冯克勤《代数数论》题解与勘误

尔濯

目录

1 代数数域和代数整数环

1.1 代数数域

Exercise 1.1.1. 代数数集合是可数的，超越数集合是不可数的。

Proof: 用 I 表示所有整系数多项式之集，A_i 表示 $i \in I$ 的所有根组成的集合，则全体代数数集合 A 可以表为:

$$A = \{\alpha : \alpha\text{为某个整系数多项式的根}\} = \bigcup_{i\in I} A_i$$

显然 A_i 为有限集进而为可数集，如果我们证明全体整系数多项式之集可数，那么全体代数数可数。

记第 n 个素数为 p_{n-1}, 我们去证明 I 到 $\mathbb{Z}_{>0}$ 有一个单射。考虑映射:

$$a_n x^n + \cdots + a_1 x + a_0 \to \prod_{i=0}^{n} p_i^{f(a_i)}$$

其中

$$f(x) = \begin{cases} 2x & x > 0 \\ 1 - 2x & x \le 0 \end{cases}$$

这显然是单射，从而证明了代数数可数，假如超越数也可数，与 $\mathbb{R}$ 不可数矛盾。

Exercise 1.1.2. *(a)* 每个二次数域都可以表成 $\mathbb{Q}(\sqrt{d})$, 其中 d 为无平方因子整数。
(b) 如果 d, d' 为不同的无平方因子整数，则 $\mathbb{Q}(\sqrt{d}) \neq \mathbb{Q}(\sqrt{d'})$
(c) 二次数域必为有理数域的伽罗瓦扩张，试求其伽罗瓦群。

Proof: 在二次数域 K 中取一个与 1 线性无关的数 α, 考虑其最小多项式为二次首一有理系数多项式，用求根公式将 α 解出得到:

$$\alpha = a + b\sqrt{d}, \quad a, b \in \mathbb{Q}, d \in \mathbb{Z}$$

从而不难证明:$\mathbb{Q}(\sqrt{d}) = K$

如果 $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{d'})$ 那么 $\sqrt{d} = a + b\sqrt{d'} \quad a, b \in \mathbb{Q}$，平方以后得到 $a = 0$, 从而推出 $m\sqrt{d} = n\sqrt{d'}, \quad m, n \in \mathbb{Z}$, 平方后比较两边 d, d' 素因子幂次，借助无平方因子，得到 $d = d'$。

再考虑一个二次数域 $K = \mathbb{Q}(\sqrt{d})$, 由于 $\sqrt{d} \to \pm\sqrt{d}$ 诱导出来两个不同的 K 的自同构，所以Galois群为二阶循环群。

Exercise 1.1.3. *(a)* 求下列代数数的次数和最小多项式:

$$\sqrt{2} + \sqrt{3} + \sqrt{5}, \sqrt{2 + \sqrt{2}}, \sqrt{2} + e^{2\pi i/3}$$

(b) 求 $\sqrt{2}+\sqrt{3}+\sqrt{5}$ 在 $\mathbb{Q}(\sqrt{30})$ 的共轭元。

Proof: $\sqrt{2+\sqrt{2}}$ 显然是 $f_2(x)=x^4-4x^2+2$ 的根 (由两次平方得来)，而 $f_2(x)$ 由爱森斯坦判别法是不可约多项式，因此是其最小多项式。

对于 $\sqrt{2}+\sqrt{3}+\sqrt{5}$, 可以通过移项和平方构造出一个 8 次多项式使其以 $\sqrt{2}+\sqrt{3}+\sqrt{5}$ 作为根，现在我们证明:

$$[\mathbb{Q}(\sqrt{2}+\sqrt{3}+\sqrt{5}):\mathbb{Q}]=8$$

由此可以得到需要的结论, 这需要一个引理:

