# The Mordell-Faltings theorem

`https://seasawher.github.io/kitamado/`

@seasawher

2019 年 6 月 1 日

# 1 Some basics of algebraic number theory

### Lemma 1.3

> **quotation.** Recall that $(\ ,\ )_{\mathrm{Tr}_{K/\mathbb{Q}}}$ is non-degenerate if the Gramm matrix with respect to one (and hence any) basis of $L$ over $F$ is invertible.

*Proof.* Almost trivial. Try to prove it. □

### Proposition 1.4

> **quotation.** Let $\{\beta_1, \cdots, \beta_n\}$ be the dual basis of $\{\alpha_1, \cdots, \alpha_n\}$ with respect to $(\ ,\ )_{\mathrm{Tr}_{K/\mathbb{Q}}}$. Then, for any $x \in O_K$, we have $x = (x, \alpha_1)_{\mathrm{Tr}_{K/\mathbb{Q}}}\beta_1 + \cdots + (x, \alpha_n)_{\mathrm{Tr}_{K/\mathbb{Q}}}\beta_n$.

*Proof.* Since the trace form $(\ ,\ )_{\mathrm{Tr}_{K/\mathbb{Q}}}$ is nondegenerate, $K \to K^*$ s.t. $x \mapsto (\cdot, x)_{\mathrm{Tr}_{K/\mathbb{Q}}}$ is a isomorphism. Let $p_i \colon K \to \mathbb{Q}$ be a projection map such that $p_i(x_1\alpha_1 + \cdots + x_n\alpha_n) = x_i$. Then, we set $\beta_j$ the preimage of $p_j$.

□

### Lemma 1.7

> **quotation.** To see this, we take $t \in P(O_K)_P$ with $t \notin P^2(O_K)_P$.

**remark.** From Nakayama's lemma.

### Adjacent to Lemma 1.8

> **quotation.** For a nonzero prime ideal $P$ of $O_K$, we set $P \cap \mathbb{Z} = (p)$, where $p$ is a prime of $Z$. Because $O_K$ is a free $Z$-module of rank $[K : \mathbb{Q}]$, $O_K/P$ is a finite extension of $\mathbb{Z}/(p)$ with degree at most $[K : \mathbb{Q}]$.

*Proof.* There is a canonical surjection $O_K/pO_K \to O_K/P$, so we get $\#(O_K/P) \leq \#(O_K/pO_K)$. But we obtain $O_K/pO_K \cong O_K \otimes_{\mathbb{Z}} \mathbb{Z}/p\mathbb{Z}$. Since $O_K$ is a free $\mathbb{Z}$-module of rank $n = [K : \mathbb{Q}]$, we conclude $O_K/pO_K \cong (\mathbb{Z}/p\mathbb{Z})^n$. So, $\#(O_K/P) \leq \#(O_K/pO_K) = p^n$. □

## Lemma 1.8

> **quotation.**
> $$\bigoplus_{i=1}^{r} O_K/P_i^{e_i} = \bigoplus_{i=1}^{r} (O_K/P_i^{e_i})_{P_i}$$

*Proof.* Because $O_K/P_i^{e_i}$ is a local ring with maximal ideal $P_i/P_i^{e_i}$. □

## Adjacent to Theorem 1.9

> **quotation.** we consider the value $\sqrt{\det(\langle e_i, e_j \rangle)}$.

**remark.** Why we get $\det(\langle e_i, e_j \rangle)$? Apply Gram-Schmidt orthonormalization.

## Adjacent to Theorem 1.9

> **quotation.** Then $\mathrm{vol}(M, \langle , \rangle)$ is equal to the volume of the $n$-dimensional parallelpiped $\Pi$ spanned by $e_1, \cdots, e_n$,

*Proof.* Let $F\colon (V, \langle , \rangle) \to \mathbb{R}^n$ be an isometric isomorphism. Then, we generate

$$\begin{aligned} \mathrm{vol}(M, \langle , \rangle)^2 &= \det(\langle e_i, e_j \rangle) \\ &= \det(\langle Fe_i, Fe_j \rangle) \end{aligned}$$

We set $E = (Ee_1, \cdots, Fe_n)$. $E \in M_n(\mathbb{R})$. Then we get $(\langle Fe_i, Fe_j \rangle)_{i,j} = {}^tEE$, and $\mathrm{vol}(M, \langle , \rangle) = |\det E|$. From Yukie[3] Theorem 4.9.1, $|\det E| = \mathrm{vol}(\Pi)$. □

## Proposition 1.11

> **quotation.** The form $\langle , \rangle_K$ is an inner product on $V$.

