The handle http://hdl.handle.net/1887/36589 holds various files of this Leiden University dissertation.

**Author:** Zhuang, Weidong  
**Title:** Symmetric diophantine approximation over function fields  
**Issue Date:** 2015-12-03
Chapter 4

Reduction theory for binary forms over $k(t)$

In this chapter we work out a reduction theory for binary forms over $k(t)$. This is a function field analogue of the reduction theory over number fields developed in [9]. We follow the arguments from [9].

Recall that $K = k(t)$ and $S$ a finite set of valuations of $K$ containing the infinite valuation $\nu_\infty$. For a binary form $F(X, Y) = a_0X^n + a_1X^{n-1}Y + \cdots + a_nY^n \in \mathcal{O}_S[X, Y]$, let

$$H_S(F) = \prod_{\nu \in S} \max(|a_0|_\nu, \ldots, |a_n|_\nu).$$

We say that two binary forms $F, G \in \mathcal{O}_S[X, Y]$ are $\text{GL}(2, \mathcal{O}_S)$-equivalent if for some $u \in \mathcal{O}_S^\times$ and $(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}) \in \text{GL}_2(\mathcal{O}_S)$, we have

$$G(X, Y) = uF(aX + bY, cX + dY).$$

This equivalence relation preserves the $S$-value of the discriminant: $|D(F)|_S = |D(G)|_S$.

**Definition 4.0.** A binary form $F \in \mathcal{O}_S[X, Y]$ is called $S$-reduced if $H_S(F) \leq H_S(G)$ for each binary form $G$ that is $\text{GL}(2, \mathcal{O}_S)$-equivalent to $F$. 

53
This is well-defined since $H_S(F)$ always lies in $e^Z$ and for $F \in \mathcal{O}_S[X,Y]$ we have $H_S(F) \geq 1$.

Remark that by (1.2.1), we have $|D(F)|_S \leq H_S(F)^{2n-2}$.

### 4.1 Discriminant and genus

Let $F \in \mathcal{O}_S[X,Y]$ be a binary form with $D(F) \neq 0$ and $\deg F = n$. The ring $\mathcal{O}_S$ is a localization of $k[t]$, hence it is a principal ideal domain. So we may factor $F$ as $F = F_1 \cdots F_d$ where $F_i \in \mathcal{O}_S[X,Y]$ is an irreducible binary form over $K$. If $F_i(1,0) \neq 0$ we may assume that $F_i = F_i(1,0)N_{K_i/K}(X - \alpha_i Y)$ with $K_i = K(\alpha_i)$, where $\alpha_i$ is a root of $F_i(X,1)$. Let $\mathcal{O}_i$ be the integral closure of $\mathcal{O}_S$ in $K_i$. Since $\mathcal{O}_S$ is a principal ideal domain, $\mathcal{O}_i$ is a free $\mathcal{O}_S$-module of rank $[K_i : K]$. Assume it has an $\mathcal{O}_S$-basis $\{\omega_1, \ldots, \omega_{d_i}\}$ where $d_i = [K_i : K] = \deg F_i$. The relative discriminant $D_i = D_{K_i/K}(\omega_1, \ldots, \omega_{d_i})$ of an $\mathcal{O}_S$-basis $\omega_1, \ldots, \omega_{d_i}$ is determined up to a multiplication by an element of $\mathcal{O}_S^\times$, hence the discriminant ideal $D_i/\mathcal{O}_S$ of $\mathcal{O}_i$ over $\mathcal{O}_S$ generated by $D_i$ is uniquely determined.

**Lemma 4.1.1.** With the notation as above, we have $D_i|D(F_i)$ for $i = 1, \ldots, d$.

**Proof.** The proof is similar to that of Lemma 3 of [2]. We have included it for convenience of the reader.

We may assume without loss of generality that $F(1,0) \neq 0$ for if not, we may replace $F$ by $F(X, mX + Y)$ for some integer $m$ with $F(1, m) \neq 0$, which does not affect $F_i$ and $D(F_i)$ for $i = 1, \ldots, d$. Fix $i \in \{1, \ldots, n\}$. If $F_i$ has degree 1 then $(D_i) = (1), D(F_i) = 1$. Assume that $F_i$ has degree $d_i \geq 2$. By assumption $F(1,0) \neq 0$, hence

$$F_i = b_0 X^{d_i} + b_1 X^{d_i-1} Y + \cdots + b_{d_i} Y^{d_i} = b_0 N_{K_i/K}(X - \alpha_i Y),$$

where $b_j \in \mathcal{O}_S$ and $b_0 = F_i(1,0) \neq 0$. 

Let
\[
\begin{align*}
\theta_1 &= b_0 \alpha_i + b_1, \\
\theta_2 &= b_0 \alpha_i^2 + b_1 \alpha_i + b_2, \\
\vdots \\
\theta_{d_i-1} &= b_0 \alpha_i^{d_i-1} + b_1 \alpha_i^{d_i-2} + \cdots + b_{d_i-1}.
\end{align*}
\]