Lemma 1.1. *$p_1,\dots,p_n$ 为不同素数，则:*

$$[\mathbb{Q}(\sqrt{p_1},\dots,\sqrt{p_n}):\mathbb{Q}]=2^n$$

这个引理蕴含着 $p_1,\dots,p_n$ 的任意子集的乘积 (共 2^n 个，空集视为 1) 在 $\mathbb{Q}$ 上的线性无关性。我们用归纳法证明一个更强的结论:$A=\{x_1,\dots,x_n\}$ 是 $\mathbb{Z}$ 的子集使得任意 A 的非空子集的元素相乘不为 $\mathbb{Z}$ 中平方元，则:

$$[\mathbb{Q}(\sqrt{x_1},\dots,\sqrt{x_n}):\mathbb{Q}]=2^n$$

$n=1$ 时显然，$n=2$ 时，$[\mathbb{Q}(\sqrt{x_1},\sqrt{x_2}):\mathbb{Q}]=[\mathbb{Q}(\sqrt{x_1},\sqrt{x_2}):\mathbb{Q}(\sqrt{x_2})][\mathbb{Q}(\sqrt{x_2}):\mathbb{Q}]$ 只需证明:$[\mathbb{Q}(\sqrt{x_1},\sqrt{x_2}):\mathbb{Q}(\sqrt{x_2})]=2$，假如 $\sqrt{x_1}=a+b\sqrt{x_2},\quad a,b\in\mathbb{Q},b=\frac{p}{q}$, 平方后得到 $a=0$, 从而有: $q^2x_1x_2=p^2x_2^2$, 左边必有一个素因子幂次为奇数，矛盾。

用归纳法，假设对所有 $<n$ 的数成立，$n\geq 3$。

设 $L=\mathbb{Q}(\sqrt{p_1},\dots,\sqrt{p_{n-2}})$, 则由归纳假设只需证明: $[L(\sqrt{x_{n-1}},\sqrt{x_n}):L]=4$，如果 $\sqrt{x_{n-1}},\sqrt{x_n},\sqrt{x_{n-1}x_n}$ 之中有 $\in L$ 的元素, 则会与 $n-1$ 时的结论矛盾。因此 $[L(\sqrt{x_{n-1}},\sqrt{x_n}):L]=2[L(\sqrt{x_{n-1}},\sqrt{x_n}):L(\sqrt{x_{n-1}}]$, 而如果 $\sqrt{x_n}=l_1+l_2\sqrt{x_{n=1}}$，移向平方后与 $\sqrt{x_nx_{n-1}}\notin L$ 矛盾，从而我们完成了引理的证明。

令 $x=\sqrt{2}+\sqrt{3}+\sqrt{5}$，移向平方两次可以得到 $\mathbb{Q}(\sqrt{2}+\sqrt{3}+\sqrt{5})\supseteq\mathbb{Q}(\sqrt{30})$, 因此只需证明: $[\mathbb{Q}(\sqrt{2}+\sqrt{3}+\sqrt{5}):\mathbb{Q}(\sqrt{30})]=4$

事实上 $\sqrt{2}+\sqrt{3}+\sqrt{5}$ 是 $x^4-20x^2-8\sqrt{30}x-24$ 的根，而如果他还是 $\mathbb{Q}(\sqrt{30})$ 上一个二次多项式的根 (扩张次数只能是二的幂)，将多项式设出来，然后利用引理得到的线性无关性可得该待定系数得到的方程无解，从而 $x^4-20x^2-8\sqrt{30}x-24$ 是 $\sqrt{2}+\sqrt{3}+\sqrt{5}$ 在 $\mathbb{Q}(\sqrt{30})$ 上的最小多项式，这也完成了第二问的证明，即共轭元素为 $x^4-20x^2-8\sqrt{30}x-24$ 的四个根。

令 $c=\sqrt{2}+e^{2\pi\mathrm{i}/3}$, 计算得知 $\sqrt{2}=\frac{c^2+c+3}{1+2c}$，从而 $[\mathbb{Q}(c):\mathbb{Q}]=[\mathbb{Q}(c):\mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=4$ ，上式成立只需注意到 c 为虚数故前者不可能为 1

因此，$(x^2+x+3)^2-2(1+2x)^2$ 为其最小多项式

Exercise 1.1.4. *全体代数数构成域，且为有理数域的无限次扩张。*

Proof: 前一个命题是域论基本结论，可以参考 [?] 的 Chapter 13。后者只需注意到由爱森斯坦判别法，对于任意正整数 n, x^n-2 为 $\mathbb{Q}[x]$ 上不可约多项式, 从而: $\left\{(\sqrt[n]{2})^a : 0 \leq a \leq n-1\right\}$ 在 $\mathbb{Q}$ 上线性无关。

