代数数论　　2018 春

考试时间：**2:00 - 4:00** 。共 **10** 题，每题 **10** 分。

如下是 $\mathbb{Q}(\zeta_{15})$ 的子域扩张图：

$$\begin{tikzcd}
 & \mathbb{Q}(\zeta_{15}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\zeta_5) \arrow[dr, dash] & \mathbb{Q}(\sqrt{5},\sqrt{-3}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \mathbb{Q}(\zeta_{15}+\zeta_{15}^{-1}) \arrow[dl, dash] \\
\mathbb{Q}(\sqrt{-3}) \arrow[dr, dash] & \mathbb{Q}(\sqrt{5}) \arrow[d, dash] & \mathbb{Q}(\sqrt{-15}) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

1.　求素数 2 和 5 在 $\mathbb{Q}(\zeta_{15})$ 的分歧指数与惯性指数。

证明. 利用如下事实：设 p 是个素数，$\mathbb{Q}(\zeta_{p^n})$ 中分歧的只有素数 p，且 p 是完全分歧，$(p)=(1-\zeta_{p^n})^{\phi(p^n)}$.

2 在 $\mathbb{Q}(\zeta_3),\mathbb{Q}(\zeta_5)$ 中均不分歧。所以 2 在 $\mathbb{Q}(\zeta_{15})$ 中不分歧。即分歧指数为 1.

2 在 $\mathbb{Q}(\zeta_{15})$ 中的惯性指数等于 $2 \bmod 15$ 在 $(\mathbb{Z}/15\mathbb{Z})^\times$ 中的阶 4, 所以惯性指数为 4.

5 在 $\mathbb{Q}(\zeta_5)$ 中的分歧指数为 4, 在 $\mathbb{Q}(\zeta_3)$ 中不分歧，所以 5 在 $\mathbb{Q}(\zeta_{15})$ 的分歧指数为 4.

5 在 $\mathbb{Q}(\zeta_3)$ 中的惯性指数等于 $5 \bmod 3$ 在 $(\mathbb{Z}/3\mathbb{Z})^\times$ 中的阶 2. 或者利用勒让德符号 $\left(\dfrac{-3}{5}\right)=-1$ 知 5 在 $\mathbb{Q}(\sqrt{-3})$ 中惯性。所以 5 的惯性指数为 ≥ 2, 而 5 的分歧指数是 4, 而 $[\mathbb{Q}(\zeta_{15}):\mathbb{Q}]=8$ 知 5 的惯性指数为 2.

2.　决定素数 2 和 5 在 $\mathbb{Q}(\zeta_{15})$ 中的分解域与惯性域。

证明. 由于 2 在 $\mathbb{Q}(\zeta_{15})$ 中不分歧，所以它的惯性群平凡，惯性域为 $\mathbb{Q}(\zeta_{15})$.

2 的分解群由 Frob_2 生成，在标准同构 $\mathrm{Gal}(\mathbb{Q}(\zeta_{15})/\mathbb{Q}))\cong(\mathbb{Z}/15\mathbb{Z})^\times$ 下，Frob_2 生成的群对应于 $\{2 \bmod 15, 4 \bmod 15, 8 \bmod 15, 1 \bmod 15\}\subset(\mathbb{Z}/15\mathbb{Z})^\times$. 它所对应的子域即惯性域是 $\mathbb{Q}(\sqrt{-15})$.

或者利用 2 的分解域是最大的子域使得 2 完全分裂，由于 2 的分裂指数为 2，所以这个域是二次域，由于 2 在 $\mathbb{Q}(\sqrt{-15})$ 中分裂，所以这是它的分解域。

对于 5，在 $\mathbb{Q}(\zeta_5)$ 中完全分歧, 在 $\mathbb{Q}(\zeta_3)$ 中不分歧。设 I_5 为 5 的惯性群，则在同构

$\mathrm{Gal}(\mathbb{Q}(\zeta_{15}))\cong\mathrm{Gal}(\mathbb{Q}(\zeta_3)/\mathbb{Q})\times\mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$ 下，I_5 的像为 $\mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$. 所以 I_5 所确定的域为 $\mathbb{Q}(\zeta_3)$. 即惯性域为 $\mathbb{Q}(\zeta_3)=\mathbb{Q}(\sqrt{-3})$.

