arXiv:2302.03101v1 [math.NT] 6 Feb 2023

形如 $\mathcal{O}_K[\gamma]\cap K$ 的环中的稠密性问题。

DEEPESH SINGHAL、YUXIN LIN

摘要。我们固定一个数域 K，并研究环 $\mathcal{O}_K[\gamma]\cap K$ 的统计性质，其中 γ 遍历次数为固定值 $n\geq 2$ 的代数数。给定 $k\geq 1$，我们明确计算满足 $\mathcal{O}_K[\gamma]\cap K=\mathcal{O}_K[1/k]$ 的 γ 的密度，并证明该密度与数域 K 无关。特别地，我们证明满足 $\mathcal{O}_K[\gamma]\cap K=\mathcal{O}_K$ 的 γ 的密度为 $\zeta(n+1)\zeta(n)$。在一篇近期论文中，作者将 $X(K,\gamma)$ 定义为 Spec $(\mathcal{O}_K)$ 的某个有限子集，并证明 $X(K,\gamma)$ 决定了环 $\mathcal{O}_K[\gamma]\cap K$。我们证明，若 $\mathfrak{p}_1$、$\mathfrak{p}_2\in\in$ Spec $(\mathcal{O}_K)$ 满足 $\mathfrak{p}_1\cap\mathbb{Z}\neq\mathfrak{p}_2\cap\mathbb{Z}$，则事件 $\mathfrak{p}_1\in X(K,\gamma)$ 和 $\mathfrak{p}_2\in X(K,\gamma)$ 相互独立。作为 $t\to\infty$，我们研究满足 $|X(K,\gamma)|=t$ 的 γ 的密度的渐近性。

1. 引言

设 $\overline{\mathbb{Q}}$ 为 $\mathbb{Q}$ 的代数闭包，$\overline{\mathbb{Z}}$ 为代数整数环。对于 $\gamma\in\overline{\mathbb{Q}}$，我们将 γ 在 $\mathbb{Z}[x]$ 中的最小多项式记为 $F_\gamma(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0$。因此，$F_\gamma(x)$ 在 $\mathbb{Z}[x]$ 中不可约，$F_\gamma(\gamma)=0$，$a_n>0$，且 $\gcd(a_0,a_1,\ldots,a_n)=1$。我们还将 $\deg(\gamma)=n$ 记为 γ 的次数，并将其高度记为 $H(\gamma)=\max_{0\leq i\leq n}|a_i|$。我们按次数和高度对代数数排序。记

$$\mathcal{A}_n(H)=\{\gamma\in\overline{\mathbb{Q}}\mid \deg(\gamma)=n,\ H(\gamma)\leq H\}.$$

注意，对于任意 n, H，集合 $\mathcal{A}_n(H)$ 都是有限的。令 $\mathcal{A}_n=\bigcup_{H=1}^{\infty}\mathcal{A}_n(H)$。我们在 $\mathcal{A}_n$ 上定义概率分布 $\mathbb{P}_n$，使得给定性质 P

$$\mathbb{P}_n[P]=\lim_{H\to\infty}\frac{\#\{\gamma\in\mathcal{A}_n(H)\mid \gamma \text{ satisfies } P\}}{\#A_n(H)}.$$

以下结果由 van der Waerden [11] 证明。

定理 1.1 ([11])。对于任意 $n\geq 1$，我们有

$$\mathbb{P}_n\big[\textit{Galois closure of } \mathbb{Q}(\gamma) \textit{ has Galois group } S_n\big]=1.$$

我们证明，给定一个数域 K，$\mathbb{Q}(\gamma)$ 几乎总是与 K 的交集平凡。

定理 1.2。固定一个数域 K 和正整数 n，则有

$$\mathbb{P}_n[K\cap\mathbb{Q}(\gamma)=\mathbb{Q}]=1.$$

Drungilas、Dubickas 和 Jankauskas 在 [6], 中证明，环 $\mathbb{Z}[\gamma]\cap\mathbb{Q}$ 由量 $e(\gamma)=\gcd(a_1,a_2,\ldots,a_n)$ 确定。

T定理 1.3. [6, 定理 5] 给定一个代数数 $\gamma \in \overline{\mathbb{Q}}$，我们有

$$\mathbb{Z}[\gamma] \cap \mathbb{Q} = \{\alpha \in \mathbb{Q} \mid \textit{for all primes } p, \textit{ if } v_p(\alpha) < 0, \textit{ then } p \mid e(\gamma)\}.$$

推论1.3.1。给定 $\gamma \in \overline{\mathbb{Q}}$，我们有 $\mathbb{Z}[\gamma] \cap \mathbb{Q} = \mathbb{Z}$ 当且仅当 $e(\gamma) = 1$。

显然，所有代数整数都满足 $e(\gamma) = 1$。然而，即使 γ 不是代数整数，也可能有$e(\gamma) = 1$（例如 $\gamma = \frac{1}{2+i}$）。我们研究 $e(\gamma)$ 的分布，其中 γ 在次数为 n 的代数数中变化。

命题 1.4。给定 $n \geq 2$ 和 $k \geq 1$，我们有

$$\mathbb{P}_n[e(\gamma) = k] = \frac{\zeta(n+1)}{\zeta(n)} \frac{\phi(k)}{k^{n+1}}.$$

注意，对于 $n \geq 2$，我们有 $\frac{\zeta(n+1)}{\zeta(n)} \sum_{k=1}^{\infty} \frac{\phi(k)}{k^{n+1}} = 1$。对于数域 K，我们将 K 中的代数整数环记为 $\mathcal{O}_K$，并将 $\mathcal{O}_K$ 的非零素理想集合记为 Spec($\mathcal{O}_K$)。将 γ在 K 上的最小多项式记为 f_K，$\gamma(x) = b_n x^n + \cdots + b_0 \in K[x]$。因此，$f_K$，$\gamma(x)$在 $K[x]$中不可约，f_K，$\gamma(\gamma) = 0$ 和 $b_n = 1$。Singhal和Lin在[10] 中研究形如 $\mathcal{O}_K[\gamma] \cap K$的环。为此，他们定义了某些有限的素理想集合 $X(K, \gamma) \subseteq$ Spec($\mathcal{O}_K$)。

定理 1.5. [10, 定理 1.3] 给定一个数环 $\mathcal{O}_K$、一个代数数 γ和一个素数 $\mathfrak{p} \in$ 谱($\mathcal{O}_K$)，以下条件等价：

- 对于每个 $i \in [1, n]$: $v_{\mathfrak{p}}(b_i) > v_{\mathfrak{p}}(b_0)$。
- $\exists \alpha \in \mathfrak{p}$：$\frac{1}{\alpha} \in \mathcal{O}_K[\gamma]$。
- 对于每个 $\mathfrak{q} \in$ 谱($\mathcal{O}_{K[\gamma]}$)：若 $\mathfrak{q} \cap \mathcal{O}_K = \mathfrak{p}$，则 $v_{\mathfrak{q}}(\gamma) < 0$。

Singhal和Lin [10] 将 $X(K, \gamma)$ 定义为谱($\mathcal{O}_K$)中满足定理 1.5 任一等价条件的素理想集合。他们还指出，

$$X(\mathbb{Q}, \gamma) = \{p \in \mathrm{Spec}(\mathbb{Z}) \mid p \mid e(\gamma)\}.$$

他们如下刻画环 $\mathcal{O}_K[\gamma] \cap K$ 与 $X(K, \gamma)$ 的关系，从而推广了定理 1.3。

定理 1.6. [10, 命题 1。6] 对于 $\alpha \in K$，我们有 $\alpha \in \mathcal{O}_K[\gamma]$ 当且仅当

$$\{\mathfrak{p} \in \textit{Spec}(\mathcal{O}_K) \mid v_{\mathfrak{p}}(\alpha) < 0\} \subseteq X(K, \gamma).$$

如果对于任意满足 $\mathfrak{p} \cap \mathbb{Z} = \mathfrak{p}' \cap \mathbb{Z}$ 的 $\mathfrak{p}$、$\mathfrak{p}' \in \mathcal{O}_K$，$\mathfrak{p}$、$\mathfrak{p}' \in X$ 要么同时属于 X，要么都不属于 X，我们就称子集 $X \subseteq$ Spec($\mathcal{O}_K$) 稳定。例如，如果 $K = \mathbb{Q}[i]$ 且 $\gamma = \frac{1}{2+i}$，那么 $X(K, \gamma) = \{(2+i)\}$，它并不稳定。

命题 1.7。给定数域 K 和整数 $n \geq 2$，我们有

$$\mathbb{P}_n[X(K, \gamma) \textit{ is stable }] = 1.$$

我们定义常数 $\alpha_{p,\ n}=\frac{1-\frac{1}{p^n}}{1-\frac{1}{p^{n+1}}}$和 $\beta_{p,\ n}=\frac{1}{p^n}\frac{1-\frac{1}{p}}{1-\frac{1}{p^n}}$。需要注意的是$0<\alpha_{p,\ n},\beta_{p,\ n}<1$, $\alpha_{p,\ n}(1+\beta_{p,\ n})=1$和 $\zeta_{(n+1)\zeta(n)}=\prod_p\alpha_{p,\ n}$。对于给定的数域 K和有限稳定子集 $X\subseteq$谱$(\mathcal{O}_K)$，我们计算 $X(K,\gamma)=X$的概率。

命题 1.8。给定 $n\geq 2$、数域 K 和有限稳定子集 $X\subseteq$谱$(\mathcal{O}_K)$。令 $X_1=\{\mathfrak{p}\cap\mathbb{Z}\mid\mathfrak{p}\in X\}$，则我们有

$$\mathbb{P}_n\big[X(K,\gamma)=X\big]=\frac{\zeta(n+1)}{\zeta(n)}\prod_{p\in X_1}\beta_{p,n}.$$

我们还研究环 $\mathcal{O}_K[\gamma]\cap K$ 的分布。注意，如果 k_1 和 k_2 是具有相同素因子的正整数，那么 $\mathcal{O}_K[\frac{1}{k_1}]=\mathcal{O}_K[\frac{1}{k_2}]$。

定理 1.9。给定数域 K 和正整数 $n\geq 2$、$k\geq 1$，我们有 ve

$$\mathbb{P}_n\Big[\mathcal{O}_K[\gamma]\cap K=\mathcal{O}_K\Big[\frac{1}{k}\Big]\Big]=\frac{\zeta(n+1)}{\zeta(n)}\prod_{p|k}\beta_{p,n}.$$

需要注意的是，概率不依赖于数域 K。

推论 1.9.1。给定数域 K 和 $n\geq 2$，我们有

$$\mathbb{P}_n\big[\mathcal{O}_K[\gamma]\cap K=\mathcal{O}_K\big]=\frac{\zeta(n+1)}{\zeta(n)}.$$

接下来，我们证明，给定有理素数 p，$\mathcal{O}_K$中所有位于 p 之上的素数属于 $X(K,\gamma)$ 的概率为 $\alpha_{p.n}\beta_{p,\ n}$。此外，对于互不相同的有理素数，这些事件彼此独立。

命题 1.10。给定数域 K、有限子集 $X\subseteq$ 谱$(\mathcal{O}_K)$ 和 $n\geq 2$。设 $Y=\{\mathfrak{p}\cap\mathbb{Z}\mid\mathfrak{p}\in X\}$。那么

$$\mathbb{P}_n[X\subseteq X(K,\gamma)]=\prod_{p\in Y}\alpha_{p,n}\beta_{p,n}.$$

对于数域 K 和有理素数 p，我们将 $\mathcal{O}_K$中位于 p之上的素数个数记为 $r_K(p)$。我们研究集合 $X(K,\gamma)$ 的大小统计。

命题 1.11。给定数域 K 和 $n\geq 2$，我们有

$$\mathbb{E}_n[|X(K,\gamma)|]=\sum_p\alpha_{p,n}\beta_{p,n}r_K(p),\quad Var_n\ [|X(K,\gamma)|]=\sum_p\alpha_{p,n}\beta_{p,n}(1-\alpha_{p,n}\beta_{p,n})r_K(p)^2.$$

定理 1.12. 设 K 和 $n\geq 2$ 为数域，令 $\mu=\lfloor\frac{d}{n}\rfloor$。给定 $\epsilon>0$，对于充分大的 t，我们有

$$t^{-(1+\epsilon)nt}<\mathbb{P}_n[|X(K,\gamma)|=t]<t^{-\frac{1}{\mu+1+\epsilon}t}.$$

Singhal和Lin [10] 证明， $\mathcal{O}_K[\gamma] \cap K$ 的类群由 $\mathrm{Cl}(\mathcal{O}_K)$ 中由 $[\mathfrak{p}]$ 生成的子群决定，其中 $\mathfrak{p} \in X(K,\gamma)$ 如下。

命题 1.13. [10, 命题 1.7] 若 K 是一个数域且 $\gamma \in \overline{\mathbb{Q}}$，则 $\mathcal{O}_K[\gamma] \cap K$ 是一个戴德金整环，其类群为

$$Cl(\mathcal{O}_K[\gamma] \cap K) \cong Cl(\mathcal{O}_K)/\langle [\mathfrak{p}] \mid \mathfrak{p} \in X(K,\gamma)\rangle.$$

我们研究虚二次域 K 中 $\mathrm{Cl}(\mathcal{O}_K)$ 的子群 $\left\langle [\mathfrak{p}], \mathfrak{p} \in X(K,\gamma)\right\rangle$。

定理 1.14. 设 G 是一个非 2-挠有限阿贝尔群（特别地， G 非平凡）。固定 $n \geq 2$。对于每个虚二次域 K，将其判别式记为 d_K。则有

$$\lim_{d_K \to -\infty} \mathbb{P}_n\left[\left\langle [\mathfrak{p}], \mathfrak{p} \in X(K,\gamma)\right\rangle \cong G\right] = 0.$$

记 $\mathcal{A}'_m(H) = \{\alpha \in \overline{\mathbb{Z}} \mid \deg(\alpha) = m, H(\alpha) \leq H\}$。对于每个 $\alpha \in \mathcal{A}'_m(H)$， p 在 $\mathcal{O}_{\mathbb{Q}(\alpha)}$ 中分裂为 $r_{\mathbb{Q}(\alpha)}(p)$ 个素数，其中 $1 \leq r_{\mathbb{Q}(\alpha)} \leq m$。给定 $i \in [1,m]$，我们考虑这样一个问题：当我们遍历 $\alpha \in \mathcal{A}'_m(H)$ 时， $r_{\mathbb{Q}(\alpha)} = i$ 出现的频率如何。记

$$g(m,i,p) = \lim_{H\to\infty} \frac{\#\{\alpha \in \mathcal{A}'_m(H) \mid r_{\mathbb{Q}(\alpha)}(p) = i\}}{\#\mathcal{A}'_m(H)}.$$