We claim that they are integral over \( \mathcal{O}_S \). This is equivalent to the assertion that \( \theta_j - b_j \) is integral over \( \mathcal{O}_S \) for \( j = 1, \ldots, d_i-1 \); we prove this by induction on \( j \). For \( j = 1 \), since \( \sum_{h=0}^{d_i} b_h \alpha_i^{d_i-h} = 0 \), we have \( \sum_{h=0}^{d_i} b_h b_0^{d_i-h} (b_0 \alpha_i)^{d_i-h} = 0 \), hence \( \theta_1 - b_1 \) is integral over \( \mathcal{O}_S \). Now let \( j \geq 2 \) and suppose the claim is true for \( j-1 \). Then using \( \theta_j = \alpha_i \theta_{j-1} + b_j \) and \( \theta_{j-1} \alpha_i^{d_i-j+1} = \sum_{h=d_i-j+1}^{d_i} b_{d_i-j} \alpha_i^h \), we deduce from \( \sum_{h=0}^{d_i} b_h \alpha_i^{d_i-h} = 0 \) that
\[
\begin{align*}
(\theta_j - b_j)^{d_i-j+1} + \sum_{h=0}^{d_i-j} b_{d_i-j} \theta_{j-1}^{d_i-j-h} (\theta_j - b_j)^h \\
&= \theta_{j-1}^{d_i-j+1} \alpha_i^{d_i-j+1} + \sum_{h=0}^{d_i-j} \theta_{j-1}^{d_i-j} b_{d_i-j} \alpha_i^h \\
&= \theta_{j-1}^{d_i-j+1} \alpha_i^{d_i-j+1} - \theta_{j-1}^{d_i-j} \sum_{h=d_i-j+1}^{d_i} b_{d_i-j} \alpha_i^h \\
&= 0.
\end{align*}
\]

Therefore \( \theta_j - b_j \) is integral over \( \mathcal{O}_S[\theta_{j-1}] \), and hence it is integral over \( \mathcal{O}_S \) by the induction hypothesis. This completes the induction hypothesis.

Consider the relative discriminant of \( \{1, \theta_1, \ldots, \theta_{d_i-1}\} \):
\[
D_{K_i/K}(1, \theta_1, \ldots, \theta_{d_i-1}) = \det \left( \begin{array}{cccc}
1 & b_1 & 0 & \cdots \\
b_1 & b_0 & 0 & \cdots \\
\vdots & \vdots & \vdots & \ddots \\
b_{d_i-1} & \cdots & b_1 & b_0
\end{array} \right)^2 \quad D_{K_i/K}(1, \alpha_i, \ldots, \alpha_i^{d_i-1})
= b_0^{2d_i-2} \prod_{1 \leq h < t \leq d_i} (\alpha_i^{(h)} - \alpha_i^{(t)})^2
= D(F_i),
\]
(4.1.1)
where $\alpha_i^{(h)}$ denotes the $h$-th conjugate of $\alpha_i$ in $K_i$, and the last equality comes from the definition. Also, we have $\theta_j = \sum_h a_{jh}\omega_h$ with $a_{jh} \in \mathcal{O}_S$. Then we have

$$D_{K_i/K}(1, \theta_1, \ldots, \theta_d-1) = \det(a_{jh})^2 D_{K_i/K}(\omega_1, \ldots, \omega_d).$$  \hspace{1cm} (4.1.2)

Now (4.1.1) and (4.1.2) complete the proof. \hfill \Box

Because taking the discriminant commutes with localization (see [15]), the ideal $D_{\mathcal{O}_i/\mathcal{O}_S}$ of $\mathcal{O}_S$ is also generated by the relative discriminant ideal $D_{\mathcal{O}_{K_i}}$ of the integral closure $\mathcal{O}_{K_i}$ of $k[t]$ in $K_i$, so $D_{\mathcal{O}_i/\mathcal{O}_S} = D_{\mathcal{O}_{K_i}/k[t]}\mathcal{O}_S$. See also Chapter III, §2, [18].

**Lemma 4.1.2.** Let $K_1, \ldots, K_d$ be as before. For $i = 1, \ldots, d$, let $g_{K_i}$ be the genus of $K_i$. If $\#S > 1$, then

$$\prod_{i=1}^d e^{2g_{K_i}} \leq e^{(\#S-2)(n-d)}|D(F)|_S.$$

**Proof.** By Lemma 1.2.3, we have an element $p$ of $k$ such that if $\nu = \nu_p$ is its corresponding valuation,

$$\nu(D_{\mathcal{O}_{K_i}}) = \sum_{\omega|\nu} \nu(\mathcal{O}_{\mathcal{O}_{K_i}/k[t]}) = \sum_{\omega|\nu} (e(\omega|\nu) - 1).$$

Further, by the Riemann-Hurwitz formula,

$$2g_{K_i} - 2 = [K_i : K](2g_K - 2) + \sum_{\nu} \sum_{\omega|\nu} (e(\omega|\nu) - 1)$$

$$= -2d_i + \sum_{\nu \in S} \sum_{\omega|\nu} (e(\omega|\nu) - 1) + \sum_{\nu \in S} \nu(D_{\mathcal{O}_{K_i}})$$

$$\leq -2d_i + \sum_{\nu \in S} \sum_{\omega|\nu} (e(\omega|\nu) - 1) + \sum_{\nu \in S} \nu(D(F_i)),$$

where the last inequality comes from Lemma 4.1.1.

Since $f(\omega|\nu) = 1$ for each $\omega|\nu$, we have $\sum_{\omega|\nu} e(\omega|\nu) = d_i$. By the definition of the resultant, we have

$$D(F) = \prod_{1 \leq i < j \leq r} R(F_i, F_j)^2 \prod_{i=1}^d D(F_i),$$  \hspace{1cm} (4.1.3)
where \( R(F_i, F_j) \in \mathcal{O}_S \). Hence \( \prod_{i=1}^{d} D(F_i)|D(F) \).

