb{Q}$ is equal to $\Phi_n(x)$; it is clear that $f(x)|\Phi_n(x)$. We will show that for any integer a relatively prime to n, ζ^a is a zero of $\Phi_n(x)$.

We take a prime p *not* dividing n.

<u>Claim:</u> ζ^p is also a zero of $f(x)$.

This claim would imply that if $a = p_1^{\alpha_1}\cdots p_r^{\alpha_r}$ is relatively prime to n, $\zeta^a = \zeta^{p_1^{\alpha_1}\cdots p_r^{\alpha_r}}$. Iteratively, we can prove that ζ is a zero of $f(x)$ implying ζ^a is a zero of $f(x)$. From this, we deduce that $f(x) = \Phi_n(x)$. (This is why we did not specify a primitive nth root of unity.)

Now, we prove the Claim. Suppose this is not true. Let $g(x) = m_{\zeta^p,\mathbb{Q}}(x)$ be the minimal polynomial of ζ^p over $\mathbb{Q}$.

As $f(x) \neq g(x)$, we have $\gcd(f(x), g(x)) = 1$ and thus

$$f(x)g(x) \mid \Phi_n(x).$$

On the other hand, $g(\zeta^p) = 0$ implies that ζ is a zero of $g(x^p)$. This implies that

$$f(x) \mid g(x^p) \quad \Rightarrow \quad g(x^p) = f(x)h(x) \text{ in } \mathbb{Z}[x],$$

for some $h(x) \in \mathbb{Z}[x]$. Taking this equation modulo p, we have

$$\bar{g}(x)^p = \bar{g}(x^p) = \bar{f}(x)\bar{h}(x) \quad \text{in } \mathbb{F}_p[x].$$

This implies that $\bar{f}(x)$ and $\bar{g}(x)$ have a common factor in $\mathbb{F}_p[x]$.

Yet $\bar{f}(x)\bar{g}(x)$ divides $\bar{\Phi}_n(x)$, which further divides $x^n - 1$. This implies that $x^n - 1$ has repeated zeros in its splitting field over $\mathbb{F}_p$. But

$$\left(x^n - 1, D(x^n - 1)\right) = \left(x^n - 1, nx^{n-1}\right) = \left(x^n - 1, x^{n-1}\right) = (1).$$

This contradicts with the properties of repeated zeros. The Claim is proved.

This completes the proof of irreducibility of $\Phi_n(x)$. □

Exercice 2

习题1.3. 求元素 $\sqrt{2}+\sqrt{3}$ 在域 K 上的极小多项式，其中

(1) $K = \mathbb{Q}$; (2) $K = \mathbb{Q}(\sqrt{2})$; (3) $K = \mathbb{Q}(\sqrt{6})$.

Let $x = \sqrt{2}+\sqrt{3}$, then

$$\begin{aligned} x &= \sqrt{2}+\sqrt{3} \\ x^2 &= 5+2\sqrt{6} \\ x^3 &= 11\sqrt{2}+9\sqrt{3} \\ x^4 &= 20\sqrt{6}+49 \end{aligned}$$

(1) we know that $f(x) \coloneqq (x^2-5)^2 - 24 = 0$, and $f(x) = x^4 - 10x^2 + 1$ is irreducible over $\mathbb{Q}$ by Eisenstein criterion, thus is the minimal polynomial of $\sqrt{2}+\sqrt{3}$ over $\mathbb{Q}$.

(2) we know that $f(x) \coloneqq (x-\sqrt{2})^2 - 3 = 0$ and $f(x) = x^2 - 2\sqrt{2}x - 1$ is of degree 2. The minimal polynomial cannot have degree 1 since $\sqrt{2}+\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$, but divides $f(x)$, thus equals to $f(x)$ due to the uniqueness.

(3) we know that $f(x) \coloneqq x^2 - 5 - 2\sqrt{6} = 0$. Similar to the assertion in (2), $f(x)$ is the minimal polynomial of $\sqrt{2}+\sqrt{3}$ over $\mathbb{Q}(\sqrt{6})$.