也可利用 5 的惯性域是最大的子域 K 使得 5 在 $K/\mathbb{Q}$ 中不分歧，则从上面的域扩张关系图上知 5 的惯性域是 $\mathbb{Q}(\sqrt{-3})$.

由于 5 的分解群的阶为分歧指数 $\times$ 惯性指数 $=8$. 所以分解群为 $\mathrm{Gal}(\mathbb{Q}(\zeta_{15})/\mathbb{Q})$, 对应的分解域为 $\mathbb{Q}$.

3.　证明扩张 $\mathbb{Q}(\zeta_{15})/\mathbb{Q}(\zeta_{15}+\zeta_{15}^{-1})$ 在每个素理想处均不分歧，在每个无穷素位处均分歧。

证明．由 $\mathbb{Q}(\zeta_{15})=\mathbb{Q}(\zeta_{15}+\zeta_{15}^{-1})(\zeta_3)$, 知只可能在 3 之上的素理想分歧。由 $\mathbb{Q}(\zeta_{15})=\mathbb{Q}(\zeta_{15}+\zeta_{15}^{-1})(\zeta_5)$ 知只可能在 5 之上的素理想分歧。故在每个素理想处不分歧。

容易看出这个结论与证明可推广为：当 n 不是个素数幂时，$\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_n+\zeta_n^{-1})$ 中的素理想均不分歧。

由于 $\zeta_{15}+\zeta_{15}^{-1}$ 的共轭根的形式为 $\zeta_{15}^k+\zeta_{15}^{-k}$, 均是实数，所以 $\mathbb{Q}(\zeta_{15}+\zeta_{15}^{-1})$ 只有实嵌入，而 $\mathbb{Q}(\zeta_{15})$ 只有复嵌入，所以无穷素位均分歧。

4. 求 $\mathbb{Q}(\sqrt{5})$ 的基本单位，求 $\mathbb{Q}(\sqrt{-15}),\mathbb{Q}(\sqrt{-3}),\mathbb{Q}(\sqrt{5})$ 的类数。

证明．$(1,1)$ 是 $x^2-5y^2=\pm4$ 的整数解，且显然是纵坐标最小的正整数解，所以 $\frac{1+\sqrt{5}}{2}$ 是 $\mathbb{Q}(\sqrt{5})$ 的基本单位。

$\mathbb{Q}(\sqrt{-3}),\mathbb{Q}(\sqrt{5})$ 的 Minkowski 常数均小于 2, 所以类数为 1.

$\mathbb{Q}(\sqrt{-15})$ 的 Minkowski 常数小于 3, 所以它的类群由 2 之上的素理想 $(2,1+\sqrt{-15})$ 生成，由 $\frac{x^2+15y^2}{4}=2$ 无整数解以及 $\frac{x^2+15y^2}{4}=4$ 有整数解 $(1,1)$ 知 $(2,1+\sqrt{-15})$ 在类群中阶为 2. 故类数为 2.

5. 令 $F=\mathbb{Q}(\sqrt{5},\sqrt{-3})$，求 F 的类数。

证明．由于 $\mathbb{Q}(\sqrt{-5}),\mathbb{Q}(\sqrt{-3})$ 的判别式互素，由教材 24 页引理 9，F 的判别式 $d(F)=5^2\times(-3)^2=225$. 显然 F 有两对复嵌入。F 的 Minkowski 常数

$$M_F=(\frac{4}{\pi})^2\frac{4!}{4^4}\sqrt{|d_F|}<3$$

设 $\mathfrak{p}$ 是 $\mathcal{O}_F$ 整除 (2) 的素理想，则由 (2) 在 $\mathbb{Q}(\sqrt{5})$ 中惯性在 $\mathbb{Q}(\sqrt{-15})$ 中分裂知 $f(\mathfrak{p}/2)=g(\mathfrak{p}/2)=2$. 注意到 $\frac{\sqrt{5}+\sqrt{-3}}{2}=\frac{1+\sqrt{5}}{2}-\frac{1-\sqrt{-3}}{2}$ 是代数整数，且

$$N_{F/\mathbb{Q}(\sqrt{5})}(\frac{\sqrt{5}+\sqrt{-3}}{2})=2$$

知 $\mathfrak{p}=(\frac{\sqrt{5}+\sqrt{-3}}{2})$, 从而 F 的类数是 1.

