Chapter 1: 从代数整数到理想类群

1.1 这一章在干什么？

代数数论在干的事情无非就是把我们在整数里面干的事情放在更大的数域里面再干一遍，但是由于更大的数域会有更复杂的结构，所以我们要发展更多的方法来研究一些全新的东西.

最基本的 ideal 就是唯一分解的性质，这个东西我们从小学就开始接触，在学习初等数论的时候我相信一定会知道一个东西叫做算数基本定理，说的是**所有正整数都可以唯一分解为不同素数的乘积**.

但是不幸运的事情是，这件事情在一些环里面是做不到的，比如考虑 $\mathbb{Z}[\sqrt{-5}]$ 就不是一个 UFD，因为

$$6 = 2 \times 3 = (1+\sqrt{-5})(1-\sqrt{-5})$$

这件事情会导致我们无法像在整数里面进行一些素数的分解，这是一件很难受的事情，这个东西让我们很难像初等数论一样考虑一些模掉素数的操作.

幸运的是我们在某些情况下会有素理想的唯一分解，比如在 $\mathbb{Z}$ 中，我们就知道

$$(pq) = (p)(q)$$

当 $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ 时，我们有

$$(n) = \prod_{i=1}^{k} (p_i)^{\alpha_i}$$

这件事情在一般的 Dedekind domain 中都可以成立，而我们会在后面看到数域的代数整数环都是 Dedekind domain，这为我们的研究提供了很大的便利.

但是事实其实仍然不像整数中那样方便，因为 Dedekind domain 中的素理想模样可能并不是由素元生成的主理想，还可能是两个元素生成的理想，这就引导出了分式理想和理想类群的概念.

在基本的代数数论中，最重要的定理其实就是数域的理想类群是有限的.

在研究的过程中我们毫无疑问需要一些工具来帮我们研究，我们会遇到一些基础的域的不变量，也就是 trace，norm，和 discriminant. 在此基础上我们可以发展出理想的 norm. 再结合一些“数的几何”，我们可以得到很多很好的结果.

1.2 数域与代数整数环

当我们说一个域 K 是数域的时候，我们实际上是在说 K 是 $\mathbb{Q}$ 的一个有限扩张，我们知道 $\mathbb{Z}$ 在 K 中的整闭包构成了 K 的一个子环，我们记为 $\mathcal{O}_K$，称为 K 的**代数整数环**.

那么肯定想问什么是整元，在一般的环 R 中，如果对于 x，存在 $a_1, \cdots, a_n \in R$，使得

$$x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n = 0$$

那么就称 x 在 R 上是**整元**. 对于整元的研究可以在一些交换代数的书上找到，我们并不十分关注这些东西，只需要一些最基础的结果.

一个有趣的问题是，如果 x 是整元，y 也是整元，那么 $x+y$ 与 xy 是否仍然是整元？这个问题的答案是肯定的，我们即将看到整元是构成环的，但是我们会有两个路径来得到这个结论，我们先看一个比较 tricky 的方法.

考虑 x,y 都是 R 上的整元，哦忘记说了，在代数数论里面，我们一般只讨论有幺元的交换环，所以在没有特别提及的情况下所有的环 R 都是交换幺环. 考虑 x,y 满足的方程

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0, \quad y^m + b_{m-1}y^m + \cdots + b_1 y + b_0 = 0$$

我们知道 x,y 分别是下面两个矩阵的特征值：

$$A = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ -a_0 & -a_1 & -a_2 & \dots & -a_{n-1} \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ -b_0 & -b_1 & -b_2 & \dots & -b_{m-1} \end{pmatrix}$$

于是通过一些线性代数的知识我们知道 $x+y$ 与 xy 分别是下面两个矩阵的特征值

$$A \otimes I_m + I_n \otimes B, \quad A \otimes B$$

由于矩阵的特征多项式一定是首一的，所以自然而然就有 $x+y, xy$ 仍然是整元，所以整元构成一个环.

上面的方法是构造性的，下面我们给出一个稍微本质一些的看法，利用有限生成模来刻画在有些时候会更加方便.

我们先介绍一个技术性引理：

引理 1.2.1

M 是有限生成 A 模，$\mathfrak{a}$ 是 A 的一个理想，φ 是 M 的一个自同态，且 $\varphi(M) \subset \mathfrak{a}M$，则存在 $a_1, \cdots, a_n \in \mathfrak{a}$，使得

$$\varphi^n + a_1\varphi^{n-1} + \cdots + a_n = 0$$

证明: 令 x_i 为 M 的生成元，有 $\varphi(x_i) = \sum a_{ij}x_j$.

则我们有

$$0 = \varphi(x_i) - \sum_{j=1}^{n} a_{ij}x_j = \sum_{j=1}^{n} (\delta_{ij}\varphi - a_{ij})(x_j) = 0$$

令

$$P = \begin{pmatrix} \varphi - a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & \varphi - a_{22} & \cdots & -a_{2n} \\ \vdots & \vdots & & \vdots \\ -a_{n1} & -a_{n2} & \cdots & \varphi - a_{nn} \end{pmatrix}$$

我们知道

$$P \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = 0$$

令 P^* 为 P 的伴随，有 $P^*P = \det(P)I$，我们有

$$\operatorname{diag}\{\det(P), \cdots, \det(P)\} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = 0$$

也就是 $\det(P)x_i = 0$，而注意到 $\det(P)$ 是一个关于 φ 的首一 n 次多项式，从而成立. □

命题 1.2.1: 整元的刻画

$A \subset B$，则 *TFAE:*

(1) $x \in B$ 是 A 上的整元.

(2) $A[x]$ 是有限生成 A 模.

(3) $A[x]$ 包含于 B 的一个子环 C，其中 C 是有限生成 A 模.

(4) 存在一个忠实的 $A[x]$-模 M*(*即 $\operatorname{Ann}_{A[x]}(M) = 0$*)*，作为 A 模是有限生成的.

证明: (1) 推 (2)：显然.

(2) 推 (3)：取 $C = A[x]$ 即可.

(3) 推 (4)：取 $M = A[x]$，容易知道 $1 \in M$，从而忠实.

(4) 推 (1)：考虑 M 到自身的同态 $x\colon M \to M$，$m \mapsto xm$，由于 M 作为 A 模是有限生成的，引理告诉我们存在 $a_1, \cdots, a_n \in A$ 使得有

$$x^n + a_1x^{n-1} + \cdots + a_n = 0$$

从而 $x^n + \cdots + a_n \in A[x]$ 将 M 零化，因此由忠实性我们知道

$$x^n + a_1x^{n-1} + \cdots + a_n = 0 \in A[x]$$

于是我们知道 $x \in B$ 在 A 上是整元. □

定义 1.2.1: 整闭包与整闭性

设 $A \subset B$ 为子环，令

$$C := \{b \in B\colon b \text{ 是 } A \text{ 上的整元}\}$$

称 C 为 A 在 B 中的**整闭包**，如果 $C = A$，则称 A 在 B 中是**整闭的**. 如果 $C = B$，则称 B **在** A **上是整的**.