此外，记 $g(m,i)$ 为 $=\lim_{p\to\infty} g(m,i,p)$。

定理 1.15。给定 m 和 i，使得 $1 \leq i \leq m$, $g(m, i)$ 是 $\prod_{j=0}^{m-1} (y+j)m!$ 中 y^i 的系数。

本文组织如下。第 2 节中，我们证明命题 1.4，以及当 $K = \mathbb{Q}$ 时命题 1.8、定理 1.9 和命题 1.10 的特殊情形。第 3 节中，我们证明定理 1.2。第 4 节中，我们利用前两节的结果证明命题 1.7，并完成命题 1.8、定理 1.9 和命题 1.10 的证明。第 5 节中，我们研究 $X(K,\gamma)$ 的大小统计，并证明命题 1.11 和定理 1.12。第 6 节中，我们研究虚二次域 K 中由 $X(K,\gamma)$ 生成的类群子群，并证明定理 1.14。最后，第 7 节中，我们证明定理 1.15。

2. Base ring $\mathbb{Z}$.

记

$$\mathcal{L}_n(H) = \{A(x) \in \mathbb{Z}[x] \mid \deg(A(x)) = n, H(A(x)) \leq H, A(x) \text{ is irreducible in } \mathbb{Z}[x]\}.$$

波利亚和塞格在 [9] 中证明

$$\#\mathcal{L}_n(H) = \frac{(2H)^{n+1}}{\zeta(n+1)} + O_n(H^n \log^2(H)).$$

记号 O_n 表示隐含常数仅取决于 n。显然，$\#\mathcal{A}_n(H)=\frac{n}{2}\mathcal{L}_n(H)$。因此

$$\#\mathcal{A}_n(H)=\frac{n}{2}\frac{(2H)^{n+1}}{\zeta(n+1)}+O_n(H^n\log^2(H)).$$

引理 2.1。给定 $n\geq 2$ 和一个子集 $Y\subseteq\mathbb{N}_{>0}$，我们有

$$\#\{\gamma\in\mathcal{A}_n(H)\mid e(\gamma)\in Y\}=\frac{n}{2}\frac{(2H)^{n+1}}{\zeta(n)}\sum_{k\in Y}\sum_{k\leq H}\frac{\phi(k)}{k^{n+1}}+O_n\left(H^n\log^2(H)\right).$$

证明。记

$$\mathcal{C}_n(H)=\{(c_1,\dots,c_n)\in\mathbb{Z}^n\mid \gcd(c_1,\dots,c_n)=1,|c_i|\leq H\}.$$

Nymann 在 [8] 中证明，对于 $n\geq 2$,

$$\#\mathcal{C}_n(H)=\frac{(2H)^n}{\zeta(n)}+O_n(H^{n-1}\log(H)).$$

记

$$\mathcal{C}_n(k,H)=\{c_0+\cdots+c_nx^n\in\mathbb{Z}[x]\mid \gcd(c_0,c_1,\dots,c_n)=1,\gcd(c_1,\dots,c_n)=k,|c_i|\leq H\}.$$

我们看到

$$\begin{aligned}\#\mathcal{C}_n(k,H)&=\#\{c_0\in[-H,H]\mid\gcd(c_0,k)=1\}\#\mathcal{C}_n\left(\frac{H}{k}\right)\\&=\left(\frac{\phi(k)}{k}2H+O(k)\right)\left(\frac{(2H)^n}{k^n\zeta(n)}+O_n\left(\frac{H^{n-1}}{k^{n-1}}\log(H)\right)\right)\\&=\frac{\phi(k)}{k^{n+1}}\frac{(2H)^{n+1}}{\zeta(n)}+O_n\left(\frac{H^n}{k^{n-1}}\log(H)+\frac{H^{n-1}}{k^{n-2}}\log(H)\right).\end{aligned}$$

接下来，我们有

$$\begin{aligned}\#\{\gamma\in\mathcal{A}_n(H)\mid e(\gamma)\in Y\}&=\sum_{k\in Y}\frac{n}{2}\#\left(\mathcal{C}_n(k,H)\cap\mathcal{L}_n(H)\right)\\&=\frac{n}{2}\sum_{k\in Y}\#\mathcal{C}_n(k,H)-\frac{n}{2}\#\left(\left(\bigcup_{k\in Y}\mathcal{C}_n(k,H)\right)\setminus\mathcal{L}_n(H)\right).\end{aligned}$$

接下来，

$$\begin{aligned}\#\left(\left(\bigcup_{k\in Y}\mathcal{C}_n(k,H)\right)\setminus\mathcal{L}_n(H)\right)&\leq\#\mathcal{C}_{n+1}(H)-\#\mathcal{L}_n(H)\\&=\frac{(2H)^{n+1}}{\zeta(n+1)}+O_n(H^n)-\frac{(2H)^{n+1}}{\zeta(n+1)}-O_n(H^n\log^2(H))\\&=O_n\left(H^n\log^2(H)\right).\end{aligned}$$

最后，注意，如果 $k > H$，那么 $C_n(k, H) = \emptyset$。因此，我们有

$$\begin{aligned}
&\#\{\gamma \in \mathcal{A}_n(H) \mid e(\gamma) \in Y\} = \frac{n}{2}\frac{(2H)^{n+1}}{\zeta(n)} \sum_{k\in Y\ k\le H} \frac{\phi(k)}{k^{n+1}} \\
&+ O_n\Big(H^n \log^2(H) + H^n \log(H) \sum_{k\in Y\ k\le H} \frac{1}{k^{n-1}} + H^{n-1}\log(H) \sum_{k\in Y\ k\le H} \frac{1}{k^{n-2}}\Big) \\
&= \frac{n}{2}\frac{(2H)^{n+1}}{\zeta(n)} \sum_{k\in Y\ k\le H} \frac{\phi(k)}{k^{n+1}} + O_n\left(H^n \log^2(H)\right). \qquad \square
\end{aligned}$$

推论 2.1.1。 给定 $n \ge 2$ 和一个子集 $Y \subseteq \mathbb{N}_{>0}$，我们有

$$\mathbb{P}_n[e(\gamma) \in Y] = \frac{\zeta(n+1)}{\zeta(n)} \sum_{k\in Y} \frac{\phi(k)}{k^{n+1}}.$$

证明。

$$\begin{aligned}
\mathbb{P}_n\left[e(\gamma) \in Y\right] &= \lim_{H\to\infty} \frac{\#\left\{\gamma \in \mathcal{A}_n(H) \mid e(\gamma) \in Y\right\}}{\#\mathcal{A}_n(H)} \\
&= \lim_{H\to\infty} \frac{\frac{n}{2}\frac{(2H)^{n+1}}{\zeta(n)} \sum_{k\in Y\ k\le H} \frac{\phi(k)}{k^{n+1}} + O_n\left(H^n \log^2(H)\right)}{\frac{n}{2}\frac{(2H)^{n+1}}{\zeta(n+1)} + O_n(H^n \log^2(H))} \\
&= \frac{\zeta(n+1)}{\zeta(n)} \lim_{H\to\infty} \sum_{k\in Y\ k\le H} \frac{\phi(k)}{k^{n+1}} = \frac{\zeta(n+1)}{\zeta(n)} \sum_{k\in Y} \frac{\phi(k)}{k^{n+1}}. \qquad \square
\end{aligned}$$

命题 1.4。 给定 $n \ge 2$ 和 $k \ge 1$,

$$\mathbb{P}_n[e(\gamma) = k] = \frac{\zeta(n+1)}{\zeta(n)} \frac{\phi(k)}{k^{n+1}}.$$

证明。 这由推论 2.1.1 得出。 $\square$

令 $\mathcal{P}_{\text{fin}}$(谱(ℤ)) 为谱(ℤ) 的所有有限子集构成的集合。

引理 2.2. 给定 $n \ge 2$ 和 $\mathcal{X} \subseteq \mathcal{P}_{fin}$(谱(ℤ))，我们有

$$\mathbb{P}_n[X(\mathbb{Q}, \gamma) \in \mathcal{X}] = \frac{\zeta(n+1)}{\zeta(n)} \sum_{X\in\mathcal{X}} \prod_{p\in X} \beta_{p,n}.$$

证明。设 $Y = \{k \in \mathbb{Z}_{>0} \mid \{p \mid p \mid k\} \in \mathcal{X}\}$。由于 $X(\mathbb{Q}, \gamma) = \{p \mid p \mid e(\gamma)\}$，我们知道 $X(\mathbb{Q}, \gamma) \in \mathcal{X}$ 当且仅当 $e(\gamma) \in Y$。因此，

$$\begin{aligned}\mathbb{P}_n[X(\mathbb{Q}, \gamma) \in \mathcal{X}] = \mathbb{P}_n[e(\gamma) \in Y] &= \frac{\zeta(n+1)}{\zeta(n)} \sum_{k \in Y} \frac{\phi(k)}{k^{n+1}} \\ &= \frac{\zeta(n+1)}{\zeta(n)} \sum_{X \in \mathcal{X}} \sum_{\substack{k \geq 1 \\ \{p \mid p \mid k\} = X}} \frac{\phi(k)}{k^{n+1}} = \frac{\zeta(n+1)}{\zeta(n)} \sum_{X \in \mathcal{X}} \prod_{p \in X} \left(\sum_{t=1}^{\infty} \frac{\phi(p^t)}{p^{t(n+1)}} \right) \\ &= \frac{\zeta(n+1)}{\zeta(n)} \sum_{X \in \mathcal{X}} \prod_{p \in X} \beta_{p,n}. \end{aligned}$$

□

推论 2.2.1. 给定有限子集 $X \subseteq$ 谱$(\mathbb{Z})$ 和 $n \geq 2$，我们有 e

$$\mathbb{P}_n[X(\mathbb{Q}, \gamma) = X] = \frac{\zeta(n+1)}{\zeta(n)} \prod_{p \in X} \beta_{p,n}.$$

命题 2.3. 给定 $n \geq 2$ 和 $k \geq 1$，我们有

$$\mathbb{P}_n\left[\mathbb{Z}[\gamma] \cap \mathbb{Q} = \mathbb{Z}\left[\frac{1}{k}\right]\right] = \frac{\zeta(n+1)}{\zeta(n)} \prod_{p \mid k} \beta_{p,n}.$$

证明。令 $X = \{p \mid p \mid k\}$。现在，根据定理 1.3，我们知道 $\mathbb{Z}[\gamma] \cap \mathbb{Q} = \mathbb{Z}[\frac{1}{k}]$ 当且仅当 $X(\mathbb{Q}, \gamma) = X$。因此，根据推论 2.2.1，我们有

$$\mathbb{P}_n\left[\mathbb{Z}[\gamma] \cap \mathbb{Q} = \mathbb{Z}\left[\frac{1}{k}\right]\right] = \mathbb{P}_n\left[X(\mathbb{Q}, \gamma) = X\right] = \frac{\zeta(n+1)}{\zeta(n)} \prod_{p \mid k} \beta_{p,n}.$$

□

命题 2.4. 给定 $n \geq 2$ 和有限素数集 $X \subseteq$ 谱$(\mathbb{Z})$，我们有

$$\mathbb{P}_n[X \subseteq X(\mathbb{Q}, \gamma)] = \prod_{p \in X} \alpha_{p,n} \beta_{p,n}.$$

证明。令 $\mathcal{X} = \{Y \in \mathcal{P}_{\text{fin}}(\text{谱}(\mathbb{Z})) \mid X \subseteq Y\}$。因此，根据引理 2.2，我们有 e

$$\begin{aligned}\mathbb{P}_n[X \subseteq X(\mathbb{Q}, \gamma)] = \mathbb{P}_n[X(\mathbb{Q}, \gamma) \in \mathcal{X}] &= \frac{\zeta(n+1)}{\zeta(n)} \sum_{Y \in \mathcal{X}} \prod_{p \in Y} \beta_{p,n} \\ &= \frac{\zeta(n+1)}{\zeta(n)} \prod_{p \in X} \beta_{p,n} \prod_{p \notin X} (1 + \beta_{p,n}) \\ &= \prod_{p} \alpha_{p,n} \prod_{p \in X} \beta_{p,n} \prod_{p \notin X} \alpha_{p,n}^{-1} = \prod_{p \in X} \alpha_{p,n} \beta_{p,n}. \end{aligned}$$

□

P命题 2.5。 给定 $n \geq 2$ 以及一个素数集合 $X \subseteq$ 谱$(\mathbb{Z})$，我们有

$$\mathbb{P}_n[X(\mathbb{Q}, \gamma) \subseteq X] = \prod_{p \notin X} \alpha_{p,n}.$$

证明。 令 $\mathcal{X} = \{Y \in \mathcal{P}_{\text{fin}}(\text{Spec}(\mathbb{Z})) \mid Y \subseteq X\}$。因此，由引理 2.2 可得

$$\begin{aligned}\mathbb{P}_n[X(\mathbb{Q}, \gamma) \subseteq X] = \mathbb{P}_n[X(\mathbb{Q}, \gamma) \in \mathcal{X}] &= \frac{\zeta(n+1)}{\zeta(n)} \sum_{Y \in \mathcal{X}} \prod_{p \in Y} \beta_{p,n} \\ &= \frac{\zeta(n+1)}{\zeta(n)} \prod_{p \in X} (1 + \beta_{p,n}) = \prod_{p} \alpha_{p,n} \prod_{p \in X} \alpha_{p,n}^{-1} = \prod_{p \notin X} \alpha_{p,n}^{-1}. \qquad \square\end{aligned}$$

3. 概率伽罗瓦理论

本节将证明定理 1.2。众所周知，对于 $n \neq 4$， S_n 的正规子群只有 $\{id\}$、 A_n 和 S_n。由此很容易看出，对于任意 $n \geq 1$ 和 $2 < k < n$， S_n 没有指数为 k的子群。此外， A_n 是 S_n 中唯一指数为 2 的子群。

引理 3.1。 给定一个数域 K 和整数 $n \geq [K : \mathbb{Q}] + 1$，可得

$$\mathbb{P}_n[K \cap \mathbb{Q}(\gamma) = \mathbb{Q}] = 1.$$

证明。 考虑 $\gamma \in \mathcal{A}_n$，使得 $\mathbb{Q}(\gamma)$的伽罗瓦闭包的伽罗瓦群为 S_n。令γ_2、.....、 γ_n为 γ在 $\mathbb{Q}$上的共轭元，则 $L = \mathbb{Q}(\gamma, \gamma_2, \ldots\ldots, \gamma_n)$是 $\mathbb{Q}(\gamma)$的伽罗瓦闭包。令 H为 L 在 $K \cap \mathbb{Q}(\gamma)$上的伽罗瓦群，则 $H \subseteq S_n$。 现在， $K \cap \mathbb{Q}(\gamma) \subseteq \mathbb{Q}(\gamma)$，因此 $S_{n-1} \subseteq H$。这意味着 H 的指数至多为 n。因此，H的指数属于 $\{1, 2, n\}$。

