

代数数论 2021 春练习题

李加宁

中国科学技术大学

日期: 2021 年 5 月 18 日

1 理想语言

习题 1.1. 设 L/K 是 n 次有限可分扩张.

(1) 证明如下迹与范的性质 (其定义见讲义 2.1 开头): $\text{Tr}_{L/K}(\alpha) = \sum \sigma(\alpha)$, $N_{L/K}(\alpha) = \prod \sigma(\alpha)$, 在求和与求积号中, σ 都是跑遍 $\text{Hom}_K(L, \bar{K})$.

(2) 设 $\alpha_1, \dots, \alpha_n \in L$, 证明有矩阵乘积

$$(\text{Tr}(\alpha_i \alpha_j))_{i,j} = (\sigma_i(\alpha_j))_{i,j} (\sigma_i(\alpha_j))_{i,j}^t.$$

从而判别式 $d_{L/K}(\alpha_1, \dots, \alpha_n) = (\det(\sigma(\alpha_j))_{\sigma,j})^2$. (回忆, 一组元素的判别式 $d_{L/K}$ 是迹诱导的双线性配对 $\text{Tr}_{L/K}(xy)$ 在这组元素下度量矩阵的行列式)

(3) 对于 $f(T) \in K[T]$ 次数为 n , 设 $\alpha_1, \dots, \alpha_n$ 是 $f(T)$ 在 \bar{K} 中的 n 个根 (带重数). 定义多项式的判别式 $\text{disc}(f) = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2$. 证明当 $f(T)$ 不可约时, 即 $L = K(\alpha)$,

$$\text{disc}(f) = d_{L/K}(1, \alpha, \dots, \alpha^{n-1}).$$

(4) 若 $L = K(\alpha)$, $f(T)$ 是 α 在 K 上的首一极小多项式, 证明

$$d_{L/K}(1, \alpha, \dots, \alpha^{n-1}) = (-1)^{\frac{n(n-1)}{2}} N_{L/K}(f'(\alpha)).$$

(5) 对 $f(T) = T^n + a$, $T^n + aT + b$, $a, b \in K$, 给出 $\text{disc}(f)$ 的一个公式.

习题 1.2. (1) 证明对每个代数数 α , 存在 $0 \neq n \in \mathbb{Z}$ 使得 $n\alpha$ 是代数整数.

(2) 证明对 \mathbb{Q} 的代数扩域 L (不一定是有限扩张), $\mathcal{O}_L := \bar{\mathbb{Z}} \cap L$ 的分式域是 L .

如果你知道环 (以下环都交换含 1) 的局部化的概念 (例如 Atiyah, Macdonald 交换代数导引第三章开头), 做做习题 1.3:

习题 1.3. 设 $A \subset B$ 是环. 设 C 是 A 在 B 中的整闭包, 设 $S \subset A$ 是个乘法封闭集, 证明 $S^{-1}A$ 在 $S^{-1}B$ 中的整闭包是 $S^{-1}C$.

注 1.1. 上述练习中, 取 $A = \mathbb{Z}$, $B = \bar{\mathbb{Q}}$, $S = \mathbb{Z} \setminus \{0\}$. 则 $S^{-1}A = \mathbb{Q}$, 故 $S^{-1}A$ 在 B 中的整闭包就是 $B = S^{-1}B$ 自身. 那么, 根据习题 1.3 的结论就有 $\bar{\mathbb{Q}} = S^{-1}\bar{\mathbb{Z}}$. 也就是说 $\bar{\mathbb{Q}}$ 中的元素都可以写成 $\frac{\alpha}{s}$, $\alpha \in \bar{\mathbb{Z}}$, $s \in \mathbb{Z}$ 的形式.

习题 1.4. 设 R 是诺特整环, I 是 R 的一个非零分式理想. (分式理想, I^{-1} , 及可逆的定义见 < 讲义定义 2.9 >)

(1) 证明 I^{-1} 也是分式理想.

(2) 证明 I 可逆当且仅当存在分式理想 J 使得 $IJ = (1)$.

习题 1.5. 在 $\mathbb{Z}[\sqrt{-3}]$ 中, 对 $\mathfrak{m} = (2, 1 + \sqrt{-3})$, 计算 \mathfrak{m}^{-1} , $\mathfrak{m}\mathfrak{m}^{-1}$. 说明 \mathfrak{m} 不是 $\mathbb{Z}[\sqrt{-3}]$ 的可逆理想.