现在我们知道 $\mathscr{O}_K$ 到底是什么意思了，也就是说 $\mathbb{Z} \subset \mathbb{Q} \subset K$ 是 K 的一个子环，所有在 $\mathbb{Z}$ 上整的数构成了 K 的一个子环，为 $\mathbb{Z}$ 在 K 中的整闭包. 我们称 $\mathbb{Z}$ 上的整元为**代数整数**，$\mathscr{O}_K$ 就是所有代数整数构成的环，所以叫代数整数环.

作为一些例子，我们可以来计算一下二次域的代数整数环是什么. 给定一个无平方因子的整数 d，令 $K = \mathbb{Q}(\sqrt{d})$，设 x 是 K 中的代数整数，设 $x = a + b\sqrt{d}(b \neq 0)$，我们知道 x 的最低次的零化首一多项式为

$$x^2 - 2a + (a^2 - b^2d) = 0$$

我们需要 $2a$，a^2-b^2d 都是整数，这个时候需要对 d 模 4 的余数进行讨论，通过一些简单的初等数论我们知道下面的结论

$$\mathscr{O}_F=\begin{cases}\mathbb{Z}[\sqrt{d}], & d\equiv 2,3 \mod 4\\ \mathbb{Z}[(1+\sqrt{d})/2], & d\equiv 1 \mod 4\end{cases}$$

更多的例子我们会在后面的实操环节中给出.

1.3 代数整数环是 Dedekind domain

为了说明这个事情我们需要一系列准备，这些准备会帮我们说明 $\mathscr{O}_K$ 是一个一维的，整闭的，Noether 的整环.

而我们如果用 fancy 一点的说法就是说 $\mathscr{O}_K$ 是一个 Dedekind domain. 之所以谈论 Dedekind domain 是因为它有很好的性质，这个我们在第一节中就已经提到过，在其中有美好的性质，即素理想唯一分解，我们会在后面来说明. 这一节主要来证明它是一个 Dedekind domain.

1.3.1 Norm 与 Trace

考虑一个数域 $K/\mathbb{Q}$，设 $n=[K:\mathbb{Q}]$，则我们可以考虑从 K 到 $\mathbb{C}$ 的嵌入，一个从 K 到 $\mathbb{C}$ 的嵌入实际上就是一个域同态，我们现在开始思考如何确定这些嵌入到底是什么.

由于 $\mathbb{Q}$ 是特征零的，所以我们知道 K 是 $\mathbb{Q}$ 的有限可分扩张，于是由本原元定理知道是单扩张，我们可以写成 $K=\mathbb{Q}(\alpha)$，由于域同态是保证素域 $\mathbb{Q}$ 中元素不变的，所以 $\sigma\colon K\to\mathbb{C}$ 完全由 $\sigma(\alpha)$ 决定，又由于 $\sigma(\alpha)$ 仍然满足 α 在 $\mathbb{Q}$ 上的极小多项式，于是 $\sigma(\alpha)$ 只有 $[K:\mathbb{Q}]=n$ 个选择，也就是说从 K 到 $\mathbb{C}$ 有且仅有 n 个嵌入，我们记为

$$\sigma_1,\cdots,\sigma_{r_1},\quad \sigma_{r_1+1},\cdots,\sigma_{r_1+r_2},\overline{\sigma_{r_1+1}},\cdots,\overline{\sigma_{r_1+r_2}}$$

其中 $\sigma_1,\cdots,\sigma_{r_1}$ 为实嵌入，$\sigma_{r_1+1},\cdots,\sigma_{r_1+r_2},\overline{\sigma_{r_1+1}},\cdots,\overline{\sigma_{r_1+r_2}}$ 为复嵌入及其共轭. 我们自然有一个关系

$$r_1+2r_2=n$$

并且我们可以得到一个很好的嵌入

$$\begin{aligned}K &\to \mathbb{R}^{r_1}\times\mathbb{C}^{r_2}\\ x &\mapsto (\sigma_1(x),\cdots,\sigma_{r_1}(x),\sigma_{r_1+1}(x),\cdots,\sigma_{r_1+r_2}(x))\end{aligned}$$

Note 1.3.1

实际上这个映射也可以来自

$$K\hookrightarrow K\otimes_{\mathbb{Q}}\mathbb{R},\quad x\mapsto x\otimes 1$$

与实线性空间的同构

$$K\otimes_{\mathbb{Q}}\mathbb{R}\to\mathbb{R}^{r_1}\times\mathbb{C}^{r_2}$$

我可以详细解释一下，设 $K=\mathbb{Q}(\alpha)$，$p(x)$ 为 α 在 $\mathbb{Q}$ 上的极小多项式，我们有

$$K\cong Q[x]/(p(x))$$

于是有

$$K\otimes_{\mathbb{Q}}\mathbb{R}\cong(\mathbb{Q}[x]/(p(x)))\otimes_{\mathbb{Q}}\mathbb{R}\cong\mathbb{R}[x]/(p(x))$$

第二个同构是张量积替换系数导致的，详细的说就是如果有环的同态 $A\to B$，则有

$$A[x]\otimes_A B\cong B[x]$$

一个比较简单的看法是

$$A[x] \otimes_A B \cong \left(\bigoplus_{i=0}^{\infty} Ax^i\right) \otimes_A B \cong \bigoplus_{i=0}^{\infty} (Ax^i \otimes_A B)$$

又由于 $Ax^i \cong A$，这个同构是自然的，所以我们有

$$\bigoplus_{i=0}^{\infty} (Ax^i \otimes_A B) \cong \bigoplus_{i=0}^{\infty} (A \otimes_A B) \cong \bigoplus_{i=0}^{\infty} B \cong \bigoplus_{i=0}^{\infty} Bx^i = B[x]$$

好现在回来，我们如何去分析 $\mathbb{R}[x]/(p(x))$ 的结构呢？虽然 $p(x)$ 在 $\mathbb{Q}$ 上不可约，但是它在 $\mathbb{R}$ 上一般是可约的，我们知道 $\mathbb{R}$ 上的不可约多项式只有两种，一种是一次因式，一种是不可约的二次多项式，所以 $p(x)$ 可以分解为一堆一次因式的乘积和一堆不可约二次多项式的乘积.

一次因式形如 $(x-\alpha_i)$，对应 $p(x)$ 的每个实根 α_i，这样的因子有 r_1 个.

二次因式形如 (x^2+bx+c)，对应 $p(x)$ 的每一对共轭复根 $\beta_j, \overline{\beta_j}$. 这样的因子有 r_2 个.