**remark.** $\langle , \rangle_K$ is trivially an inner product on $K$. Why should we show this?

Let $S$ be a $\mathbb{Q}$ vector space and $\langle , \rangle$ a inner product on $S$. Then, bilinear form extended to $S \otimes_{\mathbb{Q}} \mathbb{R}$ may not be an inner product. For example, set $S = \mathbb{Q}[\sqrt{2}]$ and $\langle x, y \rangle = xy$.

## Lemma 1.12

> **quotation.** $\#(O_K/I)$ is finite. Then $I$ is a free $\mathbb{Z}$-module of rank $n$.

*Proof.* $I \subset O_K$ is a free $\mathbb{Z}$-module. Since $\#(O_K/I)$ is finite, we get $\forall x \in K\ \exists n \in \mathbb{Z}$ s.t. $nx \in I$. So we obtain $I \otimes_{\mathbb{Z}} \mathbb{Q} = K$. The rank of $I$ is $n$. □

## Lemma 1.16

> **quotation.** We have $[K' : K] = e_1 f_1 + \cdots + e_r f_r$.

*Proof.* See the proof of Prop 1.4. We obtain $O_{K'} \subset O_K\beta_1 \oplus \cdots \oplus O_K\beta_n$ for some $\beta_i \in K'$. That implies there is an injection such that $O_{K'} \to \bigoplus_i O_K$. Because localization is a flat module, we get $(O_{K'})_P \subset (O_K)_P\beta_1 \oplus \cdots \oplus (O_K)_P\beta_n$. Since $(O_K)_P$ is a PID, $(O_{K'})_P$ is a free $(O_K)_P$-module. The rank is $[K' : K]$ because

$$(O_{K'})_P \otimes_{(O_K)_P} K = (O_{K'} \otimes_{O_K} (O_K)_P) \otimes_{(O_K)_P} K = O_{K'} \otimes_{O_K} K = K'.$$

Thus, as a $O_K/P$ module,

$$\begin{aligned} O_{K'}/PO_{K'} &\cong O_K/P \otimes_{O_K} O_{K'} \\ &\cong (O_K/P \otimes_{O_K} (O_K)_P \otimes_{(O_K)_P} (O_K)_P) \otimes_{O_K} O_{K'} \\ &\cong (O_K/P \otimes_{O_K} (O_K)_P) \otimes_{(O_K)_P} (O_{K'})_P \\ &\cong \bigoplus_{[K':K]} (O_K/P \otimes_{O_K} (O_K)_P) \\ &\cong \bigoplus_{[K':K]} O_K/P. \end{aligned}$$

Then it follows that

$$\begin{aligned} \#(O_K/P)^{[K':K]} &= \#(O_{K'}/PO_{K'}) \\ &= \prod_i \#(O_{K'}/P_i'^{e_i}) \\ &= \prod_i \#(O_{K'}/P_i')^{e_i} \\ &= \prod_i \#(O_K/P)^{e_i f_i}. \end{aligned}$$

Thus $[K' : K] = \sum_i e_i f_i$. □

## Adjacent to Lemma 1.17

> **quotation.** We take a integral basis $\{\omega_1, \cdots, \omega_n\}$ of $O_K$, we denote by $\{\beta_1, \cdots, \beta_n\}$ the dual basis with respect to $(\ ,\ )_{\mathrm{Tr}_{K/\mathbb{Q}}}$. Then we have $\mathcal{M} = \mathbb{Z}\beta_1 + \cdots + \mathbb{Z}\beta_n$.

*Proof.* See the note of Prop 1.4. □

## Lemma 1.17

> **quotation.** Indeed, because $\#(O_K/\mathcal{D}_K) = \#(\mathcal{M}/O_K)$,

*Proof.* See Yukie[1] Proposition 1.8.6. □

## Theorem 1.18

> **quotation.** Then we have
> $$|D_{K/\mathbb{Q}}| \leq \prod_{p \in S} p^{n-1+n\log_p(n)}.$$

*Proof.* We may assume that $S = \{p \in \mathbb{Z} \mid p \text{ is ramified}\}$. Set $B = O_K$ and $I = D_K$.

