立教大学

国際学術交流報告書

第六輯

代数群の整数論とその応用

小野　孝

立教大学

1986年

ISSN 0388-5305

立教大学国際学術交流報告書　第六輯

St. Paul's International Exchange Series Occasional Papers VI

Arithmetic of Algebraic Groups and its Applications

(Dedicated to John Tate)

Lectures by Takashi Ono

given at
Rikkyo University, Tokyo
Spring, 1985.

Notes by N. Aoki

ST. PAUL'S UNIVERSITY

1986

立教大学

国際学術交流報告書

第六輯

代数群の整数論とその応用

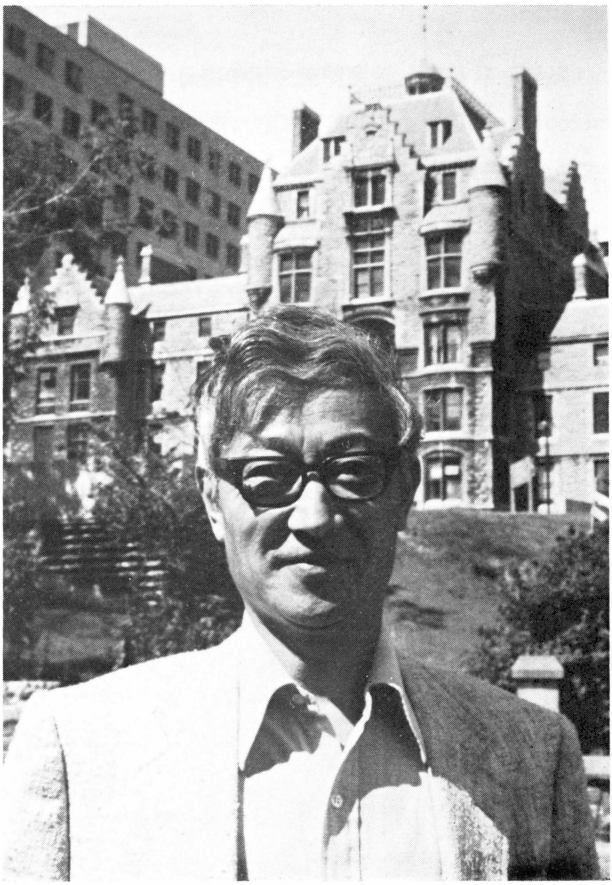
(J. テイトに捧ぐ)

小野　孝

(青木　昇記)

立教大学

1986年



まえがき

1980年に発足した本学の国際学術交流制度も，満5年を経過し，いよいよ充実してまいりました。1985年度は招聘研究員として Johns Hopkins 大学教授小野孝博士をお迎えすることができました。小野博士は代数群論の研究に於て先駆的な仕事をなされた国際的な数学者と承っております。

活発に活躍しておられる現役の数学者との交流が，学問の風通しをよくし，多くの成果を生み出すことを期待したいと思います。

1985年10月

立教大学総長

高　橋　健　人

FOREWORD

This book reproduces, with Notes and Bibliography, a set of ten lectures given at Rikkyo University, Tokyo, from April 11 to June 20, 1985, i.e. every Thursday of that interval except May 2 which belongs to the Golden Week.

These lectures are concerned with an interpretation and a generalization of the genus theory of C. F. Gauss on binary quadratic forms in the language of arithmetic of algebraic groups, especially of algebraic tori. The theory of Gauss may be described as establishing an equality between a kind of "Euler number $E(K/\boldsymbol{Q})$" of a quadratic field K over $\boldsymbol{Q}$ and other arithmetical invariants of K. The definition of such an "Euler number" can easily be generalized to an arbitrary relative extension K/k of number fields and general arithmetic theory of tori, e.g. the theory of isogenies, class numbers, Tamagawa numbers, etc., furnishes us with tools to determine $E(K/k)$. The process is most successful when K/k is a cyclic Kummer extension.

I wish to express my thanks to Mr. N. Aoki who took notes, to Ms. Y. Uchida who typed the manuscript and to Messrs. M. Endo, T. Arakawa and F. Sato who took the trouble to prepare the whole volume for print and thereby detected various mistakes which appeared in its original form.

Last but not least, I express my thanks to President T. Takahashi of Rikkyo University and to Ms. K. Nakao in the office of International Exchange Programs of the University who made my visit possible.

The Johns Hopkins University
August 27, 1985 Takashi ONO

NOTATION AND CONVENTIONS

As usual, $\boldsymbol{Z}$, $\boldsymbol{Q}$, $\boldsymbol{R}$, $\boldsymbol{C}$ are the integers, the rational numbers, the real numbers, the complex numbers, respectively. For a rational prime p, $\boldsymbol{Z}_p$, $\boldsymbol{Q}_p$ are the p-adic integers, p-adic numbers, respectively. We think of ∞ as the last prime and put $\boldsymbol{Z}_\infty = \boldsymbol{Q}_\infty = \boldsymbol{R}$. For an associative ring R with 1, we denote by $R^\times$ the group of units, i.e. invertible elements of R. $M_n(R)$ is the ring of matrices of degree n over a ring R. We put $GL_n(R) = M_n(R)^\times$. When R is commutative $SL_n(R)$ is the group of matrices in $GL_n(R)$ of determinant $= 1$. $\bar{K}$ is the algebraic closure of a field K. $\# X$ is the cardinality of a set X. $\boldsymbol{R}_+^\times$ denotes the multiplicative group of positive real numbers. When k is an algebraic number field of finite degree over $\boldsymbol{Q}$, we denote by k_v the completion of k with respect to a valuation v of k; if v is discrete, we use often notation $\mathfrak{p}$ for v and denote by $\mathfrak{o}_\mathfrak{p}$ the ring of $\mathfrak{p}$-adic integers in $k_\mathfrak{p}$.

TABLE OF CONTENTS

Arithmetic of Algebraic Groups and its Applications

(Dedicated to John Tate)

by
Takashi ONO

I. Classes of Binary Quadratic Forms

Consider a quadratic form

$$f=ax^2+bxy+cy^2\,,\qquad a,b,c\in\boldsymbol{Z}\,.$$

Assume that the discriminant $\Delta_f=b^2-4ac\neq 0$. One can write

$$f(z)={}^tzFz\qquad\text{with}\quad z=\begin{pmatrix}x\\y\end{pmatrix},\quad F=\begin{pmatrix}a & b/2\\ b/2 & c\end{pmatrix}.$$

We introduce two equivalence relations $\sim$ and $\overset{+}{\sim}$. Let $g=a'x^2+b'xy+c'y^2$ be another integral quadratic form with the matrix G.

DEFINITION 1.

$$f\sim g \overset{\text{def}}{\Longleftrightarrow} g(z)=f(\gamma z)\,,\qquad \exists\,\gamma\in GL_2(\boldsymbol{Z})\,,$$
$$f\overset{+}{\sim}g \overset{\text{def}}{\Longleftrightarrow} g(z)=f(\gamma z)\,,\qquad \exists\,\gamma\in SL_2(\boldsymbol{Z})\,.$$

Obviously $f\overset{+}{\sim}g\Rightarrow f\sim g$, but the converse is not true. For example, put

$$f=3x^2+2xy+5y^2\,,\qquad F=\begin{pmatrix}3 & 1\\ 1 & 5\end{pmatrix}$$
$$g=3x^2-2xy+5y^2\,,\qquad G=\begin{pmatrix}3 & -1\\ -1 & 5\end{pmatrix}.$$

We have $\Delta_f=\Delta_g=-2^3\cdot 7$. Since ${}^tTFT=G$ with $T=\left(\begin{smallmatrix}1 & 0\\ 0 & -1\end{smallmatrix}\right)$, we have $f\sim g$. If $f\overset{+}{\sim}g$, there must be an integral matrix U with $\det U=-1$ such that ${}^tUFU=F$. Write $U=\left(\begin{smallmatrix}x & y\\ z & u\end{smallmatrix}\right)$, $xu-yz=-1$. From ${}^tUF=FU^{-1}$, we get

$$\begin{pmatrix} 3x+z & x+5z \\ 3y+u & y+5u \end{pmatrix} = \begin{pmatrix} -3u+z & 3y-x \\ -u+5z & y-5x \end{pmatrix}.$$

Eliminating u from the relations

$$\begin{cases} 3x+z=-3u+z \\ x+5z=3y-x \\ xu-yz=-1 \end{cases}$$

we get

$$\begin{cases} 3y=2x+5z \\ x^2+yz=1\,. \end{cases}$$

Eliminating y from the last relations, we have

$$3x^2+(2x+5z)z=3\,, \qquad \text{i.e.} \quad (3x+z)^2+14z^2=9\,.$$

If $z=0$, then $x=\pm 1$ and so $3y=\pm 2$, which is impossible. If $z\neq 0$, then $14z^2\leq 9$ which is impossible, too. Hence $f \overset{+}{\sim} g$ is not true.

Let us recall some standard notions on quadratic fields.[1] Let m ($\neq 0, 1$) be a square-free integer and $K=\boldsymbol{Q}(\sqrt{m})$. Denote by Δ_K the discriminant of K. If we put

$$\omega=\begin{cases} \sqrt{m}\,, & m\equiv 2, 3 \pmod 4\,, \\ (1+\sqrt{m})/2\,, & m\equiv 1 \pmod 4\,, \end{cases}$$

then, $1, \omega$ form the canonical basis of the ring $\mathfrak{o}_K$ of integers, $\mathfrak{o}_K=\boldsymbol{Z}+\boldsymbol{Z}\omega=[1, \omega]$. We have

$$\Delta_K \overset{\text{def}}{=} \begin{vmatrix} 1 & \omega \\ 1 & \omega' \end{vmatrix}^2 = \begin{cases} 4m\,, & m\equiv 2, 3 \pmod 4 \\ m\,, & m\equiv 1 \pmod 4 \end{cases}$$

where ω' is the conjugate of ω. We denote by I_K the group of (fractional) ideals of K, by P_K the subgroup of I_K of principal ideals. Furthermore, we put

$$P_K^+=\{\mathfrak{a}=(\alpha)\in P_K\,;\ N\alpha>0\}\,.^{2)}$$

We have

$$(1) \qquad [P_K:P_K^+]=\begin{cases} 1\,, & m<0 \text{ or } m>0\,,\ \exists\varepsilon\in\mathfrak{o}_K^\times\,,\ N\varepsilon=-1\,, \\ 2\,, & m>0\,,\ N\varepsilon=1\,,\ \forall\varepsilon\in\mathfrak{o}_K^\times\,. \end{cases}$$

Next, we define the factor groups:

$$H_K = I_K/P_K\,, \qquad h_K = \# H_K\,,$$
$$H_K^+ = I_K/P_K^+\,, \qquad h_K^+ = \# H_K^+\,.$$

Hence, $h_K^+ = h_K$ or $2h_K$ by (1). h_K is the class number of K and h_K^+ is the class number of K in the narrow sense. We denote the equivalence of ideals mod P_K (resp. mod P_K^+) by $\mathfrak{a} \sim \mathfrak{b}$ (resp. $\mathfrak{a} \overset{+}{\sim} \mathfrak{b}$).

An ideal $\mathfrak{a} \subset \mathfrak{o}_K$ is called primitive if it is not divisible by a natural number >1. Such an ideal has the canonical basis:

$$\mathfrak{a} = [a, h+\omega]\,, \qquad a = N\mathfrak{a}\,, \quad h \ (\mathrm{mod}\, a)\,.$$

Furthermore, we have

$$a \mid N(h+\omega)\,. \tag{2}$$

Conversely, if a Z-module $\mathfrak{m} = [a, h+\omega]$ in $\mathfrak{o}_K$ has the property (2), then $\mathfrak{m}$ becomes an ideal and $a, h+\omega$ form a generator of $\mathfrak{m}$ as an $\mathfrak{o}_K$-module: $\mathfrak{m} = (a, h+\omega)$. When $\mathfrak{a} = [a, h+\omega]$ is an ideal and $a = a_1 \cdot a_2$, one verifies that $\mathfrak{a} = \mathfrak{a}_1 \cdot \mathfrak{a}_2$ where $\mathfrak{a}_i$ is the ideal $[a_i, h+\omega]$, $i = 1, 2$.

Back to quadratic forms, for a fixed quadratic field K, consider the set

$$Q(\Delta_K) = \left\{ f = ax^2 + bxy + cy^2\,; \quad \begin{array}{l} a, b, c \in \boldsymbol{Z}\,, \\ \Delta_f = \Delta_K \ (f > 0 \text{ if } \Delta_K < 0) \end{array} \right\}.^{3)}$$

Since the equivalence $\overset{+}{\sim}$ makes sense in $Q(\Delta_K)$, we can consider the quotient:

$$\tilde{Q}(\Delta_K) = Q(\Delta_K)/\overset{+}{\sim}\,.$$

THEOREM 1. *There is a bijection* $i_K\colon H_K^+ \xrightarrow{\sim} \tilde{Q}(\Delta_K)$.