Exercice 3

习题1.5. 设 F/K 为域的代数扩张, D 为整环且 $K \subseteq D \subseteq F$. 求证 D 为域.

For any $0 \neq d \in D \subseteq F$, we have $f(d) = 0$ for some $f \in K[x]$.

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$$

WLOG, assume that $a_0 \neq 0$, then

$$d^{-1} = -\underbrace{a_0^{-1}}_{\in K \subseteq D} \underbrace{(d^{n-1} + a_{n-1}d^{n-2} + \cdots + a_1)}_{\in D} \in D$$

Thus D is field.

Exercice 4

习题1.10. 令 $K = \mathbb{Q}(\alpha)$ 其中 α 是方程 $x^3 - x - 1 = 0$ 的一个根. 求 $\gamma = 1 + \alpha^2$ 在 $\mathbb{Q}$ 的最小多项式.

$$\gamma = 1 + \alpha^2$$
$$\gamma^2 = 3\alpha^2 + \alpha + 1$$
$$\gamma^3 = 7\alpha^2 + 5\alpha + 2$$

We have

$$\gamma^3 - 5\gamma^2 + 8\gamma - 5 = 0$$

In $\mathbb{F}_2$, the polynomial

$$\gamma^3 - 5\gamma^2 + 8\gamma - 5 \equiv \gamma^3 + \gamma^2 + 1 \mod 2$$

is irreducible. Then $\gamma^3 - 5\gamma^2 + 8\gamma - 5$ is not reducible over $\mathbb{Q}$, thus the minimal polynomial of γ over $\mathbb{Q}$ is

$$x^3 - 5x^2 + 8x - 5$$

Exercice 5

习题1.12. 设 u 是多项式 x^3-6x^2+9x+3 的一个根.

(1) 求证 $[\mathbb{Q}(u):\mathbb{Q}]=3$.

(2) 试将 $u^4,(u+1)^{-1},(u^2-6u+8)^{-1}$ 表示成 $1,u,u^2$ 的 $\mathbb{Q}$-线性组合.

(1)

$$f(x):=x^3-6x^2+9x+3$$

is irreducible over $\mathbb{Q}$ by Eisenstein criterion, thus is the minimal polynomial of u over $\mathbb{Q}$. By the definition of minimal polynomial,

$$[\mathbb{Q}(u):\mathbb{Q}]=3$$

(2) We have

$$u^3-6u^2+9u+3=0$$

Then

$$\begin{aligned} u^4 &= u(6u^2-9u-3) \\ &= 6u^3-9u^2-3u \\ &= 6(6u^2-9u-3)-9u^2-3u \\ &= 27u^2-57u-18 \end{aligned}$$

We know that

$$((u+1)-1)^3-6((u+1)-1)^2+9((u+1)-1)+3=0$$

i.e.

$$(u+1)^3-9(u+1)^2+24(u+1)-13=0$$

Thus

$$(u+1)^{-1}=\frac{1}{13}[(u+1)^2-9(u+1)+24]=\frac{u^2}{13}-\frac{7u}{13}+\frac{16}{13}$$

(3) Suppose that

$$(u^2-6u+8)^{-1}=au^2+bu+c$$

Then

$$(u^2-6u+8)(au^2+bu+c)=1$$

i.e.

$$\begin{aligned}
1 &= au^4 + (b-6a)u^3 + (8a+c-6)u^2 + (8b-6c)u + 8c \\
&= au(6u^2-9u-3) + (b-6a)(6u^2-9u-3) + (8a+c-6)u^2 + (8b-6c)u + 8c \\
&= (18a-3b+8c) + (51a-b-6c)u + (-6-37a+6b+c)u^2 + 6au^3 \\
&= (18a-3b+8c) + (51a-b-6c)u + (-6-37a+6b+c)u^2 + 6a(6u^2-9u-3) \\
&= (-3b+8c) + (-3a-b-6c)u + (-a+6b+c)u^2
\end{aligned}$$

Let

$$\begin{cases} -3b+8c &= 1 \\ -3a-b-6c &= 0 \\ -a+6b+c &= 0 \end{cases}$$

Then

$$(a,b,c) = \left(-\frac{35}{179}, -\frac{9}{179}, \frac{19}{179}\right)$$

Thus

$$(u^2-6u+8)^{-1} = -\frac{35}{179}u^2 - \frac{9}{179}u + \frac{19}{179}$$

Exercice 6

习题1.15. 设 M/K 为域的扩张, M 中元素 u, v 分别是 K 上的 m 次和 n 次代数元素. $F = K(u)$, $E = K(v)$.