所以，$p(x)$ 在 $\mathbb{R}[x]$ 中可以分解为：

$$p(x) = \prod_{i=1}^{r_1} (x-\alpha_i) \cdot \prod_{j=1}^{r_2} q_j(x)$$

其中 $q_j(x)$ 是对应第 j 对共轭复根的二次不可约多项式. 由于这些因子在 $\mathbb{R}[x]$ 中是互素的，根据中国剩余定理，我们有环的同构：

$$\mathbb{R}[x]/(p(x)) \cong \left(\bigoplus_{i=1}^{r_1} \frac{\mathbb{R}[x]}{(x-\alpha_i)}\right) \oplus \left(\bigoplus_{j=1}^{r_2} \frac{\mathbb{R}[x]}{(q_j(x))}\right) \cong \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$$

跑题了，我们现在回来定义我们的 Trace 与 Norm，对于 $\alpha \in K$，我们定义

$$T_{K/\mathbb{Q}}(\alpha) = \sum_{i=1}^{n} \sigma(\alpha), \quad N_{K/\mathbb{Q}}(\alpha) = \prod_{i=1}^{n} \sigma(\alpha)$$

我们很容易说明这样定义的 trace 和 norm 都是落在 $\mathbb{Q}$ 中的，我们有若干种思考的方式，其中最本质的我认为是利用 Galois 理论来说明，考虑 $\mathbb{Q}$ 的代数闭包 $\overline{\mathbb{Q}}$，对任意的 $\tau \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$，我们知道

$$\tau(T_{K/\mathbb{Q}}(\alpha)) = \sum_{i=1}^{n} \tau \circ \sigma_i(\alpha)$$

我们容易知道 $\{\tau \circ \sigma_i\}$ 其实就是 $\{\sigma_i\}$ 的一个置换，于是 $T_{K/\mathbb{Q}}(\alpha)$ 落在不变子域里面，所以在 $\mathbb{Q}$ 中，对于 norm 是同理的. 其实我们还有很多不同的视角，我们在此时其实并不特别关心，更多的内容放在本章的拾遗中. 目前来说只知道定义就非常足够了.

1.3.2 数的几何 1: Lattice

这一块其实可以直接承认，然后跳过证明，都是一些技术性质的内容. 考虑域 k 为 $\mathbb{Q}$ 或者 $\mathbb{R}$，则一个 k 上有限维线性空间 V 的**格(lattice)** Λ 是一个 V 的离散加法子群并且 $k\Lambda = V$. 其中离散的意思是 V 的每一个有界子集都只含有有限个 Λ 中的元素.

注意 $k\Lambda$ 在这里的意思是对 Λ 进行线性扩张，即

$$k\Lambda = \{tv \mid t \in k, v \in \Lambda\}$$

也就是说这个格 Λ 是 full rank 的，我们有下面的结论：

命题 1.3.1

V 是一个有限维 k-线性空间，$\Lambda \subset V$ 是一个 $\mathbb{Z}$-模，并且 $k\Lambda = V$. 令 $n = \dim_k V$，*TFAE:*

(1) Λ 是离散的.

(2) Λ 由 n 个元素生成.

(3) $\Lambda \cong \mathbb{Z}^n$ *as* $\mathbb{Z}$-模.

证明: 证明我现在不想敲，可以参见 Baker p 13. □

1.3.3 整数环与其理想是Lattice

我们现在回来研究一下 $\mathscr{O}_K$ 的结构，我们直接给出一个 claim，告诉我们 $\mathscr{O}_K$ 在 K 中的结构是怎样的，这会帮助我们研究很多东西.

定理 1.3.1

数域 K 是 $\mathbb{Q}$ 的 n 次扩张，把 K 看成 $\mathbb{Q}$ 的 n-维线性空间，则 $\mathscr{O}_K$ 是 K 中的一个 *lattice.*

证明: 我们要使用上面的等价关系，这需要先说明 $\mathscr{O}_K$ 可以张成 K，我们取定一组 K 的 $\mathbb{Q}$-基

$$\alpha_1, \cdots, \alpha_n$$

我们知道 α_i 是代数数，于是肯定满足一个首一有理系数的方程

$$\alpha_i^m + \frac{a_{m-1}}{b_{m-1}}\alpha_i^{m-1} + \cdots + \frac{a_1}{b_1}\alpha_i + \frac{a_0}{b_0} = 0$$

我们大胆一点，直接让 $s = b_0 b_1 \cdots b_{m-1}$，则在等式两边同时乘 s^m，有

$$(s\alpha_i)^m + \frac{sa_{m-1}}{b_{m-1}}(s\alpha_i)^{m-1} + \cdots + \frac{s^{m-1}a_1}{b_1}(s\alpha_i) + \frac{s^m a_0}{b_0} = 0$$

所以 $s\alpha_i$ 是一个代数整数，即 $s\alpha_i \in \mathscr{O}_K$. 因此我们知道 $\alpha_i \in \mathbb{Q}\mathscr{O}_K$，所以我们知道 $\mathbb{Q}\mathscr{O}_K = K$.
于是我们不妨假设从一开始 $\alpha_1, \cdots, \alpha_n$ 就都在 $\mathscr{O}_K$ 中，下面假设 $\mathscr{O}_K$ 不是离散的，也就是说在有界区域

$$S = \{\sum_{i=1}^n \lambda_i \alpha_i \in K \cong \mathbb{Q}^n \mid |\lambda_i| \leq 1\}$$

中，有无穷多个 $\mathscr{O}_K$ 中的元素，也就是说会存在任意小的某些 $|\lambda_i| \in \mathbb{Q}$ 使得对 $\alpha \in \mathscr{O}_K$，有

$$\alpha = \sum_{i=1}^n \lambda_i \alpha_i$$

这是因为对于任意的 $\varepsilon > 0$，满足绝对值大于等于 ε 的有理数总是只有有限多个，所以如果不离散，总是可以取到一些任意小的 λ_i，此时我们可以计算 α 的范数，即

$$N_{K/\mathbb{Q}}(\alpha) = \prod_{i=1}^n \left(\sum_{j=1}^n \lambda_j \sigma_i(\alpha_j)\right)$$

显然构成了一个关于 $\lambda_1, \cdots, \lambda_n$ 的 n 次齐次复系数多项式，那么由于 $|\lambda_i| \leq 1$，并且其中有某些 λ_i 可以任意小，所以存在非零的 α 使得

$$N_{K/\mathbb{Q}}(\alpha) < 1$$

但是由于 $\alpha \in \mathscr{O}_K$ 是代数整数，所以 $\sigma_i(\alpha)$ 也是代数整数，所以由于代数整数构成环，$N_{K/\mathbb{Q}}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)$ 还是代数整数，再结合范数落在 $\mathbb{Q}$ 中，我们知道 $\mathbb{Q}$ 中的代数整数只有整数，并且由于 α 非零，所以范数非零，于是

$$N_{K/\mathbb{Q}}(\alpha) \geq 1$$

矛盾，所以 $\mathscr{O}_K$ 是 K 的离散子群，于是由命题知道由 n 个元素生成，同构于 $\mathbb{Z}^n$. □

Note 1.3.2

另外一条路：容易知道 rank n，下面来说明离散. 只需要说明存在 $\omega_1, \cdots, \omega_n$ 使得

$$\mathscr{O}_K = \mathbb{Z}\omega_1 \oplus \cdots \oplus \mathbb{Z}\omega_n$$

前半部分同理，我们得到了 $\alpha_1, \cdots, \alpha_n \in \mathscr{O}_K$ 使得构成线性空间的一组基，则对于任意的 $\gamma \in \mathscr{O}_K$，都存在一组系数 $x_1, \cdots, x_n \in \mathbb{Q}$ 使得

