

# Problem Set 3

1. (P13 Exer 2.)

- (1) 求证每个二次 (数) 域均可表达成  $\mathbb{Q}(\sqrt{d})$ , 其中  $d$  是无平方因子整数;
- (2) 如果  $d$  和  $d'$  均是无平方因子整数, 并且  $d \neq d'$ , 则  $\mathbb{Q}(\sqrt{d}) \neq \mathbb{Q}(\sqrt{d'})$ ;
- (3) 二次域  $K$  必然是  $\mathbb{Q}$  的 Galois 扩张, 试求其 Galois 群.

2. (P13 Exer 6.) 设  $f(x) \in K[x]$  是数域  $K$  上的  $n$  次不可约首 1 多项式,  $\alpha_1, \dots, \alpha_n$  是它的  $n$  个根, 称  $d(f) = \prod_{1 \leq r < s \leq n} (\alpha_r - \alpha_s)^2$  是多项式  $f(x)$  的判别式.

- (1) 求证  $d(f)$  是  $K$  中元素;
- (2) 设  $f(x) = x^n + a$ ,  $a \in \mathbb{Q}$ ,  $\sqrt[n]{-a} \in \mathbb{Q}$ , 求证

$$d(f) = (-1)^{n(n-1)/2} n^n a^{n-1};$$

- (3) 设  $f(x) = x^n + ax + b$  是  $\mathbb{Q}[x]$  中不可约多项式, 求证

$$d(f) = (-1)^{n(n-1)/2} ((-1)^{n-1} (n-1)^{n-1} a^n + n^n b^{n-1}).$$

(注: 当  $n = 2$  和  $3$  时,  $d(f)$  即为 2 次和 3 次多项式通常所谓的判别式).

3. (P14 Exer 8) 如果  $n \neq n'$ ,  $n \not\equiv 2 \pmod{4}$ ,  $n' \not\equiv 2 \pmod{4}$ , 求证  $\mathbb{Q}(\zeta_n) \neq \mathbb{Q}(\zeta_{n'})$ .

4. (P14 Exer 9) 令  $K = \mathbb{Q}(\zeta_n)$ , 则:

(1) 当  $n \equiv 1 \pmod{2}$  时,  $W_K = \{\zeta_{2n}^k \mid 0 \leq k \leq 2n-1\}, |W_K| = 2n$ ;

(2) 当  $n \equiv 0 \pmod{4}$  时,  $W_K = \{\zeta_n^k \mid 0 \leq k \leq n-1\}, |W_K| = n$ .

5. (P14 Exer 13) 设  $L|K$  是数域的扩张. 对于  $\alpha \in L$ , 定义映射

$$\begin{aligned}\varphi_\alpha: L &\rightarrow L \\ \beta &\mapsto \varphi_\alpha(\beta) = \alpha\beta.\end{aligned}$$

求证

(1)  $\varphi_\alpha$  是  $K$ -向量空间  $L$  中的线性变换;

(2) 如果  $A_\alpha$  是线性变换  $\varphi_\alpha$  对于向量空间  $L$  的任意一组  $K$ -基的变换方阵, 则

$$N_{L|K}(\alpha) = \det(A_\alpha), T_{L|K}(\alpha) = \text{tr}(A_\alpha),$$

其中  $\text{tr}(A_\alpha)$  表示方阵  $A$  的迹.

6. (P24 Exer 1) 求证

(1) 如果  $\alpha$  是代数整数, 则  $\alpha$  的每个共轭元素也是代数整数;

(2) 设  $L|K$  是数域的扩张, 则

$$N_{L|K}(\mathcal{O}_L) \subset \mathcal{O}_K, T_{L|K}(\mathcal{O}_L) \subset \mathcal{O}_K;$$

(3) 设  $L|K$  是数域的扩张,  $\alpha \in L$ , 则  $\alpha \in \mathcal{O}_L \iff \alpha$  在  $K$  上的极小多项式属于  $\mathcal{O}_K[x]$ .

7. (P24 Exer 2) 求证对于每个代数数  $\alpha$ , 均存在整数  $n \in \mathbb{Z}$  使得  $n\alpha$  是代数整数.

8. (P24 Exer 3 Dedekind)

(1) 证明  $x^3 + x^2 - 2x + 8$  是  $\mathbb{Q}[x]$  中的不可约多项式. 下令  $\theta$  为此多项式的一个根,  $K = \mathbb{Q}(\theta)$ ;

(2) 证明  $d_K(1, \theta, \theta^2) = 4 \cdot 503$ ;

(3) 证明  $\theta' = \frac{4}{\theta} \in \mathcal{O}_K$ ,  $\{1, \theta, \theta'\}$  是域  $K$  的一组整基, 并且  $d(K) = 503$ ;

(4) 证明对于每个  $\alpha \in \mathcal{O}_K$ ,  $\{1, \alpha, \alpha^2\}$  均不可能是域  $K$  的一组整基.