Here, the map i_K is the following. We agree to orient a basis of an ideal $\mathfrak{a} = [\alpha, \beta]$ by the rule:

$$\begin{cases} \begin{vmatrix} \beta & \beta' \\ \alpha & \alpha' \end{vmatrix} > 0 & \text{if} \quad m > 0\,, \\ \dfrac{1}{i} \begin{vmatrix} \beta & \beta' \\ \alpha & \alpha' \end{vmatrix} > 0 & \text{if} \quad m < 0\,. \end{cases}$$

Then, i_K is the one induced by $\cdot$

$$\mathfrak{a} \mapsto f_{\mathfrak{a}}=\frac{N(x\alpha+y\beta)}{N\mathfrak{a}}.$$

Remark 1. Note that for a primitive ideal $\mathfrak{a}=[a, h+\omega]$ this order of basis is the right one. It is useful to notice that

(i) $m\equiv 2, 3 \pmod 4$

$$\mathfrak{a}=[a, h+\omega] \mapsto f_{\mathfrak{a}}=ax^2+2hxy+cy^2,$$
$$h^2-ac=\Delta_K/4=m,$$

(ii) $m\equiv 1 \pmod 4$

$$\mathfrak{a}=[a, h+\omega] \mapsto f_{\mathfrak{a}}=ax^2+(2h+1)xy+cy^2,$$
$$(2h+1)^2-4ac=\Delta_K=m.$$

In particular, for $\mathfrak{a}=\mathfrak{o}_K=[1, \omega]$, we have

$$f_{\mathfrak{o}_K}=\begin{cases} x^2-my^2, & m\equiv 2, 3 \pmod 4, \\ x^2+xy+\dfrac{(1-m)}{4}y^2, & m\equiv 1 \pmod 4. \end{cases}$$

Remark 2. Thanks to i_K, one can define a group structure in the set $\tilde{Q}(\Delta_K)$. Gauss (1801) defined directly a group structure in $\tilde{Q}(\Delta_K)$ (the composition theory of quadratic forms).[4] The notion of ideals was introduced by Dedekind (1871).[5]

Let us recall here an important theorem due to Kummer. Let $K=\boldsymbol{Q}(\theta)$ be an algebraic number field of degree n, $\theta\in\mathfrak{o}_K$ and $f(x)$ be the monic minimal polynomial for θ. Put

$$\Delta(\theta)=\begin{vmatrix} 1 & \theta & \theta^2 & \cdots & \theta^{n-1} \\ 1 & \theta' & (\theta')^2 & \cdots & (\theta')^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \theta^{(n-1)} & (\theta^{(n-1)})^2 & \cdots & (\theta^{(n-1)})^{n-1} \end{vmatrix}^2.$$

Then we have $\Delta(\theta)=m(\theta)^2\Delta_K$, $m(\theta)\in Z$.

THEOREM 2.[6] *Let p be a rational prime such that $p\nmid m(\theta)$. If*

$$f\equiv f_1^{e_1}\cdots f_g^{e_g} \pmod p,$$

f_i being a monic polynomial in $\boldsymbol{Z}[x]$, $1 \leq i \leq g$, then

$$p = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g},$$

where $\mathfrak{p}_i$ is a prime ideal in K such that $\mathfrak{p}_i = (p, f_i(\theta))$, $\deg \mathfrak{p}_i = \deg f_i$, $1 \leq i \leq g$.

Example 1. $m = -14 \equiv 2 \pmod 4$. $K = \boldsymbol{Q}(\omega)$, $\omega = \sqrt{-14}$, $\Delta_K = -2^3 \cdot 7$. As for the Minkowski constant, we get

$$M_K = \frac{2}{\pi}\sqrt{|\Delta_K|} \fallingdotseq 0.63662 \times 2\sqrt{14} \fallingdotseq 4.76 .$$

Since 2 and 3 are only rational primes $\leq M_K$, one sees that $H_K^+ = H_K$ (since $m < 0$) is generated by classes of prime factors $\mathfrak{p}_2$, $\mathfrak{p}_3$ of 2, 3, respectively. Notice that $\Delta(\omega) = \Delta_K$, i.e. $m(\omega) = 1$.

(i) $p = 2$.

$$f(x) = x^2 + 14 \equiv x^2 \pmod 2$$

Hence $2 = \mathfrak{p}_2^2$ with $\mathfrak{p}_2 = (2, \omega) = [2, \omega]$.

(ii) $p = 3$.

$$f(x) = x^2 + 14 \equiv x^2 - 1 \equiv (x+1)(x-1) \pmod 3 .$$

Hence $3 = \mathfrak{p}_3 \mathfrak{p}_3'$ with $\mathfrak{p}_3 = (3, 1+\omega) = [3, 1+\omega]$.

$$\mathfrak{p}_3' = (3, -1+\omega) = [3, -1+\omega] = [3, 2+\omega] .$$

Since $N(2+\omega) = 2^2 + 14 = 18 = 2 \cdot 3^2$, we have

$$\begin{aligned} 1 &\sim (2+\omega) = [N(2+\omega), 2+\omega] = [2 \cdot 3^2, 2+\omega] \\ &= [2, 2+\omega][3, 2+\omega]^2 = [2, \omega][3, 2+\omega]^2 \\ &= \mathfrak{p}_2(\mathfrak{p}_3')^2 \\ &\sim \mathfrak{p}_2 \mathfrak{p}_3^{-2} \quad (\text{since } \mathfrak{p}_3 \mathfrak{p}_3' = 3 \sim 1) . \end{aligned}$$

Therefore, we have $\mathfrak{p}_3^2 \sim \mathfrak{p}_2$, i.e. H_K is a cyclic group generated by the class of $\mathfrak{p}_3$.

On the other hand, $\mathfrak{p}_2^2 = 2 \sim 1$ but $\mathfrak{p}_2 \not\sim 1$. (If $\mathfrak{p}_2 = (x + y\omega)$, then $2 = N(x+y\omega) = x^2 + 14y^2$, which is impossible.) Hence $H_K = \boldsymbol{Z}/4\boldsymbol{Z}$ and $h_K^+ = h_K = 4$.

The bijection $i_K : H_K^+ \rightarrow \tilde{Q}(\Delta_K)$ is induced by the following:

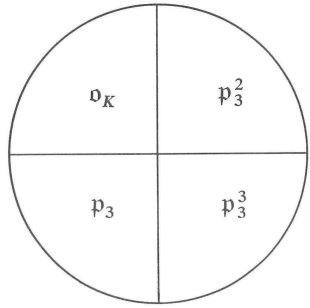
$$\mathfrak{o}_K=[1,\ \omega] \mapsto f_{\mathfrak{o}_K}=x^2+14y^2$$

$$\mathfrak{p}_3=[3,\ 1+\omega] \mapsto f_{\mathfrak{p}_3}=3x^2+2xy+5y^2$$

$$\mathfrak{p}_3^2 \sim \mathfrak{p}_2=[2,\ \omega] \mapsto f_{\mathfrak{p}_2}=2x^2+7y^2$$

$$\mathfrak{p}_3^3 \sim \mathfrak{p}_3'=[3,\ 2+\omega] \mapsto f_{\mathfrak{p}_3'}=3x^2+4xy+6y^2\ .$$

$\boldsymbol{Q}(\Delta_K)$ $\qquad$ $K=\boldsymbol{Q}(\sqrt{-14})$



II. Genera of Binary Quadratic Forms

Consider a rational quadratic form of n variables:

$$f=\sum f_{ij}x_ix_j={}^txFx\ , \qquad x=\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix},$$

$$F={}^tF=(f_{ij})\in M_n(\boldsymbol{Q})\ , \qquad \det f=\det F\neq 0\ .$$

Let $g={}^txGx$ be another such form. For a group Γ, we can speak of the equivalence

$$f \underset{\Gamma}{\sim} g \overset{\text{def}}{\Longleftrightarrow} g(x)=f(\gamma x)\ , \qquad \exists\,\gamma\in\Gamma\ .$$

In Section I, we used $\Gamma=GL_2(\boldsymbol{Z})$ and $SL_2(\boldsymbol{Z})$. In general, when we use $\Gamma=GL_n(\boldsymbol{Z})$, $GL_n(\boldsymbol{Q})$, $GL_n(\boldsymbol{R})$, $GL_n(\boldsymbol{Z}_p)$, $GL_n(\boldsymbol{Q}_p)$, we write

$$f \underset{\boldsymbol{Z}}{\sim} g\ , \qquad f \underset{\boldsymbol{Q}}{\sim} g\ , \qquad f \underset{\boldsymbol{R}}{\sim} g\ , \qquad f \underset{\boldsymbol{Z}_p}{\sim} g\ , \qquad f \underset{\boldsymbol{Q}_p}{\sim} g\ ,$$

respectively. When we use $\Gamma = SL_n(\boldsymbol{Z})$, we write

$$f \overset{+}{\sim} g .$$

Usually, we consider ∞ as the last rational prime and put $\boldsymbol{Z}_\infty = \boldsymbol{Q}_\infty = \boldsymbol{R}$. So, when we write p, $p = \infty$ is included unless otherwise stated.

Hasse (1923) proved the Hasse principle:

THEOREM 1.[1]

$$f \underset{\boldsymbol{Q}}{\sim} g \Longleftrightarrow f \underset{\boldsymbol{Q}_p}{\sim} g \qquad \forall p .$$

The implication $f \underset{\boldsymbol{Z}}{\sim} g \Rightarrow f \underset{\boldsymbol{Z}_p}{\sim} g$ is trivial, but, as we shall see later, the converse is not true. This motivates the following:

DEFINITION 1.

$$f \approx g \overset{\text{def}}{\Longleftrightarrow} f \underset{\boldsymbol{Z}_p}{\sim} g , \qquad \forall p .$$

When that is so, we say that f and g are in the same genus. Since $f \underset{\boldsymbol{Z}}{\overset{+}{\sim}} g \Rightarrow f \approx g$, a genus consists of a certain (finite) number of classes. Back to $n=2$, consider the quotient spaces:

$$\tilde{Q}(\Delta_K) = Q(\Delta_K) \Big/ \underset{\boldsymbol{Z}}{\overset{+}{\sim}} = Q(\Delta_K) \Big/ \overset{+}{\sim} , \qquad \tilde{\tilde{Q}}(\Delta_K) = Q(\Delta_K) \Big/ \approx .$$

Gauss characterised $f \approx g$ by "characters".[2] By virtue of the bijection i_K: $H_K^+ \rightarrow \tilde{Q}(\Delta_K)$ (Section I, Th. 1), those "characters" become characters of the group H_K^+. For each p, the "character" is a map

$$\psi_p : \tilde{Q}(\Delta_K) \longrightarrow \{\pm 1\}$$

such that

$$f \underset{\boldsymbol{Z}_p}{\sim} g \Longleftrightarrow \psi_p(f) = \psi_p(g) .$$

ψ_p can be introduced by Hilbert symbols.[3] For $a, b \in \boldsymbol{Q}_p^\times$, put

$$(a, b)_p = \begin{cases} 1 & \text{if } ax^2 + by^2 = z^2 \text{ has a solution} \\ & (x, y, z) \neq (0, 0, 0) \text{ in } \boldsymbol{Q}_p^3 , \\ -1 & \text{otherwise} . \end{cases}$$

This pairing induces a non-degenerate, symmetric, bilinear map

$$\boldsymbol{Q}_p^{\times}/(\boldsymbol{Q}_p^{\times})^2 \times \boldsymbol{Q}_p^{\times}/(\boldsymbol{Q}_p^{\times})^2 \longrightarrow \{\pm 1\}\,.$$

Furthermore, we have

PROPOSITION 1.

(i) $(a, b)_\infty = 1$ *if* $a>0$ *or* $b>0$.

(ii) *For* $p \neq 2, \infty$, *write* $a=p^\alpha u$, $b=p^\beta v$, $\alpha, \beta \in Z$, $u, v \in Z_p^{\times}$. *Then*

$$(a, b)_p = \left(\frac{-1}{p}\right)^{\alpha\beta}\left(\frac{u}{p}\right)^{\beta}\left(\frac{v}{p}\right)^{\alpha}.$$

(iii) *For* $p=2$, *write* $a=2^\alpha u$, $b=2^\beta v$ *as in* (ii). *Then*

$$(a, b)_2 = (-1)^{\varepsilon(u)\varepsilon(v)+\alpha\omega(v)+\beta\omega(u)}$$

where

$$\varepsilon(u) = \begin{cases} 0\,, & u \equiv 1 \pmod 4 \\ 1\,, & u \equiv 3 \pmod 4\,, \end{cases}$$

$$\omega(u) = \begin{cases} 0\,, & u \equiv 1, 7 \pmod 8 \\ 1\,, & u \equiv 3, 5 \pmod 8\,. \end{cases}$$

(iv) $\prod_p (a, b)_p = 1$, $a, b \in \boldsymbol{Q}^{\times}$.

(v) *For* $a, b \in \boldsymbol{Q}_p^{\times}$, *put* $k = \boldsymbol{Q}_p(\sqrt{b})$. *Then*

$$(a, b)_p = 1 \Longleftrightarrow a = N_{k/\boldsymbol{Q}_p}(c)\,, \qquad \exists\, c \in k^{\times}\,.$$

(vi) $(a, -a)_p = 1$, $a \in \boldsymbol{Q}_p^{\times}$.

Now, for $f \in \boldsymbol{Q}(\Delta_K)$, $\alpha \in \boldsymbol{Q}_p^{\times}$ we write

$$f \xrightarrow[\boldsymbol{Q}_p]{} \alpha \quad (f \text{ represents } \alpha)$$

when $f(x_0, y_0) = \alpha$, $(x_0, y_0) \in \boldsymbol{Q}_p^2$.

PROPOSITION 2. *Given* $f \in \boldsymbol{Q}(\Delta_K)$, $(\alpha, \Delta_K)_p$ *does not depend on* α *such that* $f \xrightarrow[\boldsymbol{Q}_p]{} \alpha$.

In fact, since we are dealing with the field $\boldsymbol{Q}_p$, we may assume that $f = Ax^2 + By^2$, $A, B \in \boldsymbol{Q}_p^{\times}$. If $f \xrightarrow[\boldsymbol{Q}_p]{} \alpha$, then $Ax_0^2 + By_0^2 = \alpha$, $(x_0, y_0) \in \boldsymbol{Q}_p^2$, and so

$$(Ax_0)^2 + ABy_0^2 = \alpha A\,, \quad \text{or} \quad (\alpha A)x^2 + (-AB)y^2 = z^2$$

has a solution $(1, y_0, Ax_0) \neq (0, 0, 0)$. Since $\Delta_K = -4AB$, we have $1 = (\alpha A, \Delta_K)_p = (\alpha, \Delta_K)_p (A, \Delta_K)_p$ which implies that $(\alpha, \Delta_K)_p = (A, \Delta_K)_p$, Q.E.D.