$$\gamma = x_1\alpha_1 + \cdots + x_n\alpha_n$$

令 $\sigma_1, \cdots, \sigma_n$ 为 n 个嵌入，我们知道

$$\sigma_i(\gamma) = x_1\sigma_i(\alpha_1) + \cdots + x_n\sigma_i(\alpha_n)$$

利用 Cramer 法则，我们计算出

$$x_j = \frac{\gamma_j}{\delta}, \quad \delta = |\sigma_i(\alpha_j)|$$

其中的 γ_j 为使用 $\sigma_i(\gamma)$ 替换掉系数行列式的第 j 列得到的行列式，注意到 δ 是代数整数的多项式，从而仍然是代数整数，而

$$d := \delta^2 = d_K(\alpha_1, \cdots, \alpha_n) \in \mathbb{Z}$$

属于 $\mathbb{Z}$ 是因为判别式都是有理数，并且此处的判别式是代数整数的多项式，从而是代数整数，所以是有理整数，也就是 $\mathbb{Z}$. 于是我们知道

$$\gamma_j\delta = x_j d \in \mathbb{Q} \cap \mathscr{O}_K = \mathbb{Z}$$

于是令 $\gamma_j\delta = m_j \in \mathbb{Z}$，有

$$x_j = \frac{m_j}{d} \implies \gamma \in \mathbb{Z}\frac{\alpha_1}{d} \oplus \cdots \oplus \mathbb{Z}\frac{\alpha_n}{d}$$

注意到 d 与 γ 的选择无关，所以

$$\mathscr{O}_K \subset \mathbb{Z}\frac{\alpha_1}{d} \oplus \cdots \oplus \mathbb{Z}\frac{\alpha_n}{d}$$

于是 $\mathscr{O}_K$ 是 PID 上自由模的子模，从而自由，结合秩为 n，命题得证.

现在我们知道 $\mathscr{O}_K$ 作为自由 Abel 群的 rank 是 n，所以存在 $\alpha_1, \cdots, \alpha_n \in \mathscr{O}_K$，使得

$$\mathscr{O}_K = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n$$

我们称 $\alpha_1, \cdots, \alpha_n$ 是 $\mathscr{O}_K$ 的一组**整基**，注意这里的整基不一定是唯一的.

我们现在考虑 $\mathscr{O}_K$ 的理想 I 的结构，显然我们知道 I 作为 $\mathbb{Z}$-模是 $\mathscr{O}_K$ 的子模，由于 PID 上自由模的子模还是自由模，我们知道 I 是自由 $\mathbb{Z}$-模，并且由之前定理中的证明过程我们知道，对于任意的 $\alpha \in K$，都存在一个充分大的整数 m 使得 $m\alpha \in \mathscr{O}_K$，于是我们任取 $n \in I \cap \mathbb{Z}$(这里需要说明 $I \cap \mathbb{Z}$ 中有非零元，这个通过考虑 I 中某个元素的 Norm 立刻得到)，有 $nm\alpha \in I$，所以任给 K 的一组基 α_i，我们可以把它 scalar 一下放到 I 中，也就是说 I 会张成 K，即 $\mathbb{Q}I = K$. 再结合 I 是 $\mathscr{O}_K$ 的子模，所以由 $\mathscr{O}_K$ 的离散性知道 I 肯定是离散的，也就是说 I 也是 K 的一个 lattice.

我们把结论写成定理的推论：

推论 1.3.1

I 是 $\mathcal{O}_K$ 的非零理想，则 I 是 K 的一个 lattice.

此时，回忆一下我们在抽象代数中学过的知识，$\mathcal{O}_K$ 是一个有限维自由 $\mathbb{Z}$-模，I 是一个满秩的子模，同时也是自由模，那么会存在 $\mathcal{O}_K$ 的一组基 $\alpha_1, \cdots, \alpha_n$ 与 $d_1, \cdots, d_n$，使得

$$I = \mathbb{Z}(d_1\alpha_1) \oplus \cdots \oplus \mathbb{Z}(d_n\alpha_n), \quad d_i \mid d_{i+1}, \forall 1 \leq i \leq n-1$$

于是我们知道

$$\mathcal{O}_K/I \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_n\mathbb{Z}$$

是有限的. 这个事实在后面我们定义理想的 norm 时会用到，此时暂且按下不表.

1.3.4 $\mathcal{O}_K$ 是 Noether 环

现在我们可以说明它是 Noether 的了，这其实很容易，因为 $\mathcal{O}_K$ 是有限生成 $\mathbb{Z}$-模，并且 $\mathbb{Z}$ 是 Noether 模，那么我们知道 $\mathcal{O}_K$ 是 Noether $\mathbb{Z}$-模，于是所有理想都是有限生成的 $\mathbb{Z}$-模，即作为 Abel 群是有限生成的，于是所有理想作为 $\mathcal{O}_K$ 的理想自然也是有限生成的.

当然我们还可以提供别的视角，显然 $\mathcal{O}_K$ 是有限生成 $\mathbb{Z}$ 代数，于是由 Hilbert 基定理我们知道 $\mathcal{O}_K$ 也是 Noehter 环.

1.3.5 $\mathcal{O}_K$ 是整闭的

我们说一个环是整闭的，就是说它在它的分式域中是整闭的，容易知道 $\mathcal{O}_K$ 的分式域就是 K，所以只需要对于任意的 $\alpha \in K$ 是 $\mathcal{O}_K$ 上的整元，说明 $\alpha \in \mathcal{O}_K$ 即可.

我们知道存在 $a_1, \cdots, a_n \in \mathcal{O}_K$ 使得

$$\alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0$$

知道 $\mathcal{O}_K[\alpha]$ 是有限生成 $\mathcal{O}_K$-模，而 $\mathcal{O}_K$ 是有限生成 $\mathbb{Z}$-模，于是由有限生成的传递性，我们知道 $\mathcal{O}_K[\alpha]$ 是有限生成 $\mathbb{Z}$-模，所以是 Noether $\mathbb{Z}$-模，于是 $\mathbb{Z}[\alpha] \subset \mathcal{O}_K[\alpha]$ 作为其子模是有限生成的，也就是说 α 在 $\mathbb{Z}$ 上整，于是 $\alpha \in \mathcal{O}_K$.

所以我们证明了 $\mathcal{O}_K$ 是整闭的.

1.3.6 $\dim \mathcal{O}_K = 1$

我们很容易知道 $\mathcal{O}_K$ 是整环，所以这等价于说 $\mathcal{O}_K$ 中的素理想都是极大理想，这等价于说 $\mathcal{O}_K$ 商掉任何一个素理想都是域.