Exercise 1.1.5. *一个代数整数是单位根的充要条件是每个共轭元素模长为 1*

Proof: 该证明参考了 MSE 上的讨论: https://math.stackexchange.com/questions/4323

只证明全部共轭元素模长为 1 则为单位根, 另一边是显然的。

对于代数整数 α，设其最小多项式为:$f(x) = x^n + \cdots + a_1x + a_0$, 其中 $a_i \in \mathbb{Z}$, 设其全部共轭元素为 $\alpha_1, \ldots, \alpha_n$, 其中 $\alpha = \alpha_1$, 则 $f(x) = \prod_{i=1}^{n}(x-\alpha_i)$, 再考虑一列多项式 $f_m(x) = \prod_{i=1}^{n}(x-\alpha_i^m)$, 由韦达定理，每个根都模长为 1 的 n 次整系数多项式的每个系数有上界 (只与 n 有关), 因此只有有限多个每个根都模长为 1 的 n 次整系数多项式。考虑对称多项式基本定理 [?]，$f_m(x)$ 均为整系数多项式, 因此在 $f_m(x)$ 中取出任意多项 (不妨取 $n+1$ 项) 使得他们表示同一个多项式, 对比这些项的根, 如果第一项为 $f_s(x)$, 则有根 α^s, 之后 n 项里面, 要么有 α^t 使得 $\alpha^t = \alpha^t$，此时 α 已经为单位根，要么由抽屉原理有 $\alpha^s = \alpha_i^{t_1} = \alpha_i^{t_2}$, 此时 α_i 为单位根, 设 $\alpha_i^{n_0} = 1$, 由等式 $\alpha^{sn_0} = \alpha^{t_1 n_0} = 1$ 知 α 为单位根, 证毕!

有趣的是, 有人还指出: 存在模长为 1 的代数整数不是单位根，也就是说这个命题进一步减弱条件就不再成立。

参考:http://ramanujan.math.trinity.edu/rdaileda/research/papers/p1.pdf

2 整数环中的素理想分解

2.1 伽罗瓦扩域中的素理想分解

Exercise 2.1.1. 设 $K/\mathbb{Q}$ 为数域的 *Abel* 扩张，K_I 为 p 相对于 $K/\mathbb{Q}$ 的惯性域，则 K_I 为使得 p 非分歧的最大子域。

Proof: 考虑下列域、伽罗瓦群、素理想、剩余类域的对应图：

$$\begin{array}{cccc} L & \{e\} & P_1 & O_L/P_1 \\ | \ e & | & | & | \\ K_I & I & P_I & O_I/P_I \\ | \ f & | & | & | \\ K_D & D & P_D & O_D/P_D \\ | \ g & | & | & | \\ \mathbb{Q} & \mathrm{Gal}(L/\mathbb{Q}) & p\mathbb{Z} & \mathbb{Z}/p\mathbb{Z} \end{array}$$

要证明 K_I 是 $p\mathbb{Z}$ 的最大不分歧子域，考虑一个域 M，$p\mathbb{Z}$ 在 M 上不分歧，则 p 在 MK_I 上不分歧，从而我们得到：

$$[MK_I:\mathbb{Q}] = f \times (p\mathbb{Z}\text{在}MK_I\text{的分裂次数}) \le f \times (p\mathbb{Z}\text{在}L\text{的分裂次数}) = fg = [K_I:\mathbb{Q}]$$

从而 $[MK_I:\mathbb{Q}] \le [K_I:\mathbb{Q}] \le [MK_I:\mathbb{Q}]$, 证毕。

3 理想类数与理想类群

3.1 类群与类数

Exercise 3.1.1. 设 A 是数域 K 的分式理想，求证：

(a)A 为整理想 $\Leftrightarrow A \subseteq O_k$

(b)$A^{-1} = \{\alpha \in K : \alpha A \subseteq O_k\}$

Proof: (a) 的充分性显然，对于必要性，设 $\mu A = I$,I 为 O_k 中理想。直接按理想的定义验证 A 构成 O_k 中理想，比如 $\forall x, y \in A$,$\mu(x+y) \in I = \mu A =$, 从而 $x + y \in A$