Step 1 Let $p \in \mathbb{Z}$ be a prime number. Then $B_p$ and $I_p$ are free $\mathbb{Z}_p$-module of rank $n$. So there is a matrix $C \in M_n(\mathbb{Z}_p) \cap GL_n(\mathbb{Q}_p)$ such that the following diagram

$$\begin{tikzcd}
I_p \arrow[r] \arrow[d] & B_p \arrow[d] \\
\mathbb{Z}_p^n \arrow[r, "C"] & \mathbb{Z}_p^n
\end{tikzcd}$$

commute. Then

$$\begin{aligned}
\#(B/I \otimes_{\mathbb{Z}} \mathbb{Z}_p) &= \#(\operatorname{Coker} C) \\
&= \#(\mathbb{Z}_p/(\det C)\mathbb{Z}_p) \\
&= \#(\widehat{\mathbb{Z}}_p/(\det C)\widehat{\mathbb{Z}}_p) && \text{(See Yukie[1] Proposition 1.2.13)} \\
&= \#(B/I \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}}_p).
\end{aligned}$$

Step 2 It follows that

$$\begin{aligned}
B/I \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}}_p &\cong B/I \otimes_B B \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}}_p \\
&\cong B/I \otimes_B \bigoplus_i \widehat{B}_{P_i} && \text{(See Yukie[1] Theorem 1.3.23 )} \\
&\cong \bigoplus_i \widehat{B}_{P_i}/P_i^{\mathrm{ord}_{P_i}(I)}\widehat{B}_{P_i} \\
&\cong \bigoplus_i B/P_i^{\mathrm{ord}_{P_i}(I)}
\end{aligned}$$

Step 3 Set $J = I \cap \mathbb{Z}$. Because $B/I$ is finitely generated $\mathbb{Z}$-module, we get

$$\mathrm{Supp}_{\mathbb{Z}}(B/I) = V(\mathrm{ann}_{\mathbb{Z}}(B/I)) = V(J).$$

See Matsumura[4] adjacent to Theorem 4.4 if you do not understand the first equation. And for any prime number $p \in \mathbb{Z}$, then we obtain

$$\begin{aligned} p \notin \mathrm{Supp}_{\mathbb{Z}}(B/I) &\iff B/I \otimes_{\mathbb{Z}} \mathbb{Z}_p = 0 \\ &\iff \#(B/I \otimes_{\mathbb{Z}} \mathbb{Z}_p) = 1 \\ &\iff \forall i\ \#(B/P_i^{\mathrm{ord}_{P_i}(I)}) = 1 \\ &\iff \mathrm{ord}_{P_i}(I) = 0 \\ &\iff p \text{ is unramified} \end{aligned}$$

Thus we conclude $V(J) = \mathrm{Supp}_{\mathbb{Z}}(B/I) = S$.

Step 4 Then we get

$$\begin{aligned} \#(B/I \otimes_{\mathbb{Z}} \mathbb{Z}_p) &= \prod_i \#(B/P_i^{\mathrm{ord}_{P_i}(I)}) \\ &= \prod_i \#(B/P_i)^{\mathrm{ord}_{P_i}(I)} \\ &= \prod_i \#(\mathbb{Z}/p)^{f_i \,\mathrm{ord}_{P_i}(I)}. \end{aligned}$$

So we conclude $\log_p(\#(B/I \otimes_{\mathbb{Z}} \mathbb{Z}_p)) \leq n - 1 + n \log_p(n)$.

Step 5 Recall that $J = \mathrm{ann}_{\mathbb{Z}}(B/I)$. Then we get

$$\begin{aligned} B/I &\cong (B/I)/J(B/I) \\ &\cong \bigoplus_{p \in S} (B/I)/p^e(B/I) && (e \text{ depends on } p) \\ &\cong \bigoplus_{p \in S} B/(p^e B + I) \\ &\cong \bigoplus_{p \in S} B/(p^e B + I) \otimes_{\mathbb{Z}} \mathbb{Z}_p \\ &\cong \bigoplus_{p \in S} B_p/(p^e B_p + I_p) \\ &\cong \bigoplus_{p \in S} B_p/(J B_p + I_p) \\ &\cong \bigoplus_{p \in S} B_p/I_p \end{aligned}$$

Now we conclude that

$$\left|D_{K/\mathbb{Q}}\right| = \#(B/I) = \prod_{p \in S} \#(B_p/I_p) \leq \prod_{p \in S} p^{n-1+n\log_p(n)}.$$

□

# 2 Theory of heights

### Theorem 2.3

> **quotation.** We set $n = [K : \mathbb{Q}]$. Let $\{\omega_1, \cdots, \omega_n\}$ be the integral basis of $O_K$. Then $\{x\omega_1, \cdots, x\omega_n\}$ is a basis of V.