对于 $\mathfrak{p} \in \operatorname{Spec} \mathcal{O}_K$ 非零，我们考虑 $\mathfrak{p} \cap \mathbb{Z}$，我们容易说明存在非零元在 $\mathfrak{p} \cap \mathbb{Z}$ 中，这是因为任取 $\alpha \in \mathfrak{p}$ 非零，则 $N\alpha \in \mathfrak{p} \cap \mathbb{Z}$ 非零，由于素理想的拉回还是素理想，所以 $\mathfrak{p} \cap \mathbb{Z} = (p)$，其中 p 是素数.

我们知道 $\mathcal{O}_K$ 是 $\mathbb{Z}$ 模，在 $\mathfrak{p}$ 的拉回下，我们知道 $\mathcal{O}_K/\mathfrak{p}$ 是 $\mathbb{Z}/p\mathbb{Z}$ 模(这里你需要自己check一下良定义)，也就是说 $\mathcal{O}_K/\mathfrak{p}$ 是 $\mathbb{Z}/p\mathbb{Z}$ 的有限维线性空间，于是 $\mathcal{O}_K/\mathfrak{p}$ 是有限整环，我们知道有限整环都是域，所以 $\mathfrak{p}$ 是极大理想.

等等我发现我好像写麻烦了，之前我们已经说明了对于 $\mathcal{O}_K$ 的任何理想 I，$\mathcal{O}_K/I$ 都是有限的，所以对于任意素理想 $\mathfrak{p}$，都有 $\mathcal{O}_K/\mathfrak{p}$ 是有限的整环，所以是域. 嗯这样把我们之前得到的结论用上了，大大简化过程.

1.3.7 Dedekind domain 中理想可以被素理想唯一分解

在这里我们并不详细给出证明，证明放在拾遗中，我们仅陈述一个重要结果.

定理 1.3.2: 理想唯一分解

在 Dedekind domain R 中，对于任意的理想 $\mathfrak{a}$，存在素理想 $\mathfrak{p}_1,\cdots,\mathfrak{p}_n$ 和正整数 $e_1,\cdots,e_n$ 使得

$$\mathfrak{a}=\mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_n^{e_n}$$

如果还有素理想 $\mathfrak{q}_1,\cdots,\mathfrak{q}_m$ 与正整数 $f_1,\cdots,f_m$ 使得

$$\mathfrak{a}=\mathfrak{q}_1^{f_1}\mathfrak{q}_2^{f_2}\cdots\mathfrak{q}_n^{f_n}$$

那么 $m=n$，并且可以重新排列 $\mathfrak{q}_i$ 与 f_i，使得 $\mathfrak{p}_i=\mathfrak{q}_i$，$e_i=f_i$.

1.4 分式理想与理想类群

1.4.1 代数整数环中的分式理想

在这里我们可能需要一些交换代数的内容，不过其实可以直接定义分式理想，所谓分式理想就类似于给理想加上一些分母，我们这里不对一般的 Dedekind domain 讨论，只讨论代数整数环的情况，但是对于一般的 Dedekind domain 情况是完全类似.

给定数域 K，其代数整数是 $\mathscr{O}_K$，我们定义 $\mathscr{O}_K$ 的**分式理想**就是一个有限生成 $\mathscr{O}_K$-模 $M\subset K$.

一个等价定义是说分式理想是一个 $\mathscr{O}_K$-模 $M\subset K$，使得存在 $d\in\mathscr{O}_K-\{0\}$ 有 $dM\subset\mathscr{O}_K$. 这两个定义的等价性利用 $\mathscr{O}_K$ 的 Noether 是很容易推的，我就不写了，下面我们阐述一些分式理想的基本性质.

显然通常意义下的 $\mathscr{O}_K$ 的中的理想都是分式理想，而分式理想也可以通过给 $\mathscr{O}_K$ 中理想添加分母的方式得到，这给了分式理想的一些刻画.

命题 1.4.1

分式理想都是可逆理想.

我们可能需要先定义以下什么是可逆理想，一个 $\mathscr{O}_K$-模 $M\subset K$ 称为**可逆理想**，如果存在 $\mathscr{O}_K$-模 $N\subset K$，使得 $MN=\mathscr{O}_K$. 事实上这样的 N 是唯一的并且等于 $(\mathscr{O}_K:M):=\{x\in K:xM\subset\mathscr{O}_K\}$.

唯一且等于 $(\mathscr{O}_K:M)$ 的原因是：显然我们有

$$N\subset(\mathscr{O}_K:M)=(\mathscr{O}_K:M)MN=((\mathscr{O}_K:M)M)N\subset\mathscr{O}_KN=N$$

于是我们可以看到所有的分式理想在乘法意义下构成一个 Abel 群，我们把这个群记为 I_K. 特别地，我们平时所称的理想，现在称之为**整理想(integral ideals)** 是 $x=1$ 的分式理想，任何元素 $u\in K$ 都可以生成一个分式理想，记为 (u) 或者 $u\mathscr{O}_K$，称之为主理想. 所有的主理想构成 I_K 的一个子群，记为 P_K.

1.4.2 理想类群

我们回忆一下现在我们有哪些数学对象？有数域 K，代数整数环 $\mathscr{O}_K$，分式理想群 I_K，主理想群 P_K，那么这些东西能不能通过某种方式全部联系在一起呢？其实是有的，我们会有下面这样一个群正合列，这个正合列我们要花大力气来研究：

$$1\to\mathscr{O}_K^\times\to K^\times\to I_K$$

思考 $K^\times$ 在 I_K 中的像，其实就是 P_K，有了一个分式理想构成的群，又有了一个子群，因为是 Abel 的，所以子群都是正规子群，看到正规子群难道不会有把它商掉的欲望吗，所以我们就这么干了. 我们称 $\mathscr{O}_K$ 的**理想类群**为

$$\mathrm{Cl}(K) = I_K/P_K = \mathrm{Coker}(K^\times \to I(K))$$

所以我们会得到正合列

$$1 \to \mathscr{O}_K^\times \to K^\times \to I_K \to \mathrm{Cl}(K) \to 1$$

这个正合列一头一尾两个群就是我们代数数论一开始主要的研究对象，在这一章中我们研究的是 $\mathrm{Cl}(K)$ 理想类群，在下一章中，我们将会研究 $\mathscr{O}_K$ 的单位群 $\mathscr{O}_K^\times$ 并且给出 Dirichlet 单位定理.

1.5 类数有限定理

现在我们来证明代数数论中最重要的定理(应该没有之一(也许等到 Adele 与 Idele 就有了)).

定理 1.5.1: 类数有限定理

我们称 $h_K = |\mathrm{Cl}(K)|$ 为 K 的类数，对于数域 K，我们有 $h_K < +\infty$.

要证明一个东西是有限的，我们能采取的办法其实不多，大部分本质上都是“小于等于某个数的正整数只有有限个”. 这里也是利用这个东西来说明，那么要说明这个就要搞出来一些数字才能行，对于单个的元素我们当然有 trace 和 norm 了，但是对于理想我们现在还是不知道怎么刻画.