- 若 H 的指数为 n，则 $H = S_{n-1}$，因此 $K \cap \mathbb{Q}(\gamma) = \mathbb{Q}(\gamma)$。这意味着$Q(\gamma) \subseteq K$。但这是不可能的，因为 $[\mathbb{Q}(\gamma) : \mathbb{Q}] = n > [K : \mathbb{Q}]$。
- 若 H 的指数为 2，则 $H = A_n$，但这是不可能的，因为 $S_{n-1} \subseteq H$ 和$S_{n-1} \nsubseteq A_n$。

因此， H 的指数为 1，这意味着 $H = S_n$ 和 $K \cap \mathbb{Q}[\gamma] = \mathbb{Q}$。现在，我们有

$$1 \geq \mathbb{P}_n[K \cap \mathbb{Q}(\gamma) = \mathbb{Q}] \geq \mathbb{P}_n\big[\text{Galois closure of } \mathbb{Q}(\gamma) \text{ has Galois group } S_n\big] = 1. \quad \square$$

我们已经证明了 $[K$ 时定理 1.2 的特殊情形： $\mathbb{Q}] < n$。为了完成定理 1.2 的证明，我们还需要以下引理。

引理 3。 **2.** 给定 $n \geq 2$ 和一个无平方因子整数 m （m 可以为负），我们有

$$\mathbb{P}_n[\exists y \in \mathbb{Z} : Disc(F_\gamma) = my^2] = 0.$$

我们将使用 [3] 和 [4] 中的以下结果来证明引理 3.2。

引理 3.3 ([3])。 给定 $\epsilon > 0$ 和 $d \in \mathbb{N}_{\geq 1}$，存在一个常数 $c(d, \epsilon)$，使得如果 F是边长为H的正方形内一条次数为 d 的不可约平面代数曲线的子集，那么 F上的格点数被 $c(d, \epsilon)H^{\frac{1}{d}+\epsilon}$所界定。

引理 3.4 ([4])。 设 $f(X, t_1, \ldots, t_s) \in \mathbb{Z}[X, t_1, \ldots, t_s]$ 是一个不可约多项式。那么

$$\begin{aligned}&\#\big\{(\alpha_1, \ldots, \alpha_s) \in \mathbb{Z}^s \mid |\alpha_i| \leq H, f(X, \alpha_1, \ldots, \alpha_s) \text{ is not irreducible in } \mathbb{Z}[X]\big\}\\ &= O(H^{s-\frac{1}{2}} \log(H)).\end{aligned}$$

设 A_0、A_1、…、A_n 是不定元，且 $f(x) = A_0x^n + A_1x^{n-1} + \cdots + A_n$。众所周知，$\mathrm{Disc}(f)(A_0, A_1, \ldots, A_n)$ 是一个关于 $\mathbb{Z}[A_0, \ldots, A_n]$的次数为 $2n-2$ 的不可约齐次多项式。

引理 3.5。 将 $Disc(f)(A_0, \ldots, A_n)$ 表示为关于$A_0, \ldots, A_n$的单项式的线性组合。考虑 $t_0, \ldots, t_{n-2}, t_n \in \mathbb{Z}_{\geq 0}$，其中 $t_0 + \cdots + t_{n-2} + t_n = n - 2$。如果$t_0 \neq n-2$，则 $A_0^{t_0} \ldots A_{n-2}^{t_{n-2}} A_n^{t_n} A_{n-1}^n$的系数为零。此外，$A_{n-1}^n A_0^{n-2}$的系数为 $\pm(n-1)^{n-1}$。

证明。 众所周知，$\mathrm{Disc}(f)(A_0, \ldots, A_n)$ 可用西尔维斯特矩阵表示如下：

$$\mathrm{Disc}(f)(A_0, \ldots, A_n) = \frac{(-1)^{\frac{n(n-1)}{2}}}{A_n} \det(S(f(x), f'(x))).$$

西尔维斯特矩阵是一个 $2n-1 \times 2n-1$ 矩阵。其非零元素如下：

$$a_{ij} = \begin{cases} A_{n+i-j} & \text{if } 1 \leq i \leq n-1, i \leq j \leq i+n, \\ (i+1-j)A_{i+1-j} & \text{if } n \leq i \leq 2n-1, i-(n-1) \leq j \leq i. \end{cases}$$

下面写出 $n = 5$ 的西尔维斯特矩阵。

$$S(f(x), f'(x)) = \begin{bmatrix} A_5 & A_4 & A_3 & A_2 & A_1 & A_0 & 0 & 0 & 0 \\ 0 & A_5 & A_4 & A_3 & A_2 & A_1 & A_0 & 0 & 0 \\ 0 & 0 & A_5 & A_4 & A_3 & A_2 & A_1 & A_0 & 0 \\ 0 & 0 & 0 & A_5 & A_4 & A_3 & A_2 & A_1 & A_0 \\ 5A_5 & 4A_4 & 3A_3 & 2A_2 & 1A_1 & 0 & 0 & 0 & 0 \\ 0 & 5A_5 & 4A_4 & 3A_3 & 2A_2 & 1A_1 & 0 & 0 & 0 \\ 0 & 0 & 5A_5 & 4A_4 & 3A_3 & 2A_2 & 1A_1 & 0 & 0 \\ 0 & 0 & 0 & 5A_5 & 4A_4 & 3A_3 & 2A_2 & 1A_1 & 0 \\ 0 & 0 & 0 & 0 & 5A_5 & 4A_4 & 3A_3 & 2A_2 & 1A_1 \end{bmatrix}.$$

注意，矩阵上半部分有 $n-1$ 行，下半部分有 n 行。我们要计算这个行列式中 $A_0^{t_0} \ldots A_{n-2}^{t_{n-2}} A_n^{1+t_n} A_{n-1}^n$ 的系数。展开行列式时，每次选取 $2n-1$ 个元素，使得每行和每列都恰好选到一个元素。在第 2 列到 $n+1$ 列中有 A_{n-1}，而在

没有其他列。因此，为了得到 $A_0^{t_0}\dots A_{n-2}^{t_{n-2}}A_n^{1+t_n}A_{n-1}^n$，我们必须为每个 $2\le j\le n+1$ 在第 j^{th} 列中选取一个 A_{n-1}。

我们声称，为了得到 $A_0^{t_0}\dots A_{n-2}^{t_{n-2}}A_n^{1+t_n}A_{n-1}^n$，对于 $[3,n+1]$ 中的每个 j，在 j^{th} 列中必须选取矩阵下半部分的 $(n-1)A_{n-1}$；对于 $[3,n]$ 中的每个 j，在 $(j+n-1)^{th}$ 列中必须选取矩阵上半部分的 A_0。我们对 j 使用反向归纳法证明这一点。对于 $j=n+1$，注意到 $(n+1)^{th}$ 列中只有一个 A_{n-1}，即 $a_{2n-1,\ n+1}=(n-1)A_{n-1}$。因此，在 $(n+1)^{th}$ 列中，我们必须选取下半部分的 A_{n-1}。

接下来，假设归纳假设成立：对于某个 $j\in[3,n]$，我们知道对于每个 $k\in[j+1,n+1]$，在 k^{th} 列中必须选取矩阵下半部分的 A_{n-1}；对于每个 $k\in[j+1,n]$，在 $(k+n-1)^{th}$ 列中必须选取矩阵上半部分的 A_0。现在，$(j+n-1)^{th}$ 列中的非零项为 $a_{t,\ j+n-1}$，对应于 $j-1\le t\le n-1$ 和 $j+n-1\le t\le 2n-1$。然而，对于 $j\le t\le n-1$，我们已经选取了 $a_{t,t+1+(n-1)}=A_0$。对于 $j+n-1\le t\le 2n-1$，我们已经选取了 $a_{t,\ t+2-n}=(n-1)A_{n-1}$。因此，在 $(j+n-1)^{th}$ 列中，我们必须选取 $a_{j-1,j+n-1}=A_0$（它位于上半部分）。接下来，在 j^{th} 列中有两个 A_{n-1}：$a_{j-1,j}$, $a_{n+j-2,j}$。然而，我们已经选取了 $A_0=a_{j-1,j+n-1}$。因此，我们必须选取 $a_{n+j-2,j}=(n-1)A_{n-1}$（它位于下半部分）。这就完成了归纳步骤。

我们已经证明，对于 $3\le j\le n+1$，必须选择 $a_{n+2-j,\ j}=(n-1)A_{n-1}$；对于 $3\le j\le n$，则必须选择 $a_{j-1,\ j-1+n}=A_0$。这意味着第 3 列到第 $2n-1$ 列的贡献为 $(n-1)^{n-1}A_0^{n-2}A_{n-1}^{n-1}$。现在剩下第 1、2 列和第 1、$n$ 行。各项为 $a_{1,\ 1}=A_n$、$a_{1,\ 2}=A_{n-1}$、$a_{n,\ 1}=nA_n$ 和 $a_{n,\ 2}=(n-1)A_{n-1}$。这里的贡献为 $-A_nA_{n-1}$。

因此，若 $t_0\neq n-2$，则该行列式中 $A_0^{t_0}\dots A_{n-2}^{t_{n-2}}A_n^{1+t_n}A_{n-1}^n$ 的系数为 0。而 $A_0^{n-2}A_n^1A_{n-1}^n$ 的系数为 $-(n-1)^{n-1}$。结论由此得出。□

引理 *3.2* 的证明。我们知道，$\mathrm{Disc}(f)(A_0,\dots,A_n)$ 是次数为 $2n-2$ 的齐次多项式。因此，存在一个常数 C（仅取决于 n），使得对于所有满足 $|\alpha_i|\le H$ 的 $\alpha_0,\dots,\alpha_n\in\mathbb{Z}$，都有 $|\mathrm{Disc}(f)(\alpha_0,\dots,\alpha_n)|\le CH^{2n-2}$。因此，若 $\gamma\in A_n(H)$ 且 $\mathrm{Disc}(F_\gamma)=my^2$，则 $|y|\le\sqrt{C}H^{n-1}$。

令 $d=\deg_{A_{n-1}}(\mathrm{Disc}(f))$。由引理 3.5 可知 $d\ge n$。令 $I(\mathbb{Z}[A_{n-1}])$ 为 $\mathbb{Z}[A_{n-1}]$ 中不可约多项式的集合。由引理 3.4 可知

$$\begin{aligned}&\#\big\{(\alpha_1,\dots,\alpha_n)\in\mathbb{Z}^n\mid|\alpha_i|\le H,\mathrm{Disc}(f)(\alpha_1,\dots,\alpha_{n-1},A_{n-1},\alpha_n)\notin I(\mathbb{Z}[A_{n-1}])\big\}\\&\quad=O(H^{n-\frac{1}{2}}\log(H)).\end{aligned}$$

给定 $(\alpha_1,\dots,\alpha_n)\in[-H,H]^n$ 使得 $\mathrm{Disc}(f)(\alpha_1,\dots,\alpha_{n-1},A_{n-1},\alpha_n)\in I(\mathbb{Z}[A_{n-1}])$，我们看到 $my^2-\mathrm{Disc}(f)(\alpha_1,\dots,\alpha_{n-1},A_{n-1},\alpha_n)$ 是关于变量 y,A_{n-1} 的不可约曲线。取 $0<\epsilon<\frac{1}{2n(n-1)}$。满足 $\overline{|\alpha|}\le H$ 的 $\alpha\in\mathbb{Z}$ 的数量，使得

$\text{Disc}(f)(\alpha_1, \ldots, \alpha_{n-1}, \alpha, \alpha_n) = my^2$ 有解（对于 y）的数量至多等于满足 $|A_{n-1}|$, $|y| \leq \sqrt{C}H^{n-1}$ 的 $\text{Disc}(f)(\alpha_1, \ldots, \alpha_{n-1}, A_{n-1}, \alpha_n)$ 的解的数量。根据引理 3.3，这至多为

$$c(d,\epsilon)\left(\sqrt{C}H^{n-1}\right)^{\frac{1}{d}+\epsilon} = O(H^{\frac{n-1}{d}+\epsilon(n-1)}) = O(H^{1-\frac{1}{2n}}).$$

Now,

$$\begin{aligned}
&\#\{\gamma \in A_n(H) \mid \exists y \in \mathbb{Z}: \text{判别式}(F_\gamma(x)) = my^2\} \\
&\leq n\#\{g(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x] \mid |a_i| \leq H, \ \exists y \in \mathbb{Z}: \text{判别式}(g(x)) = my^2\} \leq n\#\{(\alpha_1, \ldots, \\
&\alpha_n) \in \mathbb{Z}^n \mid |\alpha_i| \leq H, \text{判别式}(f)(\alpha_1, \ldots, \alpha_{n-1}, A_{n-1}, \alpha_n) \notin I(\mathbb{Z}[A_{n-1}])\}(2H+1) \\
&+ n \sum_{\in \mathbb{Z}^n \mid \alpha_i \mid \leq H} \#\{\alpha \in \mathbb{Z} \mid |\alpha| \leq H, \exists y \in \mathbb{Z}: \text{判别式}(f)(\alpha_1, \ldots, \alpha_{n-1}, \alpha, \alpha_n) = my^2\}_{(\alpha_1,\ldots,\alpha_n)} \\
&\text{判别式}(f)(\alpha_1,\ldots,A_{n-1},\alpha_n)\in I(\mathbb{Z}[A_{n-1}]) \leq nO\left(H^{n-\frac{1}{2}}\text{对数}(H)\right)(2H+1) + n(2H+1)^n O(H^{1-\frac{1}{2n}}) \\
&= O(H^{n+1-\frac{1}{2n}})。
\end{aligned}$$

因此,

$$\begin{aligned}
\mathbb{P}_n[\exists y \in \mathbb{Z} : \text{Disc}(F_\gamma) = my^2] &= \lim_{H\to\infty} \frac{\#\{\gamma \in A_n(H) \mid \exists y \in \mathbb{Z} : \text{Disc}(F_\gamma(x)) = my^2\}}{\#\mathcal{A}_n(H)} \\
&\leq \lim_{H\to\infty} \frac{O(H^{n+1-\frac{1}{2n}})}{\frac{n}{2}\frac{(2H)^{n+1}}{\zeta(n+1)} + O_n(nH^n \log^2(H))} = 0. \qquad \square
\end{aligned}$$