习题 1.6. (1) 证明在 UFD 中素元和不可约元是一回事. (所谓素元是指其生成的主理想是素理想.)

(2) 证明对于 Dedekind 整环 R , R 是 UFD 能推出 R 是 PID .

习题 1.7. 设 R 是 Dedekind 整环, K 是其分式域. 令 \mathcal{I}_K 是其 (非零) 分式理想群. 给定非零素理想 \mathfrak{p} , 定义

$$v_{\mathfrak{p}} : \mathcal{I}_K \rightarrow \mathbb{Z}, \quad I \mapsto a_{\mathfrak{p}} \text{ 如果 } I = \prod_{\mathfrak{p}} \mathfrak{p}^{a_{\mathfrak{p}}} \text{ 是素理想分解式.}$$

将 $v_{\mathfrak{p}}((\alpha))$ 写成 $v_{\mathfrak{p}}(\alpha)$, 从而 $v_{\mathfrak{p}}$ 定义了 K^\times 到 \mathbb{Z} 的同态:

$$v_{\mathfrak{p}} : K^\times \rightarrow \mathbb{Z}, \text{ 我们还约定 } v_{\mathfrak{p}}(0) = \infty.$$

证明: (1) $v_{\mathfrak{p}}(I + J) = \min\{v_{\mathfrak{p}}(I), v_{\mathfrak{p}}(J)\}$, $v_{\mathfrak{p}}(I \cap J) = \max\{v_{\mathfrak{p}}(I), v_{\mathfrak{p}}(J)\}$. (即"加"是"最大公因子", "交"是"最小公倍数理想")

(2) 若 $\alpha, \beta \in K^\times$, $v_{\mathfrak{p}}(\alpha + \beta) \geq \min\{v_{\mathfrak{p}}(\alpha), v_{\mathfrak{p}}(\beta)\}$, 且 $v_{\mathfrak{p}}(\alpha) \neq v_{\mathfrak{p}}(\beta)$ 时, 成立等号.

习题 1.8 (中国剩余定理). 证明: 设 R 是 Dedekind 整环, 设 $I \subset R$ 是理想, $I = \prod_{1 \leq i \leq g} \mathfrak{p}^{e_i}$ 是其素理想分解. 则

$$R/I \cong \prod_{1 \leq i \leq g} R/\mathfrak{p}^{e_i}.$$

习题 1.9. (1) 证明只有有限个素理想的 Dedekind 整环是主理想整环.

(2) 由此推出 $\mathbb{Z}[\sqrt{-5}]$ 有无穷多个素理想.

(3) 通过考虑 $\mathbb{Z} \subset \mathbb{Z}[\sqrt{-5}]$ 得出 \mathbb{Z} 也有无穷个素理想. 由此得出素数无穷: -)

习题 1.10. 如果你知道什么是模的张量积还有代数的张量积, 试证明: (K_∞ 的定义以及映射 $K \rightarrow K_\infty$ 在讲义第三讲里) 存在 \mathbb{R} -代数同构 $K \otimes_{\mathbb{Q}} \mathbb{R} \cong K_\infty$ 使得下图交换 (竖箭头是自然映射)

$$\begin{array}{ccc} K & & \\ \downarrow & \searrow & \\ K \otimes_{\mathbb{Q}} \mathbb{R} & \longrightarrow & K_\infty \end{array}$$

习题 1.11 (格的定义). 设 Γ 是 n -维实线性空间 V 的子集. 则下面的 (1) 与 (2) 等价, (i) 与 (ii) 等价. 若满足 (1) 或 (2), 称 Γ 是 V 的格. 若满足 (i) 或 (ii), 称 Γ 是 V 的满格或完全格.

(1) Γ 是 V 的离散子群;

(2) 存在线性无关的向量 $\alpha_1, \dots, \alpha_k$ 使得 $\Gamma = \mathbb{Z}\alpha_1 + \dots + \mathbb{Z}\alpha_k$.

(i) Γ 是 V 的离散子群且 V/Γ 紧;

(ii) 存在线性无关的向量 $\alpha_1, \dots, \alpha_n$ 使得 $\Gamma = \mathbb{Z}\alpha_1 + \dots + \mathbb{Z}\alpha_n$.