现在我们来梳理一下，$\mathscr{O}_K$ 是代数整数环，$\mathfrak{a}$ 是 $\mathscr{O}_K$ 的一个整理想，我们要想办法给这个理想装备一个数字，那么这个数字要怎么来才合理呢？回忆一下，我们应该知道 $\mathscr{O}_K/\mathfrak{a}$ 是有限的，那么这个有限的数字只依赖于 $\mathfrak{a}$，所以，聪明的你应该知道我们该如何定义了，定义出的这个数字称之为**理想的 norm**，之所以称为 norm 是因为它和元素的 norm 是相容的，我们等会再说，现在先定义

$$N\mathfrak{a} = [\mathscr{O}_K : \mathfrak{a}]$$

和元素的相容性是指

$$N(x) = Nx\mathscr{O}_K = |N_{K/\mathbb{Q}}(x)|$$

理想的范数是积性的，即对于理想 $\mathfrak{a}, \mathfrak{b}$，有

$$N\mathfrak{a}\mathfrak{b} = N\mathfrak{a}N\mathfrak{b}$$

这些证明我们暂且不去管他，留在本章拾遗中证明. 下面我们要 claim 一个重要的引理.

引理 1.5.1

给定 $M > 0$，只有有限多个理想 $\mathfrak{a}$ 满足 $N\mathfrak{a} \le M$.

证明: 只需要证明只有有限多个素理想满足即可，而我们注意到对于素理想 $\mathfrak{p}$，考虑 $\mathfrak{p} \cap \mathbb{Z} = (p)$，我们知道 $\mathscr{O}_K/\mathfrak{p}$ 是 $\mathbb{Z}/p\mathbb{Z}$ 的有限维线性空间，于是

$$N\mathfrak{p} = [\mathscr{O}_K : \mathfrak{p}] = p^n$$

并且满足 $\mathfrak{q} \cap \mathbb{Z} = (p)$ 的素理想 $\mathfrak{q}$ 只有有限个，这是因为

$$\mathfrak{q} \supset p\mathscr{O}_K$$

也就是说 $\mathfrak{q} \mid p\mathscr{O}_K$，而 $p\mathscr{O}_K$ 存在唯一素理想分解，所以只有有限个 $\mathfrak{q}$ 的范数是 p 的幂，再结合素数的有限性和整数的离散性，我们知道最多有有限个素理想的范数小于等于 M. □

1.5.1 数的几何 2: Minkowski 定理

为了证明定理，我们需要一个关键的引理来帮助我们. 在此之前我们需要定义一下欧式空间 $\mathbb{R}^n$ 中 Lattice 的体积.

给定一个 $\mathbb{R}^n$ 中格 H，我们知道存在 $\mathbb{R}^n$ 中的一组基 $\alpha_1, \cdots, \alpha_n$ 使得

$$H = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n$$

我们令

$$P(\alpha_1, \cdots, \alpha_n) = \{\sum_{i=1}^{n} a_i\alpha_i \mid 0 \le a_i < 1\}$$

容易知道 $P(\alpha_1, \cdots, \alpha_n)$ 构成了 $\mathbb{R}^n/H$ 的陪集代表元，取 $e_1 = (1, 0, \cdots, 0), \cdots, e_n = (0, \cdots, 0, 1)$为 $\mathbb{R}^n$ 的标准基，设 $\alpha_i = \sum_{j=1}^{n} r_{ij}e_j$，用 m 表示 $\mathbb{R}^n$ 上的 Lebesgue 测度，我们知道

$$m(P(\alpha_1, \cdots, \alpha_n)) = |\det(r_{ij})|$$

假设 $\alpha'_1, \cdots, \alpha'_n$ 是 H 的另外一组基，假设

$$\alpha'_i = \sum_{j=1}^{n} a_{ij}\alpha_j$$

其中 $a_{ij} \in \mathbb{Z}$ 并且由于两者都是基，所以有 $|\det(a_{ij})| = 1$，于是我们知道

$$m(P(\alpha'_1, \cdots, \alpha'_n)) = |\det(r_ij) \cdot \det(a_{ij})| = |\det(r_{ij})| = m(P(\alpha_1, \cdots, \alpha_n))$$

于是我们知道 $m(P(\alpha_1, \cdots, \alpha_n))$ 与 H 的基的选取无关，所以是关于 H 的不变量，我们将它定义为 H 的**体积**，表示为 $V(H)$. 我们很容易直观地看出来，H 在 $\mathbb{R}^n$ 中分布越是稀疏，它的体积就越大.

下面我们需要定义 $\mathbb{R}^n$ 中一些特殊的子集，我们称 S 是**凸集合**，如果

$$\forall x, y \in S \Rightarrow \frac{1}{2}(x + y) \in S$$

我们称 S 是**关于原点对称的**，如果

$$\forall x \in S \Rightarrow -x \in S$$

好啦，现在我们可以看到我们需要的很重要的定理了.

定理 1.5.2: Minkowski

设 S 是 $\mathbb{R}^n$ 中关于原点对称的紧凸集，$\Lambda \subset \mathbb{R}^n$ 是一个 *lattice(默认满秩)*，如果有

$$V(S) \ge 2^n V(\Lambda)$$

那么 $S \cap (A \backslash \{0\}) \neq \emptyset$.

证明: 我懒得敲了，看冯克勤吧. □

1.5.2 判别式(discriminant)

为了定义理想的 norm，我们还剩最后一块拼图，这个拼图就是判别式，当然判别式的作用肯定不仅仅是这些，更多的作用我们会在拾遗中见到.

首先我们需要定义对任意 n 个元素的判别式 d_K，给定 $\alpha_1,\cdots,\alpha_n\in K$，我们定义

$$d_{K/\mathbb{Q}}(\alpha_1,\cdots,\alpha_n)=|\det(\sigma_i(\alpha_j))|^2$$

回忆，对于数域 K，可能会存在不同的整基，假设 $\beta_1,\cdots,\beta_n$ 和 $\gamma_1,\cdots,\gamma_n$ 都是 K 的整基，那么由整基的定义我们知道存在元素都在 $\mathbb{Z}$ 中的两个矩阵 M,N 使得

$$\begin{pmatrix}\beta_1\\ \vdots\\ \beta_n\end{pmatrix}=M\begin{pmatrix}\gamma_1\\ \vdots\\ \gamma_n\end{pmatrix},\quad \begin{pmatrix}\gamma_1\\ \vdots\\ \gamma_n\end{pmatrix}=N\begin{pmatrix}\beta_1\\ \vdots\\ \beta_n\end{pmatrix}$$

于是有 $M=N^{-1}$，容易看出来 $|M|=|N|=\pm1$. 令 $\sigma_1,\cdots,\sigma_n$ 是 K 到 $\mathbb{C}$ 的 n 个嵌入，我们知道 $n=[K:\mathbb{Q}]$，我们不难发现

$$(\sigma_i(\beta_j))=M(\sigma_i(\gamma_j))\Rightarrow d_{K/\mathbb{Q}}(\beta_1,\cdots,\beta_n)=|M|^2d_{K/\mathbb{Q}}(\gamma_1,\cdots,\gamma_n)=d_{K/\mathbb{Q}}(\gamma_1,\cdots,\gamma_n)$$

于是我们发现不同的整基具有相同的判别式，所以整基的判别式是数域的一个不变量，我们将其称之为域 K 的**判别式**，记为 d_K 或者 $d(K)$. 容易证明(放在拾遗里面了)，域 K 的判别式不为 0，并且 d_K 是一个整数.