This makes the following definition possible.

DEFINITION 2. For $f \in Q(\Delta_K)$, we put

$$\psi_p(f) = (\alpha, \Delta_K)_p$$

where

$$f \xrightarrow[\boldsymbol{Q}_p]{} \alpha , \qquad \alpha \in \boldsymbol{Q}_p^{\times} .$$

Since $f \underset{\boldsymbol{Z}}{\pm} g$ implies $f \underset{\boldsymbol{Z}_p}{\sim} g$ and then $f \underset{\boldsymbol{Q}_p}{\sim} g$, $f \underset{\boldsymbol{Q}_p}{\to} \alpha$ if and only if $g \underset{\boldsymbol{Q}_p}{\to} \alpha$. Hence $\psi_p(f) = \psi_p(g)$. Therefore we may view ψ_p as a function on $\tilde{Q}(\Delta_K)$. We only state the following important result:

THEOREM 2.[4] *For $f, g \in Q(\Delta_K)$,*

(i) $\psi_\infty(f) = \psi_\infty(g) = 1$ *and* $f \underset{\boldsymbol{Z}_\infty}{\sim} g$,

(ii) $\psi_p(f) = \psi_p(g) = 1$ *and* $f \underset{\boldsymbol{Z}_p}{\sim} g$, *when* $p \nmid \Delta_K$

(iii) $\psi_p(f) = \psi_p(g) \Leftrightarrow f \underset{\boldsymbol{Z}_p}{\sim} g$, *when* $p \mid \Delta_K$.

In view of Definition 1, this implies the following

THEOREM 3. *Let $f, g \in Q(\Delta_K)$. We have*

$$f \approx g \iff \psi_p(f) = \psi_p(g) \qquad \forall p .$$

THEOREM 4.

$$\#(\tilde{\tilde{Q}}(\Delta_K)) = 2^{t-1} ,$$

where t means the number of distinct prime factors of Δ_K.

This follows form Theorem 2, Theorem 3 and Proposition 1, (iv). Let i_K be the bijection $H_K^+ \xrightarrow{\sim} \tilde{Q}(\Delta_K)$ in Theorem 1 in Section I. Put $\chi_p = \psi_p \cdot i_K$. Our situation is:

$$\begin{array}{ccc} \text{(group)}\ H_K^+ & \xrightarrow{i_K} & \tilde{Q}(\Delta_K)\ \text{(set)} \\ & \searrow^{\chi_p} \quad \swarrow_{\psi_p} & \\ & \{\pm 1\} & \end{array}$$

("character") ("character")

THEOREM 5. *χ_p is a character of the ideal class group H_K^+.*

In fact, take any class $[\mathfrak{a}]\in H_K^+$, where $\mathfrak{a}=[a, h+\omega]$, the canonical basis of primitive ideal $\mathfrak{a}$ (cf. Remark 1 in Section I). Since $f_{\mathfrak{a}}\underset{Q}{\to}a=N\mathfrak{a}$, we have

$$\chi_p([\mathfrak{a}])=\psi_p(f_{\mathfrak{a}})=(a, \Delta_K)_p=(N\mathfrak{a}, \Delta_K)_p\,.$$

If $\mathfrak{b}\in[\mathfrak{a}]$, then $\mathfrak{b}=(\rho)\mathfrak{a}$, $N\rho>0$, hence $N\mathfrak{b}=N\rho N\mathfrak{a}$. By Proposition 1, (v) we have $(N\mathfrak{a}, \Delta_K)_p=(N\mathfrak{b}, \Delta_K)_p$, which proves our theorem.

Let us define a subgroup G_K of H_K^+ by

$$G_K=\bigcap_p \operatorname{Ker}\chi_p\,.$$

Since

$$\begin{aligned}\mathfrak{a}\equiv\mathfrak{b}\ (\text{mod. } G_K) &\Longleftrightarrow \chi_p(\mathfrak{a})=\chi_p(\mathfrak{b}) \qquad \forall p\\ &\Longleftrightarrow \psi_p(f_{\mathfrak{a}})=\psi_p(f_{\mathfrak{b}}) \qquad \forall p\\ &\Longleftrightarrow f_{\mathfrak{a}}\approx f_{\mathfrak{b}}\,,\end{aligned}$$

the bijection $i_K\colon H_K^+\to\tilde{Q}(\Delta_K)$ induces the bijection

$$H_K^+/G_K \xrightarrow{\sim} \tilde{\tilde{Q}}(\Delta_K)\,.$$

G_K is called the group of principal genus. Call h_K^* the order of G_K. h_K^* is at the same time equal to the number of classes in an arbitrary genus.

$$\begin{array}{c} H_K^+ \\ | \\ 2^{t-1} \\ | \\ G_K \\ | \\ h_K^* \\ | \\ 1 \end{array}$$

Theorem 4 yields

THEOREM 6. $h_K^+=h_K^*\cdot 2^{t-1}$.

THEOREM 7. $G_K=(H_K^+)^2$.

Here, $G_K\supset(H_K^+)^2$ is trivial. To see $G_K\subset(H_K^+)^2$, take an ideal class $[\mathfrak{a}]\in G_K$.

Since $f_{\mathfrak{a}} \underset{\boldsymbol{Z}_p}{\sim} f_{\mathfrak{o}_K}$ for all p, we have $f_{\mathfrak{a}} \underset{\boldsymbol{Q}}{\sim} f_{\mathfrak{o}_K}$. For oriented basis $\mathfrak{a}=[\alpha, \beta]$, $\mathfrak{o}_K=[1, \omega]$, we have

$$f_{\mathfrak{a}}=\frac{N(x\alpha+y\beta)}{N\mathfrak{a}}, \qquad f_{\mathfrak{o}_K}=N(x+y\omega).$$

Let $\gamma \in \boldsymbol{Q}^{\times}$ be a number represented by both of $f_{\mathfrak{a}}$ and $f_{\mathfrak{o}_K}$. Thus, $(N\xi)/(N\mathfrak{a})=N\eta$ for some $\xi, \eta \in K^{\times}$ and so $N\mathfrak{a}=N\rho>0$, $\rho=\xi/\eta \in K^{\times}$. We have $N(\mathfrak{a}\rho^{-1})=1$. Since we are dealing with the ideal classes in the narrow sense, we may assume from the beginning that $N\mathfrak{a}=1$. Let now $\mathfrak{p}$, $\mathfrak{q}$ be typical prime ideals of K such that

(i) $p=\mathfrak{p}\mathfrak{p}'$, $\mathfrak{p} \neq \mathfrak{p}'$ ($\mathfrak{p}'$ being the conjugate of $\mathfrak{p}$),

(ii) $q=\mathfrak{q}$ or $\mathfrak{q}^2$ ($\mathfrak{q}'=\mathfrak{q}$ in this case)

and let

$$\mathfrak{a}=\prod \mathfrak{p}^a \mathfrak{p}'^b \prod \mathfrak{q}^c$$

the prime decomposition of $\mathfrak{a}$. Since

$$1=N\mathfrak{a}=\prod p^{a+b} \prod q^{ec}, \qquad e=1 \text{ or } 2,$$

we must have $a+b=0$ and $c=0$. In order words,

$$\mathfrak{a}=\prod \mathfrak{p}^a(\mathfrak{p}')^{-a} \sim \prod \mathfrak{p}^a \mathfrak{p}^a=(\prod \mathfrak{p}^a)^2=\mathfrak{b}^2, \qquad \text{Q.E.D.}$$

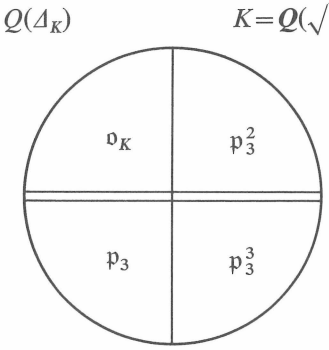
Example 1. Notation being as in Example of Section I. $\Delta_K=4m=-2^3 \cdot 7$ ($m=-14$). Since $h_K=4$ and $t=2$, we have $h_K^*=2$. This means that $Q(\Delta_K)$ consists of two genera and each genus consists of two classes.

Since H_K^+ is a cyclic group (of order 4) generated by (class of) $\mathfrak{p}_3$, the principal genus $G_K=(H_K^+)^2$ consists of $\mathfrak{o}_K$ and $\mathfrak{p}_3^2$ and the coset $\mathfrak{p}_3 G_K$ makes up the other genus. Note that

$$f_{\mathfrak{o}_K}=x^2+14y^2 \approx f_{\mathfrak{p}_3{}^2} \sim f_{\mathfrak{p}_2}=2x^2+7y^2,$$

$$f_{\mathfrak{p}_3}=3x^2+2xy+5y^2 \approx f_{\mathfrak{p}_3{}^3} \sim f_{\mathfrak{p}_3{}'}=3x^2+4xy+6y^2.$$

The form $g=3x^2-2xy+5y^2$ is in $Q(\Delta_K)$, too. As we saw in Section I, g is not in the class of $f_{\mathfrak{p}_3}$. But, since, both g and $f_{\mathfrak{p}_3}$ represent 3 over $\boldsymbol{Q}$, g belongs to the genus of $f_{\mathfrak{p}_3}$ and so to the class of $\mathfrak{p}_3' \sim \mathfrak{p}_3^3$.



Example 2. Using Theorem 6, one can find a quadratic field which has a big class number. Let $m=1-2^{225}\equiv 1 \pmod 4$. Since $\omega=(1+\sqrt{m})/2$, we have $N\omega=(1-m)/4=2^{223}$ where 223 is prime. $-m$ is square-free and decomposes into primes as follows:

$$\begin{aligned}-m&=2^{225}-1\\&=7\cdot 31\cdot 73\cdot 151\cdot 601\cdot 631\cdot 1801\cdot 23311\cdot 100801\cdot 115201\\&\quad\times 617401\cdot 10567201\cdot 1348206751\cdot 13861369826299351\ .^{5)}\end{aligned}$$

Since $\Delta_K=m$, we have $t=14$ and $h_K=2^{13}h_K^*$. Consider the ideal $\mathfrak{a}=[2,\omega]$. One sees easily that $\mathfrak{a}\not\sim 1$.

Now, $\mathfrak{a}^{223}=[2,\omega]^{223}=[2^{223},\omega]=[N\omega,\omega]\sim 1$ which implies that $223\mid h_K^*$. Hence h_K is a multiple of $2^{13}\times 223=1826816$.

III. A Generalization of Genera

One can generalize the notion of the genus unlimitedly. We first need an algebraic group.[1)] Let Ω be a universal domain containing $\boldsymbol{Q}$.[2)] A subgroup $G\subset GL_n(\Omega)$ is called an algebraic group (defined) over $\boldsymbol{Q}$ if there is an algebraic set $A\subset M_n(\Omega)=\Omega^{n^2}$ over $\boldsymbol{Q}$ such that $G=A\cap GL_n(\Omega)$. $G=GL_n(\Omega)$ is an algebraic group over $\boldsymbol{Q}$. In particular, $G=GL_1(\Omega)=\Omega^\times=G_m$ is such a group. If R is a commutative subring of Ω with $1\in R$, we have the group

$$GL_n(R)=M_n(R)^\times=\{x\in M_n(R);\ \det(x)\in R^\times\}\ .$$

With an algebraic group G over $\boldsymbol{Q}$ we can associate a group $G(R)=G\cap GL_n(R)$. Important cases are $R=\boldsymbol{C}$, $\boldsymbol{R}$, $\boldsymbol{Q}$, $\boldsymbol{Z}$, $\boldsymbol{Q}_p$, $\boldsymbol{Z}_p$. When Ω is of

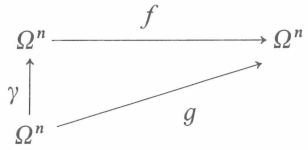
characteristic $p>0$, we can speak of algebraic group G over some subfield k of Ω, usually $k=\boldsymbol{F}_q$, a finite field with q elements, q being a power of p. For a group G over $\boldsymbol{Q}$, we have the following descriptions:

$G(\boldsymbol{R})$ = real Lie group (locally compact)
$G(\boldsymbol{Z})$ = discrete subgroup of $G(\boldsymbol{R})$
$G(\boldsymbol{Q}_p)$ = p-adic Lie group (locally compact)
$G(\boldsymbol{Z}_p)$ = open compact subgroup of $G(\boldsymbol{Q}_p)$.

DEFINITION 1. Let f, g be polynomial maps: $\Omega^n \to \Omega^m$ defined over $\boldsymbol{Q}$ and $G \subset GL_n(\Omega)$ be an algebraic group over $\boldsymbol{Q}$. Then,

$$f \underset{G}{\approx} g \overset{\text{def}}{\Longleftrightarrow} f \underset{G(\boldsymbol{Q})}{\sim} g \quad \text{and} \quad f \underset{G(\boldsymbol{Z}_p)}{\sim} g, \qquad \forall p .$$

Here $f \underset{G(R)}{\sim} g$ means that the diagram



is commutative for some $\gamma \in G(R)$.

Remark 1. $\quad f \underset{G(\boldsymbol{Z})}{\sim} g \Longrightarrow f \underset{G}{\approx} g .$

Therefore a genus defined by the relation $\underset{G}{\approx}$ consists again of certain number of classes defined by the relation $\underset{G(\boldsymbol{Z})}{\sim}$.