(1) 求证 $[FE:K] \leqslant mn$.

(2) 如果 $(m,n)=1$, 则 $[FE:K] = mn$.

(1) $1, u, u^2, \ldots, u^{m-1}$ is the K -basis for F, and $1, v, v^2, \ldots, v^{n-1}$ is the K -basis for E. Then

$$FE = K(u,v)$$

has elements of the form

$$\sum_{\substack{i=0,1,\ldots,m-1 \\ j=0,1,\ldots,n-1}} a_{ij}u^iv^j$$

From $FE = F(v)$, we see that $1, v, \ldots, v^{n-1}$ span FE over F. Hence $[FE:F] \leq n = [E:K]$ with equality iff these elements are linearly independent over F. Since $[FE:K] = [FE:F][F:K]$, we are done!

(2)

$$m = [F : K] \mid [F : K] \cdot [FE : F] = [FE : K]$$

$$n = [E : K] \mid [FE : K]$$

Since $(m, n) = 1$, $mn \mid [FE : K]$. By (1), we have $[FE : K] \leq mn$. Thus

$$[FE : K] = mn$$

Exercice 7

习题4.2. 列出 $\mathbb{F}_2$ 上全部次数 $\leqslant 4$ 的不可约多项式, 列出 $\mathbb{F}_3$ 上全部 2 次不可约多项式.

$\mathbb{F}_2$ 上全部次数 ≤ 4 的不可约多项式

$$x$$

$$x - 1$$

$$x^2 + x + 1$$

$$x^3 + x^2 + 1$$

$$x^3 + x + 1$$

$$x^4 + x^3 + 1$$

$$x^4 + x^2 + 1$$

$$x^4 + x + 1$$

$$x^4 + x^3 + x^2 + x + 1$$

$\mathbb{F}_3$ 上全部 2 次不可约多项式

$$x^2 + 1$$

$$x^2 + x + 2$$

$$x^2 + 2x + 2$$

$$2x^2 + 2$$

$$2x^2 + 2x + 1$$

$$2x^2 + x + 1$$

Exercice 8

习题4.4. 设 $\alpha_1^2 = 2$, $\alpha_2^2 = 3$. 求 $\alpha_1 + \alpha_2$ 在 $\mathbb{Q}$, $\mathbb{F}_5$, $\mathbb{F}_7$ 上的不可约多项式.

Over $\mathbb{Q}$, denote $\gamma = \alpha_1 + \alpha_2$, then

$$\gamma^2 = 5 + 2\alpha_1\alpha_2$$

Then

$$(\gamma^2 - 5)^2 = (2\alpha_1\alpha_2)^2 = 24$$

i.e.

$$\gamma^4 - 10\gamma^2 + 1 = 0$$

On the other hand,

$$[\mathbb{Q}(\alpha_1 + \alpha_2) : \mathbb{Q}] = \underbrace{[\mathbb{Q}(\alpha_1 + \alpha_2) : \mathbb{Q}(\alpha_1)]}_{=[\mathbb{Q}(\alpha_1)(\alpha_2):\mathbb{Q}(\alpha_1)]}[\mathbb{Q}(\alpha_1) : \mathbb{Q}] \stackrel{?}{=} 2 \cdot 2 = 4$$

We just need to show that $\alpha_2 \notin \mathbb{Q}(\alpha_1)$. Assume that $\alpha_2 \in \mathbb{Q}(\alpha_1)$, then $\alpha_2 = a + b\alpha_1$ for some $a, b \in \mathbb{Q}$, then

$$3 = \alpha_2^2 = a^2 + 2b^2 + 2ab\alpha_1$$

Then $\alpha_1 = \frac{3-a^2-2b^2}{2ab} \in \mathbb{Q}$, if $ab \neq 0$. Thus $3 = \left(\frac{p}{q}\right)^2$ for some $p, q \in \mathbb{Z}$. Then

$$3q^2 = p^2$$

The order of 3 in $3q^2$ is odd while in p^2 is even, which is a contradiction.