6. 记 χ_{-15} 为 $\mathbb{Q}(\sqrt{-15})$ 的非平凡 Dirichlet 特征，$L(s,\chi_{-15})$ 为其 L 函数，求 $L(1,\chi_{-15})$.

证明．

方法 1：如果做了 Gauss 和符号的习题，可直接按 $L(1,\chi)$ 的公式计算，即教材 211 页。

方法 2：利用 zeta 函数分解以及类数公式：

$$\zeta_{\mathbb{Q}(\sqrt{-15})}(s)=\zeta(s)L(1,\chi_{-15}),$$

则

$$L(1,\chi_{-15})=\lim_{s\to1^+}\frac{\zeta_{\mathbb{Q}(\sqrt{-15})}(s)}{\zeta(s)}=\frac{2\pi\times2}{2\times\sqrt{15}}=\frac{2\pi}{\sqrt{15}}$$

最后两个等号用了 $\mathbb{Q}(\sqrt{-15})$ 的复嵌入对数为 1, 实嵌入个数为 0, 类数为 1, 正则子为 1, 单位根个数为 2, 判别式为 -15.

7. 证明 $\mathcal{O}_F^\times=\epsilon^{\mathbb{Z}}\times\mu_6$. 其中 μ_6 是 6 次单位根群，$\epsilon=\frac{1+\sqrt{5}}{2}$.

证明. 第一步：求 F 的单位根群 W_F，显然 $\mu_6 \subset W_F \subsetneq W_{\mathbb{Q}(\zeta_{15})} = \mu_{30}$. 得 $W_F = \mu_6$.

第二步：由于 F 的 $r_2 = 2, r_1 = 0$, 存在 $u \in \mathcal{O}_F^\times$ 使得 $\mathcal{O}_F^\times = u^{\mathbb{Z}} \times \mu_6$. 而 $\epsilon^{\mathbb{Z}} \times \mu_6 \subset \mathcal{O}_F^\times$. 故 $\epsilon = u^k w$, $k \in \mathbb{Z}, w \in \mu_6$. 我们需要证明 $k = 1$. 而 $R_F := \log|\sigma(u)|^2 = 2k \log \frac{1+\sqrt{5}}{2}$, 其中 σ 是 F 的一个复嵌入。$k = 1$ 等价于 $R_F = 2k \log \frac{1+\sqrt{5}}{2}$.

下面来利用类数公式来证明 F 的正则子 $R_F = 2 \log \frac{1+\sqrt{5}}{2}$：

$\mathrm{Gal}(F/\mathbb{Q})$ 是 4 阶群，它的 3 个非平凡特征为 $\mathrm{Gal}(\mathbb{Q}(\sqrt{5})/\mathbb{Q}), \mathrm{Gal}(\mathbb{Q}(\sqrt{-3})/\mathbb{Q}), \mathrm{Gal}(\mathbb{Q}(\sqrt{-15})/\mathbb{Q})$ 的非平凡特征，即三个二次子域的非平凡 Dirichlet 特征，记为 $\chi_5, \chi_{-3}, \chi_{-15}$. 根据 zeta 函数的分解有

$$\zeta_F(s) = \zeta(s) L(s, \chi_5) L(s, \chi_{-3}) L(s, \chi_{-15}).$$

利用 $\mathbb{Q}(\sqrt{5}), \mathbb{Q}(\sqrt{-3}), \mathbb{Q}(\sqrt{-15})$ 的类数公式求得

$$L(1, \chi_5) = \lim_{s \to 1^+} \frac{\zeta_{\mathbb{Q}(\sqrt{5})}(s)}{\zeta(s)} = \frac{2}{\sqrt{5}} \log \frac{1+\sqrt{5}}{2}$$

$$L(1, \chi_{-3}) = \lim_{s \to 1^+} \frac{\zeta_{\mathbb{Q}(\sqrt{-3})}(s)}{\zeta(s)} = \frac{\pi}{3\sqrt{3}}$$

$$L(1, \chi_{-15}) = \lim_{s \to 1^+} \frac{\zeta_{\mathbb{Q}(\sqrt{-15})}(s)}{\zeta(s)} = \frac{2\pi}{\sqrt{15}}$$