(提示: 对每个  $\alpha \in \mathcal{O}_K$ , 证明  $d_K(1, \alpha, \alpha^2)$  必为偶数).

9. (P24 Exer 4) 对于每个数域  $K$ , 记它的复嵌入有  $r_2$  对, 证明

$$(-1)^{r_2} d(K) > 0.$$

10. (P24 Exer 5 Stickelberger) 对于每个数域  $K$ , 证明  $d(K) \equiv 0$  或者  $1 \pmod{4}$ .

11. (P24 Exer 6) 设  $\theta$  是  $f(x) = x^3 + 5x + 4$  的一个根,  $K = \mathbb{Q}(\theta)$ , 证明  $d(K) = -4 \cdot 233$ .

12. (P24 Exer 7) 设  $p$  为奇素数,  $\omega = \zeta_p$ ,  $K = \mathbb{Q}(\omega)$ .

(1) 证明  $K_0 = \mathbb{Q}(\omega + \omega^{-1})$  是  $K$  的极大实子域 (即  $K$  的每个实子域均是  $K_0$  的子域), 并且  $[K_0 : \mathbb{Q}] = \frac{p-1}{2}$ ;

(2) 证明  $\mathcal{O}_{K_0} = \mathbb{Z}[\omega + \omega^{-1}]$ , 并且  $\{\omega + \omega^{-1}, \omega^2 + \omega^{-2}, \dots, \omega^{(p-1)/2} + \omega^{-(p-1)/2}\}$  是域  $K_0$  的一组整基;

(3) 计算域  $K_0 = \mathbb{Q}(\zeta_7 + \zeta_7^{-1})$  的判别式.

13. (P35 Exer 2) 设  $A$  和  $B$  是 Dedekind 整环  $R$  中的两个理想,  $A = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ ,  $B = \mathfrak{p}_1^{f_1} \cdots \mathfrak{p}_r^{f_r}$ , 其中  $\mathfrak{p}_1 \cdots \mathfrak{p}_r$  是  $R$  中不同的素理想, 而  $e_i, f_i \geq 0$ , 证明,

(1)  $A|B \iff e_i \leq f_i. (1 \leq i \leq r);$

(2)  $A \cap B = \mathfrak{p}_1^{t_1} \cdots \mathfrak{p}_r^{t_r}, t_i = \max(e_i, f_i), (1 \leq i \leq r); A + B = \mathfrak{p}_1^{m_1} \cdots \mathfrak{p}_r^{m_r}, m_i = \min(e_i, f_i), (1 \leq i \leq r).$

14. (P35 Exer 3) 设  $A$  为数域  $K$  的分式理想, 证明

$$A^{-1} = \{\alpha \in K \mid \alpha A \subset \mathcal{O}_K\}.$$

15. (P35 Exer 6) 设  $A$  和  $B$  是数域  $K$  的两个理想.

(1) 证明若  $A|B$ , 则  $N_K(A)|N_K(B)$ . 试问反过来是否成立?

(2) 若  $N_K(A)$  为素数, 证明  $A$  必为  $\mathcal{O}_K$  的素理想. 试问反过来是否成立?

16. (P35 Exer 7) 设  $A$  是数域  $K$  的理想,  $A = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$  为  $A$  的素理想分解式, 以  $(\mathcal{O}_K/A)^\times$  表示有限环  $\mathcal{O}_K/A$  的单位群, 令  $\varphi(A) = |(\mathcal{O}_K/A)^\times|$ , 证明,

(1)  $\varphi(\mathfrak{p}_i^{e_i}) = N_K(\mathfrak{p}_i)^{e_i-1}(N_K(\mathfrak{p}_i) - 1);$

(2)  $\varphi(A) = N_K(A) \cdot \prod_{\mathfrak{p}|A} (1 - \frac{1}{N_K(\mathfrak{p})}).$

17. (P36 Exer 8) 设  $K = \mathbb{Q}(\alpha)$ ,  $\alpha^3 = \alpha + 1$ . 证明,

(1)  $\mathcal{O}_K = \mathbb{Z}(\alpha);$

(2)  $23\mathcal{O}_K = \mathfrak{p}_1^2 \mathfrak{p}_2$ , 其中  $\mathfrak{p}_1 = (23, \alpha - 10)$ ,  $\mathfrak{p}_2 = (23, \alpha - 3);$

(3)  $\mathfrak{p}_1, \mathfrak{p}_2$  是  $\mathcal{O}_K$  中不同的素理想;

(4)  $N_K(\mathfrak{p}_1) = N_K(\mathfrak{p}_2) = 23.$

18. (P36 Exer 9) 试问二次域  $\mathbb{Q}(\sqrt{10})$  中的理想  $(2, \sqrt{10})$  是否为主理想?