定理 1.2. 给定一个固定域 K 和正整数 n，我们有

$$\mathbb{P}_n[K \cap \mathbb{Q}(\gamma) = \mathbb{Q}] = 1.$$

证明. 固定 n。我们对 $[K$ 进行归纳: $\mathbb{Q}]$。基例 $[K: \mathbb{Q}] \leq n-1$ 由引理 3.1 给出。

现在考虑某个满足 $[K: \mathbb{Q}] \geq n$ 的 K。由归纳假设可知，对所有真子域 $K' \subsetneq K,$ ，都有 $\mathbb{P}_n[K' \cap \mathbb{Q}(\gamma) = \mathbb{Q}] = 1$。这意味着

$$\mathbb{P}_n[K \cap \mathbb{Q}(\gamma) = \mathbb{Q}] = 1 - \mathbb{P}_n[K \cap \mathbb{Q}(\gamma) = K].$$

注意，若 $K \cap \mathbb{Q}(\gamma) = K$，则 $K \subseteq \mathbb{Q}(\gamma)$。然而 $[\mathbb{Q}(\gamma): \mathbb{Q}] = n$ 且 $[K: \mathbb{Q}] \geq n$。这迫使 $K = \mathbb{Q}(\gamma)$。这意味着

$$\mathbb{P}_n[K \cap \mathbb{Q}(\gamma) = \mathbb{Q}] = 1 - \mathbb{P}_n[K = \mathbb{Q}(\gamma)].$$

现在，若 $[K: \mathbb{Q}] \geq n+1$，则 $\mathbb{P}_n[K = \mathbb{Q}(\gamma)] = 0$，结论得证。因此，设$[K: \mathbb{Q}] = n$。

• 情况 1： K 的伽罗瓦闭包的伽罗瓦群不是 S_n。由命题 1.1 可知，

$$\mathbb{P}_n\big[\text{Galois closure of } \mathbb{Q}(\gamma) \text{ has Galois group } S_n\big] = 1.$$

因此 $\mathbb{P}_n[K = \mathbb{Q}(\gamma)] = 0$。

• 情况 2： K 的伽罗瓦闭包确实具有 S_n 伽罗瓦群。设伽罗瓦闭包为 L。S_n 中指数为 2 的唯一子群是 A_n，因此 L 有唯一的二次子域 K_1。设 $K_1 = \mathbb{Q}(\sqrt{m})$，其中 $m \in \mathbb{Z}$ 为无平方因子。现在，若对于某个 $\gamma \in \mathcal{A}_n$ 有 $K = \mathbb{Q}(\gamma)$，则 $K_1 = \mathbb{Q}(\sqrt{\text{判别式}(F_\gamma)})$。因此

$$\mathbb{P}_n[K = \mathbb{Q}(\gamma)] \le \mathbb{P}_n[\exists y \in \mathbb{Z} : \mathrm{Disc}(F_\gamma) = my^2] = 0,$$

其中最后一步应用了引理 3.2。

在这两种情况下，我们都看到 $\mathbb{P}_n[K = \mathbb{Q}(\gamma)] = 0$，因此 $\mathbb{P}_n[K \cap \mathbb{Q}(\gamma) = \mathbb{Q}] = 1$。至此归纳步骤完成，因而证明也完成了。□

4. Base ring $\mathcal{O}_K$

本节将证明命题 1.7、命题 1.8、定理 1.9 和命题 1.10。我们将需要以下来自 [10] 的引理。

引理 4.1。 [10, 引理 3,1] 若 $K \subseteq L$ 是数域，则

$$X(K,\gamma) = \{\mathfrak{p} \in \text{谱}(\mathcal{O}_K) \mid \text{对每个 } \mathfrak{q} \in \text{谱}(\mathcal{O}_L), \text{ 若 } \mathfrak{q} \cap \mathcal{O}_K = \mathfrak{p} \text{ 则 } \mathfrak{q} \in X(L,\gamma)\},$$

$$X(L,\gamma) \supseteq \{\mathfrak{q} \in \mathit{Spec}(\mathcal{O}_L) \mid \mathfrak{q} \cap \mathcal{O}_K \in X(K,\gamma)\}.$$

此外，若 $L \cap K(\gamma) = K$，则有

$$X(L,\gamma) = \{\mathfrak{q} \in \mathit{Spec}(\mathcal{O}_L) \mid \mathfrak{q} \cap \mathcal{O}_K \in X(K,\gamma)\}.$$

命题 1.7。 给定一个数域 K 和整数 $n \ge 2$，有

$$\mathbb{P}_n[X(K,\gamma) \text{ is stable }] = 1.$$

证明。 由引理 4.1 可知，若 $\mathbb{Q}(\gamma) \cap K = \mathbb{Q}$，则 $X(K,\gamma)$ 是稳定的。因此，由定理 1.2 即可得证。□

引理 4.2。 给定 $\mathcal{X} \subseteq \mathcal{P}_{\mathit{fin}}(\text{谱}(\mathcal{O}_K))$，令

$$\mathcal{Y} = \Big\{Y \in \mathcal{P}_{\mathit{fin}}(\mathit{Spec}(\mathbb{Z})) \mid \{\mathfrak{p} \in \mathit{Spec}(\mathcal{O}_K) \mid \mathfrak{p} \cap \mathbb{Z} \in Y\} \in \mathcal{X}\Big\}.$$

于是，我们有

$$\mathbb{P}_n[X(K,\gamma) \in \mathcal{X}] = \mathbb{P}_n[X(\mathbb{Q},\gamma) \in \mathcal{Y}] = \frac{\zeta(n+1)}{\zeta(n)} \sum_{Y \in \mathcal{Y}} \prod_{p \in Y} \beta_{p,n}.$$

证明。 由定理 1.2、引理 2.2 和引理 4.1，我们知道

$$\begin{aligned}\mathbb{P}_n[X(K,\gamma)\in\mathcal{X}] &= \mathbb{P}_n[X(K,\gamma)\in\mathcal{X} \text{ and } \mathbb{Q}(\gamma)\cap K=\mathbb{Q}]\\ &= \mathbb{P}_n[X(\mathbb{Q},\gamma)\in\mathcal{Y} \text{ and } \mathbb{Q}(\gamma)\cap K=\mathbb{Q}]\\ &= \mathbb{P}_n[X(\mathbb{Q},\gamma)\in\mathcal{Y}] = \frac{\zeta(n+1)}{\zeta(n)}\sum_{Y\in\mathcal{Y}}\prod_{p\in Y}\beta_{p,n}.\end{aligned}$$

□

命题 1.8. 给定 $n\geq 2$、数域 K 和有限稳定子集 $X\subseteq$谱$(\mathcal{O}_K)$。设 $X_1=\{\mathfrak{p}\cap\mathbb{Z}\mid\mathfrak{p}\in X\}$，则有

$$\mathbb{P}_n\big[X(K,\gamma)=X\big]=\frac{\zeta(n+1)}{\zeta(n)}\prod_{p\in X_1}\beta_{p,n}.$$

证明。 这由引理 4.2 得出。 □

命题 4.3. 给定数域 K、子集 $X\subseteq$ 谱$(\mathcal{O}_K)$ 以及 $n\geq 2$。设$Y=\{p\in$ 谱$(\mathbb{Z})\mid$， $\mathcal{O}_K$ 中位于 p 之上的所有素数都在 $X\}$ 中。那么

$$\mathbb{P}_n[X(K,\gamma)\subseteq X]=\prod_{p\notin Y}\alpha_{p,n}.$$

证明。 这由引理 4.2 和命题 2.5 得出。 □

T定理 1.9. 给定数域 K 和整数 $n\geq 2$、 $k\geq 1$，有

$$\mathbb{P}_n\big[\mathcal{O}_K[\gamma]\cap K=\mathcal{O}_K[1/k]\big]=\frac{\zeta(n+1)}{\zeta(n)}\prod_{p\mid k}\beta_{p,n}.$$

证明。 令 $X=\{\mathfrak{p}\in\mathrm{Spec}(\mathcal{O}_K)\mid k\in\mathfrak{p}\}$。注意到 X 是稳定的，因此，

$$\mathbb{P}_n[X(K,\gamma)=X]=\frac{\zeta(n+1)}{\zeta(n)}\prod_{p\mid k}\beta_{p,n}.$$

我们将证明，当且仅当 $\mathcal{O}_K[\gamma]\cap K=\mathcal{O}_K[\frac{1}{k}]$ 时， $X(K,\gamma)=X$。令 $\gamma_1=\frac{1}{k}$，于是 $\mathcal{O}_K[\gamma_1]\cap K=\mathcal{O}_K[\frac{1}{k}]$。由于 $f_{K,\,\gamma_1}(x)=x-\frac{1}{k}$，由定理 1.5 可知 $X(K,\gamma_1)=X$。定理 1.6 告诉我们，当且仅当 $X(K,\gamma)=X(K,\gamma_1)$ 时， $\mathcal{O}_K[\gamma]\cap K=\mathcal{O}_K[\gamma_1]\cap K$。这意味着，当且仅当 $X(K,\gamma)=X$ 时， $\mathcal{O}_K[\gamma]\cap K=\mathcal{O}_K[\frac{1}{k}]$。□

命题 1.10。 给定一个数域 K、有限子集 $X\subseteq\mathrm{Spec}(\mathcal{O}_K)$ 和 $n\geq 2$。令 $Y=\{\mathfrak{p}\cap\mathbb{Z}\mid\mathfrak{p}\in X\}$。那么

$$\mathbb{P}_n[X\subseteq X(K,\gamma)]=\prod_{p\in Y}\alpha_{p,n}\beta_{p,n}.$$

证明。 这由引理 4.2 和命题 2.4 得出。 □

5. Statistics of the size of $X(K,\gamma)$

记作 $a_{K,n,t} = \mathbb{P}_n\left[|X(K,\gamma)| = t\right]$。回忆一下，$r_K(p)$ 是 $\mathcal{O}_K$ 上方 p 的素数个数。

命题 5.1。设 K 是一个数域，$n \geq 2$ 和 $t \geq 0$ 是整数，则

$$\mathbb{P}_n[|X(K,\gamma)| = t] = \frac{\zeta(n+1)}{\zeta(n)} \sum_{\substack{Y \in \mathcal{P}_{fin}(Spec(\mathbb{Z})) \\ \sum_{p\in Y} r_K(p) = t}} \prod_{p \in Y} \beta_{p,n}.$$

证明。设 $\mathcal{X} = \{X \in \mathcal{P}_{\text{fin}}(\text{Spec}(\mathcal{O}_K)) \mid |X| = t\}$ 且

$$\mathcal{Y} = \left\{Y \in \mathcal{P}_{\text{fin}}(\text{Spec}(\mathbb{Z})) \mid \{\mathfrak{p} \in \text{Spec}(\mathcal{O}_K) \mid \mathfrak{p} \cap \mathbb{Z} \in Y\} \in \mathcal{X}\right\}.$$

因此，$\mathcal{Y} = \left\{Y \in \mathcal{P}_{\text{fin}}(\text{Spec}(\mathbb{Z})) \mid \sum_{p\in Y} r_K(p) = t\right\}$。结论由引理 4.2 得出。□

定义

$$f_{K,n}(z) = \frac{\zeta(n+1)}{\zeta(n)} \prod_{p \in \text{Spec}(\mathbb{Z})} (1 + z^{r_K(p)}\beta_{p,n}).$$

回顾一下，$\beta_{p,\,n} = \frac{1}{p^n}\frac{1-\frac{1}{p}}{1-\frac{1}{p^n}}$。我们立即得到以下结论。

引理 5.2. 对于任意素数 p 和 $n \geq 2$，有 $\frac{1}{2p^n} < \beta_{p,\,n} < \frac{1}{p^n}$。

引理 5.3. 给定 $n \geq 2$ 和一个数域 K，满足 $[K:\ \mathbb{Q}] = d$, $f_{K,\,n}$ 是亏格为 $\lfloor \frac{d}{n} \rfloor$的整函数。

证明. 首先注意，由于 $n \geq 2$ 和 $\beta_{p,\,n} < \frac{1}{p^n}$，总和 $\sum_p \beta_{p,\,n}$ 收敛。接下来，对于$R > 1$, 考虑一个满足 $|z| < R$的复数。那么我们有

$$\sum_p |z^{r_K(p)}\beta_{p,n}| < R^d \sum_p \beta_{p,n} < \infty.$$

这意味着定义 $f_{K,\,n}$ 的乘积在紧集上一致收敛，因此 $f_{K,\,n}$ 是一个整函数。

接下来，注意到 $f_{K,\,n}$ 的零点为 $-\beta_p^{-\frac{1}{r_K}}\left(\sqrt[n]{p}\, e^{\frac{2\pi i a}{r_K\, p}}\right)$，() 其中 p 为有理素数，$0 \leq a < r_K$为整数（p）。我们先计算 $f_{K,\,n}$的秩。令 $\mu = \lfloor \frac{d}{n} \rfloor$，则（$\mu+1$）$\frac{n}{d} > 1$且 $\mu\frac{n}{d} \leq 1$。现在

$$\sum_p \sum_{a=0}^{r_K(p)-1} \left|\beta_{p,n}^{\frac{1}{r_K(p)}}\right|^{\mu+1} \leq d\sum_p \left|\beta_{p,n}^{\frac{1}{r_K(p)}}\right|^{\mu+1} \leq d\sum_p \left|\beta_{p,n}^{\frac{1}{d}}\right|^{\mu+1} \leq d\sum_p \frac{1}{p^{(\mu+1)\frac{n}{d}}},$$

由于 $(\mu+1)\,\frac{n}{d}>1$，该级数收敛。接下来，注意到

$$\sum_{p}\sum_{a=0}^{r_K(p)-1}\left|\beta_{p,n}^{\frac{1}{r_K(p)}}\right|^{\mu}\geq\sum_{p}\left|\beta_{p,n}^{\frac{1}{r_K(p)}}\right|^{\mu}\geq\sum_{p:r_K(p)=d}\left|\beta_{p,n}^{\frac{1}{d}}\right|^{\mu}\geq\frac{1}{2^{\frac{\mu}{d}}}\sum_{p:r_K(p)=d}\frac{1}{p^{\mu\frac{n}{d}}}\geq\frac{1}{2^{\frac{\mu}{d}}}\sum_{p:r_K(p)=d}\frac{1}{p}.$$

根据切博塔廖夫密度定理，我们知道，在 K 中完全分裂的有理素数具有正的自然密度。这意味着（由阿贝尔求和）级数 $\sum_{p:r_K(p)=d}\frac{1}{p}$ 发散。因此，定义 $f_{K,n}$ 的乘积的秩为 μ，故其亏格为 $\mu=\lfloor\frac{d}{n}\rfloor$。□