得

$$\lim_{s \to 1^+} \frac{\zeta_F(s)}{\zeta(s)} = \frac{2^{r_1}(2\pi)^{r_2} h_F R_F}{|W_F|\sqrt{|d_F|}} = L(1, \chi_5) L(1, \chi_{-3}) L(1, \chi_{-15})$$

其中 $r_2 = 2, |W_F| = 6, |d_F| = 225$ 是易算的 (d_F 的计算可用教材 24 页引理 9), 而第 5 题计算了 $h_F = 1$,

知 $R_F = 2 \log \frac{1+\sqrt{5}}{2}$.

8. 证明 $x^3 - 2$ 在 $\mathbb{Q}_5$ 中只有一个根。写出它（5 进展开下，精确到 5^2 位）。

证明. 记 $f(x) = x^3 - 2$. 由于 $f(x) = 0 \bmod 5$ 只有一个解 $3 \bmod 5$，且 $f'(3) \not\equiv 0 \bmod 5$. 所以根据 Hensel 引理存在唯一的解 $a \in \mathbb{Z}_5$ 使得 $f(a) = 0$ 且 $a \equiv 3 \bmod 5$. 令一方面若 $f(b) = 0$, 则 $b \equiv 3 \bmod 5$. 所以根据 Hensel 引理的唯一性知 $b = a$.

解的近似值可通过 Hensel 引理的证明来求：

令 $a_0 = 3$,

设 $a_1 = a_0 + t_0 5$, $f(a_1) = f(a_0) + f'(a_0) 5 t_0 = 25 + 27 \times 5 t_0 \equiv 0 \bmod 5^2$. 得 $t = 0$.

设 $a_2 = a_1 + t_1 5^2$, $f(a_2) = f(a_1) + f'(a_1) 5^2 t_1 \equiv 0 \bmod 5^3$

$f(x+3) = (x+3)^3 - 2 = x^3 + 9x^2 + 27x + 25$

在 $\mathbb{F}_5[x]$ 中，$x^3 - 2$ 的不可约分解为 $(x-3)(x^2+3x+4)$.

根据 Hensel 引理, (教材 274 页定理 8.6.) 在 $\mathbb{Z}_5[x]$ 中，$x^3 - 2 = g(x)h(x)$, 且 $g(x) \equiv x - 3 \bmod 5, h(x) \equiv x^2 + 3x + 4 \bmod 5$, 显然 $h(x)$ 不可约。所以 $x^3 - 2 = 0$ 在 $\mathbb{Z}_5$ 中有且只有一个根。

根的近似值可由 Hensel 引理的证明中得到, 记 $f(x) = x^3 - 2$.

令 $a_0 = 3$, 则 $f(a_0) \bmod 0 \equiv 5$.

设 $a_1 = a_0 + t_0 5$, $f(a_1) = f(a_0) + f'(a_0) 5 t_0 = 25 + 27 \times 5 t_0 \equiv 0 \bmod 5^2$. 得 $t = 0$.

设 $a_2 = a_1 + t_1 5^2$, $f(a_2) = f(a_1) + f'(a_1) 5^2 t_1 \equiv 0 \bmod 5^3$ 得 $t_1 = 2$. 即 $a_2 = 3 + 2 \times 5^2$.

得 $a = 3 + 2 \cdot 5^2 + O(5^3)$.