Using \( \sum_{i=1}^{d} d_i = n \), we get
\[
\sum_{i=1}^{d} (2g_{K_i} - 2) \leq \sum_{i=1}^{d} (-2d_i + \sum_{\nu \in S} (d_i - 1)) + \sum_{\nu \notin S} \nu(D(F))
\]
\[
= (n - d)\#S - 2n - \sum_{\nu \in S} \nu(D(F)).
\]

Thus, we conclude that \( \prod_{i=1}^{d} e^{2g_{K_i}} \leq e^{(\#S - 2)(n - d)}|D(F)|_S \).

\section*{4.2 Preparations on polynomials}

Let \( K = k(t) \). We still denote by \( |\cdot|_\nu \) the unique extension of \( |\cdot|_\nu \) to \( \overline{K}_\nu \). Recall that for \( P \in \overline{K}_\nu[X_1, \ldots, X_m] \) we have defined \( |P|_\nu = \max(|a_1|_\nu, \ldots, |a_n|_\nu) \), where \( a_1, \ldots, a_n \) are the non-zero coefficients of \( P \). For a finite set \( S \) of valuations containing \( \{\nu_\infty\} \), \( P \in K[X_1, \ldots, X_m] \), define
\[
|P|_S = \left( \prod_{\nu \in M_K \setminus S} |P|_\nu \right)^{-1} \text{ for } P \neq 0,
\]
and \( \left|0\right|_S = 0 \) by convention. This is well-defined since \( |P|_\nu = 1 \) for almost all \( \nu \in M_K \). For \( P = a \) a constant, we have by the product formula \( |P|_S = \prod_{\nu \in S} |a|_\nu \). If \( P \in \mathcal{O}_S[X_1, \ldots, X_m]\{0\} \), then \( |P|_S \geq 1 \). Clearly, \( |aP|_S = |a|_S|P|_S \) for \( a \in K^*, P \in K[X_1, \ldots, X_m] \). Define the inhomogeneous height of \( P \in K[X_1, \ldots, X_m] \) by
\[
H^*(P) = \prod_{\nu \in M_K} \max(1, |P|_\nu).
\]

For \( P \in \mathcal{O}_S[X_1, \ldots, X_m] \), we have \( |P|_\nu \leq 1 \) for every \( \nu \notin S \), hence
\[
H^*(P) = \prod_{\nu \in S} \max(1, |P|_\nu).
\]

Similarly, for a finite extension \( L \) of \( K \), and \( P \in L[X_1, \ldots, X_m] \), we define
\[
H^*(P) = \left( \prod_{\omega \in M_L} \max(1, |P|_\omega) \right)^{1/[L:K]}.
\]
Lemma 4.2.1. Let $P \in \mathcal{O}_S[X,Y]$ be a binary form. Then there exists $u \in \mathcal{O}_S^*$ such that $H^*(uP) = \prod_{\nu \in S} |P|_{\nu}$.

Proof. We may write $P = \frac{1}{a}(b_0X^n + b_1X^{n-1}Y + \cdots + b_nY^n) \in \mathcal{O}_S[X,Y]$, where $a, b_i \in k[t](1 \leq i \leq n)$, $\gcd(b_0, \ldots, b_n, a) = 1$ and $\frac{b_i}{a} \mid_{\nu} \leq 1$ for every $\nu \notin S$. Since $\gcd(b_0, \ldots, b_n, a) = 1$ we have in fact $\frac{a}{b_i} \mid_{\nu} = 1$ for $\nu \notin S$, i.e., $a \in \mathcal{O}_S^*$.

Assume that $\gcd(b_0, \ldots, b_n) = b \prod_{i=1}^l (t - p_i)^{h_i}$ with $h_i > 0, p_i \in S, 1 \leq i \leq l$ and $b \in k[t]$ a polynomial with zeros outside $S$. Let

$$b'_i = \frac{b_i}{l \prod_{i=1}^l (t - p_i)^{h_i}}, \quad u = \frac{a}{l \prod_{i=1}^l (t - p_i)^{h_i}}.$$

Then

$$b'_i \in \mathcal{O}_S \cap k[t](0 \leq i \leq n), \quad u \in \mathcal{O}_S^*$$

and

$$P = \frac{1}{u}(b'_0X^n + b'_1X^{n-1}Y + \cdots + b'_nY^n).$$

We deduce that

$$H^*(uP) = \prod_{\nu \in \mathcal{S}} \max(1, |uP|_{\nu}) = \max(1, |uP|_{\infty}) = \max_{0 \leq i \leq n}(\deg b'_i).$$

On the other hand, we have that $\gcd(b'_0, \ldots, b'_n) = b$ is coprime with $t - p$ for each $p \in S$ with $p \neq \infty$, hence $\max_{1 \leq i \leq n}(|b'_i|_{\nu}) = 1$ for $\nu \in S \setminus \{\infty\}$. Recalling that $u \in \mathcal{O}_S^*$, we see that

$$\prod_{\nu \in \mathcal{S}} |P|_{\nu} = \prod_{\nu \in \mathcal{S}} \max_{0 \leq i \leq n}(|b'_i|_{\nu}) = \frac{\prod_{\nu \in \mathcal{S}} \max_{0 \leq i \leq n}(|b'_i|_{\nu})}{\prod_{\nu \in \mathcal{S}} |u|_{\nu}} = \prod_{\nu \in \mathcal{S}} \max_{0 \leq i \leq n}(|b'_i|_{\nu}) = H^*(uP).$$

Clearly, this result only depends on the coefficients and hence can be extended for polynomials in more variables.
For $F(X, Y) = a_0 X^n + a_1 X^{n-1} Y + \cdots + a_n Y^n \in \mathcal{O}_S[X, Y]$, let $L$ be its splitting field over $K$, and $G = \text{Gal}(L/K)$ the corresponding Galois group. In this case, $N_{L/K}(P) = \prod_{\sigma \in G} \sigma(P)$.