习题 1.12 (微积分习题). 对 $t \geq 0$, 令

$$X_t = \{(x_1, \dots, x_{r_1}, z_1, \dots, z_{r_2}) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \mid \sum_{i=1}^{r_1} |x_i| + 2 \sum_{j=1}^{r_2} \sqrt{z_j \bar{z}_j} \leq t\}$$

则 $\mu(X) = 2^{r_1} (\pi/2)^{r_2} \frac{t^{r_1+r_2}}{(r_1+r_2)!}$. (\mathbb{C} 的测度我在讲义中约定过)

习题 1.13. 计算 $\mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{-6}), \mathbb{Q}(\sqrt{10})$ 的类群与类数.

习题 1.14 (思考题). 设 p 是素数, 证明 $\mathbb{Q}(\zeta_p)$ 的整数环是 $\mathbb{Z}[\zeta_p]$.

习题 1.15. 设 θ 是 $f(T) = T^3 - T^2 - 2T - 8$ 的一个根, $K = \mathbb{Q}(\alpha)$. 求 K 的一组整基. 证明不存在 $\alpha \in \mathcal{O}_K$ 使 $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

习题 1.16. (1) 试举例存在数域 K 中的元素在每个嵌入 $K \rightarrow \mathbb{C}$ 下的绝对值都是 1, 但它不是单位根.

(2) 试举例存在 K 和元素 $\alpha \in \mathcal{O}_K$ 使得 α 在某个嵌入 $K \rightarrow \mathbb{C}$ 下的绝对值 $|\sigma(\alpha)|_\sigma$ 是 1, 但它不是单位根.

习题 1.17. 设 $K = \mathbb{Q}(\sqrt{d})$, 称 $\epsilon = a + b\sqrt{d}$ 是 K 的基本单位如果 $\mathcal{O}_K^\times = \langle \epsilon, -1 \rangle$ 且 $a, b > 0$. 求 $K = \mathbb{Q}(\sqrt{223})$ 的基本单位. 求证 $x^2 - 223y^2 = \pm 3$ 有 \mathbb{Q} -解但没有 \mathbb{Z} -解.

习题 1.18. 回忆我们有 \mathcal{O}_K 在 K_∞ 下离散. 利用 Minkowski 定理证明, 对任意的 $\sigma' \in S_\infty$, \mathcal{O}_K 在 $\prod_{\sigma \in S_\infty \setminus \{\sigma'\}} K_\sigma$ 中稠密.

注: 这个结论推广了如 $\mathbb{Z}[\sqrt{2}] \subset \mathbb{R}^2, a + b\sqrt{2} \mapsto (a + b\sqrt{2}, a - b\sqrt{2})$ 中离散, 但 $\mathbb{Z}[\sqrt{2}] \subset \mathbb{R}$ 中稠密的现象.

第四周作业: 冯克勤-代数数论, 科学出版社 2000: 第 64-65 页习题 1, 2, 3, 4, 7.

习题 1.19. 设 p 是素数, k 是正整数. 设 $\zeta = \exp(\frac{2\pi i}{p^k})$ 是 p^k 次本原单位根. 证明 $1 - \zeta$ 的极小多项式 $f(T)$ 是 p -Eisenstein 的, 证明 $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \phi(p^k) = p^k - p^{k-1}$, 这里 ϕ 是欧拉函数. 证明 $\mathbb{Z}[\zeta]$ 是 $\mathbb{Q}(\zeta)$ 的整数环.

习题 1.20. 思考题: 是否存在 \mathbb{Q} 的无限代数扩张 $\Omega \subset \bar{\mathbb{Q}}$ 使得 $\mathcal{O}_\Omega := \Omega \cap \bar{\mathbb{Z}}$ 是 Dedekind 整环.

习题 1.21. 设 K/\mathbb{Q} 在素数 p 处完全分歧, 证明存在 $\pi \in \mathcal{O}_K$ 使得 $K = \mathbb{Q}(\pi)$ 且 π 的极小多项式是 p -Eisenstein 的.

习题 1.22. 设 m 是正整数, 证明 $\mathbb{Q}(\zeta_m)$ 的整数环是 $\mathbb{Z}[\zeta_m]$. (提示: 可利用讲义中第 9 节一般 Dedekind 整环的内容或者参考冯老师书).