Remark 2. The reader must notice that there is an inconsistency in the old definition of class and genus for quadratic forms. Namely in Section II we defined $f \overset{+}{\underset{\boldsymbol{Z}}{\sim}} g$ and $f \approx g$ by

(i) $f \overset{+}{\underset{\boldsymbol{Z}}{\sim}} g \Longleftrightarrow f \underset{SL_n(\boldsymbol{Z})}{\sim} g,$

(ii) $f \approx g \Longleftrightarrow f \underset{GL_n(\boldsymbol{Z}_p)}{\sim} g \quad \forall p \Longleftrightarrow f \underset{GL_n}{\approx} g.$

From the point of view of algebraic groups, we prefer to use one algebraic group instead of SL_n and GL_n above. We shall use SL_n in view of the following

PROPOSITION 1. *Let f, g be non-singular quadratic forms of n variables*

over $\boldsymbol{Q}$. *Then we have*

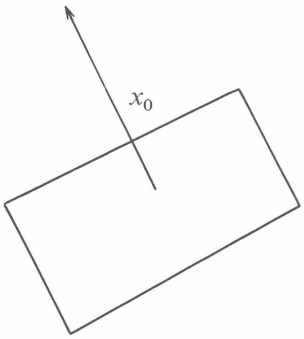
$$f \underset{GL_n}{\approx} g \Longleftrightarrow f \underset{SL_n}{\approx} g .$$

Proof. ($\Leftarrow$) is trivial. To prove ($\Rightarrow$), we need a lemma:

LEMMA. If f is a non-singular quadratic form of n variables over $\boldsymbol{Q}$, $O(f)(\boldsymbol{Q})$ and $O(f)(\boldsymbol{Z}_p)$ $(\forall p)$ contain matrices of determinant -1. (Note that $O(f)(\boldsymbol{Z}) = O^+(f)(\boldsymbol{Z})$ wnen $f = 3x^2 + 2xy + 5y^2$. See the first example in Section I.)

Proof of Lemma.[3] Since $\boldsymbol{Q}$ and $\boldsymbol{Z}_\infty = \boldsymbol{Q}_\infty = \boldsymbol{R}$ are fields, the lemma is obvious. So, assume that $p \neq \infty$. Since $|f(x)|_p$ is continuous on the compact set $\boldsymbol{Z}_p^n$, it attains the maximum at $x = x_0 \in \boldsymbol{Z}_p^n$:

$$|f(x_0)|_p = \sup_{x \in \boldsymbol{Z}_p^n} |f(x)|_p .$$



Clearly, $f(x_0) \neq 0$. Let $\langle x, y \rangle$ be the inner product defined by

$$2\langle x, y \rangle = f(x+y) - f(x) - f(y) .$$

Call σ the symmetry given by

$$\sigma(x) = x - \frac{2\langle x_0, x \rangle}{f(x_0)} x_0 , \qquad x \in \boldsymbol{Q}_p^n .$$

We have $\det \sigma = -1$. We shall show that $\sigma \in O(f)(\boldsymbol{Z}_p)$. Since $\sigma^2 = 1$, it is enough to show that $\sigma(\boldsymbol{Z}_p^n) \subseteq \boldsymbol{Z}_p^n$. Now for $x \in \boldsymbol{Z}_p^n$, we have

$$\begin{aligned} |2\langle x_0, x \rangle|_p &\leq \sup(|f(x+x_0)|_p, |f(x)|_p, |f(x_0)|_p) \\ &= |f(x_0)|_p , \end{aligned}$$

or $|2\langle x_0, x\rangle/f(x_0)|_p \leq 1$ and so $\sigma(\boldsymbol{Z}_p^n) \subseteq \boldsymbol{Z}_p^n$. Q.E.D.

Proof of ($\Rightarrow$). Notice first that $f \underset{GL_n}{\approx} g \Rightarrow \det f = \det g$. Hence $g = f\gamma_p$, $\gamma_p \in GL_n(\boldsymbol{Z}_p)$, $\det \gamma_p = \pm 1$, $\forall p$. When $\det \gamma_p = -1$, we can adjust γ_p by Lemma so that $\det \gamma_p = +1$. Hence $f \underset{SL_n}{\approx} g$. Since quadratic forms satisfy Hasse principle, we have

$$\begin{aligned} f \underset{GL_n}{\approx} g &\Longrightarrow f \underset{\boldsymbol{Q}_p}{\sim} g \\ &\overset{\text{Hasse}}{\Longrightarrow} f \underset{\boldsymbol{Q}}{\sim} g \\ &\Longrightarrow f \underset{GL_n(\boldsymbol{Q})}{\sim} g \\ &\overset{\text{Lemma}}{\Longrightarrow} f \underset{SL_n(\boldsymbol{Q})}{\sim} g . \end{aligned}$$

Q.E.D.

Back to a general algebraic group G over $\boldsymbol{Q}$, the associated adele group is given by

$$G(\boldsymbol{A}) = G(\boldsymbol{R}) \times \prod_{p \neq \infty}{}' G(\boldsymbol{Q}_p)$$

where $\prod'$ means the restricted direct product.[4] Thus,

$$\begin{aligned} x = (x_\infty, \cdots, x_p, \cdots) \in G(\boldsymbol{A}) \\ \overset{\text{def}}{\Longleftrightarrow} x_p \in G(\boldsymbol{Q}_p) \quad \forall p \ (=\infty) \quad \text{and} \quad x_p \in G(\boldsymbol{Z}_p) \quad \forall' p . \end{aligned}$$

($\forall' p \Leftrightarrow$ for almost all $p \Leftrightarrow$ for all but a finite number of p)

Put

$$G(\boldsymbol{A})_\infty = G(\boldsymbol{R}) \times \prod_{p \neq \infty} G(\boldsymbol{Z}_p)$$

and topologize $G(\boldsymbol{A})$ so that $G(\boldsymbol{A})_\infty$ is an open subgroup. Since $G(\boldsymbol{R})$ is locally compact and $\prod_{p \neq \infty} G(\boldsymbol{Z}_p)$ is compact, $G(\boldsymbol{A})$ becomes locally compact. The subgroup $G(\boldsymbol{Q})$ of G can be embedded in $G(\boldsymbol{A})$ diagonally (i.e. $x \longmapsto (x, \cdots, x, \cdots)$). Since $G(\boldsymbol{Q}) \cap G(\boldsymbol{A})_\infty = G(\boldsymbol{Z})$, $G(\boldsymbol{Q})$ is discrete in $G(\boldsymbol{A})$. It is well-known that the set

$$G(\boldsymbol{Q}) \backslash G(\boldsymbol{A}) / G(\boldsymbol{A})_\infty$$

of double cosets is finite (Borel, 1963).[5] We put

$$h_G = \#\left(G(\boldsymbol{Q}) \backslash G(\boldsymbol{A}) / G(\boldsymbol{A})_\infty\right),$$

the class number of G.

For a polynomial map defined over $\boldsymbol{Q}$:

$$f\colon \Omega^n \longrightarrow \Omega^m ,$$

put

$$\mathscr{G}_G(f) \overset{\text{def}}{=} \{g;\ g \underset{G}{\approx} f\}$$

$$\tilde{\mathscr{G}}_G(f) \overset{\text{def}}{=} \mathscr{G}_G(f) \Big/ \underset{G(\boldsymbol{Z})}{\sim}$$

$$G(f) \overset{\text{def}}{=} \{\sigma \in G;\ f\sigma = f\} ,$$

where the latter being an algebraic subgroup of G defined over $\boldsymbol{Q}$. For $g \in \mathscr{G}_G(f)$ there are $t \in G(\boldsymbol{Q})$ and $u \in G(\boldsymbol{A})_\infty$ such that $g = f \cdot t$, $g = f \cdot u$. Then we have $f = ftu^{-1}$ and $s = tu^{-1}$ belongs to $G(f)(\boldsymbol{A})$.

THEOREM 1. *Notation being as above,*

(1) *the map* $[g] \longmapsto [s]$ *is well-defined from* $\tilde{\mathscr{G}}_G(f)$ *to* $G(f)(\boldsymbol{Q})\backslash G(f)(\boldsymbol{A})/G(f)(\boldsymbol{A})_\infty$,

(2) *the map is injective.*

(3) *If* $h_G = 1$, *then the map is surjective and we get the identification*

$$\tilde{\mathscr{G}}_G(f) = G(f)(\boldsymbol{Q})\backslash G(f)(\boldsymbol{A})/G(f)(\boldsymbol{A})_\infty .$$

Proof. With obvious notation, (1) and (2) mean that

$$[g] = [g'] \Longleftrightarrow [s] = [s'] .$$

$(\Rightarrow)$ $\qquad [g] = [g'] \Rightarrow g' = gv , \qquad v \in G(\boldsymbol{Z}) .$

Hence,

$$g' = ft' = gv = ftv , \qquad g' = fu' = gv = fuv .$$

Or,

$$t'v^{-1}t^{-1} \in G(f)(\boldsymbol{Q}) , \qquad u'v^{-1}u^{-1} \in G(f)(\boldsymbol{A})_\infty$$

and

$$s' = t'u'^{-1} = (t'v^{-1}t^{-1})(tu^{-1})(uvu'^{-1}) \in G(f)(\boldsymbol{Q})sG(f)(\boldsymbol{A})_\infty ,$$

i.e. $[s'] = [s]$.

$(\Leftarrow)$ $\qquad [s'] = [s] \Rightarrow s' = asb , \qquad a \in G(f)(\boldsymbol{Q}) , \quad b \in G(f)(\boldsymbol{A})_\infty .$

Then,

$$g'=ft'=fs'u'=fasbu'=fsbu'=ftu^{-1}bu'=g(u^{-1}bu')\,,$$

where

$$v=u^{-1}bu'\in G(\boldsymbol{A})_\infty\,.$$

We must show that $v\in G(\boldsymbol{Z})$. In fact,

$$s'=asb\Rightarrow t'u'^{-1}=atu^{-1}b\,,$$

i.e.

$$t^{-1}a^{-1}t'=u^{-1}bu'=v\in G(\boldsymbol{Q})\cap G(\boldsymbol{A})_\infty=G(\boldsymbol{Z})\,.$$

We have then $[g']=[g]$.

(3) Assume that $h_G=1$. Consider any element $[s]$ of $G(f)(\boldsymbol{Q})\backslash G(f)(\boldsymbol{A})/G(f)(\boldsymbol{A})_\infty$. Since $G(f)(\boldsymbol{A})\subset G(\boldsymbol{A})=G(\boldsymbol{Q})G(\boldsymbol{A})_\infty$ by the assumption, we can write

$$s=tu^{-1}\,,\qquad t\in G(\boldsymbol{Q})\,,\quad u\in G(\boldsymbol{A})_\infty\,.$$

Put $g=ft$, i.e. $g\underset{G(\boldsymbol{Q})}{\sim}f$. On the other hand, since $s\in G(f)\,\boldsymbol{A})$, we have $g=fu$, i.e. $g\underset{G(\boldsymbol{A})_\infty}{\sim}f$. Therefore we have $g\underset{G}{\approx}f$, i.e. $g\in\mathscr{G}_G(f)$. It is obvious that $[g]\longmapsto[s]$, which proves (3).

Example 1. Let f be a non-singular quadratic form over $\boldsymbol{Q}$. It can be shown that $h_{SL_n}=1$ (cf. Section IV). Therefore

$$\tilde{\mathscr{G}}_{SL_n}(f)=\mathscr{G}_{SL_n}(f)\Big/\underset{SL_n(\boldsymbol{Z})}{\sim}=O_n^+(f)(\boldsymbol{Q})\backslash O_n^+(f)(\boldsymbol{A})/O_n^+(f)(\boldsymbol{A})_\infty$$

since $G(f)=\{\sigma\in SL_n;\, f\sigma=f\}=O_n^+(f)$.

IV. Class Number of Algebraic Groups

The class number of an algebraic group G over $\boldsymbol{Q}$ is defined by

$$h_G=\#(G(\boldsymbol{Q})\backslash G(\boldsymbol{A})/G(\boldsymbol{A})_\infty)\,.$$

We shall consider simple examples for which $h_G=1$.

(i) $G=G_a=\Omega$. As a matrix group, G is described as

$$G=\left\{\begin{pmatrix}1 & x\\ 0 & 1\end{pmatrix};\ x\in\Omega\right\}$$

which is a unipotent group.

(ii) $G=G_m=\Omega^\times=GL_1(\Omega)$ is a torus.

(iii) $G=SL_2(\Omega)$ is the simplest example of a semi-simple group.

(i) $G=G_a$. In this case, $G(\boldsymbol{A})=\boldsymbol{A}$,[1] $G(\boldsymbol{Q})=\boldsymbol{Q}$ and a fundamental domain for $\boldsymbol{Q}\backslash\boldsymbol{A}$ is

$$\tilde{F}=[0,1)\times\prod_{p\neq\infty}\boldsymbol{Z}_p\,.$$

From this follows that $h_G=1$ and that $\boldsymbol{Q}\backslash\boldsymbol{A}$ is compact.

(ii) $G=G_m$. In this case, $G(\boldsymbol{Q})\backslash G(\boldsymbol{A})/G(\boldsymbol{A})_\infty=\boldsymbol{A}^\times/\boldsymbol{Q}^\times\boldsymbol{A}_\infty^\times$ which is isomorphic to the ideal class group of $\boldsymbol{Q}$, i.e. $h_G=h_{\boldsymbol{Q}}=1$.[2] Consider the norm (volume) map:

$$\|\quad\|:\boldsymbol{A}^\times\longrightarrow\boldsymbol{R}_+^\times$$

given by $\|x\|=\prod_p|x_p|_p$, $x=(\cdots,x_p,\cdots)$. Put

$$\boldsymbol{A}_1^\times\overset{\text{def}}{=}\{x\in\boldsymbol{A}^\times;\ \|x\|=1\}\,.$$

Then by the product formula $\boldsymbol{Q}^\times\subset\boldsymbol{A}_1^\times$ and $\boldsymbol{A}^\times/\boldsymbol{A}_1^\times\approx\boldsymbol{R}$ by $x\longmapsto\log\|x\|$. From $\boldsymbol{A}^\times=\boldsymbol{Q}^\times\boldsymbol{A}_\infty^\times$, it follows that $\boldsymbol{A}_1^\times=\boldsymbol{Q}^\times\boldsymbol{A}_{\infty,1}^\times$ where

$$\boldsymbol{A}_{\infty,1}^\times=\boldsymbol{A}_1^\times\cap\boldsymbol{A}_\infty^\times=\{\pm1\}\times\prod_{p\neq\infty}\boldsymbol{Z}_p^\times\,.$$

As a fundamental domain for $\boldsymbol{A}_1^\times/\boldsymbol{Q}$ we can take

$$\tilde{F}=\{1\}\times\prod_{p\neq\infty}\boldsymbol{Z}_p^\times$$

and it follows that $\boldsymbol{A}_1^\times/\boldsymbol{Q}$ is compact.