**Lemma 4.2.2.** Let $F = aN_{L/K}(l)$. Then there are $a' \in K^*$ and $\lambda \in L^*$ such that $F = a'N_{L/K}(l')$ where $l' = \lambda l \in \mathcal{O}_T[X, Y]$, and

$$e^{-2g_L} \prod_{\nu \in M_K \setminus S} |F|_{\nu}^{-1} \leq |a'|_S \leq \prod_{\nu \in M_K \setminus S} |F|_{\nu}^{-1}.$$ 

**Proof.** Notice that by section 1.4 the sets $\mathcal{E}(\omega|\nu)$ are a partition of $G = \text{Gal}(L/K)$, so

$$|N_{L/K}(l)|_{\nu} = \prod_{\sigma \in G} |\sigma(l)|_{\nu} = \prod_{\omega|\nu \in \mathcal{E}(\omega|\nu)} |\sigma(l)|_{\nu} = \prod_{\omega|\nu} |l|_{\omega}.$$ 

Let $\omega_0 \in T$. Then by Lemma 3.2.3, there exists $\lambda \in L^*$ such that

$$\begin{cases}
|\lambda|_{\omega_0} \leq e^{2g_L} \prod_{\nu \in S} |N_{L/K}(l)|_{\nu}, \\
|\lambda|_{\omega} \leq 1 \quad &\text{for } \omega \in T \setminus \{\omega_0\}, \\
|\lambda|_{\omega} \leq |l|_{\omega}^{-1} \quad &\text{for } \omega \in M_L \setminus T.
\end{cases}$$

For this $\lambda$ and $a' = aN_{L/K}(\lambda)^{-1}$, we see that $F = a'N_{L/K}(\lambda l)$ and the coefficients of $\lambda l$ are in $\mathcal{O}_T$. Hence, we have $N_{L/K}(l') \in \mathcal{O}_S[X, Y]$. So we have

$$|F|_{\nu} = |a'|_{\nu} |N_{L/K}(l')|_{\nu} \leq |a'|_{\nu} \text{ for } \nu \not\in S.$$ 

From the product formula, we deduce that $|a'|_S \leq \left( \prod_{\nu \in M_K \setminus S} |F|_{\nu} \right)^{-1}$ and

$$|a'|_S = |a|_S |N_{L/K}(\lambda)|^{-1}_S = |a|_S \prod_{\omega \in T} |\lambda|_{\omega}^{-1} \geq e^{-2g_L} |a|_S \prod_{\nu \in M_L \setminus S} |N_{L/K}(l)|_{\nu}^{-1} \geq e^{-2g_L} \prod_{\nu \in M_K \setminus S} |F|_{\nu}^{-1}.$$ 

$\square$
Chapter 4. Reduction theory for binary forms over \( k(t) \)

**Lemma 4.2.3.** Let \( F(X,Y) = a_0X^n + a_1X^{n-1}Y + \cdots + a_nY^n \in \mathcal{O}_S[X,Y] \) be a binary form with \( D(F) \neq 0 \). Then we have a factorization \( F = a_1 \prod_{i=1}^n l_i \), where \( a \in K^* \) and the \( l_i \) are linear forms in \( \mathcal{O}_T[X,Y] \) such that for every \( \sigma \in G, \sigma(l_1), \ldots, \sigma(l_n) \) is a permutation of \( l_1, \ldots, l_n \).

**Proof.** Since \( K[X,Y] \) is a UFD, we may assume \( F = f_1 \cdots f_g \) with \( f_i \) irreducible over \( K \), \( 1 \leq i \leq g \).

For a fixed \( i \) with \( 1 \leq i \leq g \), if \( f_i \neq Y \), we may write \( f_i = c_i N_{L_i/K}(l_i) \), with \( L_i \) a subfield of \( L/K \) generated by a root of \( f_i(X,1) \), and \( c_i \in K, l_i \in L_i[X,Y] \). By Lemma 4.2.2, we have \( f_i = c'_i N_{L_i/K}(l'_i) \) with \( c'_i \in K, l'_i \in \mathcal{O}_T[X,Y] \).

So we have \( F = a \prod_{i=1}^g N_{L_i/K}(l'_i) \) with \( a \in K, l'_i \in \mathcal{O}_T[X,Y] \). This gives a factorization into linear forms of \( \mathcal{O}_T[X,Y] \), up to a scalar in \( K \).

For every \( \sigma \in \text{Gal}(L/K) \), the restriction \( \sigma|_{L_i} \) is a \( K \)-isomorphism of \( L_i \), hence \( \sigma \) acts as a permutation. This completes the proof.

**Remark 4.2.4.** In accordance with Lemma 4.2.3, later we will view \( \sigma \in G \) as a permutation of \( (1, \ldots, n) \) such that \( \sigma(l_i) = l_{\sigma(i)} \) for \( i = 1, \ldots, n \).