习题 1.23. 证明: 若二次域 K 的判别式是 d , 则包含 K 的最小分圆域是 $\mathbb{Q}(\zeta_{|d|})$.

习题 1.24 (分歧指数与惯性指数的传递公式). 设 $L/E/K$ 是数域的扩张, 设 \mathfrak{P} 是 L 的一个非零素理想, $\mathfrak{P}_E = \mathfrak{P} \cap E, \mathfrak{p} = \mathfrak{P} \cap K$ 分别是 E, K 在 \mathfrak{P} 之下的素理想. 证明

$$e(\mathfrak{P}/\mathfrak{p}) = e(\mathfrak{P}/\mathfrak{P}_E)e(\mathfrak{P}_E/\mathfrak{p}), \quad f(\mathfrak{P}/\mathfrak{p}) = f(\mathfrak{P}/\mathfrak{P}_E)f(\mathfrak{P}_E/\mathfrak{p}).$$

习题 1.25. 求 $K = \mathbb{Q}(\sqrt{223})$ 的类群.

- 习题 1.26.** (1) 是否存在首一不可约多项式 $f(T) \in \mathbb{Z}[T]$ 使得 $f(T)$ 模每个素数都可约?
 (2) (思考题) 是否存在首一不可约多项式 $f(T) \in \mathbb{Z}[T]$ 使得 $f(T)$ 模每个素数方幂都可约?
 (3) (思考题) 是否存在首一不可约多项式 $f(T) \in \mathbb{Z}[T]$ 使得 $f(T)$ 模每个整数都可约?

冯克勤书第二章第三节习题 3, 4, 5, 7 选做两题.

2 赋值语言

习题 2.1. 证明 \mathbb{Z}_p 是列紧的. 利用度量空间中列紧等价于紧, 知 \mathbb{Z}_p 紧.

\mathbb{Z}_p 的等价描述: 对每个 n , 我们有自然映射 $\mathbb{Z}/p^{n+1}\mathbb{Z} \rightarrow \mathbb{Z}/p^n\mathbb{Z}$. 定义**逆向极限**

$$\varprojlim \mathbb{Z}/p^n\mathbb{Z} = \{(x_n) \in \prod_{n \geq 1} \mathbb{Z}/p^n\mathbb{Z} : x_{n+1} \mapsto x_n, \forall n\}.$$

将 $\mathbb{Z}/p^n\mathbb{Z}$ 赋予离散拓扑, $\prod_{n \geq 1} \mathbb{Z}/p^n\mathbb{Z}$ 乘积拓扑, $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$ 子空间拓扑.

习题 2.2. 验证这样定义的拓扑是使得对每个 n , 如下自然投射连续的最粗拓扑:

$$\varprojlim \mathbb{Z}/p^n\mathbb{Z} \rightarrow \mathbb{Z}/p^n\mathbb{Z}, \quad (x_n)_n \mapsto x_n.$$

习题 2.3. 证明自然映射 $\mathbb{Z}_p \rightarrow \prod_n \mathbb{Z}/p^n\mathbb{Z} \cong \prod_n \mathbb{Z}/p^n\mathbb{Z}$ 是单射, 且它的像是 $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$. 并且诱导了拓扑环同构 (既是环同构又是同胚)

$$\mathbb{Z}_p \cong \varprojlim \mathbb{Z}/p^n\mathbb{Z}. \quad (2.1)$$

习题 2.4. 考虑同态

$$\mathbb{Z} \rightarrow \prod_n \mathbb{Z}/p^n\mathbb{Z}, \quad x \mapsto (x \bmod p^n)_n.$$

这是个单同态. 证明 \mathbb{Z} 在右边的闭包是 $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$. 我们有如下交换图

$$\begin{array}{ccc} \mathbb{Z} & \hookrightarrow & \varprojlim \mathbb{Z}/p^n\mathbb{Z} \\ \downarrow & & \downarrow \cong \\ \mathbb{Z}_p & \xrightarrow{\cong} & \varprojlim \mathbb{Z}_p/p^n\mathbb{Z}_p. \end{array}$$

由此知 \mathbb{Z}_p 是 $\prod \mathbb{Z}/p^n\mathbb{Z}$ 的闭集, 而后者根据点集拓扑学知是紧空间, 从而 \mathbb{Z}_p 作为紧空间的闭集也是紧的.