(iii) $G=SL_2(\Omega)$. We begin with a general lemma:

LEMMA 1. *Let $G=NH$ be a semi-direct product of an algebraic group G over $\boldsymbol{Q}$ with N normal. If $h_N=h_H=1$, then $h_G=1$.*

In fact,

$$\begin{aligned}G(\boldsymbol{A})&=N(\boldsymbol{A})H(\boldsymbol{A})=N(\boldsymbol{A})H(\boldsymbol{Q})H(\boldsymbol{A})_\infty\\&=H(\boldsymbol{Q})N(\boldsymbol{A})H(\boldsymbol{A})_\infty=H(\boldsymbol{Q})N(\boldsymbol{Q})N(\boldsymbol{A})_\infty H(\boldsymbol{A})_\infty=G(\boldsymbol{Q})G(\boldsymbol{A})_\infty\,,\end{aligned}$$

which shows that $h_G=1$.

We apply Lemma 1 to the group

$$B=\left\{\begin{pmatrix} a & 0 \\ c & a^{-1} \end{pmatrix};\ a\in\Omega^{\times},\ c\in\Omega\right\}\subset SL_2(\Omega)$$

and the semi-direct product $B=NH$ where

$$N=\left\{\begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix};\ c\in\Omega\right\},\qquad H=\left\{\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix};\ a\in\Omega^{\times}\right\}.$$

By (i), (ii) we have $h_N=h_H=1$. Hence, by Lemma 1, we have $h_B=1$. To show that $h_G=1$, it is enough to show that, for $p\neq\infty$,

$$(*)\qquad G(\boldsymbol{Q}_p)=B(\boldsymbol{Q}_p)G(\boldsymbol{Z}_p)\,.$$

In fact, applying $(*)$ for p-component of $x=(x_\infty,\cdots,x_p,\cdots)\in G(\boldsymbol{A})$, we have

$$x_p=b_p y_p\,,\qquad b_p\in B(\boldsymbol{Q}_p)\,,\qquad y_p\in G(\boldsymbol{Z}_p)\,.$$

Therefore

$$x=(1,\cdots,b_p,\cdots)(x_\infty,\cdots,y_p,\cdots)\in B(\boldsymbol{A})G(\boldsymbol{A})_\infty\,.$$

Since $h_B=1$, we have

$$B(\boldsymbol{A})G(\boldsymbol{A})_\infty=B(\boldsymbol{Q})B(\boldsymbol{A})_\infty G(\boldsymbol{A})_\infty\subseteq G(\boldsymbol{Q})G(\boldsymbol{A})_\infty\,,$$

or

$$G(\boldsymbol{A})=G(\boldsymbol{Q})G(\boldsymbol{A})_\infty\,,$$

i.e. $h_G=1$.

Proof of $(*)$. Take any

$$x=\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in G(\boldsymbol{Q}_p)\,.$$

If $b=0$, then

$$x=\begin{pmatrix} a & 0 \\ c & a^{-1} \end{pmatrix}\in B(\boldsymbol{Q}_p)\,.$$

If $a=0$, then

$$\begin{pmatrix} 0 & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}=\begin{pmatrix} b & 0 \\ d & -c \end{pmatrix}\in B(\boldsymbol{Q}_p) \quad \text{with} \quad \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\in G(\boldsymbol{Z}_p)\,.$$

So we may assume that $a\neq 0$, $b\neq 0$. Put $a=p^{\nu}u$, $b=p^{\mu}v$, $u, v\in \boldsymbol{Z}_p^{\times}$. Multiplying $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ if necessary, we may assume that $\nu\leq\mu$. Then, we have

$$\begin{pmatrix} p^{\nu}u & p^{\mu}v \\ c & d \end{pmatrix}\begin{pmatrix} u^{-1} & -p^{\mu-\nu}v \\ 0 & u \end{pmatrix}=\begin{pmatrix} p^{\nu} & 0 \\ cu^{-1} & p^{-\nu} \end{pmatrix}\in B(\boldsymbol{Q}_p)$$

with

$$\begin{pmatrix} u & -p^{\mu-\nu}v \\ 0 & u \end{pmatrix}\in G(\boldsymbol{Z}_p)\,,$$

which completes the proof of (*).

Remark 1. The argument of (iii) can be generalized to prove that $h_G=1$ for $G=SL_n$ and $G=GL_n$.

In case $G=SL_2$, a fundamental domain for $G(\boldsymbol{Q})\backslash G(\boldsymbol{A})$ is given by

$$\tilde{F}=F\times\prod_{p\neq\infty}G(\boldsymbol{Z}_p)$$

where F is a fundamental domain for $G(\boldsymbol{Z})\backslash G(\boldsymbol{R})$ to be determined. Let $G(\boldsymbol{R})$ act on the upper half plane $\mathfrak{H}$ by the rule

$$x\cdot z=\frac{az+b}{cz+d}\,,\qquad x=\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in G(\boldsymbol{R})\,.$$

The action is transitive and the isotropy group at $i\in\mathfrak{H}$ is

$$K=\{x\in G(\boldsymbol{R});\ xi=i\}=O_2^{+}(\boldsymbol{R})$$

which is a maximal compact subgroup. We have

$$G(\boldsymbol{R})/K\approx\mathfrak{H}\,.$$

Actually $G(\boldsymbol{R})/\{\pm 1\}$ acts on $\mathfrak{H}$ effectively.

Let D be the standard fundamental domain for $G(\boldsymbol{Z})\backslash\mathfrak{H}$. Call ϕ the map $x\longmapsto xi$, $x\in G(\boldsymbol{R})$. Then we can use

$$F=\text{a fundamental domain for}\quad\{\pm 1\}\backslash\phi^{-1}(D)\,.$$

Later we need the area of D. Take the usual non-euclidean metric

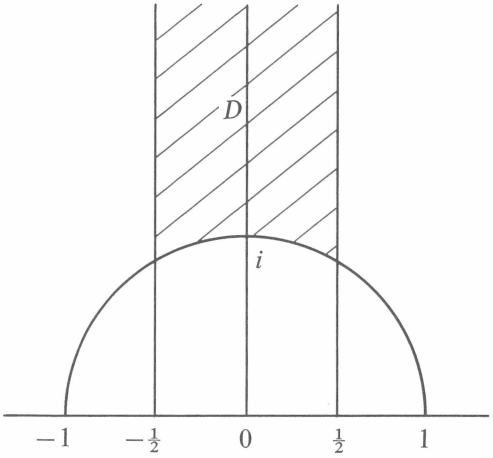
$$ds^2=\frac{dx^2+dy^2}{y^2}, \qquad g=(g_{ij})=\begin{pmatrix}1/y^2 & 0\\ 0 & 1/y^2\end{pmatrix}.$$

The volume element ω is

$$\omega=\sqrt{\det(g_{ij})}dx\wedge dy=\frac{dx\wedge dy}{y^2}.$$

Then, we have

$$\int_D \omega=\int_D \frac{dx\wedge dy}{y^2}=\int_{-1/2}^{1/2} dx\int_{\sqrt{1-x^2}}^{\infty}\frac{dy}{y^2}=\int_{-1/2}^{1/2} dx[-1/y]_{\sqrt{1-x^2}}^{\infty}$$
$$=\int_{-1/2}^{1/2}\frac{dx}{\sqrt{1-x^2}}=2[\sin^{-1}x]_0^{1/2}=2\cdot\frac{\pi}{6}=\frac{\pi}{3}.$$



V. $G(\boldsymbol{Q})\backslash G(\boldsymbol{A})_1$

Let $G\subset GL_n$, $G'\subset GL_{n'}$ be connected algebraic groups over $\boldsymbol{Q}$ and f: $G\to G'$ be a homomorphism over $\boldsymbol{Q}$. It is useful to know that f can be described as

$$f(x)=(\det x)^{\nu}P(x), \qquad \nu\in\boldsymbol{Z}, \quad P(x)\text{: a polynomial map over } \boldsymbol{Q},$$

$x=(x_{ij})\in M_n(\Omega)$. For $R=\boldsymbol{Q}$, $\boldsymbol{Q}_p$, $\boldsymbol{A}$, f induces a map f_R: $G(R)\to G'(\boldsymbol{R})$. For any extension k of $\boldsymbol{Q}$, $k\subset\Omega$, we can speak of homomorphisms over k. In

particular a (rational) character $\xi: G \to G_m$, i.e. a homomorphism (over Ω) of G in GL_1 is important. Characters form naturally an additive group (character module):

$$\hat{G} = \mathrm{Hom}(G, \boldsymbol{G}_m)$$

which is $\boldsymbol{Z}$-free of finite rank. It can be shown that each $\xi \in \hat{G}$ is defined over $\bar{\boldsymbol{Q}}$. Hence $\hat{G}$ gets a structure of a $\mathfrak{g} = \mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$-module. The submodule formed by ξ's invariant under the action of $\mathfrak{g}$ is denoted by

$$\hat{G}(\boldsymbol{Q}) = (\hat{G})^{\mathfrak{g}} .$$

Given a character $\xi \in \hat{G}(\boldsymbol{Q})$, we can consider the sequence:

$$G(\boldsymbol{A}) \xrightarrow{\xi_A} \boldsymbol{A}^{\times} \xrightarrow{\| \ \|} \boldsymbol{R}_+^{\times} .$$

We put

$$G(\boldsymbol{A})_1 \overset{\mathrm{def}}{=} \bigcap_{\xi \in \hat{G}(\boldsymbol{Q})} \mathrm{Ker}(\| \ \| \circ \xi_{\boldsymbol{A}}) .$$

By the product formula, we have $G(\boldsymbol{Q}) \subset G(\boldsymbol{A})_1$. We have

$$G(\boldsymbol{A})/G(\boldsymbol{A})_1 \approx \boldsymbol{R}^{r_Q} , \qquad r_Q = \mathrm{rank}\, \hat{G}(\boldsymbol{Q}) .$$

It is known (Borel, 1963) that

$$\int_{G(\boldsymbol{Q})\backslash G(\boldsymbol{A})_1} \omega < +\infty$$

where ω is a Haar measure of the locally compact group $G(\boldsymbol{A})_1$.[1] Actually, $G(\boldsymbol{A})_1$ is unimodular in the sense of integration theory on topological groups. As for the compactness,

$G(\boldsymbol{Q})\backslash G(\boldsymbol{A})_1$ is compact
$\Leftrightarrow$ any unipotent element of $G(\boldsymbol{Q})$ is contained in the radical of $G(\boldsymbol{Q})$.[2]

In particular, when G is semi-simple,

$G(\boldsymbol{Q})\backslash G(\boldsymbol{A})_1$ is compact
$\Leftrightarrow G(\boldsymbol{Q})$ has no non-trivial unipotent element.

This is a generalization of the following statement on quadraic forms over $\boldsymbol{Q}$ of n (≥ 3) variables:

$O_n^+(f)(\boldsymbol{Q})\backslash O_n^+(f)(\boldsymbol{A})$ is compact
$\Leftrightarrow v_{\boldsymbol{Q}}(f)=0$
$\Leftrightarrow$ "$f(x)=0\Leftrightarrow x=0$ for $x\in\boldsymbol{Q}^n$",

where $v_{\boldsymbol{Q}}(f)$ means the Witt index of f over $\boldsymbol{Q}$. Finally, note that $G(\boldsymbol{Q})\backslash G(\boldsymbol{A})_1$ is compact when G is abelian because $G(\boldsymbol{Q})$ is its own radical.

In Section IV we considered simple examples for which $h_G=1$. Here, we shall consider the general case. Let G be any connected algebraic group in GL_n defined over $\boldsymbol{Q}$. Recall that

$$h=h_G=\#(G(\boldsymbol{Q})\backslash G(\boldsymbol{A})/G(\boldsymbol{A})_\infty)\,.$$

Let

$$G(\boldsymbol{A})=\sum_{i=1}^{h} G(\boldsymbol{Q})x_iG(\boldsymbol{A})_\infty\,,\qquad x_i\in G(\boldsymbol{A})\,,$$

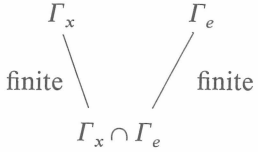
be the decomposition into double cosets. We want to determine a fundamental domain for $G(\boldsymbol{Q})\backslash G(\boldsymbol{A})$. We first determine a fundamental domain for $G(\boldsymbol{Q})\backslash G(\boldsymbol{Q})x_iG(\boldsymbol{A})_\infty$. For $x\in G(\boldsymbol{A})$ put

$$\Gamma_x=G(\boldsymbol{Q})\cap xG(\boldsymbol{A})_\infty x^{-1}\subset G(\boldsymbol{R})\,.$$

In particular, for $x=e$, we have

$$\Gamma_e=G(\boldsymbol{Q})\cap G(\boldsymbol{A})_\infty=G(\boldsymbol{Z})\,.$$

Γ_x is discrete in $G(\boldsymbol{R})$ for all $x\in G(\boldsymbol{A})$ and Γ_x, Γ_e are commensurable each other:



Let F_x be a fundamental domain for $\Gamma_x\backslash G(\boldsymbol{R})$ and put

$$\tilde{F}_x=F_x\times\prod_{p\neq\infty} x_pG(\boldsymbol{Z}_p)x_p^{-1}\,,\qquad x=(x_p)\,.$$

Then $\tilde{F}_x$ is a fundamental domain for $G(\boldsymbol{Q})\backslash G(\boldsymbol{Q})xG(\boldsymbol{A})_\infty x^{-1}$ and hence $\tilde{F}_xx$ is a fundamental domain for $G(\boldsymbol{Q})\backslash G(\boldsymbol{Q})xG(\boldsymbol{A})_\infty$. Doing this for all representatives x_i, $1\leq i\leq h$, we obtain a fundamental domain

$$\tilde{F}=\sum_{i=1}^{h}\tilde{F}_{x_i}x_i$$

for $G(\boldsymbol{Q})\backslash G(\boldsymbol{A})$.