(b) 需要使用本书第二章第一节的引理 5，对于 O_k 的非零理想 I，以及其中非零元 $\alpha \in I$，我们构造:

$$J = \{\beta \in O_k : \beta I \subseteq (\alpha)\}$$

从而有：$IJ = (\alpha)$，进而：

$$A^{-1} = \frac{\mu}{\alpha}J = \left\{\frac{\mu}{\alpha}\beta : \beta \in O_k, \frac{\mu\beta}{\alpha}A \subseteq O_k\right\} = \{\gamma : \gamma \in K, \gamma A \subseteq O_k\}$$

上式最后一个等号左边包含右边是因为任意 $\gamma \in K$, 我们有:

$$\beta = \frac{\alpha}{\mu}\gamma \in \gamma A \subseteq O_k$$

Exercise 3.1.2. *O_k 为主理想整环等价于 $h(K) = 1$*

Proof: 只需证 O_k 为主理想整环，则所有分式理想为主分式理想，考虑分式理想 $A = \frac{1}{\mu}I$, 设 $I = (\beta)$，则

$$A = \frac{1}{\mu}I = \frac{1}{\mu}(\beta) = \frac{\beta}{\mu}O_k$$

Exercise 3.1.3. *设 $a, b, c \in \mathbb{R}$,$4ac - b^2 > 0$, 求证当 $f \geq \frac{2}{\pi}\sqrt{4ac - b^2}$ 时，存在 $(0, 0) \neq (a, b) \in \mathbb{Z}^2$, 使得 $ax^2 + bxy + cy^2 \leq f$*

Proof: 考虑 $\mathbb{R}^2$ 上的格 $\mathbb{Z}^2$，其体积为 $V(\mathbb{Z}^2) = 1$, 因此只需证明，关于原点对称的紧集

$$A = \left\{(x, y) \in \mathbb{R}^2 : ax^2 + bxy + cy^2 \leq f\right\}$$

的测度 ≥ 4.

由于正交变换下，测度保持不变，对实对称矩阵 $J = \begin{bmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{bmatrix}$ 用一个正交矩阵对角化得到 $TJT^{-1} = \mathrm{diag}(\lambda_1, \lambda_2)$，其中 $\lambda_i, i = 1, 2$ 为方程 $x^2 - (a + c)x + ac - \frac{b^2}{4}$ 的两个根。

从而

$$\mu(A) = \mu(\left\{(x, y) \in \mathbb{R}^2 : \lambda_1 x^2 + \lambda_2 y^2 \leq f\right\}) = \frac{f\pi}{\sqrt{\lambda_1\lambda_2}} \geq \frac{\frac{2}{\pi}\pi\sqrt{4ac - b^2}}{\sqrt{ac - \frac{b^2}{4}}} = 4$$

由 Minkowski 定理命题得证。

4 部分细节补充

5 勘误

1. 第 28 页引理 3, 将 1 改为 I。

2. 第 42 页定理 2.7(c)，将 $\mathfrak{p}$ 更正为 p。

3. 第 50 页第一行将最后一个等号的 $\sum_{i=0}^{f-1}(\bar{\lambda})^{pi}$ 更正为 $\sum_{i=0}^{f-1}(\bar{\lambda})^{p^i}$。

4. 第 56 页 3.2 分解群与惯性群下第三行 $\bar{K}=O_{K/\mathfrak{p}}$ 更正为 $\bar{K}=O_K/\mathfrak{p}$。

5. 第 60 页引理 16(b) 最后一个指数上的符号应为 $f(\mathfrak{P}_E|\mathfrak{p})$。

6. 第 65 页倒数第 9 行，将 $\mathbb{F}p$ 更正为 $\mathbb{F}_p$。

7. 第 69 页第二行 α 更正为 a。

8. 第 107 页习题 6, 将 $p=1(\mathrm{mod}\,4)$ 更正为 $p\equiv 1(\mathrm{mod}\,4)$,$d$ 更正为 p。

9.