### 4.3 Reduced binary forms and successive minima

Let \( F(X,Y) \in \mathcal{O}_S[X,Y] \) be a binary form of degree \( n > 1 \) with \( D(F) \neq 0 \), and let \( L \) be the splitting field of \( F(X,Y) \) over \( K \) and \( G = \text{Gal}(L/K) \). By Lemma 4.2.3 we have a factorization \( F = a \prod_{i=1}^n l_i \) with \( l_i \in L[X,Y] \) and for each \( \sigma \in G \) a permutation \( \sigma(l_1), \ldots, \sigma(l_n) \) of \( l_1, \ldots, l_n \).

For \( \omega \in M_L \) and \( \sigma \in G \), there is \( \omega \circ \sigma \in M_L \) such that \( |x|_{\omega \circ \sigma} = |\sigma(x)|_\omega \) for \( x \in L \), and \( \omega \circ \sigma \in T \) if and only if \( \omega \in T \).

**Definition 4.3.1.** We call \( \mathcal{A} = (A_{i\omega} : \omega \in T, i = 1, \ldots, n) \) an admissible tuple if \( A_{i\omega} > 0 \) and \( A_{\sigma(i)\omega} = A_{i\omega \circ \sigma} \) for \( \omega \in T, \sigma \in G, i = 1, \ldots, n \).
4.3. Reduced binary forms and successive minima

For \( \nu \in S \), denote by \( A(\nu) \) the set of valuations of \( L \) lying above \( \nu \), and put

\[
C_\nu = \{ x \in K_\nu^2 : |l_i(x)|_\omega \leq A_{i\omega} \text{ for } i = 1, \ldots, n, \omega|\nu \}. \tag{4.3.1}
\]

It is easy to check that this is a \( \nu \)-adic symmetric convex body since \( D(F) \neq 0 \). Consider \( C = \prod_{\nu \in S} C_\nu \) and let \( \lambda_1, \lambda_2 \) be the successive minima of \( C \). Here \( C_\nu \) and \( C \) depend on \( A \), but for convenience we omit the subscript \( A \) here. To estimate \( \lambda_1 \lambda_2 \), we try to rewrite \( C_\nu \) so that Theorem 3.2.1 can be applied to it.

**Lemma 4.3.2.** Let \( A \) be an admissible tuple and let \( \lambda_1, \lambda_2 \) be the successive minima of \( C \). Assume \( n \geq 2 \). Then

\[
\lambda_1 \lambda_2 \geq \left( \prod_{\omega \in T} \max_{1 \leq i < j \leq n} \frac{\det(l_i, l_j)|_\omega}{A_{i\omega}A_{j\omega}} \right)^{1/[L:K]}, \tag{4.3.2}
\]

\[
\lambda_1 \lambda_2 \leq e^{(n+1)\#S} \left( \prod_{\omega \in T} \max_{1 \leq i < j \leq n} \frac{\det(l_i, l_j)|_\omega}{A_{i\omega}A_{j\omega}} \right)^{1/[L:K]} \tag{4.3.3}
\]

**Proof.** First, let \( s(\omega) = [L_\omega : K_\infty] \) if \( \omega|\infty \) and \( s(\omega) = 0 \) otherwise. As \( C_\nu = \{ x \in K_\nu^2 : |l_i(x)|_\omega \leq A_{i\omega} \text{ for } i = 1, \ldots, n, \omega|\nu \} \), we have

\[
\lambda C_\nu = \{ |l_i(x)|_\omega \leq \lambda^{s(\omega)} A_{i\omega} \text{ for } i = 1, \ldots, n, \omega|\nu \}\}
\]

By Theorem 3.1.8, we can choose an \( O_S \)-basis \( \{ y_1, y_2 \} \) of \( O_S^2 \) such that \( y_i \in \lambda_i C, i = 1, 2 \). Since \( \det(l_i, l_j) \det(y_1, y_2) = \det \left( \begin{array}{cc} l_i(y_1) & l_i(y_2) \\ l_j(y_1) & l_j(y_2) \end{array} \right) \), we deduce that

\[
\frac{\det(l_i, l_j)|_\omega}{A_{i\omega}A_{j\omega}} = \frac{1}{|\det(y_1, y_2)|_\omega A_{i\omega}A_{j\omega}} \left| \det \left( \begin{array}{cc} l_i(y_1) & l_i(y_2) \\ l_j(y_1) & l_j(y_2) \end{array} \right) \right|_\omega \leq (\lambda_1 \lambda_2)^{s(\omega)} |\det(y_1, y_2)|_\omega.
\]

Hence

\[
\prod_{\omega \in T} \max_{1 \leq i < j \leq n} \frac{\det(l_i, l_j)|_\omega}{A_{i\omega}A_{j\omega}} \leq \frac{(\lambda_1 \lambda_2)^{\sum_{[L_\omega : K_\infty]} |L_\infty : K_\infty|}}{|\det(y_1, y_2)|_T} = (\lambda_1 \lambda_2)^{[L:K]}.
\]
This gives (4.3.2).

For the second inequality, put \( B_{i\nu} = A_{\sigma^{-1}(i),\omega}^{1/g_{i\nu}} \) with corresponding \( \omega \in \mathcal{A}(\nu) \) and \( \sigma \in \mathcal{E}(\omega|\nu) \). We show that this is independent of the choice of \( \omega, \sigma \).