命题 5.4。我们有

$$f_{K,n}(z)=\sum_{t=0}^{\infty}a_{K,n,t}z^t,\qquad\mathbb{E}_n[|X(K,\gamma)|]=f'_{K,n}(1).$$

此外，对于任意复数 c, $\mathbb{E}_n[e^{c|X(K,\gamma)|}]=f_{K,n}(e^c)$。

证明。注意到

$$\begin{aligned}f_{K,n}(z)&=\frac{\zeta(n+1)}{\zeta(n)}\prod_{p\in\mathrm{Spec}(\mathbb{Z})}(1+z^{r_K(p)}\beta_{p,n})=\frac{\zeta(n+1)}{\zeta(n)}\sum_{Y\in\mathcal{P}_{\mathrm{fin}}(\mathrm{Spec}(\mathbb{Z}))}z^{\sum_{p\in Y}r_K(p)}\prod_{p\in Y}\beta_{p,n}\\&=\frac{\zeta(n+1)}{\zeta(n)}\sum_{t=0}^{\infty}z^t\sum_{\substack{Y\in\mathcal{P}_{\mathrm{fin}}(\mathrm{Spec}(\mathbb{Z}))\\\sum_{p\in Y}r_K(p)=t}}\prod_{p\in Y}\beta_{p,n}=\sum_{t=0}^{\infty}z^t\mathbb{P}_n[|X(K,\gamma)|=t]\\&=\sum_{t=0}^{\infty}a_{K,n,t}z^t.\end{aligned}$$

接下来，这意味着

$$f'_{K,n}(1)=\sum_{t=1}^{\infty}a_{K,n,t}t=\sum_{t=1}^{\infty}t\mathbb{P}_n[|X(K,\gamma)|=t]=\mathbb{E}[|X(K,\gamma)|].$$

最后，请注意

$$f_{K,n}(e^c)=\sum_{t=0}^{\infty}a_{K,n,t}e^{ct}=\sum_{t=0}^{\infty}e^{ct}\mathbb{P}_n[|X(K,\gamma)|=t]=\mathbb{E}\left[e^{c|X(K,\gamma)|}\right].\qquad\square$$

设 $m_{K,\gamma,s}$ 为 $|X(K,\gamma)|$ 的 s^{th} 阶矩。将有理素数依次记为 $p_1=2,p_2=3,p_3=5,\ldots$。

推论 5.4.1.

$$m_{K,\gamma,s}=\sum_{\substack{Y\subseteq Spec(\mathbb{Z})\\Y\neq\emptyset,\,|Y|\leq s}}\prod_{p\in Y}\alpha_{p,n}\beta_{p,n}\sum_{A\subseteq Y}(-1)^{s-|A|}\left(\sum_{p\in Y}r_K(p)\right)^s$$

证明。 众所周知，矩母函数为 $\sum_{s=0}^{\infty} {}^{m_K}{}_{,\ s}{}^{\gamma\ s}{}_{,\ !}\ x^s = \mathbb{E}[e^{x|X(K,\gamma)|}]$。因此，我们看到

$$\begin{aligned}\sum_{s=0}^{\infty}\frac{m_{K,\gamma,s}}{s!}x^s &= f_{K,n}(e^x) = \frac{\zeta(n+1)}{\zeta(n)}\prod_p(1+e^{xr_K(p)}\beta_{p,n}) = \prod_p \alpha_{p,n}\prod_p\left(1+\beta_{p,n}\sum_{t=0}^{\infty}\frac{r_K(p)^t}{t!}x^t\right)\\ &= \prod_p\left(\alpha_{p,n}(1+\beta_{p,n})+\alpha_{p,n}\beta_{p,n}\sum_{t=1}^{\infty}\frac{r_K(p)^t}{t!}x^t\right) = \prod_p\left(1+\alpha_{p,n}\beta_{p,n}\sum_{t=1}^{\infty}\frac{r_K(p)^t}{t!}x^t\right)\\ &= \sum_{s=0}^{\infty}x^s\sum_{u=1}^{s}\sum_{1\le i_1<i_2<\cdots<i_u}\prod_{j=1}^{u}\alpha_{p_{i_j},n}\beta_{p_{i_j},n}\sum_{\substack{t_1+\cdots+t_u=s\\ t_j\ge 1}}\prod_{j=1}^{u}\frac{r_K(p_{i_j})^{t_j}}{t_j!}.\end{aligned}$$

这意味着

$$\begin{aligned}m_{K,\gamma,s} &= \sum_{u=1}^{s}\sum_{1\le i_1<i_2<\cdots<i_u}\prod_{j=1}^{u}\alpha_{p_{i_j},n}\beta_{p_{i_j},n}\sum_{\substack{t_1+\cdots+t_u=s\\ t_j\ge 1}}\frac{s!}{t_1!\dots t_u!}r_K(p_{i_1})^{t_1}\dots r_K(p_{i_u})^{t_u}\\ &= \sum_{\substack{Y\subseteq \mathrm{Spec}(\mathbb{Z})\\ Y\neq\emptyset,\ |Y|\le s}}\prod_{p\in Y}\alpha_{p,n}\beta_{p,n}\sum_{A\subseteq Y}(-1)^{s-|A|}\left(\sum_{p\in Y}r_K(p)\right)^s. \qquad \square\end{aligned}$$

命题 1.11. 给定一个数域 K 和 $n\ge 2$，我们有

$$\mathbb{E}_n[|X(K,\gamma)|] = \sum_p \alpha_{p,n}\beta_{p,n}r_K(p),\quad \mathrm{Var}_n[|X(K,\gamma)|] = \sum_p \alpha_{p,n}\beta_{p,n}(1-\alpha_{p,n}\beta_{p,n})r_K(p)^2.$$

证明. 由推论 5.4.1 可知 $\mathbb{E}_n[|X(K,\gamma)|] = m_{K,\gamma,1} = \sum_p \alpha_{p,n}\beta_{p,n}r_K(p)$，并且

$$\begin{aligned}m_{K,\gamma,2} &= \sum_p \alpha_{p,n}\beta_{p,n}r_K(p)^2 + \sum_{p<q}\alpha_{p,n}\beta_{p,n}\alpha_{q,n}\beta_{q,n}\big((r_K(p)+r_K(q))^2 - r_K(p)^2 - r_K(q)^2\big)\\ &= \sum_p \alpha_{p,n}\beta_{p,n}r_K(p)^2 + 2\sum_{p<q}\alpha_{p,n}\beta_{p,n}\alpha_{q,n}\beta_{q,n}r_K(p)r_K(q).\end{aligned}$$

因此，

$$\mathrm{Var}_n[|X(K,\gamma)|] = m_{K,\gamma,2} - m_{K,\gamma,1}^2 = \sum_p \alpha_{p,n}\beta_{p,n}(1-\alpha_{p,n}\beta_{p,n})r_K(p)^2. \qquad \square$$

引理 5.5. 给定 $\epsilon>0$，对于充分大的 t，我们有

$$\prod_{i=1}^{t}p_i < e^{(1+\epsilon)t\log(t)}.$$

证明。 令 $\vartheta(X) = \sum_{p\le X}\log(p)$。因此， $\prod_{1\le i\le t}p_i = e^{\vartheta(p_t)}$。现在已知渐近地有 $p_t\sim t\log(t)$，且 $\vartheta(X)\sim X$。结论得证。$\square$

定理 1.12。 固定一个数域 K和 $n\geq 2$。令 $\mu=\lfloor\frac{d}{n}\rfloor$。给定 $\epsilon>0$，当 t充分大时，我们有

$$t^{-(1+\epsilon)nt}<\mathbb{P}_n[|X(K,\gamma)|=t]<t^{-\frac{1}{\mu+1+\epsilon}t}.$$

证明。令 λ 为整函数 $f_{K,n}(z)$ 的阶。于是我们知道 $\mu\leq\lambda\leq\mu+1$。进一步地，由 [2, 定理 2.2。2], 我们知道

$$\lambda=\limsup_{t\to\infty}\frac{t\log(t)}{\log(|a_{K,n,t}|^{-1})}.$$

这意味着，对于足够大的 t，有 $\frac{t\log(t)}{\log(|a_{K,n,t}|^{-1})}<\lambda+\epsilon$，这意味着

$$a_{K,n,t}<e^{-\frac{1}{\lambda+\epsilon}t\log(t)}.$$

由命题 5.1，我们知道

$$a_{K,n,t}=\frac{\zeta(n+1)}{\zeta(n)}\sum_{\substack{Y\in\mathcal{P}_{\mathrm{fin}}(\mathrm{Spec}(\mathbb{Z}))\\ \sum_{p\in Y}r_K(p)=t}}\prod_{p\in Y}\beta_{p,n}.$$

定义 $c(t)$ 为满足 $\sum_{i=1}^{c}r_K(p_i)\geq t$ 的最大非负整数。因此我们有 $\sum_{i=1}^{c(t)-1}r_K(p_i)<t\leq\sum_{i=1}^{c(t)}r_K(p_i)$。这意味着 $c(t)-1<t\leq dc(t)$。接下来记 $\delta(t)=\sum_{i=1}^{c(t)}r_K(p_i)-t$。注意到 $0\leq\delta(t)<r_K(p_{c(t)})\leq d$。

现在考虑在 K 中完全分裂的 d 个最小素数（根据切博塔廖夫密度定理，这样的素数有无穷多个），设它们为 $p_{i_1},\dots,p_{i_d}$。注意到 $t\geq di_d$意味着 $c(t)\geq i_d$。因此，对于 $t\geq di_d$，我们有 $\{p_{i_1},\dots,p_{i_d}\}\subseteq\{p_1,\dots,p_{c(t)}\}$. 现在考虑 $Y_1=\{p_1,\dots,p_{c(t)}\}\setminus\{p_{i_1},\dots,p_{i_{\delta(t)}}\}$。因此

$$\sum_{p\in Y_1}r_K(p)=\sum_{i=1}^{c(t)}r_K(p_i)-\sum_{j=1}^{\delta(t)}r_K(p_{i_j})=\sum_{i=1}^{c(t)}r_K(p_i)-\delta(t)=t.$$

由引理 5.5 可知，当 t足够大时，

$$\begin{aligned}a_{K,n,t}&\geq\frac{\zeta(n+1)}{\zeta(n)}\prod_{p\in Y_1}\beta_{p,n}\geq\frac{\zeta(n+1)}{\zeta(n)}\prod_{i=1}^{c(t)}\beta_{p,n}\geq\frac{\zeta(n+1)}{\zeta(n)}\prod_{i=1}^{t}\beta_{p,n}\\&\geq\frac{\zeta(n+1)}{\zeta(n)}\prod_{i=1}^{t}\frac{1}{2p_i^n}\geq\frac{\zeta(n+1)}{\zeta(n)}\frac{1}{2^t}e^{-n(1+\frac{\epsilon}{2})t\log(t)}\geq e^{-n(1+\epsilon)t\log(t)}.\end{aligned}$$

□

回顾一下，我们有

$$\mathbb{P}_n[|X(K,\gamma)|=t]=\frac{\zeta(n+1)}{\zeta(n)}\sum_{\substack{Y\in\mathcal{P}_{\mathrm{fin}}(\mathrm{Spec}(\mathbb{Z}))\\ \sum_{p\in Y}r_K(p)=t}}\prod_{p\in Y}\beta_{p,n}.$$

设 $d = [K\colon\ \mathbb{Q}]$。给定 $Y \in \mathcal{P}_{\text{fin}}(\text{Spec}(\mathbb{Z}))$，使得 $\sum_{p\in Y} r_K(p) = t$，对于 $1 \le i \le d$，构造 $\lambda_i = \#\{p \in Y \mid r_K(p) = i\}$。注意 $\sum_{i=1}^{d} i\lambda_i = t$。如果 K 是 $\mathbb{Q}$ 上的伽罗瓦扩张，那么对于那些不整除 d 的 i，我们有 $\lambda_i = 0$。

定义 5.6。给定一个数域 K，满足 $[K\colon\ \mathbb{Q}] = d$，以及整数 $1 \le j \le d$、$t \ge 0$、$n \ge 2$。记

$$\Lambda(d,t) = \Big\{\lambda = (\lambda_1, \dots, \lambda_d) \mid \lambda_j \ge 0, \sum_{j=1}^{d} j\lambda_j = t\Big\}.$$

给定 $\lambda \in \Lambda(d,t_1)$ 和 $\lambda' \in \Lambda(d,t_2)$，通过逐坐标相加定义 $\lambda + \lambda' \in \Lambda(d,t_1+t_2)$。接下来，记

$$\Lambda^0(d,t) = \Big\{\lambda \in \Lambda(d,t) \mid \lambda_j \ne 0 \ \textit{implies}\ j|d\Big\}.$$

最后，记

$$b_{K,n,j,t} = \sum_{\substack{1\le i_1<i_2<\cdots<i_t \\ r_K(p_{i_1})=\cdots=r_K(p_{i_t})=j}} \beta_{p_{i_1},n} \dots \beta_{p_{i_t},n}.$$

引理 5.7。给定一个数域 K，满足 $[K\colon\ \mathbb{Q}] = d$，以及整数 $n \ge 2$ 和 $t \ge 0$，有

$$\mathbb{P}_n[|X(K,\gamma)| = t] = \frac{\zeta(n+1)}{\zeta(n)} \sum_{\lambda\in\Lambda(d,t)} \prod_{\substack{1\le j\le d, \\ \lambda_j\ne 0}} b_{K,n,j,\lambda_j}.$$

此外，若 K 在 $\mathbb{Q}$ 上是伽罗瓦扩张，则有

$$\mathbb{P}_n[|X(K,\gamma)| = t] = \frac{\zeta(n+1)}{\zeta(n)} \sum_{\lambda\in\Lambda^0(d,t)} \prod_{\substack{j|d, \\ \lambda_j\ne 0}} b_{K,n,j,\lambda_j}.$$

证明。第一部分由命题 5.1 得出。对于第二部分，注意到如果 K 是 $\mathbb{Q}$ 和 $j \nmid d$ 上的伽罗瓦扩张，那么 $b_{K,\ n,\ j,\ t} = 0$。□

注意，我们并不总有 $\mathbb{P}_n[|X(K,\gamma)| = t] > \mathbb{P}_n[|X(K,\gamma)| = t+1]$，例如 $\mathbb{P}_n[|X(\mathbb{Q}(\sqrt{-7})\ \gamma)| = 1] < \mathbb{P}_n[|X(\mathbb{Q}(\sqrt{-7})\ \gamma)| = 2]$。不过，我们将给出一些与 $\mathbb{P}_n[|X(K,\gamma)| = t]$ 相关的较弱单调性结果。