1.5.3 类数有限定理的证明

我们现在来说明数域的理想类群是有限的，方法是将 $\mathscr{O}_K$ 的每个分式理想嵌入 $\mathbb{R}^n$ 中成为一个格.

回忆一下我们有 r_1 个实嵌入与 r_2 对复嵌入，记为

$$\sigma_1,\cdots,\sigma_{r_1},\quad \sigma_{r_1+1},\cdots,\sigma_{r_1+r_2},\overline{\sigma_{r_1+1}},\cdots,\overline{\sigma_{r_1+r_2}}$$

我们有映射

$$\sigma\colon K\to V=\mathbb{R}^{r_1}\times\mathbb{C}^{r_2}\cong\mathbb{R}^n$$

定义为

$$\sigma(x)=(\sigma_1(x),\cdots,\sigma_{r_1}(x),\sigma_{r_1+1}(x),\cdots,\sigma_{r_1+r_2}(x))$$

我们称 σ 为 K 到 V 中的**正则嵌入**. 思考一下，K 作为 $\mathbb{Q}$-线性空间是 $\mathbb{Q}^n$，并且 $\mathscr{O}_K$ 的非零整理想是 K 中的 lattice. 那么聪明的你一定会想，$\mathfrak{a}$ 在 $\mathbb{R}$-线性空间 V 中的像 $\sigma(\mathfrak{a})$ 是否是 $V\cong\mathbb{R}^n$ 中的 lattice？幸运的是这个猜测是正确的，我们简单说明一下这个东西.

首先为了某种方便，我们给出 V 到 $\mathbb{R}^n$ 的同构，让我们在 $\mathbb{R}^n$ 中讨论

$$K\to\mathbb{R}^n,\quad \alpha\mapsto(\sigma_1(\alpha),\cdots,\alpha_{r_1}(\alpha),\mathrm{Re}(\sigma_{r_1+1}(\alpha)),\cdots,\mathrm{Re}(\sigma_{r_1+r_2}(\alpha)),\mathrm{Im}(\sigma_{r_1+1}(\alpha)),\cdots,\mathrm{Im}(\sigma_{r_1+r_2}(\alpha)))$$

在前面我们早已说明 $\mathfrak{a}$ 是秩为 n 的自由 Abel 群，即

$$\mathfrak{a}=\mathbb{Z}\alpha_1\oplus\cdots\oplus\mathbb{Z}\alpha_n$$

取 $e_1,\cdots,e_n$ 为 $V\cong\mathbb{R}^n$ 的标准基，则我们知道

$$\sigma(\alpha_i)=\sum_{j=1}^n x_{ij}e_j$$

其中

$$x_{ij}=\begin{cases}\sigma_j(\alpha_i), & 1\le j\le r_1\\ \mathrm{Re}(\sigma_j(\alpha_i)), & r_1+1\le j\le r_1+r_2\\ \mathrm{Im}(\sigma_j(\alpha_i)), & r_1+r_2+1\le j\le n\end{cases}$$

于是我们知道

$$\sigma(\mathfrak{a}) = \mathbb{Z}\sigma(\alpha_1) + \cdots + \mathbb{Z}\sigma(\alpha_n)$$

所以我们知道 $\sigma(\mathfrak{a})$ 的秩小于等于 n，下面只需要说明 $\sigma(\mathfrak{a})$ 的体积大于 0，则自然成为一个 lattice.

$$V(\sigma(\mathfrak{a})) = |\det(x_{ij})|$$

$$= \left\| \begin{vmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_{r_1}(\alpha_1) & \mathrm{Re}(\sigma_{r_1+1}(\alpha_1)) & \cdots & \mathrm{Re}(\sigma_{r_1+r_2}(\alpha_1)) & \mathrm{Im}(\sigma_{r_1+1}(\alpha_1)) & \cdots & \mathrm{Im}(\sigma_{r_1+r_2}(\alpha_1)) \\ \sigma_1(\alpha_2) & \cdots & \sigma_{r_1}(\alpha_2) & \mathrm{Re}(\sigma_{r_1+1}(\alpha_2)) & \cdots & \mathrm{Re}(\sigma_{r_1+r_2}(\alpha_2)) & \mathrm{Im}(\sigma_{r_1+1}(\alpha_2)) & \cdots & \mathrm{Im}(\sigma_{r_1+r_2}(\alpha_2)) \\ \vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots \\ \sigma_1(\alpha_n) & \cdots & \sigma_{r_1}(\alpha_n) & \mathrm{Re}(\sigma_{r_1+1}(\alpha_n)) & \cdots & \mathrm{Re}(\sigma_{r_1+r_2}(\alpha_n)) & \mathrm{Im}(\sigma_{r_1+1}(\alpha_n)) & \cdots & \mathrm{Im}(\sigma_{r_1+r_2}(\alpha_n)) \end{vmatrix} \right\|$$

$$= \left\| \begin{vmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_{r_1}(\alpha_1) & \sigma_{r_1+1}(\alpha_1) & \cdots & \sigma_{r_1+r_2}(\alpha_1) & \mathrm{Im}(\sigma_{r_1+1}(\alpha_1)) & \cdots & \mathrm{Im}(\sigma_{r_1+r_2}(\alpha_1)) \\ \sigma_1(\alpha_2) & \cdots & \sigma_{r_1}(\alpha_2) & \sigma_{r_1+1}(\alpha_2) & \cdots & \sigma_{r_1+r_2}(\alpha_2) & \mathrm{Im}(\sigma_{r_1+1}(\alpha_2)) & \cdots & \mathrm{Im}(\sigma_{r_1+r_2}(\alpha_2)) \\ \vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots \\ \sigma_1(\alpha_n) & \cdots & \sigma_{r_1}(\alpha_n) & \sigma_{r_1+1}(\alpha_n) & \cdots & \sigma_{r_1+r_2}(\alpha_n) & \mathrm{Im}(\sigma_{r_1+1}(\alpha_n)) & \cdots & \mathrm{Im}(\sigma_{r_1+r_2}(\alpha_n)) \end{vmatrix} \right\|$$