Let \( \omega', \sigma' \) be another pair with \( \omega' \in \mathcal{A}(\nu) \) and \( \sigma' \in \mathcal{E}(\omega'|\nu) \). Then \( \omega \circ \tau = \omega' \) for \( \tau = \sigma^{-1}\sigma' \), and by the admissibility of \( \mathcal{A} \),

\[
A_{\sigma^{-1}(i),\omega'} = A_{\tau^{-1}\sigma^{-1}(i),\omega'} = A_{\sigma^{-1}(i),\omega'\circ\tau^{-1}} = A_{\sigma^{-1}(i),\omega},
\]

hence the \( B_{i\nu} \) are well-defined. Moreover, since \( \mathcal{E}(\omega|\nu) \) is a right-coset of \( \text{Gal}(L_{\omega_1}/K_{\nu}) \), if \( j = \tau(i) \) for \( \tau \in \text{Gal}(L_{\omega_1}/K_{\nu}) \), then \( B_{i\nu} = B_{j\nu} \).

With this notation, by (1.4.3) we have that for \( x \in K_{\nu}^2 \) the condition

\[
|l_i(x)|_\omega \leq A_{i\omega} \text{ for } 1 \leq i \leq n, \omega \in \mathcal{A}(\nu)
\]
is equivalent to the condition

\[
|\sigma(l_i)(x)|_{\nu} \leq B_{\sigma(i),\nu} \text{ for } 1 \leq i \leq n, \omega \in \mathcal{A}(\nu), \sigma \in \mathcal{E}(\omega|\nu),
\]

that is,

\[
|l_{\sigma(i)}(x)|_{\nu} \leq B_{\sigma(i),\nu} \text{ for } 1 \leq i \leq n, \sigma \in \text{Gal}(L/K),
\]

which is equivalent to the condition

\[
|l_i(x)|_{\nu} \leq B_{i\nu} \text{ for } 1 \leq i \leq n.
\]

Altogether, we get

\[
C_{\nu} = \{ x \in K_{\nu}^2 : |l_i(x)|_{\nu} \leq B_{i\nu} \text{ for } 1 \leq i \leq n \}.
\]

Since \( |\cdot|_{\nu} \) is normalized, the value set of \( K_{\nu}^* \) is \( e^Z \), hence for \( \nu \in S \), we can choose \( a_{i\nu} \in K_{\nu}^* \), \( 1 \leq i \leq n \) satisfying

\[
\begin{align*}
B_{i\nu}/e < |a_{i\nu}|_{\nu} & \leq B_{i\nu} \text{ for } 1 \leq i \leq n, \\
a_{i\nu} = a_{j\nu} & \text{ if } i = \tau(j) \text{ for } \tau \in \text{Gal}(L_{\omega_1}/K_{\nu}).
\end{align*}
\]

Put \( m_{i\nu} = a_{i\nu}^{-1}l_i \) for \( \nu \in S, 1 \leq i \leq n \). By the choice of \( l_i \) and \( a_{i\nu} \), the system \( \{ m_{1\nu}, \ldots, m_{n\nu} \} \) is \( \text{Gal}(K_{\nu}/K_{\nu}) \)-symmetric. Further, let

\[
C'_{\nu} = \{ x \in K_{\nu}^2 : |m_{i\nu}(x)|_{\nu} \leq 1 \text{ for } 1 \leq i \leq n \}.
\]
Then \( C'_\nu \subset C_\nu \). Hence, the successive minima \( \lambda'_1, \lambda'_2 \) of \( \prod_{\nu \in S} C'_\nu \) satisfy \( \lambda_i \leq \lambda'_i \) for \( i = 1, 2 \). By Theorem 3.2.1, we have

\[
\lambda_1 \lambda_2 \leq \lambda'_1 \lambda'_2 \leq e^{(n-1)\#S} \prod_{\nu \in S} \max_{1 \leq i < j \leq n} |\det(m_{i,\nu}, m_{j,\nu})|_\nu
\]

By (4.3.4), this implies (4.3.3), and we complete the proof of our lemma.

Using Lemma 4.3.2, we can prove the following

**Theorem 4.3.3.** Let \( F \in \mathcal{O}_S[X,Y] \) be a binary form of degree \( n \) with non-zero discriminant and with splitting field \( L \) over \( K \), and choose a factorization \( F = a \prod_{i=1}^n l_i \) with \( a \in K^*, l_i \in L[X,Y]^{lm} \) such that for every \( \sigma \in G \),
Chapter 4. Reduction theory for binary forms over \( k(t) \)

\((\sigma(l_1), \ldots, \sigma(l_n))\) is a permutation of \((l_1, \ldots, l_n)\). Put

\[
M = \prod_{\omega \in T} \prod_{i=1}^{n} A_{i\omega},
\]

\[
R = \prod_{\omega \in T} \max_{1 \leq i < j \leq n} |\det(l_i, l_j)|_{\omega}.
\]

(i) If \( n \geq 2 \) and \( F \) has no factor in \( K[X,Y]^{lin} \), then \( F \) is \( \text{GL}(2, \mathcal{O}_S) \)-equivalent to a binary form \( F^* \) such that

\[
H^*(F^*) \leq e^{n(n+1)\#S} |a|_S^2 R^n/[L:K] M^2/[L:K].
\]

(ii) If \( n \geq 3 \) and \( F \) does have a factor in \( K[X,Y]^{lin} \), then \( F \) is \( \text{GL}(2, \mathcal{O}_S) \)-equivalent to a binary form \( F^* \) such that

\[
H^*(F^*) \leq \left( e^{n(n+1)\#S} |a|_S^2 R^n/[L:K] M^2/[L:K] \right)^{(n-1)/(n-2)}.
\]

Proof. By Theorem 3.1.8, we have a basis \( a_1 = (a_{11}, a_{21}), a_2 = (a_{12}, a_{22}) \) of \( \mathcal{O}_S^2 \) such that \( a_i \in \lambda_i \prod_{\nu \in S} C_{\nu} \) for \( i = 1, 2 \). Hence we have

\[
|l_i(a_1)|_{\omega} \leq \lambda_1^{s(\omega)} A_{i\omega},
\]

\[
|l_i(a_2)|_{\omega} \leq \lambda_2^{s(\omega)} A_{i\omega}, \tag{4.3.5}
\]

for \( 1 \leq i \leq n, \omega \in T \), with \( s(\omega) = [L_\omega : K_\infty] \) if \( \omega|\nu_\infty \) and zero otherwise.