From this it follows that

$G(\boldsymbol{Q})\backslash G(\boldsymbol{A})$ is compact
$\Leftrightarrow \Gamma_{x_i}\backslash G(\boldsymbol{R})$ is compact for all i
$\Leftrightarrow G(\boldsymbol{Z})\backslash G(\boldsymbol{R})$ is compact.

Since $G(\boldsymbol{Q})\backslash G(\boldsymbol{A})$ is not even of volume finite, we need to modify above argument.

LEMMA 1. $G(\boldsymbol{A})=G(\boldsymbol{A})_1 G(\boldsymbol{A})_\infty$.

Since $G(\boldsymbol{A})_1$ is a normal subgroup of $G(\boldsymbol{A})$ and $G(\boldsymbol{A})_\infty$ is an open subgroup in $G(\boldsymbol{A})$, $G(\boldsymbol{A})/G(\boldsymbol{A})_1 G(\boldsymbol{A})_\infty$ is discrete. On the other hand, $G(\boldsymbol{A})/G(\boldsymbol{A})_1 \approx \boldsymbol{R}^{r_{\boldsymbol{Q}}}$ is connected and hence $G(\boldsymbol{A})=G(\boldsymbol{A})_1 G(\boldsymbol{A})_\infty$. Q.E.D.

By Lemma 1, we can write

$$G(\boldsymbol{A})=\sum G(\boldsymbol{Q})x_i G(\boldsymbol{A})_\infty\,, \qquad x_i\in G(\boldsymbol{A})_1\,.$$

We have

$$G(\boldsymbol{A})_1=\sum_{i=1}^{h} G(\boldsymbol{Q})x_i G(\boldsymbol{A})_{1,\infty}$$

where $G(\boldsymbol{A})_{1,\infty}=G(\boldsymbol{A})_1\cap G(\boldsymbol{A})_\infty$.
Now, put

$$G(\boldsymbol{R})_1 \overset{\text{def}}{=} \{x\in G(\boldsymbol{R})\,;\,|\,\xi(x)\,|_\infty=1,\ \forall\,\xi\in\hat{G}(\boldsymbol{Q})\}\,.$$

Then, we can verify that

(i) $G(\boldsymbol{A})_{1,\infty}=G(\boldsymbol{R})_1\times\prod_{p\neq\infty} G(\boldsymbol{Z}_p)$,

(ii) $G(\boldsymbol{R})/G(\boldsymbol{R})_1\approx\boldsymbol{R}^{r_{\boldsymbol{Q}}}$, $r_{\boldsymbol{Q}}=\operatorname{rank}\hat{G}(\boldsymbol{Q})$.

Putting, as before,

$$\Gamma_x=G(\boldsymbol{Q})\cap xG(\boldsymbol{A})_{1,\infty}x^{-1}\,, \qquad x\in G(\boldsymbol{A})_1\,,$$

we can prove that

$G(\boldsymbol{Z})\backslash G(\boldsymbol{R})_1$ is compact
$\Leftrightarrow \Gamma_{x_i}\backslash G(\boldsymbol{R})$ is compact
$\Leftrightarrow G(\boldsymbol{Q})\backslash G(\boldsymbol{A})_1$ is compact
$\Leftrightarrow$ any unipotent element of $G(\boldsymbol{Q})$ is contained in the radical of $G(\boldsymbol{Q})$.

We also have:

$$\int_{G(\boldsymbol{Z})\backslash G(\boldsymbol{R})_1} \omega_\infty < +\infty \Longleftrightarrow \int_{G(\boldsymbol{Q})\backslash G(\boldsymbol{A})_1} \omega_{\boldsymbol{A}} < +\infty \ .^{3)}$$

VI. Group of Units

Let G be a connected algebraic group over $\boldsymbol{Q}$. It is known that the group $G(\boldsymbol{Z})$ of units is finitely generated.[1] We need occasionally the following Levi-Chevalley decomposition of G:[2]

$$G = NTS\,,$$

where

N = the unipotent radical of G,
$R = NT$ = the radical of G,
$H = TS$ = a reductive group,
T = a torus = the identify component of the center of H,
S = a semi-simple group = the commutator group of H.

Furthermore, $G = NH$ is a semi-direct product with N normal and $T \times S \to H$ defined by $(t, s) \longmapsto ts$ is an isogeny, i.e. a surjective homomorphism with finite kernel. As for the uniqueness, let $G = NT'S' = NH'$ be another such decomposition. Then, H' is conjugate to H by an element of $N(\boldsymbol{Q})$. Accordingly, T', S' are conjugate to T, S, respectively. Hence the decomposition is unique up to isomorphisms over $\boldsymbol{Q}$.

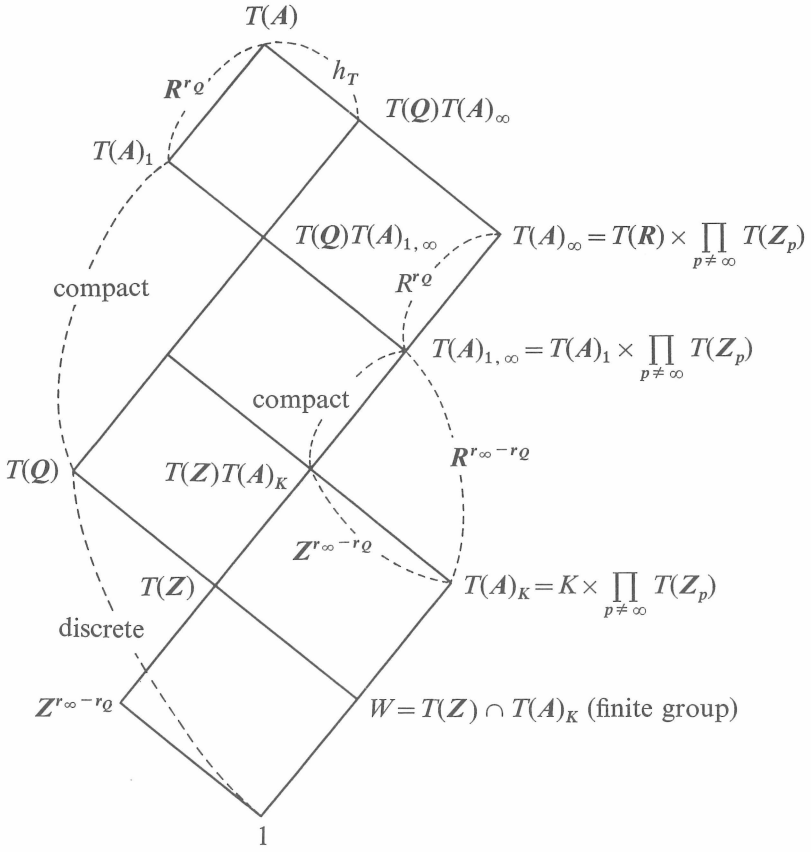
One proves that $G(\boldsymbol{Z}) \supset N(\boldsymbol{Z})T(\boldsymbol{Z})S(\boldsymbol{Z})$ and the latter has a finite index in $G(\boldsymbol{Z})$. In this section, we shall mainly consider a torus and obtain the number of generators of $T(\boldsymbol{Z})$. But, first, when $N = G_a$, we have $N(\boldsymbol{Z}) = \boldsymbol{Z}$, a group of one generator. A general unipotent group N has a semi-direct decomposition $N = N' \cdot H'$ where N' is normal and $\dim H' = 1$. Hence the structure of $N(\boldsymbol{Z})$ is determined inductively. Let now T be a torus over $\boldsymbol{Q}$. The unique maximal compact subgroup K of $T(\boldsymbol{R})$ is given by

$$K \overset{\text{def}}{=} \{x \in T(\boldsymbol{R}) ; |\xi(x)|_\infty = 1, \forall \xi \in \hat{T}(\boldsymbol{R})\} .$$

We put $r_{\boldsymbol{Q}} = \operatorname{rank} \hat{T}(\boldsymbol{Q})$, $r_\infty = \operatorname{rank} \hat{T}(\boldsymbol{R})$.
Then, we have $T(\boldsymbol{R})/K \approx \boldsymbol{R}^{r_\infty}$. If we put

$$T(\boldsymbol{A})_K \overset{\text{def}}{=} K \times \prod_{p \neq \infty} T(\boldsymbol{Z}_p) ,$$

this becomes a compact subgroup of $T(\boldsymbol{A})$. The following picture explains the structure of $T(\boldsymbol{A})$.



One obtains from this the following theorem which generalizes Dirichlet's unit theorem in algebraic number theory.

THEOREM 1. $T(\boldsymbol{Z}) \approx \boldsymbol{Z}^{r_\infty - r_Q} \times W$.[3]

Let us describe now how the original Dirichlet's theorem follows from Theorem 1.

Let K be an algebraic number field over $\boldsymbol{Q}$ of degree n. Let $\mathfrak{o}_K$ be the ring of integers of K and $\omega_1, \cdots, \omega_n$ be a basis of $\mathfrak{o}_K$. Consider the regular representation $x \longmapsto P(x)$ of K using this basis:

$$(x\omega_1, \cdots, x\omega_n) = (\omega_1, \cdots, \omega_n)P(x) ,$$

where $P(x) \in M_n(\boldsymbol{Q})$, $x \in K$. Extending scalars from K to Ω, consider the set

$$A = \{P(x) \in M_n(\Omega);\ x = \sum x_i \omega_i,\ x_i \in \Omega\}$$

which is a subalgebra of $M_n(\Omega)$ defined over $\boldsymbol{Q}$. Put

$$T = A \cap GL_n(\Omega) .$$

As we see soon, T becomes a torus defined over $\boldsymbol{Q}$. Since $A(\boldsymbol{Q}) = K$ (identification by P), we have $T(\boldsymbol{Q}) = K^\times$ and $T(\boldsymbol{Z}) = \mathfrak{o}_K^\times$.

In general, let K/k be a finite separable extension and V be a variety defined over K. Then, in almost all cases, we can find a variety W defined over k such that $\dim W = [K:k] \dim V$ and $W_k \approx V_K$. The association $V \to W$ is functorial and written: $W = R_{K/k}(V)$ (Weil functor).[4] Applying this to $V = \boldsymbol{G}_m/K$, we have $T = R_{K/\boldsymbol{Q}}(\boldsymbol{G}_m)$.

The character module $\hat{T}$ is described as follows. Let $\omega_i^{(k)}$, $1 \leq k \leq n$, be conjugates of ω_i. For $x = x_1\omega_1 + \cdots + x_n\omega_n$, $x_i \in \Omega$, put

$$x^{(k)} = x_1\omega_1^{(k)} + \cdots + x_n\omega_n^{(k)} .$$

Then, $\xi_k \in \hat{T}$ is defined by

$$\xi_k(P(x)) = x^{(k)} , \qquad P(x) \in T .$$

It can be seen that $\xi_1, \cdots, \xi_n$ form a basis of $\hat{T}$, a free module of rank n. Since

$$\begin{aligned} (\xi_1 + \cdots + \xi_n)(P(x)) &= \xi_1(P(x)) \cdots \xi_n(P(x)) \\ &= x^{(1)} \cdots x^{(n)} \\ &= N_{K/\boldsymbol{Q}}(x) , \end{aligned}$$

we have

$$\hat{T}(\boldsymbol{Q}) = \langle \xi_1 + \cdots + \xi_n \rangle = \langle N_{K/\boldsymbol{Q}} \rangle$$

by identification by P. On the other hand, after a suitable change of order, let $\xi_1, \cdots, \xi_{r_1}$ embed K in $\boldsymbol{R}$ and let $\xi_{r_1+1}, \overline{\xi_{r_1+1}}, \cdots, \xi_{r_1+r_2}, \overline{\xi_{r_1+r_2}}$ embed K in $\boldsymbol{C}$ (not in $\boldsymbol{R}$). Then we have

$$\hat{T}(\boldsymbol{R}) = \{\xi_1, \cdots, \xi_{r_1}, \xi_{r_1+1} + \overline{\xi_{r_1+1}}, \cdots, \xi_{r_1+r_2} + \overline{\xi_{r_1+r_2}}\} .$$

We have therefore shown that $r_{\boldsymbol{Q}} = \text{rank } \hat{T}(\boldsymbol{Q}) = 1$ and $r = rank\ \hat{T}(\boldsymbol{R}) = r_1 + r_2$. Theorem 1 implies that

COROLLARY 1 (Dirichlet). $\mathfrak{o}_K^{\times} \approx \boldsymbol{Z}^{r_1+r_2-1} \times W$.

VII. Reduction Modulo p

Let G be a connected algebraic group over $\boldsymbol{Q}$. We denote by $G^{(p)}$ the algebraic group defined over $\boldsymbol{F}_p = \boldsymbol{Z}/p\boldsymbol{Z}$ obtained by reduction mod. p. For almost all p, $G^{(p)}$ is just defined by a system of polynomials reduced mod. p of the defining system of polynomials for G with coefficients in $\boldsymbol{Q}$. Let

$$G = NTS$$

be a Levi-Chevalley decomposition of G explained in Section VI. Then we have a similar decomposition

$$G^{(p)} = N^{(p)}T^{(p)}S^{(p)} \qquad \text{for} \quad \forall' p .$$

Since the number of rational points over $\boldsymbol{F}_p$ is unchanged by an isogeny, we get

$$\#(G^{(p)}(\boldsymbol{F}_p)) = \#(N^{(p)}(\boldsymbol{F}_p))\ \#(T^{(p)}(\boldsymbol{F}_p))\ \#(S^{(p)}(\boldsymbol{F}_p))$$

for almost all p.