19. (P36 Exer 10)

(1) 设  $A$  是数域  $K$  中的理想,  $N_K(A) = g$ , 求证  $g \in A$ ;

(2) 对于每个正整数  $g$ , 求证  $K$  中满足  $N_K(A) = g$  的理想  $A$  只有有限多个.

20. (P36 Exer 12) 设  $\mathfrak{p}$  为数域  $K$  的素理想,  $A$  和  $B$  是  $K$  中的两个理想, 以  $\nu_{\mathfrak{p}}(A) (\geq 0)$  表示  $A$  的素因子分解式中  $\mathfrak{p}$  的指数 (若  $\mathfrak{p}$  在分解式中不出现, 则  $\nu_{\mathfrak{p}}(A) = 0$ ). 证明,

(1)  $\nu_{\mathfrak{p}}(AB) = \nu_{\mathfrak{p}}(A) + \nu_{\mathfrak{p}}(B)$ ;

(2)  $\nu_{\mathfrak{p}}(A + B) = \min(\nu_{\mathfrak{p}}(A), \nu_{\mathfrak{p}}(B))$ ,  $\nu_{\mathfrak{p}}(A \cap B) = \max(\nu_{\mathfrak{p}}(A), \nu_{\mathfrak{p}}(B))$ .

21. (P36 Exer 13) 设  $\mathfrak{p}$  为数域  $K$  的素理想, 对于  $0 \neq a \in \mathcal{O}_K$ , 定义  $\nu_{\mathfrak{p}}(a) = \nu_{\mathfrak{p}}(a\mathcal{O}_K)$ . 并且令  $\nu_{\mathfrak{p}}(0) = +\infty$ , 同时对  $n \in \mathbb{Z}$ , 规定

$$n + (+\infty) = (+\infty) + (+\infty) = (+\infty) \cdot n = (+\infty) \cdot (+\infty) = +\infty.$$

证明当  $a, b \in \mathcal{O}_K$  时,

(1)  $\nu_{\mathfrak{p}}(ab) = \nu_{\mathfrak{p}}(a) + \nu_{\mathfrak{p}}(b)$ ,  $\nu_{\mathfrak{p}}(a + b) \geq \min(\nu_{\mathfrak{p}}(a), \nu_{\mathfrak{p}}(b))$ ;

(2) 如果  $\nu_{\mathfrak{p}}(a) \neq \nu_{\mathfrak{p}}(b)$ , 则  $\nu_{\mathfrak{p}}(a + b) = \min(\nu_{\mathfrak{p}}(a), \nu_{\mathfrak{p}}(b))$ ;

(3) 试问当  $\nu_{\mathfrak{p}}(a) = \nu_{\mathfrak{p}}(b)$  时,  $\nu_{\mathfrak{p}}(a + b) = \min(\nu_{\mathfrak{p}}(a), \nu_{\mathfrak{p}}(b))$  是否成立?

22. (P87 Exer 3)

(1) 求以下实二次域类群和类数

$$K = \mathbb{Q}(\sqrt{d})$$

$$d = 2, 3, 5, 6, 7, 11, 13, 14, 15, 17, 19, 21, 22, 23;$$

(2) 求以下虚二次域类群和类数

$$K = \mathbb{Q}(\sqrt{-d})$$

$$d = 1, 2, 3, 5, 6, 7, 10, 11, 13, 15, 17, 19, 23, 43, 163;$$

(3) 求数域  $K = \mathbb{Q}(\omega)$ ,  $\omega^3 + \omega + 1 = 0$  的理想类数.

## 补充题

1. 设  $[K : \mathbb{Q}] = n$ ,  $\alpha \in \mathcal{O}_K$ ,  $\sigma_1, \dots, \sigma_n : K \rightarrow \mathbb{C}$  是  $K$  上的全部嵌入, 记

$$\prod_{i=1}^n (x - \sigma_i(\alpha)).$$

证明  $f(x) \in \mathbb{Z}[x]$ .

2. 关于第 5 题 (P14 Exer 13) 和第 14 题 (P35 Exer 3) 的注记. 这两道题本身也可以作为定义, 请自行思考如果以题中方式为定义, 相关结论如何“直接”证明. (这是开放性问题, 所谓“直接”证明不是 well-defined.)