$$= 2^{-r_2} \left\| \begin{vmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_{r_1}(\alpha_1) & \sigma_{r_1+1}(\alpha_1) & \cdots & \sigma_{r_1+r_2}(\alpha_1) & -2i\,\mathrm{Im}(\sigma_{r_1+1}(\alpha_1)) & \cdots & -2i\,\mathrm{Im}(\sigma_{r_1+r_2}(\alpha_1)) \\ \sigma_1(\alpha_2) & \cdots & \sigma_{r_1}(\alpha_2) & \sigma_{r_1+1}(\alpha_2) & \cdots & \sigma_{r_1+r_2}(\alpha_2) & -2i\,\mathrm{Im}(\sigma_{r_1+1}(\alpha_2)) & \cdots & -2i\,\mathrm{Im}(\sigma_{r_1+r_2}(\alpha_2)) \\ \vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots \\ \sigma_1(\alpha_n) & \cdots & \sigma_{r_1}(\alpha_n) & \sigma_{r_1+1}(\alpha_n) & \cdots & \sigma_{r_1+r_2}(\alpha_n) & -2i\,\mathrm{Im}(\sigma_{r_1+1}(\alpha_n)) & \cdots & -2i\,\mathrm{Im}(\sigma_{r_1+r_2}(\alpha_n)) \end{vmatrix} \right\|$$

$$= 2^{-r_2} \left\| \begin{vmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_{r_1}(\alpha_1) & \sigma_{r_1+1}(\alpha_1) & \cdots & \sigma_{r_1+r_2}(\alpha_1) & \overline{\sigma_{r_1+1}(\alpha_1)} & \cdots & \overline{\sigma_{r_1+r_2}(\alpha_1)} \\ \sigma_1(\alpha_2) & \cdots & \sigma_{r_1}(\alpha_2) & \sigma_{r_1+1}(\alpha_2) & \cdots & \sigma_{r_1+r_2}(\alpha_2) & \overline{\sigma_{r_1+1}(\alpha_2)} & \cdots & \overline{\sigma_{r_1+r_2}(\alpha_2)} \\ \vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots \\ \sigma_1(\alpha_n) & \cdots & \sigma_{r_1}(\alpha_n) & \sigma_{r_1+1}(\alpha_n) & \cdots & \sigma_{r_1+r_2}(\alpha_n) & \overline{\sigma_{r_1+1}(\alpha_n)} & \cdots & \overline{\sigma_{r_1+r_2}(\alpha_n)} \end{vmatrix} \right\|$$

所以我们知道

$$V(\sigma(\mathfrak{a})) = 2^{-r_2}|\det(\sigma_j(\alpha_i))|$$

设 $\beta_1, \cdots, \beta_n$ 是 $\mathscr{O}_K$ 的一组整基，使得 $\mathfrak{a} = \mathbb{Z}(d_1\beta_1) \oplus \cdots \oplus \mathbb{Z}(d_n\beta_n)$，由于都是 $\mathfrak{a}$ 的基，我们知道

$$|\det(\sigma_j(\alpha_i))| = |\det(\sigma_j(d_i\beta_i))|$$

注意到

$$N\mathfrak{a} = [\mathscr{O}_K : \mathfrak{a}] = |d_1 d_2 \cdots d_n| = \frac{|\det(\sigma_j(d_i\beta_i))|}{|\det(\sigma_j(\beta_i))|} = \frac{|\det(\sigma_j(\alpha_i))|}{\sqrt{|d_K|}}$$

所以我们最终得到

$$V(\sigma(\mathfrak{a})) = 2^{-r_2} N\mathfrak{a}\sqrt{|d_K|}$$

右边显然不为零，所以体积大于零，于是是满秩的，所以 $\mathfrak{a}$ 构成一个 lattice.

引理 1.5.2

存在只跟域 K 相关的常数 M，使得对于任何分式理想 $\mathfrak{a}$，都存在 $x \in \mathfrak{a}^{-1} - \{0\}$，使得

$$N(x\mathfrak{a}) \leq M$$

证明： 设 $\mathfrak{a}$ 是分式理想，考虑 $\mathfrak{a}^{-1}$ 在映射

$$K \to V = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}, \quad x \mapsto (\sigma_1(x), \cdots, \sigma_{r_1}(x), \sigma_{r_1+1}(x), \cdots, \sigma_{r_1+r_2}(x))$$

下的像，构成一个 V 中的 lattice，我们任取 V 中一个关于原点对称的紧凸集 S，设 M_0 是 V 上函数

$$|x_1 \cdots x_{r_1} x_{r_1+1}^2 \cdots x_{r_1+r_2}^2|$$

在 S 上的最大值，我们取

$$\lambda = 2\left(\frac{V(\sigma(\mathfrak{a}^{-1}))}{m(S)}\right)^{\frac{1}{n}}$$

所以我们有

$$m(\lambda S) = 2^n V(\sigma(\mathfrak{a}^{-1}))$$

于是由 Minkowski 定理我们知道存在 $\sigma(x) \in \lambda S \cap \sigma(\mathfrak{a}^{-1})$，于是我们知道

$$\begin{aligned} N(x\mathfrak{a}) &= |N_{K/\mathbb{Q}}(x)| N\mathfrak{a} = \left|\prod_{i=1}^{n} \sigma_i(x)\right| N\mathfrak{a} \\ &\leq \max_{x \in \lambda S} |x_1 \cdots x_{r_1} x_{r_1+1}^2 \cdots x_{r_1+r_2}^2| N\mathfrak{a} \\ &= \lambda^n M_0 N\mathfrak{a} = 2^n \frac{V(\sigma(\mathfrak{a}^{-1}))}{m(S)} M_0 N\mathfrak{a} \\ &= 2^n \frac{2^{-r_2} N\mathfrak{a}^{-1} \sqrt{|d_K|}}{m(S)} M_0 N\mathfrak{a} \\ &= 2^{r_1+r_2} M_0 \sqrt{|d_K|} m(S)^{-1} \end{aligned}$$

等式最右边只与 K 相关，命题成立. □

事实上，我们还可以取出一些很好的 S 让这个界更好，我们可以取

$$S = \{(x_1, \cdots, x_{r_1+r_2}) \in V \mid |x_1| + \cdots |x_{r_1}| + 2(|x_{r_1+1}| + \cdots + |x_{r_1+r_2}|) \leq 1\}$$

在这个条件下，上面证明过程中取的 M_0 为 n^{-n}，用一步均值就可以看出来. 此时我们知道上界 M 可以取为

$$\left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \sqrt{|d_K|}$$

此即我们常说的 **Minkowski bound**. 是计算理想类群的常用手段.

好了，现在我们开始玩一段文字游戏，来证明理想类群是有限的，跟上咯：**设 Minkowski bound 为 M，由于满足 norm 小于等于 M 的整理想是有限的，并且任何一个分式理想 $\mathfrak{a}$ 都可以乘上一个元素 $x \in \mathfrak{a}^{-1} - \{0\}$ 使得 $N(x\mathfrak{a}) \leq M$，注意 $x\mathfrak{a}$ 是整理想，所以每一个理想类都会对应某一个满足范数小于 M 的整理想，并且不同的理想类不可能对应同一个整理想，由后者的有限性我们知道理想类是有限的.**

所以我们最终就证明了**理想类群有限**.