引理 *5.8.* 假设给定正整数 d, a, b，使得从 $\Lambda(d,a) \times \Lambda(d,b)$ 到 $\Lambda(d,a+b)$ 的加法映射是满射。那么对于每个满足 $[K\colon\ \mathbb{Q}] = d$ 的数域 K，以及整数 $n \ge 2$，我们有 $\mathbb{P}_n[|X(K,\gamma)| = a] > \mathbb{P}_n[|X(K,\gamma)| = a+b]$。

证明。首先注意，$b_{K,\ n,\ j,\ t_1}b_{K,\ n,\ j,\ t_2}\geq b_{K,\ n,\ j,\ t_1+t_2}$。接下来，我们应用引理 5.7。

$$\begin{aligned}\mathbb{P}_n[|X(K,\gamma)|=a+b]&=\frac{\zeta(n+1)}{\zeta(n)}\sum_{\lambda\in\Lambda(d,a+b)}\prod_{\substack{1\leq j\leq d,\\ \lambda_j\neq 0}}b_{K,n,j,\lambda_j}\\&\leq\frac{\zeta(n+1)}{\zeta(n)}\sum_{\lambda'\in\Lambda(d,a)}\sum_{\lambda''\in\Lambda(d,b)}\prod_{\substack{1\leq j\leq d,\\ \lambda'_j+\lambda''_j\neq 0}}b_{K,n,j,\lambda'_j+\lambda''_j}\\&\leq\frac{\zeta(n+1)}{\zeta(n)}\sum_{\lambda'\in\Lambda(d,a)}\prod_{\substack{1\leq j\leq d,\\ \lambda'_j\neq 0}}b_{K,n,j,\lambda'_j}\sum_{\lambda''\in\Lambda(d,b)}\prod_{\substack{1\leq j\leq d,\\ \lambda''_j\neq 0}}b_{K,n,j,\lambda''_j}\\&=\mathbb{P}_n[|X(K,\gamma)|=a]\Big(\frac{\zeta(n)}{\zeta(n+1)}\mathbb{P}_n[|X(K,\gamma)|=b]\Big).\end{aligned}$$

因此，只要证明 $\frac{\zeta(n)}{\zeta(n+1)}\mathbb{P}_n[|X(K,\gamma)|=b]<1$，即可完成证明。我们有 $\mathbb{P}_n[|X(K,\gamma)|=1]=\frac{\zeta(n+1)}{\zeta(n)}$，因此 $\mathbb{P}_n[|X(K,\gamma)|=b]\leq 1-\frac{\zeta(n+1)}{\zeta(n)}$。所以，我们只需验证 $\left(\frac{\zeta(n+1)}{\zeta(n)}\right)^{-1}\left(1-\frac{\zeta(n+1)}{\zeta(n)}\right)<1$。这等价于 $\frac{\zeta(n+1)}{\zeta(n)}>\frac{1}{2}$，而这对所有$n\geq 2$都成立。□

引理 *5.9.* 设给定正整数 d,a,b，使得从 $\Lambda^0(d,a)\times\Lambda^0(d,b)$ 到 $\Lambda^0(d,a+b)$ 的加法映射是满射。那么，对于每个满足 $[K$ 的数域 $K\colon\ \mathbb{Q}]=d$，若其在 $\mathbb{Q}$ 上是伽罗瓦扩张且 $n\geq 2$ 为整数，则有 $\mathbb{P}_n[|X(K,\gamma)|=a]>\mathbb{P}_n[|X(K,\gamma)|=a+b]$。

证明。定理的证明过程与引理 5.8 的证明过程相同。□

命题 5.10. 设给定一个数域 K，其中 $[K\colon\ \mathbb{Q}]=d$, $n\geq 2$。令 $d_1=lcm(1,\ 2,\ \ldots\ldots,\ d)$。对于 $t\geq(d-1)d_1-\frac{d}{(d+1)_2}+1$, 有

$$\mathbb{P}_n[|X(K,\gamma)|=t]>\mathbb{P}_n[|X(K,\gamma)|=t+d_1].$$

令 $\tau(d)$ 为 d 的因数个数，$\sigma(d)$ 为 d 的因数和。若 K 是 $\mathbb{Q}$ 上的伽罗瓦扩张，则对于 $t\geq d(\tau(d)-1)-\sigma(d)+1$，有

$$\mathbb{P}_n[|X(K,\gamma)|=t]>\mathbb{P}_n[|X(K,\gamma)|=t+d].$$

证明。如果我们证明映射 $\lambda+\lambda'$ 从 $\Lambda(d,t)\times\Lambda(d,d_1)$ 到 $\Lambda(d,t+d_1)$ 是满射，那么第一部分就完成了。考虑 $\rho\in\Lambda(d,t+d_1)$。注意

$$\sum_{j=1}^{d}j\rho_j=t+d_1\geq dd_1-\frac{d(d+1)}{2}+1>\sum_{j=1}^{d}(d_1-j).$$

这意味着必定存在某个 j 使得 $j\rho_j > d_1 - j$，也就是说，$\rho_j > \frac{d_1}{j} - 1$。由于$j \mid d_1$，我们得出 $\rho_j \geq \frac{d_1}{j}$。考虑 $\lambda = (\rho_1, \ldots, \rho_{j-1}, \rho_j - \frac{d_1}{j}, \rho_{j+1}, \ldots, \rho_d)$ 和$\lambda' = (0, \ldots, 0, \frac{d_1}{j}, 0, \ldots, 0)$。显然，$\lambda \in \Lambda(d,t)$、$\lambda' \in \Lambda(d,d_1)$ 且 $\lambda + \lambda' = \rho$。因此，从 $\Lambda(d,t) \times \Lambda(d,d_1)$ 到 $\Lambda(d, t+d_1)$ 的映射是满射。我们看到$\mathbb{P}_n[|X(K,\gamma)| = t] > \mathbb{P}_n[|X(K,\gamma)| = t + d_1]$.

接下来，假设 K 在 $\mathbb{Q}$ 上是伽罗瓦扩张，且 $t \geq d(\tau(d) - 1) - \sigma(d) + 1$。我们需要证明，从 $\Lambda^0(d,t) \times \Lambda^0(d,d)$ 到 $\Lambda^0(d, t+d)$ 的加法映射是满射。考虑 $\rho \in \Lambda^0(d, t+d)$。注意到

$$\sum_{j|d} j\rho_j = t + d \geq d\tau(d) - \sigma(d) + 1 > \sum_{j|d}(d - j).$$

这意味着必定存在某个 $j \mid d$ 使得 $j\rho_j > d - j$，也就是说，$\rho_j > \frac{d}{j} - 1$。由于$j \mid d$，我们得出 $\rho_j \geq \frac{d}{j}$。考虑由 $\lambda = (\rho_1, \ldots, \rho_{j-1}, \rho_j - \frac{d}{j}, \rho_{j+1}, \ldots, \rho_d)$ 给出的 $\lambda \in \Lambda(d,t)$，以及由 $\lambda' = (0, \ldots, 0, \frac{d}{j}, 0, \ldots, 0)$ 给出的 $\lambda' \in \Lambda(d,d)$。显然，$\lambda + \lambda' = \rho$。因此，从 $\Lambda^0(d,t) \times \Lambda^0(d,d)$ 到 $\Lambda^0(d, t+d)$ 的映射是满射。我们看到 $\mathbb{P}_n[|X(K,\gamma)| = t] > \mathbb{P}_n[|X(K,\gamma)| = t + d]$. □

推论 5.10.1. 给定 $n \geq 2$ 和 $t \geq 0$，我们有

$$\mathbb{P}_n[|X(\mathbb{Q},\gamma)| = t] > \mathbb{P}_n[|X(\mathbb{Q},\gamma)| = t + 1].$$

命题 5.11. 设 K 是一个数域，在 $\mathbb{Q}$ 上是伽罗瓦扩张，且对于 $[K : \mathbb{Q}] = p^m$ 是一个素数幂。设给定 $n \geq 2$ 和 $t \geq 0$。则有

$$\mathbb{P}_n[|X(K,\gamma)| = t] > \mathbb{P}_n[|X(K,\gamma)| = t + p^m].$$

进一步考虑 $0 \leq j \leq m-1$ 和 $t \geq 0$。设 t 满足如下性质：不存在任何 $0 \leq a \leq p^j - 1$ 使得 $t \equiv (p-1)p^j + a \pmod{p^{j+1}}$。则有

$$\mathbb{P}_n[|X(K,\gamma)| = t] > \mathbb{P}_n[|X(K,\gamma)| = t + p^j].$$

证明. 对于第一部分，我们要证明从 $\Lambda^0(p^m,t) \times \Lambda^0(p^m,p^m) \to \Lambda^0(p^m, t+p^m)$ 出发的加法映射是满射。考虑 $\rho \in \Lambda^0(p^m, t+p^m)$，我们知道$\sum_{i=0}^m p^i \rho_{p^i} = t + p^m$。令 $j_0 = \min\{0 \leq j \leq m \mid \sum_{i=j}^m p^i \rho_{p^i} \geq p^m\}$。这意味着 $0 \leq \sum_{i=j_0}^m p^i \rho_{p^i} - p^m < p^{j_0}\rho_{p^{j_0}}$。令 $a = \sum_{i=j_0}^m p^{i-j_0}\rho_{p^i} - p^{m-j_0}$，于是 $a \in \mathbb{Z}$ 和$0 \leq a < \rho_{p^{j_0}}$。定义 $\lambda \in \Lambda^0(p^m,t)$ 和 $\lambda' \in \Lambda^0(p^m,p^m)$ 如下

$$\lambda_{p^i} = \begin{cases} 0 & \text{if } i > j_0 \\ \rho_{p^{j_0}} - a & \text{if } i = j_0 \\ \rho_{p^i} & \text{if } i < j_0, \end{cases} \qquad \lambda'_{p^i} = \begin{cases} \rho_{p^i} & \text{if } i > j_0 \\ a & \text{if } i = j_0 \\ 0 & \text{if } i < j_0. \end{cases}$$

显然，$\lambda + \lambda' = \rho$。因此，从 $\Lambda^0(p^m,t)$ 到 $\times\, \Lambda^0(p^m,p^m) \to \Lambda^0(p^m, t+p^m)$ 的加法映射是满射。

对于第二部分，假设给定了 $0\le j\le m-1$ 和 $t\ge 0$，且不存在满足 $t+p^j\equiv a \pmod{p^{j+1}}$ 的 $0\le a\le p^j-1$。我们要证明，从 $\Lambda^0(p^m,t)$ 到 $\times\Lambda^0(p^m,p^j)\to\Lambda^0(p^m,t+p^j)$ 的加法映射是满射。考虑$\rho\in\Lambda^0(p^m,t+p^j)$，我们知道 $\sum_{i=0}^m p^i\rho_{p^i}=t+p^j$。我们看到 $t+p^j\equiv\sum_{i=0}^j p^i\rho_{p^i}\pmod{p^{j+1}}$，因此$\sum_{i=0}^j p^i\rho_{p^i}\ge p^j$。令 $k_0=\min\{0\le k\le j\mid\sum_{i=k}^j p^i\rho_{p^i}\ge p^j\}$。这意味着 $0\le\sum_{i=k_0}^j p^i\rho_{p^i}-p^j<p^{k_0}\rho_{p^{k_0}}$。令 $b=\sum_{i=k_0}^j p^{i-k_0}\rho_{p^i}-p^{j-k_0}$，于是 $b\in\mathbb{Z}$且 $0\le b<\rho_{p^{k_0}}$。定义 $\lambda\in\Lambda^0(p^m,t)$ 和 $\lambda'\in\Lambda^0(p^m,p^j)$ 如下

$$\lambda_{p^i}=\begin{cases}\rho_{p^i} & \text{if } j<i\\ 0 & \text{if } k_0<i\le j\\ \rho_{p^{j_0}}-b & \text{if } i=k_0\\ \rho_{p^i} & \text{if } i<k_0,\end{cases}\qquad \lambda'_{p^i}=\begin{cases}0 & \text{if } j<i\\ \rho_{p^i} & \text{if } k_0<i\le j\\ b & \text{if } i=k_0\\ 0 & \text{if } i<k_0.\end{cases}$$

显然，$\lambda+\lambda'=\rho$。因此，加法映射 $\Lambda^0(p^m,t)\times\Lambda^0(p^m,p^m)\to\Lambda^0(p^m,t+p^m)$ 是满射。□

6. 由 $X(K,\gamma)$ 生成的类群子群。

本节将研究群 $\langle[\mathfrak{p}],\mathfrak{p}\in X(K,\gamma)\rangle$，尤其是在 K 是虚二次域时。我们将证明定理 1.14。

引理 6.1. 设给定一个数域 K 以及整数 $t\ge 1$ 和 $n\ge 2$。令 Y' 为满足以下条件的有理素数 p 的集合：在 $\mathcal{O}_K$ 中，至少有一个位于 p 之上的素理想 $\mathfrak{p}$ 满足 $\mathfrak{p}^t$ 不是主理想。那么有

$$\mathbb{P}_n\big[\langle[\mathfrak{p}],\mathfrak{p}\in X(K,\gamma)\rangle \text{ is } t\text{-torsion}\big]=\prod_{p\in Y'}\alpha_{p,n}.$$

证明。首先，$\langle[\mathfrak{p}],\mathfrak{p}\in X(K,\gamma)\rangle$ 是 t-挠的，当且仅当对每个素理想 $\mathfrak{p}\in X(K,\gamma)$，$\mathfrak{p}^t$ 都是主理想。令 X 为 $\mathcal{O}_K$ 中满足 $\mathfrak{p}^t$ 是主理想的素理想 $\mathfrak{p}$ 的集合。令 Y 为 $\mathbb{Z}$ 中的素理想 p 的集合，使得 $\mathcal{O}_K$ 中所有位于 p 之上的素理想都属于 X。那么根据命题 1.13，我们知道

$$\mathbb{P}_n\big[\langle[\mathfrak{p}],\mathfrak{p}\in X(K,\gamma)\rangle \text{ is } t\text{-torsion}\big]=\mathbb{P}_n[X(K,\gamma)\subseteq X]=\prod_{p\notin Y}\alpha_{p,n}.\qquad\square$$

引理 6.2. 对于 $n\ge 2$ 和 $N\ge 2$，我们有

$$1-\frac{1}{(n-1)(N-1)^{n-1}}<\prod_{p\ge N}\alpha_{p,n}<1<\prod_{p\ge N}\alpha_{p,n}^{-1}<1+\frac{1}{(n-1)(N-1)^{n-1}}.$$