Therefore, $ab = 0$. $b \neq 0$ since $\alpha_2 \notin \mathbb{Q}$ by the same discussion. $a \neq 0$, otherwise $\alpha_2 = b\alpha_1$ for some $b = \frac{p}{q} \in \mathbb{Q}$, where $p, q \in \mathbb{Z}$. Thus

$$3 = \frac{2p^2}{q^2} \implies 3q^2 = 2p^2$$

which is absurd. Therefore $\alpha_2 \notin \mathbb{Q}(\alpha_1)$.

As the minimal polynomial is unique, $m_{\gamma,\mathbb{Q}}(x) = x^4 - 10x^2 + 1$.

Over $\mathbb{F}_5$,

$$x^4 - 10x^2 + 1 \equiv x^4 + 1 \mod 5$$

Then $m_{\gamma,\mathbb{F}_5}(x) \mid x^4+1=(x^2+2)(x^2+3)$ in $\mathbb{F}_5$. Since $\alpha_1,\alpha_2 \notin \mathbb{F}_5$, $m_{\gamma,\mathbb{F}_5}(x)$ is nontrivial. Thus $m_{\gamma,\mathbb{F}_5}(x)$ is either x^2+2 or x^2+3.

$$\gamma^2+2=2+2\alpha_1\alpha_2$$

$$\gamma^2+3=3+2\alpha_1\alpha_2$$

Then we assert that $2\alpha_1\alpha_2 \in \mathbb{F}_5$ thus $\alpha_1\alpha_2 \in \mathbb{F}_5$. As $(\alpha_1\alpha_2)^2=\alpha_1^2\alpha_2^2=2\cdot 3=1$, we know that $\alpha_1\alpha_2=1$ or 4.

If $\alpha_1\alpha_2=1$, then

$$\gamma^2+2=(\alpha_1+\alpha_2)^2+2=2+2\alpha_1\alpha_2=4$$

$$\gamma^2+3=3+2\alpha_1\alpha_2=0$$

$m_{\gamma,\mathbb{F}_5}=x^2+3$.

If $\alpha_1\alpha_2=4$, then

$$\gamma^2+2=(\alpha_1+\alpha_2)^2+2=2+2\alpha_1\alpha_2=0$$

$$\gamma^2+3=3+2\alpha_1\alpha_2=1$$

$m_{\gamma,\mathbb{F}_5}(x)=x^2+2$.

Over $\mathbb{F}_7$,

$$x^4-10x^2+1 \equiv x^4+4x^2+1 \mod 7$$

Then $m_{\gamma,\mathbb{F}_7}(x) \mid x^4+4x^2+1=(x^2+x+6)(x^2+6x+6)$. $m_{\gamma,\mathbb{F}_7}(x)$ is either x^2+x+6 or x^2+6x+6.

$$\gamma^2+\gamma+6=4+2\alpha_1\alpha_2+\alpha_1+\alpha_2$$

$$\gamma^2+6\gamma+6=4+2\alpha_1\alpha_2+6\alpha_1+6\alpha_2$$

Since $\alpha_1^2=2$, we have $\alpha_1=3$ or 4.

If $\alpha_1=3$,

$$\gamma^2+\gamma+6=4+6\alpha_2+3+\alpha_2=0$$

Then $m_{\gamma,\mathbb{F}_7}(x)=x^2+x+6$.

If $\alpha_1=4$,

$$\gamma^2+6\gamma+6=4+8\alpha_2+24+6\alpha_2=0$$

Then $m_{\gamma,\mathbb{F}_7}(x)=x^2+6x+6$.