也可用牛顿逼近法定理 8.9(227 页),

$$a_0 = 3$$

$$a_1 = a_0 - \frac{f(a_0)}{f'(a_0)}, \frac{f(a_0)}{f'(a_0)} = \frac{25}{27}$$

$$a_2 = a_1 - \frac{f(a_1)}{f'(a_1)} = \frac{195299}{127008}, \frac{f(a_1)}{f'(a_1)} = \frac{68125}{127008}$$

则 $v_5(a-a_1) \geq v_5(\frac{f(a_1)}{f'(a_1)}) = v_5(68125/127008) = 4$.

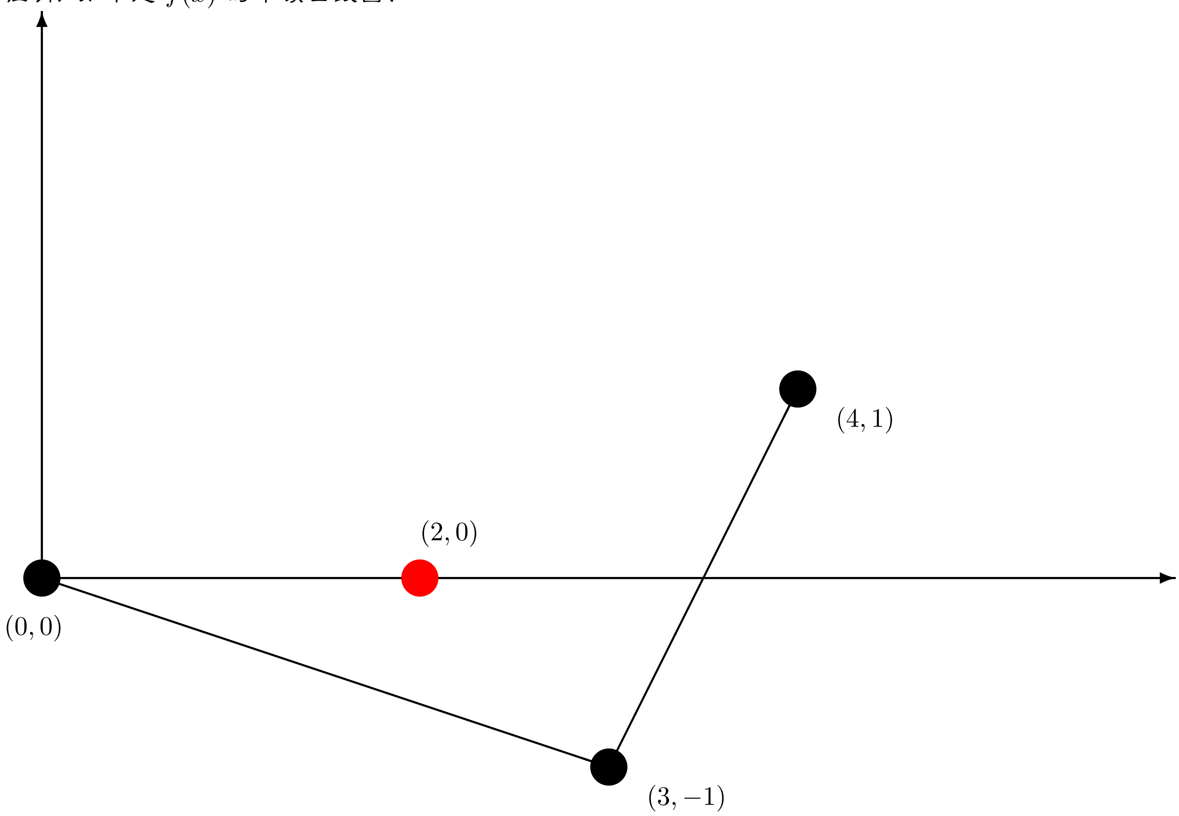
所以 a 的 5 进展开的前 4 位与 $\frac{195299}{127008}$ 的 5 进展开前四位相同。

由于 $\frac{195299}{127008} = 3 + 2\cdot 5^2 + 2\cdot 5^3 + \cdots$

所以 $a = 3 + 2\cdot 5^2 + 2\cdot 5^3 + \cdots$.