Take \( U = (a_{11} \ 0_{12}, 0_{21} \ a_{22}) \). Then \( U \in \text{GL}(2, \mathcal{O}_S) \), and \( F_U = a \prod_{i=1}^{n} m_i \) with \( m_i = l_i(a_1)X + l_i(a_2)Y \) for \( i = 1, \ldots, n \). We deduce that for \( \omega \in T \),

\[
|F_U|_{\omega} \leq |a|_\omega \prod_{i=1}^{n} \max(|l_i(a_1)|_{\omega}, |l_i(a_2)|_{\omega})
\]

\[
\leq |a|_\omega \lambda_2^{s(\omega)} \prod_{i=1}^{n} A_{i\omega}.
\]

Also, we have

\[
\prod_{\omega|\nu} |a|_{\omega} = |a|_\nu^{[L:K]}, \prod_{\omega|\nu} |F_U|_{\omega} = |F_U|_\nu^{[L:K]}
\]
4.3. Reduced binary forms and successive minima

and

\[ \sum_{\omega \in T} s(\omega) = [L : K], \]

therefore, we get

\[ \prod_{\nu \in S} |F_U|_{\nu} = (\prod_{\omega \in T} |F_U|_{\omega})^{1/[L:K]} \leq |a|_S \lambda_2^n M^{1/[L:K]}. \]

By Lemma 4.2.1, there exists \( u \in O_S^* \) such that \( F^* = uF_U \) satisfies \( H^*(F^*) = \prod_{\nu \in S} |F_U|_{\nu} \), hence

\[ H^*(F^*) \leq |a|_S \lambda_2^n M^{1/[L:K]}, \tag{4.3.6} \]

What remains is to estimate \( \lambda_2 \). First assume that \( F \) has no linear factor in \( K[X,Y] \), so \( F(a_1) \in O_S \setminus \{0\} \). Now by (4.3.5) we have

\[ 1 \leq \prod_{\omega \in T} |F(a_1)|_\omega = \prod_{\omega \in T} |a|_\omega \prod_{\omega \in T} \prod_{i=1}^n |l_i(a_1)|_\omega \leq |a|_S \lambda_1^n [L:K] M. \]

Together with Lemma 4.3.2, we deduce that

\[ \lambda_2^n \leq c^{n(n+1)\#S} |a|_S R^n/[L:K] M^{1/[L:K]}, \]

and therefore by (4.3.6),

\[ H^*(F^*) \leq c^{n(n+1)\#S} |a|_S^2 R^n/[L:K] M^{2/[L:K]}. \]

Next assume that \( F \) does have a linear factor in \( K[X,Y] \). If \( F(a_1) \neq 0 \), we still have the above result. Assume \( F(a_1) = 0 \) and \( n \geq 3 \). Without loss of generality, let \( l_1(a_1) = 0 \). Since \( D(F) \neq 0 \), we have

\[ W := a l_1(a_2) \prod_{i=2}^n l_i(a_1) \neq 0. \]

As \( a_1, a_2 \in O_S \), we have by Gauss’ Lemma

\[ |W|_{\omega} \leq |a|_\omega \prod_{i=1}^n |l_i|_\omega = |F|_\omega \leq 1 \text{ for } \omega \notin T. \]
Hence, using (4.3.5) we deduce that
\[ 1 \leq \prod_{\omega \in T} |W|_{\omega} \leq (\lambda_1^{n-1} \lambda_2)^{[L:K]} \prod_{\omega \in T} |a|_{\omega} M = |a|_{S}^{[L:K]}(\lambda_1^{n-1} \lambda_2)^{[L:K]} M. \]

Then together with Lemma 4.3.2, we obtain
\[ \lambda_2^{-2} \leq \lambda_2^{-2} \cdot (\lambda_1^{n-1} \lambda_2)|a|_{S} M^{\frac{1}{2}} \leq |a|_{S} e^{(n^2-1)S} M^{1/[L:K]} R^{(n-1)/[L:K]}, \]

and finally, by (4.3.6)
\[ H^{*}(F^{*}) \leq \left( e^{n(n+1)S} |a|_{S}^{2} R^{n/[L:K]} M^{2/[L:K]} \right)^{(n-1)}/(n-2). \]

\[ \square \]

**Remark 4.3.4.** The binary form \( F^{*} \) depends on the admissible tuple \( A \). We say that \( F^{*} \) is associated with \( A \). By taking the special case \( A_{i\omega} = 1 \) for \( 1 \leq i \leq n, \omega \in T \), we obtain:

**Corollary 4.3.5.** Let \( F \in \mathcal{O}_{S}[X,Y] \) be a binary form of degree \( n \) with non-zero discriminant. Then with the same factorization of \( F \) as in Theorem 4.3.3,