(i) N (unipotent). $\#(N^{(p)}(\boldsymbol{F}_p)) = p^{\dim N}$

(ii) T (torus).

Let $\hat{T} = \langle \xi_1, \cdots, \xi_d \rangle$ and let $K/\boldsymbol{Q}$ be a finite galois extension such that $\hat{T} = \hat{T}(K)$. We obtain an integral representation of degree d: $\mathfrak{g} \to GL_d(\boldsymbol{Z})$, $\mathfrak{g} = \text{Gal}(K/\boldsymbol{Q})$, by

$$\begin{pmatrix} \xi_1^{\sigma} \\ \vdots \\ \xi_d^{\sigma} \end{pmatrix} = M(\sigma) \begin{pmatrix} \xi_1 \\ \vdots \\ \xi_d \end{pmatrix}, \qquad \sigma \in \mathfrak{g} .$$

Choose p such that $T^{(p)}$ remains a torus and p is unramified for $K/\boldsymbol{Q}$. Call $\sigma_{\mathfrak{p}}$

($\mathfrak{p}$ is a prime ideal in K dividing p) the Frobenius substition in $\mathfrak{g}$ for $\mathfrak{p}$. Then it can be shown that

$$\#(T^{(p)}(\boldsymbol{F}_p)) = \det(p \cdot 1_d - M(\sigma_{\mathfrak{p}})) , \qquad \forall' p .^{1)}$$

(iii) $G = SL_2$. In this case, we have $G^{(p)} = SL_2$ for all p. $\#(SL_2(\boldsymbol{F}_p)) = p(p^2-1)$.

In general, we define:

$$\mu_p(G) = \frac{\#(G^{(p)}(\boldsymbol{F}_p))}{p^{\dim G}} .$$

(i) N (unipotent). $\mu_p(N) = 1$ for $\forall' p$.

(ii) T (torus).

$$\mu_p(T) = \det(1_d - p^{-1} M(\sigma_{\mathfrak{p}})) = \frac{1}{L_p(1, \chi_T)}$$

where $L_p(s, \chi_T)$ is the p-component of Artin's L-function associated with the representation $\mathfrak{g} \to GL_d(\boldsymbol{Z})$.

(iii) $G = SL_2$. $\mu_p(SL_2) = 1 - p^{-2}$.

Note that $\prod_p \mu_p(SL_2) = 1/\zeta(2) = 6/\pi^2$.

We want to generalize this last property for any semi-simple groups. So, let G be a connected semi-simple algebraic group defined over $\boldsymbol{Q}$ with $d = \dim G \geq 3$. For the moment, we take $\boldsymbol{C}$ for Ω. Hence the Lie algebra $\mathfrak{g}$ of G is a complex semi-simple Lie algebra defined over $\boldsymbol{Q}$. Call G_0 the identity component of the Lie group $G(\boldsymbol{R})$ and $\mathfrak{g}_0$ the Lie algebra of G_0. Hence, we have

$$\mathfrak{g} = \mathfrak{g}_0 \underset{\boldsymbol{R}}{\otimes} \boldsymbol{C}$$

Let K be a maximal compact subgroup of G_0 and $\mathfrak{k}$ be its Lie algebra. Let B: $\mathfrak{g} \times \mathfrak{g} \to \boldsymbol{C}$ be the Killing form defined by

$$B(X, Y) = \mathrm{tr}(\mathrm{ad}\, X \cdot \mathrm{ad}\, Y) .$$

B induces on $\mathfrak{g}_0$ the orthogonal decomposition:

$$\mathfrak{g}_0 = \mathfrak{k} + \mathfrak{k}^{\perp} ,$$

where B is <0 on $\mathfrak{k}$ and >0 on $\mathfrak{k}^{\perp}$. Therefore B is <0 on

$$\mathfrak{u}=\mathfrak{k}+\sqrt{-1}\mathfrak{k}^{\perp}.$$

Let U be the connected Lie group $\subset G$ corresponding to $\mathfrak{u}$. U is compact semi-simple and is called a compact form of G_0. U is a maximal compact subgroup of G.

Let b_v, $0\leq v\leq d$, be Betti-numbers of U. We know that $b_0=b_d=1$, $b_1=b_{d-1}=0$, $b_2=b_{d-2}=0$, $b_3=b_{d-3}>0$. As for the Poincaré polynomial of U, we know that

$$P(U;t)=\sum_{v=0}^{d} b_v t^v=\prod_{i=0}^{l}(1+t^{2a_i-1}),$$

where $l=$rank of $U=$dimension of a maximal torus of $U=$dimension of a Cartan subalgebra of $\mathfrak{g}$. Note that $a_i\geq 2$, $1\leq i\leq l$, because $b_1=b_2=0$.

Example 1. $G=SL_2$. Then, we have

$$\mathfrak{g}=\mathfrak{sl}_2(\boldsymbol{C})=\{X\in M_2(\boldsymbol{C});\ \mathrm{tr}\,X=0\},$$

$$G_0=SL_2(\boldsymbol{R}),$$

$$\mathfrak{g}_0=\mathfrak{sl}_2(\boldsymbol{R})=\{X\in M_2(\boldsymbol{R});\ \mathrm{tr}\,X=0\},$$

$$K=O_2^{+}(\boldsymbol{R})=\{x\in GL_2(\boldsymbol{R});\ {}^t x\,x=1_2,\ \det x=1\},$$

$$\mathfrak{k}=\{X\in M_2(\boldsymbol{R});\ {}^tX+X=0\}=\left\{\begin{pmatrix}0 & b\\ -b & 0\end{pmatrix};\ b\in\boldsymbol{R}\right\},$$

$$B(X,Y)=4\,\mathrm{tr}(XY),$$

$$\mathfrak{k}^{\perp}=\left\{\begin{pmatrix}x & y\\ y & -x\end{pmatrix};\ x,y\in\boldsymbol{R}\right\},$$

$$\mathfrak{u}=\mathfrak{k}+\sqrt{-1}\mathfrak{k}^{\perp}=\{X\in M_2(\boldsymbol{C});\ {}^t\bar{X}+X=0,\ \mathrm{tr}\,X=0\}$$

and

$$U=SU_2=\{x\in GL_2(\boldsymbol{C});\ {}^t\bar{x}\,x=1,\ \det x=1\}.$$

Since $U\approx S^3$ (3-sphere), we have $P(U;t)=1+t^3$, $b_0=b_3=1$, $b_1=b_2=0$, $l=1$, $a_1=2$. $T=S^1$ (circle) is a maximal torus of U and $U/T=S^3/S^1=S^2$ (Hopf fibration).

Now, we introduce the Chevalley group.[2] Let $\mathfrak{g}$ be a complex semi-simple Lie algebra with $n=\dim\mathfrak{g}$. It is known that $\mathfrak{g}$ has a basis (called

Chevalley basis) for which all structure constants C_{ij}^k are integers. Using such a basis, Aut $\mathfrak{g}$ can be embedded in GL_n as an algebraic group over $\boldsymbol{Q}$. $\boldsymbol{G}=(\mathrm{Aut}\,\mathfrak{g})_0$, the identity component, is called a Chevalley group. For every connected semi-simple algebraic group G over $\boldsymbol{Q}$, G/center becomes a $\boldsymbol{Q}$-form of a Chevalley group $\boldsymbol{G}$, i.e. G/center is isomorphic with $\boldsymbol{G}$ over $\bar{\boldsymbol{Q}}$.

Let us determine $\mu_p(\boldsymbol{G})$ for almost all p. As before, put $G_0=$the identity component of $\boldsymbol{G}(\boldsymbol{R})$, $U=$a compact form of G_0. Fixing a Cartan subalgebra of the Lie algebra of $\boldsymbol{G}$, denote by N the number of positive (negative) roots, by W the Weyl group. For each $w\in W$, put

$$N(w)=\#\{\alpha>0 \text{ (positive roots)};\ w(\alpha)<0\}\,.$$

We have $n=l+2N$, l being the dimension of the Cartan subalgebra. A maximal torus T of U has dimension l, too. It is known that

$$\#(\boldsymbol{G}^{(p)}(\boldsymbol{F}_p))=(p-1)^l p^N \sum_{w\in W} p^{N(w)}\,, \tag{1}$$

$$P(U/T;t)=\sum_{w\in W} t^{2N(w)}=(t^2-1)^{-l}\prod_{i=1}^{l}(t^{2a_i}-1)\,. \tag{2}$$

From (1), (2), putting $t=\sqrt{p}$, we have

$$\#(\boldsymbol{G}^{(p)}(\boldsymbol{F}_p))=p^N\prod_{i=1}^{l}(p^{a_i}-1)\,. \tag{3}$$

On the other hand, since

$$P(U;t)=\prod_{i=1}^{l}(1+t^{2a_i-1})\,,$$

we get

$$n=\dim U=2\sum_{i=1}^{l}a_i-l\,,\qquad \text{i.e.}\qquad \sum_{i=1}^{l}a_i=(n+l)/2=N+l$$

as $n=l+2N$. Hence, (3) implies that

$$\mu_p(\boldsymbol{G})=\frac{\#(\boldsymbol{G}^{(p)}(\boldsymbol{F}_p))}{p^n}=\prod_{i=1}^{l}(1-p^{-a_i})\,,\qquad \forall' p\,. \tag{4}$$

THEOREM 1. *Let G be a connected semi-simple algebraic group over $\boldsymbol{Q}$. Then $\prod_p \mu_p(G)$ is absolutely convergent.*

Proof. (Outline.)

Case 1. Assume that G is isogenous to a Chevalley group $\boldsymbol{G}$ over $\boldsymbol{Q}$. Then, from (4), we have

$$\prod_p \mu_p(G) \sim \prod_p \prod_{i=1}^{l} (1-p^{-a_i}) \sim \prod_{i=1}^{l} \zeta(a_i)^{-1}$$

since $a_i \geq 2$. (For $a, b \in \boldsymbol{R}$ we write $a \sim b$ when $ab^{-1} \in \boldsymbol{Q}^\times$).

Case 2. Otherwise, G is isogenous to a $\boldsymbol{Q}$-form of $\boldsymbol{G}$. We known that

$$p^N \prod_{i=1}^{l} (p^{a_i}-1) \leq \#(G^{(p)}(\boldsymbol{F}_p)) \leq p^N \prod_{i=1}^{l} (p^{a_i}+1)^{3)}$$

which implies

$$\prod_{i=1}^{l} (1-p^{-a_i}) \leq \mu_p(G) \leq \prod_{i=1}^{l} (1+p^{-a_i}) .$$

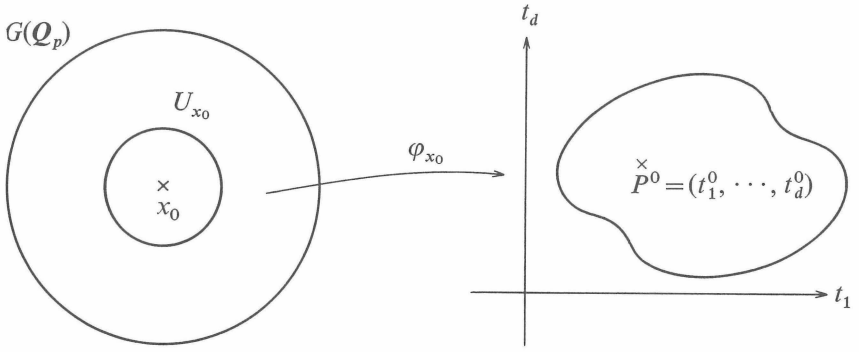
VIII. Tamagawa Numbers[1)]

Let G be a connected algebraic group over $\boldsymbol{Q}$ with $d = \dim G$. A differential form ω of degree d on G which is regular and nowhere zero is called a gauge form on G. It can be shown that there is a left invariant gauge form ω over $\boldsymbol{Q}$, unique up to multiplication by $\boldsymbol{Q}^\times$. For each $x_0 \in G$, using local coordinates $t_1, \cdots, t_d$ around x_0, we have

(i) $\omega = f\,dt_1 \wedge \cdots \wedge dt_d$, f is regular around x_0,

(ii) $f(x_0) \neq 0$.

Now, take a point $x_0 \in G(\boldsymbol{Q}_p)$ ($p = \infty$ is included).



Then, $\varphi_{x_0}: x \longmapsto (t_1(x), \cdots, t_d(x))$ induces a local homeomorphism $U_{x_0} \approx \varphi_{x_0}(U_{x_0}) \subset \boldsymbol{Q}_p^d$. On $\boldsymbol{Q}_p^d$ choose the normalized Haar measure such that $[0, 1]^d$ has measure 1 for $p=\infty$ and $\boldsymbol{Z}_p^d$ has measure 1 for $p \neq \infty$. Pulling back this measure on U_{x_0} by φ_{x_0}, we obtain a measure

$$|dt_1 \wedge \cdots \wedge dt_d|_p \qquad \text{on} \quad U_{x_0}.$$

For a gauge form ω having properties (i), (ii) above, using the power series expansion

$$f(x)=\sum_{\nu} a_\nu (t_1 - t_1^0)^{\nu_1} \cdots (t_d - t_d^0)^{\nu_d},$$

$a_\nu \in \boldsymbol{Q}_p$, $\nu=(\nu_1, \cdots, \nu_d)$, we obtain a measure

$$\omega_{U_{x_0}} = |f(x)|_p \, |dt_1 \wedge \cdots \wedge dt_d|_p. \tag{1}$$

Applying functional determinant, we can verify that this local measure extends to a left invariant Haar measure ω_p on $G(\boldsymbol{Q}_p)$. Put

$$\mu_p = \int_{G(\boldsymbol{Z}_p)} \omega_p .$$

It can be shown that

$$\mu_p = \frac{\#(G^{(p)}(\boldsymbol{F}_p))}{p^d} = \mu_p(G) \qquad \text{for} \quad \forall' p .$$

Assume, for the moment, that G is unipotent or semi-simple, or, more generally, that $\hat{G}(\boldsymbol{Q})=\{0\}$. Then, on $G(\boldsymbol{A})_\infty = G(\boldsymbol{R}) \times \prod_{p \neq \infty} G(\boldsymbol{Z}_p)$, the product measure $\prod_p \omega_p$ makes sense because $\prod_p \mu_p$ converges absolutely. Since $G(\boldsymbol{A})_\infty$ is an open subgroup in $G(\boldsymbol{A})$, $\prod_p \omega_p$ induces a Haar measure $\omega_{\boldsymbol{A}}$ on $G(\boldsymbol{A})$. Finally, let $\omega' = a\omega$, $a \in \boldsymbol{Q}^\times$, be another left invariant gauge form on G over $\boldsymbol{Q}$. By the product formula of valuations, we have

$$\omega'_{\boldsymbol{A}} = \left(\prod_p |a|_p \right) \omega_{\boldsymbol{A}} = \omega_{\boldsymbol{A}} .$$

From now on, we write $\omega_{\boldsymbol{A}} = dG(\boldsymbol{A})$ and define the Tamagawa member:

$$\tau(G) \overset{\text{def}}{=} \int_{G(\boldsymbol{Q}) \backslash G(\boldsymbol{A})} dG(\boldsymbol{A})$$

which is finite when G is unipotent or semi-simple, or, more generally, whenever $\hat{G}(\boldsymbol{Q})=\{0\}$, i.e. $G(\boldsymbol{A})_1=G(\boldsymbol{A})$.