证明。首先，对于所有素数 p，我们有 $\alpha_{p,n} < 1$。因此，$\prod_{p\geq N} \alpha_{p,n} < 1$。注意到$\beta_{p,n} = \frac{1}{p^n}\frac{1-\frac{1}{p}}{1-\frac{1}{p^{n+1}}} < \frac{1}{p^n}$。这意味着

$$\begin{aligned}\alpha_{p,n}^{-1} = \prod_{p\geq N}(1+\beta_{p,n}) &< \prod_{p\geq N}(1+\frac{1}{p^n}) < 1+\sum_{m=N}^{\infty}\frac{1}{m^n} \\ &< 1+\int_N^{\infty}\frac{1}{(x-1)^n}dx = 1+\frac{1}{(n-1)(N-1)^{n-1}}.\end{aligned}$$

由此可知

$$\prod_{p\geq N}\alpha_{p,n} > \frac{1}{1+\frac{1}{(n-1)(N-1)^{n-1}}} > 1-\frac{1}{(n-1)(N-1)^{n-1}}. \qquad \square$$

考虑特征 χ_2,

$$\chi_2(a) = \begin{cases} 0 & \text{if } 2 \mid a \\ 1 & \text{if } a \equiv \pm 1 \pmod 8 \\ -1 & \text{if } a \equiv \pm 5 \pmod 8. \end{cases}$$

对于奇素数 p，考虑特征 $\chi_p(a) = \left(\frac{a}{p}\right)$。对于每个 $n \geq 2$，定义函数

$$f_n(a) = \prod_{p:\chi_p(a)\in\{0,1\}} \alpha_{p,n}, \qquad\qquad g_n(a) = \prod_{p:\chi_p(a)\in\{1\}} \alpha_{p,n}.$$

命题 6.3. 对于每个虚二次域 K，记其判别式为d_K。固定整数 $n \geq 2$ 和奇整数 $t \geq 1$。则有

$$\lim_{d_K\to-\infty} \frac{\mathbb{P}_n\left[\left\langle[\mathfrak{p}], \mathfrak{p} \in X(K,\gamma)\right\rangle \text{ is } t\text{-torsion}\right]}{f_n(d_K)} = 1.$$

证明。固定 $N > 0$。考虑判别式为 $d_K < -4N^t$的虚二次域 K 以及一个素数 $p < N$。设 $\mathfrak{p}_1$ 是 $\mathcal{O}_K$中位于 p上方的一个素理想。我们将证明，当且仅当 $\chi_p(d_K) \in \{0,1\}$时， $\mathfrak{p}_1^t$不是主理想。

- 情况 1： $\chi_p(d_K) = -1$。在这种情况下， p 在 $\mathcal{O}_K$中仍为惰性，因此 $\mathfrak{p}_1 = (p)$ 和 $\mathfrak{p}_1^t = (p^t)$ 是主理想。
- 情况 2： $\chi_p(d_K) \in \{0,1\}$。在这种情况下， p要么在 $\mathcal{O}_K$中分裂，要么分歧。设$p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$，则 $N(\mathfrak{p}_1) = p$，且 $N(\mathfrak{p}_1^t) = p^t$（ $\mathfrak{p}_1 = \mathfrak{p}_2$是可能的）。现在，如果$\mathfrak{p}_1^t$ 是主理想，那么 $\mathcal{O}_K$ 中存在一个范数为 p^t的元素。由于 $\mathcal{O}_K$ 是由1、2、$\frac{\sqrt{d_K}}{2}$ 生成的 $\mathbb{Z}$ 模的子集，这就意味着方程$\frac{a^2}{4} - d_k\frac{b^2}{4} = p^t$有整数解。然而 $-\frac{d_k}{4} > N^t > p^t$，所以 $b = 0$。但这样一来，方程 $a^2 = 4p^t$就有整数解，这不可能，因为 t 是奇数。因此， $\mathfrak{p}_1^t$ 和 $\mathfrak{p}_2^t$ 都不可能是主理想。

令 Y_K' 表示有理素数 p 的集合，其中至少有一个位于 $\mathcal{O}_K$ 中、在p 之上的素理想 $\mathfrak{p}$ 不是主理想。我们看到，对于 $d_K<-4N^t$，有

$$\frac{\mathbb{P}_n\big[\big\langle[\mathfrak{p}],\mathfrak{p}\in X(K,\gamma)\big\rangle \text{ is } t\text{-torsion}\big]}{f_n(d_K)}=\prod_{p\in Y_K',\,p\geq N}\alpha_{p,n}\prod_{p\geq N,\chi_p(d_K)\in\{0,1\}}\alpha_{p,n}^{-1}.$$

最后注意到

$$\prod_{p\in Y_K'\,p\geq N}\alpha_{p,n}\prod_{p\geq N,\chi_p(d_K)\in\{0,1\}}\alpha_{p,n}^{-1}\leq\prod_{p\geq N}\alpha_{p,n}^{-1}\leq 1+\frac{1}{(n-1)(N-1)^{n-1}},$$

and

$$\prod_{p\in Y_K',\,p\geq N}\alpha_{p,n}\prod_{p\geq N,\chi_p(d_K)\in\{0,1\}}\alpha_{p,n}^{-1}\geq\prod_{p\geq N}\alpha_{p,n}\geq 1-\frac{1}{(n-1)(N-1)^{n-1}}.$$

由于 N 是任意的，证毕。 □

推论 6.3.1. 对于任意奇数 $t\geq 3$，我们有

$$\lim_{d_K\to-\infty}\mathbb{P}_n\big[\#\big\langle[\mathfrak{p}],\mathfrak{p}\in X(K,\gamma)\big\rangle=t\big]=0.$$

证明。 首先注意到

$$\begin{aligned}&\mathbb{P}_n\big[\#\big\langle[\mathfrak{p}],\mathfrak{p}\in X(K,\gamma)\big\rangle=t\big]\\&\leq\mathbb{P}_n\big[\big\langle[\mathfrak{p}],\mathfrak{p}\in X(K,\gamma)\big\rangle\text{ is }t\text{-torsion}\big]-\mathbb{P}_n\big[\big\langle[\mathfrak{p}],\mathfrak{p}\in X(K,\gamma)\big\rangle\text{ is 1-torsion}\big].\end{aligned}$$

因此 ，

$$\limsup_{d_K\to-\infty}\frac{\mathbb{P}_n\big[\#\big\langle[\mathfrak{p}],\mathfrak{p}\in X(K,\gamma)\big\rangle=t\big]}{f_n(d_K)}\leq 1-1=0,$$

so

$$\lim_{d_K\to-\infty}\frac{\mathbb{P}_n\big[\#\big\langle[\mathfrak{p}],\mathfrak{p}\in X(K,\gamma)\big\rangle=t\big]}{f_n(d_K)}=0.$$

接下来注意，对于任意 d_K，我们有

$$f_n(d_K)=\prod_{p:\chi_p(d_K)\in\{0,1\}}\alpha_p\geq\prod_p\alpha_p=\frac{\zeta(n+1)}{\zeta(n)}.$$

因此，我们可以得出结论:

$$\lim_{d_K\to-\infty}\mathbb{P}_n\big[\#\big\langle[\mathfrak{p}],\mathfrak{p}\in X(K,\gamma)\big\rangle=t\big]=0.$$ □

命题 6.4。 对于每个虚二次域 K，记其判别式为d_K。固定整数 $n\geq 2$ 和偶整数 $t\geq 2$。则有

$$\lim_{d_K\to-\infty}\frac{\mathbb{P}_n\big[\big\langle[\mathfrak{p}],\mathfrak{p}\in X(K,\gamma)\big\rangle\ is\ t\text{-}torsion\big]}{g_n(d_K)}=1.$$

证明。设 $t = 2t_1$，固定 $N > 0$。考虑一个判别式为 $d_K < -4N^t$的虚二次域 K，以及一个素数 $p < N$。令 $\mathfrak{p}_1$为 $\mathcal{O}_K$中位于 p上方的一个素理想。我们将证明，当且仅当 $\chi_p(d_K) = 1$时， $\mathfrak{p}_1^t$ 不是主理想。

- 情况 1： $\chi_p(d_K) = -1$。在这种情况下， p 在 $\mathcal{O}_K$中保持惰性，因此 $\mathfrak{p}_1 = (p)$和$\mathfrak{p}_1^t = (p^t)$是主理想。
- 情况 2： $\chi_p(d_K) = 0$。这意味着 p 分歧，因此 $p\mathcal{O}_K = \mathfrak{p}_1^2$。因此$\mathfrak{p}_1^t = p^{t_1}\mathcal{O}_K$。
- 情况 3： $\chi_p(d_K) = 1$。在这种情况下， p在 $\mathcal{O}_K$中分裂。设 $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$，于是 $N(\mathfrak{p}_1) = p$且 $N(\mathfrak{p}_1^t) = p^t$且 $\mathfrak{p}_1 \neq \mathfrak{p}_2$。现在，若 $\mathfrak{p}_1^t$是主理想，设 $\mathfrak{p}_1^t = \alpha\mathcal{O}_K$，则$N(\alpha) = p^t$。由于 $\mathcal{O}_K$是由$1, 2$生成的 $\mathbb{Z}$模的子集， $\frac{\sqrt{d_K}}{2}$，令$\alpha = \frac{a+b\sqrt{d_k}}{2}$。于是 $\frac{a^2}{4} - d_k\frac{b^2}{4} = p^t$。然而 $-\frac{d_k}{4} > N^t > p^t$，所以 $b = 0$。因此 $a = \pm 2p^{t_1}$且 $\alpha = \pm p^{t_1}$。这意味着 $\mathfrak{p}_1^t = \alpha\mathcal{O}_K = p^{t_1}\mathcal{O}_K$。但是$p^{t_1}\mathcal{O}_K = \mathfrak{p}_1^{t_1}\mathfrak{p}_2^{t_1}$。由此可见 $\mathfrak{p}_1 = \mathfrak{p}_2$，这就矛盾了。

令 Y_K' 表示有理素数 p 的集合，其中 $\mathcal{O}_K$ 在 p 上方至少有一个素理想 $\mathfrak{p}$ 不是主理想。因此，我们看到，对于 $d_K < -4N^t$，有

$$\frac{\mathbb{P}_n\big[\langle [\mathfrak{p}], \mathfrak{p} \in X(K,\gamma)\rangle \text{ is } t\text{-torsion}\big]}{g_n(d_K)} = \prod_{p\in Y_K',\, p\geq N} \alpha_{p,n} \prod_{p\geq N, \chi_p(d_K)=1} \alpha_{p,n}^{-1}.$$

最后，注意到

$$\prod_{p\in Y_K',\, p\geq N} \alpha_{p,n} \prod_{p\geq N, \chi_p(d_K)=1} \alpha_{p,n}^{-1} \leq \prod_{p\geq N} \alpha_{p,n}^{-1} \leq 1 + \frac{1}{(n-1)(N-1)^{n-1}},$$

and

$$\prod_{p\in Y_K',\, p\geq N} \alpha_{p,n} \prod_{p\geq N, \chi_p(d_K)=1} \alpha_{p,n}^{-1} \geq \prod_{p\geq N} \alpha_{p,n} \geq 1 - \frac{1}{(n-1)(N-1)^{n-1}}.$$

由于 N 是任意的，证毕。 □

定理 1.14. 设 G 是一个非 2-挠有限阿贝尔群（特别地， G 非平凡）。固定 $n \geq 2$。对于每个虚二次域 K，记其判别式为 d_K。则有

$$\lim_{d_K\to-\infty} \mathbb{P}_n\big[\langle [\mathfrak{p}], \mathfrak{p} \in X(K,\gamma)\rangle \cong G\big] = 0.$$

证明.设 $|G| = m$。若 m 为奇数，则由推论 6.3.1 即得结论。因此，设 m 为偶数。由于 G 不是 2-挠，我们看到

$$\begin{aligned}&\mathbb{P}_n\big[\langle [\mathfrak{p}], \mathfrak{p} \in X(K,\gamma)\rangle \cong G\big]\\ &\leq \mathbb{P}_n\big[\langle [\mathfrak{p}], \mathfrak{p} \in X(K,\gamma)\rangle \text{是 } m\text{-挠}\big] - \mathbb{P}_n\big[\langle [\mathfrak{p}], \mathfrak{p} \in X(K,\gamma)\rangle \text{是 2-挠}\big].\end{aligned}$$

因此 ，

$$\limsup_{d_K\to-\infty} \frac{\mathbb{P}_n\big[\langle [\mathfrak{p}], \mathfrak{p} \in X(K,\gamma)\rangle \cong G\big]}{g_n(d_K)} \leq 1 - 1 = 0,$$

因此

$$\lim_{d_K\to-\infty}\frac{\mathbb{P}_n\big[\langle[\mathfrak{p}],\mathfrak{p}\in X(K,\gamma)\rangle\cong G\big]}{g_n(d_K)}=0.$$

接下来，注意到对于任意 d_K，我们有

$$g_n(d_K)=\prod_{p:\,\chi_p(d_K)=1}\alpha_{p,n}\geq\prod_p\alpha_{p,n}=\frac{\zeta(n+1)}{\zeta(n)}.$$

因此，我们可以得出

$$\lim_{d_K\to-\infty}\mathbb{P}_n\big[\langle[\mathfrak{p}],\mathfrak{p}\in X(K,\gamma)\rangle\cong G\big]=0.\qquad\square$$

7. $r_K(p)$ 的分布

本节考察当我们从代数整数 $\mathcal{A}'_m(H)$ 中取样 α 时，素数 p 在 $\mathcal{O}_{\mathbb{Q}(\alpha)}$ 中的分解情况。我们的目标是证明定理 1.15。记

$$\mathcal{F}_m(H)=\{f\in\mathbb{Z}[x]\mid\deg(f)=m,H(f)\leq H,f\text{ is monic}\},$$

and

$$\mathcal{L}'_m(H)=\{f(x)\in\mathcal{F}_m(H)\mid f\text{ is irreducible in }\mathbb{Z}[x]\}.$$

显然，$\#\mathcal{A}'_m(H)=m\#\mathcal{L}'_m(H)$。由引理 3.4 可知，$\#\mathcal{L}'_m(H)=(2H+1)^m+O(H^{m-\frac12}\log(H))$。此外，注意到 $\#\mathcal{F}_m(H)=(2H+1)^m$。这意味着 $\mathcal{F}_m(H)-\mathcal{L}'_m(H)=O(H^{m-\frac12}\log(H))$ 且 $\lim_{H\to\infty}{}^{\mathcal{L}'_m(H)}\mathcal{F}_m(H)=1$。