9. 证明多项式 $f(x) = 1 + x^2 + \frac{x^3}{3} + 3x^4$ 在 $\mathbb{Q}_3$ 中有根 α 使得 $v_3(\alpha) = -2$. 求一个有理数 a 使得 $v_3(\alpha - a) \geq 2$.

证明. 如下是 $f(x)$ 的牛顿曲线图：



由上图知存在 $f(x)$ 的根 α 使得 $v_3(\alpha) = -2$, 另外两个根的加法 (指数) 赋值均为 $-\frac{1}{2}$. 从而 α 是 $f(x)$ 在 $\mathbb{Q}_3$ 中唯一的根。

令 $g(x) = 9f(x/9) = x^4 + x^3 + 27x^2 + 2187$, 对 $g(x)$ 使用 Hensel 引理 (或者牛顿逼近定理) 得解 $2 + 2\cdot 3 + 2\cdot 3^2 + 3^6 + 3^7 + 2\cdot 3^9 + \cdots$,

所以 $f(x)$ 在 $\mathbb{Q}_3$ 中的一个解是 $3^{-2}(2 + 2\cdot 3 + 2\cdot 3^2 + 3^6 + 3^7 + 2\cdot 3^9 + \cdots)$.

取有理数 $a = 3^{-2}(2 + 2\cdot 3 + 2\cdot 3^2)$ 即可。

10. 设 $f(x) = a_0 + a_1 x + \cdots a_n x^n \in \mathbb{Z}[x]$, $a_0 a_n \neq 0$. 记 $\alpha_1, \cdots, \alpha_n$ 是 $f(x)$ 的 n 个根（计重数），证明对任意 $S \subset \{1, 2, \cdots, n\}$,

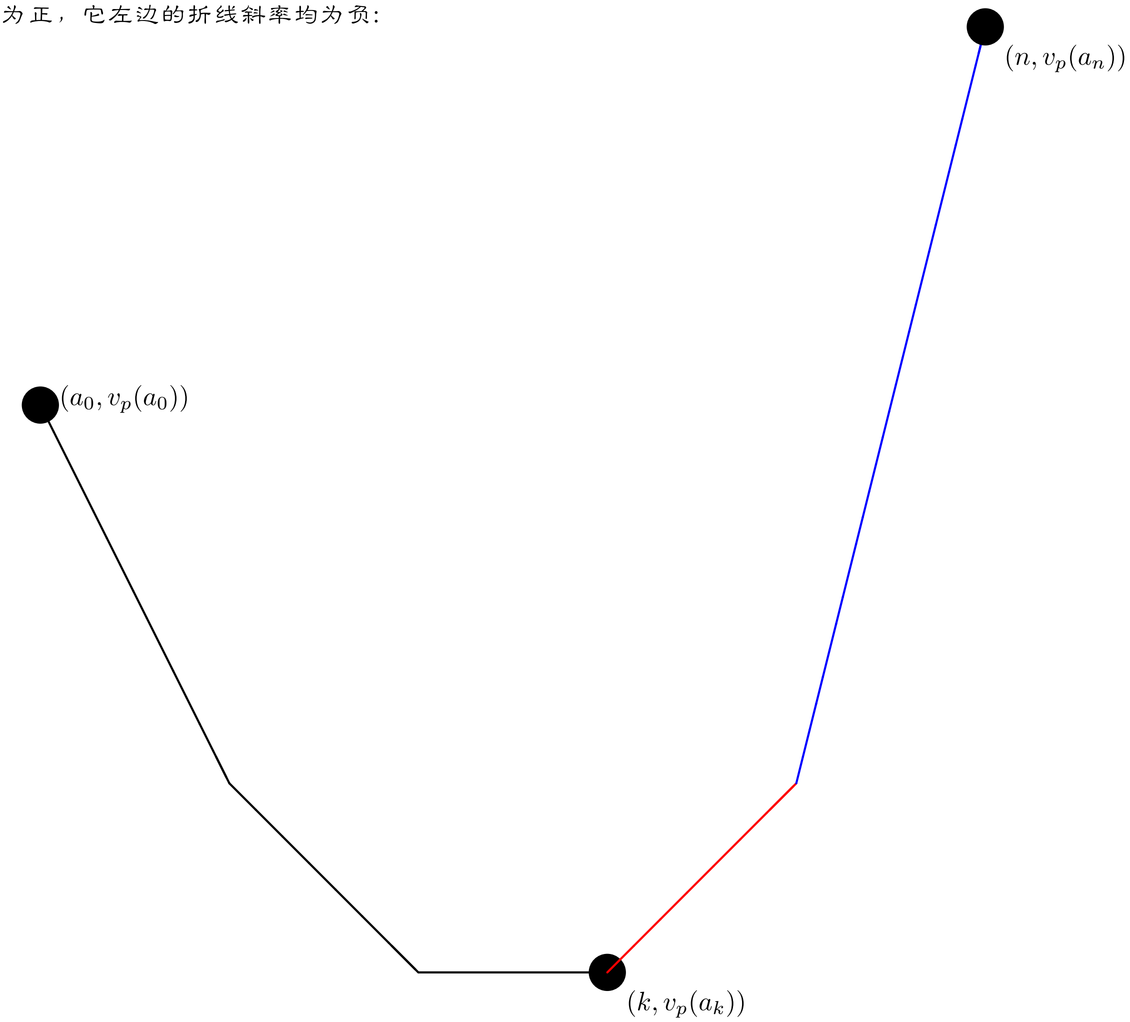
$$a_n \prod_{k\in S} \alpha_k \text{ 是代数整数.}$$