(i) if \( n \geq 2 \) and \( F \) has no factor in \( K[X,Y]^{\text{lin}} \), then \( F \) is \( \text{GL}(2, \mathcal{O}_{S}) \)-equivalent to a binary form \( F^{*} \) such that
\[ H^{*}(F^{*}) \leq e^{n(n+1)S} |a|_{S}^{2} \left( \prod_{\omega \in T} \max_{1 \leq i < j \leq n} |\det(l_i, l_j)|_{\omega} \right)^{n/[L:K]}. \]

(ii) if \( n \geq 3 \) and \( F \) does have a factor in \( K[X,Y]^{\text{lin}} \), then \( F \) is \( \text{GL}(2, \mathcal{O}_{S}) \)-equivalent to a binary form \( F^{*} \) such that
\[ H^{*}(F^{*}) \leq \left( e^{n(n+1)S} |a|_{S}^{2} \left( \prod_{\omega \in T} \max_{1 \leq i < j \leq n} |\det(l_i, l_j)|_{\omega} \right)^{n/[L:K]} \right)^{(n-1)}/(n-2). \]
4.3. Reduced binary forms and successive minima

Corollary 4.3.6. Let $F \in \mathcal{O}_S[X,Y]$ be a binary quadratic form of non-zero discriminant $D(F)$. Then $F$ is $\text{GL}(2, \mathcal{O}_S)$-equivalent to a binary form $F^*$ such that $H^*(F^*) \leq e^{6\#S}|D(F)|_S$.

Proof. If $F$ is irreducible over $K$, then we may factor as $F = al_1l_2$ with $a \in K^*, l_1, l_2 \in L[X,Y]$ conjugate over $K$ and in this case, $n = 2, [L : K] = 2$ and $D(F) = a^2 \det(l_1, l_2)^2$. Take $A_{1\omega} = A_{2\omega} = 1$ for every $\omega \in T$. By Theorem 4.3.3, there exists a binary form $F^*$ equivalent to $F$ such that $H^*(F^*) \leq e^{6\#S}|D(F)|_S$.

However, if $F$ is reducible over $K$, then $L = K, T = S$. We follow the idea in the proof of Theorem 4.3.3. We may factor $F$ as $F = l_1l_2$ with $l_1, l_2 \in K[X,Y]$ conj. Take $A_{1\infty} = |l_1|_S, A_{2\infty} = |l_2|_S, A_{i\nu} = 1$ for $\nu \in S \setminus \infty, i = 1, 2$. Further, take $a_1, a_2 \in \mathcal{O}_S^2$ as in proof of Theorem 4.3.3. Then one of $l_1(a_1), l_2(a_1)$ is non-zero, say, $l_1(a_1) \neq 0$, and we have

$$1 = \prod_{\nu \in M_K} |l_1(a_1)|_\nu \leq \prod_{\nu \in S} |l_1(a_1)|_\nu \prod_{\nu \notin S} |l_1|_\nu \leq \lambda_1 |l_1|_S \prod_{\nu \notin S} |l_1|_\nu = \lambda_1.$$

Applying Lemma 4.3.2, we get

$$\lambda_2 \leq \lambda_1 \lambda_2 \leq e^{3\#S} |\det(l_1, l_2)|_S/|l_1l_2|_S.$$

Hence there exists $F^*$ equivalent to $F$ such that

$$H^*(F^*) \leq e^{6\#S} |\deg(l_1, l_2)|_S^2 = e^{6\#S}|D(F)|_S.$$

\hfill $\Box$

Corollary 4.3.7. Let $F \in \mathcal{O}_S[X,Y]$ be a binary cubic form of non-zero discriminant $D(F)$. Then $F$ is $\text{GL}(2, \mathcal{O}_S)$-equivalent to a binary form $F^*$ such that
(i) If $F$ is irreducible over $K$, then $H^*(F^*) \leq e^{12\#S}|D(F)|^{\frac{1}{2}}$.

(ii) If $F$ is reducible over $K$, then $H^*(F^*) \leq e^{12\#S}|D(F)|_S$.

**Proof.** Factor as $F = al_1l_2l_3$. Take $A_{i\omega} = |\det(l_j, l_h)|_\omega^{-1}$ for $i = 1, 2, 3, \omega \in T$ with $\{i, j, h\} = \{1, 2, 3\}$. This gives an admissible tuple. Indeed, for $\sigma \in \text{Gal}(L/K), \omega \in T$ and $i = 1, 2, 3$, we have

$$A_{\sigma(i), \omega} = |\det(l_{\sigma(j)}, l_{\sigma(h)})|_{\omega}^{-1} = |\sigma(\det(l_j, l_h))|_{\omega}^{-1} = |\det(l_j, l_h)|_{\omega \circ \sigma}^{-1} = A_{i, \omega \circ \sigma}.$$ 

By $\prod_{\omega | \nu} |a|_\nu = |a|_{[L:K]}$, we have

$$\prod_{\omega \in T} A_{i\omega} = (\prod_{\nu \in S} |\det(l_1, l_2) \det(l_2, l_3) \det(l_3, l_1)|_{[L:K]}^{[L:K]}),$$

and further,

$$\max_{1 \leq i < j \leq 3} \frac{|\det(l_i, l_j)|_{\omega}}{A_{i\omega} A_{j\omega}} = |\det(l_1, l_2) \det(l_2, l_3) \det(l_3, l_1)|_{\omega},$$

$$a^4(\det(l_1, l_2) \det(l_2, l_3) \det(l_3, l_1))^2 = D(F).$$

Now an application of Theorem 4.3.3 gives the desired result. \qed