引理 7.1。给定一个正整数 m 和一个子集 $A\subseteq\bigcup_{H=1}^\infty\mathcal{F}_m(H)$。那么

$$\lim_{H\to\infty}\frac{\#(A\cap\mathcal{L}'_m(H))}{\#\mathcal{L}'_m(H)}=\lim_{H\to\infty}\frac{\#(A\cap\mathcal{F}_m(H))}{\#\mathcal{F}_m(H)}.$$

证明。假设 $\lim_{H\to\infty}\#(A\cap\mathcal{F}_m(H))\,\#\mathcal{F}_m(H)=a$。那么我们有

$$\limsup_{H\to\infty}\frac{\#(A\cap\mathcal{L}'_m(H))}{\#\mathcal{L}'_m(H)}\leq\limsup_{H\to\infty}\frac{\#(A\cap\mathcal{F}_m(H))}{\#\mathcal{L}'_m(H)}=\lim_{H\to\infty}\frac{\#(A\cap\mathcal{F}_m(H))}{\#\mathcal{F}_m(H)}=a.$$

进一步，注意到

$$\begin{aligned}\liminf_{H\to\infty}\frac{\#(A\cap\mathcal{L}'_m(H))}{\#\mathcal{L}'_m(H)}&\geq\liminf_{H\to\infty}\frac{\#(A\cap\mathcal{F}_m(H))-\#(\mathcal{F}_m(H)\setminus\mathcal{L}'_m(H))}{\#\mathcal{F}_m(H)}\\&=\lim_{H\to\infty}\frac{\#(A\cap\mathcal{F}_m(H))}{\#\mathcal{F}_m(H)}-\lim_{H\to\infty}\frac{O(H^{m-\frac12}\log(H))}{(2H+1)^m}=a.\end{aligned}\qquad\square$$

记

$$\mathcal{F}_{m,p}=\{f(x)\in(\mathbb{Z}/p\mathbb{Z})[x]\mid\deg(f)=m,f\text{ is monic}\}.$$

引理 7.2. 给定 $m \in \mathbb{Z}_{>0}$ 和素数 $p \geq m$，我们有 $\#\{f \in \mathcal{F}_{m,p} \mid \text{判别式}(f) = 0\} \leq p^{m-1}m$。对于 $\alpha \in \mathcal{A}'_m(H)$，若 $p \mid [\mathcal{O}_{\mathbb{Q}(\alpha)} : \mathbb{Z}[\alpha]]$，则 $p \mid \text{判别式}(\alpha)$。此外，我们有

$$\limsup_{H\to\infty} \frac{\#\{\alpha \in \mathcal{A}'_m(H) \mid p \mid Disc(\alpha)\}}{\#\mathcal{A}'_m(H)} \leq \frac{m}{p}.$$

证明。写作 $f(x) = x^m + a_1x^{m-1} + \cdots + a_m$，我们知道 $\text{Disc}(f)$ 是关于 $a_1, a_2, \ldots, a_m$ 的多项式。将其写为 $\sum_{i=0}^{m} f_i(a_1, \ldots, a_{m-2}, a_m)a_{m-1}^i$。由引理 3.5 可知，$f_m(a_1, \ldots, a_{m-2}, a_m) = \pm(m-1)^{m-1}$。一旦选定 $a_1, \ldots, a_{m-2}, a_m \in \mathbb{Z}/p\mathbb{Z}$，对于 a_{m-1} 至多有 m 种选择。因此，$\#\{f \in \mathcal{F}_{m,p} \mid \text{Disc}(f) = 0\} \leq p^{m-1}m$。

我们知道，对于任意 $\alpha \in \overline{\mathbb{Z}}$，都有 $\mathbb{Z}[\alpha] \subseteq \mathcal{O}_{\mathbb{Q}(\alpha)} \subseteq \frac{1}{\text{判别式}(\alpha)}\mathbb{Z}[\alpha]$。因此，$[\mathcal{O}_{\mathbb{Q}(\alpha)} : \mathbb{Z}[\alpha]] \mid \text{Disc}(\alpha)^m$。所以，若 $p \mid [\mathcal{O}_{\mathbb{Q}(\alpha)} : \mathbb{Z}[\alpha]]$，则 $p \mid \text{Disc}(\alpha)$。最后，注意到

$$\begin{aligned}
\frac{\#\{\alpha \in \mathcal{A}'_m(H) \mid p \mid \text{Disc}(\alpha)\}}{\#\mathcal{A}'_m(H)} &= \frac{\#\{f \in \mathcal{L}'_m(H) \mid p \mid \text{Disc}(f)\}}{\#\mathcal{L}'_m(H)} \\
&\leq \frac{\#\{f \in \mathcal{F}_m(H) \mid p \mid \text{Disc}(f)\}}{(2H+1)^m + O(H^{m-\frac{1}{2}}\log(H))} \\
&\leq \frac{\#\{f \in \mathcal{F}_{m,p} \mid \text{Disc}(f) = 0\}(\frac{2H+1}{p} + 1)^m}{(2H+1)^m + O(H^{m-\frac{1}{2}}\log(H))} \\
&\leq \frac{p^{m-1}m(\frac{2H+1}{p} + 1)^m}{(2H+1)^m + O(H^{m-\frac{1}{2}}\log(H))} \\
&= \frac{1}{p}\frac{m}{\left(\frac{2H+1}{2H+1+p}\right)^m + O\left(\left(\frac{H}{2H+1+p}\right)^m \frac{\log(H)}{\sqrt{H}}\right)}.
\end{aligned}$$

因此，

$$\limsup_{H\to\infty} \frac{\#\{\alpha \in \mathcal{A}'_m(H) \mid p \mid \text{Disc}(\alpha)\}}{\#\mathcal{A}'_m(H)} \leq \frac{m}{p}. \qquad \square$$

给定 $1 \leq i \leq m$ 和素数 p，记

$$f(m, i, p) = \frac{\#\{f \in \mathcal{F}_{m,p} \mid f \text{ has exactly } i \text{ distict irreducible factors}\}}{\#\mathcal{F}_{m,p}},$$

及 $f(m, i) = \lim_{p\to\infty} f(m, i, p)$。

引理 7.3. 给定 $1 \leq i \leq m$ 和一个素数 $p \geq m$，我们有 $g(m, i, p) = f(m, i, p) + O(\frac{1}{p})$。因此 $g(m, i) = f(m, i)$。

证明。假设存在 $\alpha \in \mathcal{A}'_m(H)$，使得 $p \nmid \text{Disc}(\alpha)$。那么我们知道 $p \nmid [\mathcal{O}_{\mathbb{Q}(\alpha)} : \mathbb{Z}[\alpha]]$。因此，根据戴德金-库默尔定理，我们知道 $r_{\mathbb{Q}(\alpha)}(p) = i$ 当

且仅当 α 的最小多项式模 p 分解为 i 个互不相同的因子时。因此，我们看到

$$\begin{aligned}
g(m,i,p) &= \lim_{H\to\infty}\frac{\#\{\alpha\in\mathcal{A}'_m(H)\mid r_{\mathbb{Q}(\alpha)}(p)=i\}}{\#\mathcal{A}'_m(H)}\\
&= \lim_{H\to\infty}\frac{\#\{\alpha\in\mathcal{A}'_m(H)\mid r_{\mathbb{Q}(\alpha)}(p)=i, p\nmid \mathrm{Disc}(\alpha)\}}{\#\mathcal{A}'_m(H)}+O\Big(\frac{1}{p}\Big)\\
&= \lim_{H\to\infty}\frac{\#\{f\in\mathcal{L}'_m(H)\mid f \bmod p \text{ has } i \text{ distinct factors}, p\nmid \mathrm{Disc}(f)\}}{\#\mathcal{L}'_m(H)}+O\Big(\frac{1}{p}\Big)\\
&= \lim_{H\to\infty}\frac{\#\{f\in\mathcal{F}_m(H)\mid f \bmod p \text{ has } i \text{ distinct factors}, p\nmid \mathrm{Disc}(f)\}}{\#\mathcal{F}_m(H)}+O\Big(\frac{1}{p}\Big)\\
&= \lim_{H\to\infty}\frac{f(m,i,p)p^m(\frac{2H+1}{p}+O(1))^m}{(2H+1)^m}+O\Big(\frac{1}{p}\Big)=f(m,i,p)+O\Big(\frac{1}{p}\Big).
\end{aligned}$$ □

现在，我们的任务归结为计算 $f(m,i)$。令 $a_m(p)$ 表示 $(\mathbb{Z}/p\mathbb{Z})[x]$ 中次数为 m 的首一不可约多项式的个数。众所周知，

$$a_m(p)=\frac{1}{m}\sum_{d\mid m}\mu(\frac{m}{d})p^d=\frac{1}{m}p^m+O(p^{\frac{m}{2}}).$$

若 λ 是一个分拆，则将 i 在 λ 中出现的次数记作 $b_i(\lambda)$。令 $\mathcal{P}(m,i)$ 表示将 m 分拆为 i 个部分的所有分拆构成的集合。

引理 7.4。 给定 $1\le i\le m$，我们有

$$f(m,i)=\sum_{\lambda\in\mathcal{P}(m,i)}\prod_{n=1}^{m}\frac{1}{n^{b_n(\lambda)}b_n(\lambda)!}.$$

证明。 首先注意到，当且仅当 $\mathrm{Disc}(f)=0$ 时，f 有重根。接下来，对于每个满足 $\mathrm{Disc}(f)\neq 0$ 的 $f\in\mathcal{F}_{m,p}$，关联分拆 λ，使得 $b_n(\lambda)$ 是 f 的次数为 n 的不可约因子的数量。现在注意到

$$\begin{aligned}
f(m,i,p)&=\frac{\#\{f\in\mathcal{F}_{m,p}\mid f \text{ has exactly } i \text{ distict irreducible factors}\}}{\#\mathcal{F}_{m,p}}\\
&=\frac{\#\{f\in\mathcal{F}_{m,p}\mid \mathrm{Disc}(f)=0\}}{\#\{f\in\mathcal{F}_{m,p}\}}+\sum_{\lambda\in\mathcal{P}(m,i)}\frac{\#\{f\in\mathcal{F}_{m,p}\mid f \text{ associated to } \lambda\}}{\#\{f\in\mathcal{F}_{m,p}\}}\\
&=O\Big(\frac{1}{p}\Big)+\sum_{\lambda\in\mathcal{P}(m,i)}\frac{1}{p^m}\prod_{n=1}^{m}\binom{a_n(p)}{b_n(\lambda)}
\end{aligned}$$

$$= O\Big(\frac{1}{p}\Big) + \sum_{\lambda\in\mathcal{P}(m,i)} \frac{1}{p^m} \prod_{n=1}^{m} \frac{(a_n(p)+O(1))^{b_n(\lambda)}}{b_n(\lambda)!}$$
$$= O\Big(\frac{1}{p}\Big) + \sum_{\lambda\in\mathcal{P}(m,i)} \frac{1}{p^m} \prod_{n=1}^{m} \frac{(\frac{1}{n}p^n+O(p^{\frac{n}{2}}))^{b_n(\lambda)}}{b_n(\lambda)!}$$
$$= \sum_{\lambda\in\mathcal{P}(m,i)} \frac{1}{p^m} \prod_{n=1}^{m} \frac{\frac{1}{n^{b_n(\lambda)}}p^{nb_n(\lambda)}+O(p^{nb_n(\lambda)-\frac{n}{2}})}{b_n(\lambda)!} + O\Big(\frac{1}{p}\Big)$$
$$= \sum_{\lambda\in\mathcal{P}(m,i)} \prod_{n=1}^{m} \frac{1}{n^{b_n(\lambda)}b_n(\lambda)!} + O\Big(\frac{1}{p}\Big). \qquad \square$$

定理 1.15。给定 m 和 i，满足 $1 \le i \le m$，$g(m,i)$ 是 y^i 在 $\prod_{j=0}^{m-1}(y+j)m!$ 中的系数。

证明。我们知道 $g(m,k) = \sum_{\lambda\in\mathcal{P}(m,k)} \prod_{n=1}^{m} \frac{1}{n^{b_n(\lambda)}b_n(\lambda)!}$。现在考虑幂级数

$$\sum_{m=0}^{\infty}\sum_{k=1}^{m} x^m y^k g(m,k) = \sum_{m=0}^{\infty}\sum_{k=1}^{m} x^m y^k \sum_{\lambda\in\mathcal{P}(m,k)} \prod_{n=1}^{m} \frac{1}{n^{b_n(\lambda)}b_n(\lambda)!} = \prod_{n=1}^{\infty}\Big(1+\sum_{l=1}^{\infty}\frac{x^{nl}y^l}{l!n^l}\Big)$$
$$= \prod_{n=1}^{\infty}\exp\Big(\frac{x^n y}{n}\Big) = \exp\Big(y\sum_{n=1}^{\infty}\frac{x^n}{n}\Big) = \exp\Big(-y\log(1-x)\Big)$$
$$= (1-x)^{-y} = \sum_{m=0}^{\infty}\binom{-y}{m}(-1)^m x^m = \sum_{m=0}^{\infty}\frac{\prod_{j=0}^{m-1}(y+j)}{m!}x^m$$

因此，$g(m,k)$ 是 $\prod_{j=0}^{m-1}(y+j)\ m!$ 中 y^k 的系数。 $\square$

参考文献

[1] S. Arno, M.L. Robinson, F. S. Wheeler，《代数数与整系数多项式的分母》，数论杂志，第 57 卷，第 2 期，1996 年，第 292–302 页。[2] R. P. Boas，《整函数》。Academic Press。（1954）。[3] E. Bombieri, J. Pila，《弧线和椭圆上的整点数》，杜克数学杂志，Duke Math. J. 59(2), 337–357，（1989）[4] S. D. Cohen，《伽罗瓦群的分布与希尔伯特不可约性定理》，伦敦数学会会刊，第 s3-43 卷，第 2 期，1981年9月，第 227–250 页。[5] D. A. Cox，《形如 x2 + ny2 的素数：费马、类域论与复乘》（1989）。[6] P. Drungilas, A. Dubickas, J. Jankauskas，《关于由代数数及其共轭生成的环的关系》。数学年刊 194, 369–385（2015）。[7] J. Neukirch, A. Schmidt, K. Wingberg（2013）。第八章，第 3 节。载于《数域的上同调》。Springer。

[8] J. E. Nymann, 《关于 k 个正整数互素的概率》, 《数论杂志》4（1972）, 469–473。[9] G. Polya 和 G. Szego, 《分析中的问题与定理 II》, 施普林格出版社, 纽约, 1976。[10] D. Singhal, Y. Lin（2022）。《代数数分母中的素数》。arXiv:2211.13822[11] B. L. van der Waerden, 《可约方程及含有 Affekt 的方程的稀少性》, 《数学与物理月刊》, 43（1936）, 第 1 期, 133–147