*Proof.* There is a $c_{ij} \in \mathbb{Z}$ such that $x\omega_i = \sum_j c_{ij}\omega_i$. Set $C = (c_{ij}) \in M_n(\mathbb{Z})$. Then $\det C = N_{K/\mathbb{Q}}(x) \neq 0$, so we get $C \in GL_n(\mathbb{Q})$. And we obtain the assertion. □

### Proposition 2.5

> **quotation.**
>
> $$h_K(x) \leq \sum_{\sigma \in K(\mathbb{C})} \log\left(\max_{1 \leq i \leq n} \{|x_i|_\sigma\}\right).$$

**remark.** **Misprint.** Add $1/[K : \mathbb{Q}]$ into the right.

### Proposition 2.6

> **quotation.** for any $x \in \overline{\mathbb{Q}}^n$.

**remark.** **Misprint.** Exclude the case $x = 0$.

### Proposition 2.8

> **quotation.** We consider two morphisms $\phi_1\colon X \to \mathbb{P}^{m_1}$ and $\phi_2\colon X \to \mathbb{P}^{m_2}$ over $\overline{\mathbb{Q}}$. If $\phi_1^*\mathcal{O}_{\mathbb{P}^{m_1}} \cong \phi_2^*\mathcal{O}_{\mathbb{P}^{m_2}}$, then there is a constant $C$ such that, for any $x \in X(\overline{\mathbb{Q}})$,
>
> $$|h_{\phi_1}(x) - h_{\phi_2}(x)| \leq C.$$

*Proof.* Remark that $\mathcal{O}_{\mathbb{P}^{m_1}}(1)$ is a Serre's twisted sheaf. See Bosch[2] 9.2/Definition 3. or Hartshorne[5] section 2.5 Adjacent to Proposition 5.12. We set $L = \phi_1^*\mathcal{O}_{\mathbb{P}^{m_1}}$ and set $k = \overline{\mathbb{Q}}$ and $\mathscr{F} = \mathcal{O}_{\mathbb{P}^{m_1}}(1)$. Since $X$ is a projective variety over $k$ and $L$ is an invertible sheaf on $X$, so $H^0(X, L) = \Gamma(X, L)$ is a $k$-vector space of finite dimension. (See Hartshorne[5] section 2.5 Theorem 5.19. and Hartshorne[5] section 2.4 Prop 4.10)

Let $\{t_0, \cdots, t_m\}$ be a basis of $H^0(X, L)$ and let $X_0, \cdots, X_{m_1}$ be the homogenous coordinates of $\mathbb{P}^{m_1}$. Note that each $X_i$ is a global section of $\mathscr{F}$. And we set $s_i = \phi_1^* X_i \in H^0(X, L)$, where $\phi_1^* X_i$ is the image of $X_i \in H^0(\mathbb{P}^m, \mathscr{F})$ by the canonical map $\mathscr{F} \to \phi_{1*}\phi_1^*\mathscr{F}$. It follows from Hartshorne[5] section 2.7 Theorem 7.1 that $s_0, \cdots, s_{m_1}$ generate $L$. Because for any $x \in X$ the each germ $(s_i)_x$ is a linear combination of $(t_j)_x$, so $t_0, \cdots, t_m$ generate $L$.

There is a morphism $\phi\colon X \to \mathbb{P}^m$ such that $L \cong \phi^*\mathcal{O}_{\mathbb{P}^m}(1)$ and $s_i = \phi^* X_i$ under this isomorphism. See Hartshorne[5] section 2.7 Theorem 7.1(b). There is another explanation on what $\phi$ is. For any $x \in X$, we can consider the germ $(t_i)_x \in L_x$. Denote $(t_i)_x$ by $t_i(x)$. Since $L$ is a line bundle, $L_x \cong k$. (**It remains to be learned.**) Then we define the map $\phi\colon X \to \mathbb{P}^m$ by $\phi(x) = (t_0(x), \cdots, t_m(x))$. Note that there is a scalar ambiguity in choice of isomorphism $L_x \to k$. If $\forall i\ t_i(x) = 0$, then $(t_i)_x$ cannot generate $L_x$, which is a contradiction. Thus for any $x \in X$, there is an index $i$ such that $t_i(x) \neq 0$.

Then, the rest of the proof is almost trivial. □

## 参考文献

[1] 雪江明彦『整数論 2 代数的整数論の基礎』(日本評論社, 2013)

[2] Siegfried Bosch『Algebraic Geometry and Commutative Algebra』(Springer, 2013)

[3] 雪江明彦『線形代数学概説』(培風館, 2006)

[4] 松村英之『可換環論』(共立出版, 1980)

[5] Robin Hartshorne『Algebraic Geometry』(Springer, 1977)