习题 2.5. \mathbb{Z}_p 中的数可唯一的写成如下形式

$$a_0 + a_1p + a_2p^2 + \cdots, \quad a_i \in \{0, 1, \cdots, p-1\}.$$

从而 \mathbb{Q}_p 中的数可唯一的写成

$$\frac{a_{-n}}{p^n} + \frac{a_{n-1}}{p^{n-1}} + \cdots + a_0 + a_1p + a_2p^2 + \cdots, \quad a_i \in \{0, 1, \cdots, p-1\}.$$

这些称作是标准展开.

习题 2.6. (1) 将 -1 写成上面练习中的形式.

(2) 将 $\frac{1}{p-1} \in \mathbb{Z}_p$ 写成上面练习中的形式.

(3) 利用 Hensel 引理证明 $T^2 + 1$ 在 \mathbb{Z}_5 中有两个不同的根, 将它的两个根写成上面练习中的形式, 精确到 $O(5^3)$ 即可.

习题 2.7. 利用 Hensel 引理或者指数对数函数证明 $1 + 8\mathbb{Z}_2 = (\mathbb{Z}_2^\times)^2$.

习题 2.8. 证明 $\mathbb{Q}_2^\times \cong \mathbb{Z} \times \mathbb{Z}_2 \times \mathbb{Z}/2\mathbb{Z}$ 以及 $\mathbb{Q}_p^\times \cong \mathbb{Z} \times \mathbb{Z}_p \times \mathbb{Z}/p-1\mathbb{Z}$. 证明 \mathbb{Q}_p^\times 的指数有限的子群都是开子群.

习题 2.9. 求 $T^3 - 2$ 在 $\mathbb{Z}_5[T]$ 中的分解. 每个多项式因子的系数精确到 $O(5^3)$. 写出 $K = \mathbb{Q}(\sqrt[3]{2})$ 到 $\overline{\mathbb{Q}}_5$ 的三个嵌入, 并说明哪些是共轭的, 哪些给出 K 相同的赋值.

写出 K 到 \mathbb{C} 的三个嵌入, 并说明哪些是共轭的, 哪些给出 K 相同的赋值.

习题 2.10. 设 A 是 Dedekind 整环, K 是其分式域, L/K 是有限扩张, B 是 A 在 L 中整闭包. 设 \mathfrak{P} 是 B 的非零素理想, 设 \mathfrak{p} 是 A 的 \mathfrak{P} 之下的素理想. 设 I_B 和 I_A 分别是 B 和 A 的分式理想群. 定义 \mathfrak{P} 的范数

$$N_{L/K}(\mathfrak{P}) = \mathfrak{p}^f, \quad f = f(\mathfrak{P}/\mathfrak{p}).$$

将其延拓为群同态

$$N_{L/K} : I_B \rightarrow I_A.$$

(1) 这个映射称作是理想的范数. 将第一章 1.3 节的结论推广到此情形.

(2) 设 $AKLB = \mathbb{Z}_p, \mathbb{Q}_p, K_v, \mathcal{O}_v$. 利用此证明若 π 是 \mathcal{O}_v 的极大理想的一个生成元,

$$\text{ord}_p(N_{K_v/\mathbb{Q}_p}(\pi)) = p^{f(v/p)}.$$

习题 2.11. (1) 设 K 是数域. 证明 \mathbb{A}_K^\times 的拓扑严格细于作为 \mathbb{A}_K 自空间的拓扑.

(2) 证明 \mathbb{A}_K 和 \mathbb{A}_K^\times 的拓扑是 Hausdorff 且局部紧的, (但本身非紧), 且具有可数基. (选一个证即可)

(3) 解决 < 数论 I > 188 页的问题 7.

习题 2.12 (弱逼近定理, Neukrich 第二章 3.4). 设 K 是任意域, $|\cdot|_1, \dots, |\cdot|_n$ 是 K 上的 n 个两两不等价的赋值. 记 K_i 是 K 在 $|\cdot|_i$ 下的完备化. 证明 K 在 (自然嵌入) $\prod_{i=1}^n K_i$ 中稠密.

注. 当 K 是数域时, 注意到强逼近定理可推出弱逼近定理. 弱逼近定理的好处是它是对任意域成立的.