证明. 设 F 为 $f(x)$ 的分裂域，则 $a_n\prod_{k\in S}\alpha_k$ 是代数整数 当且仅当对任意的 $\mathcal{O}_F$ 非零素理想 $\mathfrak{p}$ 有 $v_{\mathfrak{p}}(a_n\prod_{k\in S}\alpha_k)\geq 0$.

而 p 之上的素理想与 $\mathrm{Hom}(F,\overline{\mathbb{Q}}_p)$ 存在一一对应，我们有 $v_{\mathfrak{p}}(a_n\prod_{k\in S}\alpha_k)\geq 0$ 当且仅当 $v_p(a_n\prod_{k\in S}\alpha_k)\geq 0$, 这里 v_p 是 $\overline{\mathbb{Q}}_p^\times\longrightarrow\mathbb{Q}$ 的加法（指数）赋值。

只需证明对任意的 p, $a_n\prod_{k\in S}\alpha_k$ 的 p 进加法（指数）赋值 ≥ 0.

考察 $f(x)\in\mathbb{Q}_p[x]$ 的牛顿曲线，不妨设它的牛顿折线图如下，以坐标 $(k,v_p(a_k))$ 为起点的折线斜率为正，它左边的折线斜率均为负:



设 $v_p(\alpha_1)\geq v_p(\alpha_2)\geq\cdots\geq 0>v_p(\alpha_{k+1})\geq\cdots\geq v_p(\alpha_n)$, 我们只需证明 $v_p(a_n\alpha_{k+1}\cdots\alpha_n)\geq 0$, 设

$$v_p(\alpha_{k+1})=\cdots=v_p(\alpha_t)>v_p(\alpha_{t+1})\geq\cdots>v_p(\alpha_{s+1})=\cdots=v_p(\alpha_n)$$

根据牛顿折线定理知

$$v_p(\alpha_{k+1})=\cdots=v_p(\alpha_t)=-\text{红色折线的斜率}=-\frac{v_p(a_t)-v_p(a_k)}{t-k}$$

$$\vdots$$

$$v_p(\alpha_{s+1})=\cdots=v_p(\alpha_n)=-\text{蓝色折线的斜率}=-\frac{v_p(a_n)-v_p(a_s)}{n-s}$$

所以 $v_p(a_n\alpha_{k+1}\cdots\alpha_n)=v_p(a_n)-(v_p(a_n)-v_p(a_s)+\cdots+v_p(a_t)-v_p(a_k))=v_p(a_k)\geq 0$. 得证。