Example 1. $G=\boldsymbol{G}_a$. Then, $\omega=dt$, t being the natural coordinate function and

$$\mu_p=\int_{\boldsymbol{Z}_p}|dt|_p=1\,,\qquad p\neq\infty\,.$$

Since $\tilde{F}=[0,1)\times\prod_p \boldsymbol{Z}_p$ is a fundamental domain for $G(\boldsymbol{Q})\backslash G(\boldsymbol{A})=\boldsymbol{Q}\backslash\boldsymbol{A}$, we have

$$\tau(G)=\int_{\boldsymbol{Q}\backslash\boldsymbol{A}}\omega_{\boldsymbol{A}}=1\,.$$

Example 2.

$$G=SL_2(\Omega)=\left\{x=\begin{pmatrix}t_1 & t_2\\ t_3 & t_4\end{pmatrix},\ t_1t_4-t_2t_3=1\right\}.$$

Consider t_1, t_2, t_3, as parameters around e, i.e. $P^0=e$. We can verify that

$$\omega=\frac{dt_1\wedge dt_2\wedge dt_3}{t_1}$$

is a left invariant gauge form on G. Put, for all $p\neq\infty$,

$$G^{(1)}(\boldsymbol{Z}_p)=\left\{\begin{pmatrix}t_1 & t_2\\ t_3 & t_4\end{pmatrix}\in G(\boldsymbol{Z}_p)\,;\qquad \begin{pmatrix}t_1 & t_2\\ t_3 & t_4\end{pmatrix}\equiv\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\text{mod. } p\right\}.$$

Since $G(\boldsymbol{Z}_p)/G^{(1)}(\boldsymbol{Z}_p)=SL_2(\boldsymbol{F}_p)$ is of order $p(p^2-1)$ and $|t_1|_p=1$ on $G^{(1)}(\boldsymbol{Z}_p)$, we have

$$\begin{aligned}\mu_p&=\int_{G(\boldsymbol{Z}_p)}\omega_p=p(p^2-1)\int_{G^{(1)}(\boldsymbol{Z}_p)}|dt_1\wedge dt_2\wedge dt_3|_p\\ &=p(p^2-1)\int_{t_1\equiv 1}\int_{t_2\equiv 0}\int_{t_3\equiv 1}|dt_1|_p|dt_2|_p|dt_3|_p\\ &=\frac{p(p^2-1)}{p^3}=1-p^{-2}\,.\end{aligned}$$

Since $h_G=1$, we can take

$$\tilde{F}=F\times\prod_{p\neq\infty}G(\boldsymbol{Z}_p)$$

as a fundamental domain for $SL_2(\boldsymbol{Q})\backslash SL_2(\boldsymbol{A})$, where F is a fundamental domain for $SL_2(\boldsymbol{Z})\backslash SL_2(\boldsymbol{R})$. Hence,

$$\tau(G)=\int_F \omega_\infty \cdot \prod_{p\neq\infty}(1-p^{-2})=\frac{\int_F \omega_\infty}{\zeta(2)}.$$

As in Section IV, let ϕ be a map $G(\boldsymbol{R})\to X=\mathfrak{H}$ defined by

$$\phi(x)=x\cdot i=\frac{t_1 i+t_2}{t_3 i+t_4}.$$

Put

$$K=\{x\in G(\boldsymbol{R});\ x\cdot i=i\}$$

$$=O_2^+(\boldsymbol{R})=\left\{\begin{pmatrix} t_1 & t_2 \\ -t_2 & t_1 \end{pmatrix};\ t_1^2+t_2^2=1\right\}.$$

On K, the unit circle, $\omega_K=dt_1/2t_2$ is an invariant form and on X, $\omega_X=(dx\wedge dy)/y^2$ is invariant under the action of $G(\boldsymbol{R})$. We have

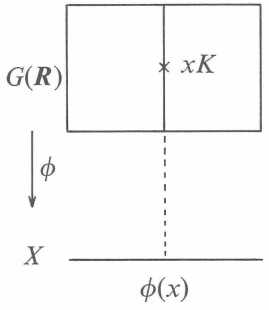
$$\int_K \omega_K=\pi\,,\qquad \int_{G(\boldsymbol{Z})\backslash X}\omega_X=\pi/3\,.^{2)}$$

If we put

$$\omega_G=\frac{dt_1\wedge dt_2\wedge dt_3}{t_1}$$

on $G(\boldsymbol{R})$, we can verify that $\omega_G=\phi^*\omega_X\wedge\omega_K$. Hence,

$$\int_{G(\boldsymbol{R})} f(x)\omega_G=\int_X \omega_X\int_K f(xk)\omega_K\,.$$



Since we can use $F=$a fundamental domain for $\{\pm 1\}\backslash\phi^{-1}(D)$, where D is the standard fundamental domain for $G(\boldsymbol{Z})\backslash X$ (i.e. $\phi^{-1}(D)=F+(-1)F$), we get, with $f=\chi_F$,

$$\begin{aligned}\int_{G(\boldsymbol{R})}\chi_F(x)\omega_G &= \frac{1}{2}\int_{G(\boldsymbol{R})}\chi_{\phi^{-1}(D)}(x)\omega_G=\frac{1}{2}\int_X\omega_X\int_K\chi_{\phi^{-1}(D)}(xk)\omega_K\\ &=\frac{1}{2}\int_X\omega_X\cdot\chi_D\int_K\omega_K=\frac{1}{2}\int_D\omega_X\int_K\omega_K\\ &=\frac{1}{2}\cdot\frac{\pi}{3}\cdot\pi=\frac{\pi^2}{6}=\zeta(2)\,.\end{aligned}$$

Therefore, we have $\tau(G)=1$.

Remark 1. The statement

(W) $\qquad\qquad \tau(G)=1 \quad \textit{when} \quad G$ is simply connected,

is known as Weil's conjecture. (W) has been settled for almost all simply connected groups, including all classical groups and quasi-split groups.

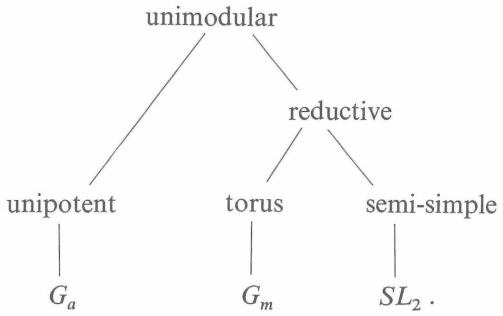
Remark 2. When $\boldsymbol{G}$ is a Chevalley group, as an application of his theory of Eisenstein series, Langlands proved that

$$\int_{\boldsymbol{G}(\boldsymbol{Z})\backslash\boldsymbol{G}(\boldsymbol{R})}\omega_\infty=\#F\prod_{i=1}^{l}\zeta(a_i)\,, \tag{2}$$

where $F=$the fundamental group of $\boldsymbol{G}$ and a_i are integers appeared in Section VII. Combining (2) with the fact that $h_{\boldsymbol{G}}=1$ and with a computation of the volume of $\boldsymbol{G}(\boldsymbol{Z}_p)$ for any prime p, we can prove that

$$\tau(\boldsymbol{G})=\#F\,.$$

Now, we shall define the Tamagawa number for any unimodular group. A connected algebraic group G is called unimodular if the left invariant gauge form is also right invariant. We have the following chains of containment



Let $\hat{G}=\mathrm{Hom}(G, G_m)$ be the character module. Choose a finite galois extension $K/\boldsymbol{Q}$ such that $\hat{G}=\hat{G}(K)$. Then, $\mathfrak{g}=\mathrm{Gal}(K/\boldsymbol{Q})$ acts on $\hat{G}$. Since $\hat{G}$ is $\boldsymbol{Z}$-free of finite rank, we may speak of the character χ_G of the corresponding integral representation of $\mathfrak{g}$. Let

$$L(s, \chi_G)=\prod_{p\neq\infty} L_p(s, \chi_G)$$

be the Artin's L-function. Then the product

$$\prod_{p\neq\infty}\left(L_p(1, \chi_G)\cdot\int_{G(\boldsymbol{Z}_p)}\omega_p\right)$$

converges absolutely because $\chi_G=\chi_T$ when $G=NTS$ (Levi-Chevalley decomposition) and

$$L_p(1, \chi_G)\mu_p(G)=L_p(1, \chi_T)\mu_p(T)\mu_p(N)\mu_p(S)=\mu_p(S)$$

for almost all p. (See Section VII, Th. 1.)

Put

$$\rho_G=\lim_{s\to 1}(s-1)^{r_{\boldsymbol{Q}}}L(s, \chi_G)>0\,,$$

where $r_{\boldsymbol{Q}}=\mathrm{rank}\,\hat{G}(\boldsymbol{Q})$. Recall that $G(\boldsymbol{A})_1=\{x\in G(\boldsymbol{A})\,;\,\|\xi_{\boldsymbol{A}}(x)\|=1, \forall\,\xi\in\hat{G}(\boldsymbol{Q})\}$ and the map

$$\psi(x)=(\log\|\xi_1(x)\|, \cdots, \log\|\xi_{r_{\boldsymbol{Q}}}(x)\|)$$

induces the isomorphism

$$G(\boldsymbol{A})_1\backslash G(\boldsymbol{A})\approx\boldsymbol{R}^{r_{\boldsymbol{Q}}}\,,$$

where $\{\xi_1, \cdots, \xi_{r_{\boldsymbol{Q}}}\}$ is a basis of $\hat{G}(\boldsymbol{Q})$. As a measure on $G(\boldsymbol{A})$, we take

$$dG(\boldsymbol{A})=\frac{1}{\rho_G}\omega_\infty \prod_{p\neq\infty} L_p(1,\chi_G)\omega_p\,.$$

It can be verified that $dG(\boldsymbol{A})$ is independent of the choice of K/k and ω. As a measure on $G(\boldsymbol{A})_1\backslash G(\boldsymbol{A})$ we copy the usual measure on $\boldsymbol{R}^{r_Q}$ which we denote by $d(G(\boldsymbol{A})_1\backslash G(\boldsymbol{A}))$. Since $G(\boldsymbol{Q})$ is discrete in $G(\boldsymbol{A})$, we define $dG(\boldsymbol{Q})$ to be the canonical discrete measure.

Finally we define the Tamagawa number $\tau(G)$ by

$$\tau(G)=\int_{G(\boldsymbol{Q})\backslash G(\boldsymbol{A})_1} d(G(\boldsymbol{Q})\backslash G(\boldsymbol{A})_1)<+\infty\,,$$

where the measure $d(G(\boldsymbol{Q})\backslash G(\boldsymbol{A})_1)$ is determined by the relation:

$$dG(\boldsymbol{A})=d(G(\boldsymbol{A})_1\backslash G(\boldsymbol{A}))d(G(\boldsymbol{Q})\backslash G(\boldsymbol{A})_1)dG(\boldsymbol{Q})\,.$$

In general, if G is a unimodular topological group and H is its closed unimodular subgroup, then by the equality $dG=d(H\backslash G)dH$ we mean the relation:

$$\int_G f(g)dG=\int_{H\backslash G} d(H\backslash G)\int_H f(hg)dH\,.$$

Practically, we can use the following definition:

$$\tau(G)=\frac{\displaystyle\int_{G(\boldsymbol{Q})\backslash G(\boldsymbol{A})} f(\psi(x))d(G(\boldsymbol{Q})\backslash G(\boldsymbol{A}))}{\displaystyle\int_{\boldsymbol{R}^{r_Q}} f(t)dt}$$

where $\psi(x)=(\log\|\xi_1(x)\|,\cdots,\log\|\xi_{r_Q}(x)\|)$.

Example 1. $G=G_m$. We have

$$\omega=\frac{dt}{t}\,,\qquad \hat{G}=\boldsymbol{Z}\,,\qquad K=\boldsymbol{Q}\,,\qquad \rho_G=\lim_{s\to 1}(s-1)\zeta(s)=1\,,$$

$$L(s,\chi_G)=\zeta(s)\,,\qquad \psi(x)=\log\|x\|\,,\qquad x\in\boldsymbol{A}^\times\,.$$

We also have $h_G=1$. Since

$$\tilde{F}=\boldsymbol{R}_+^\times\times\prod_{p\neq\infty}\boldsymbol{Z}_p^\times\,,$$

can be taken as a fundamental domain for $\boldsymbol{Q}^{\times}\backslash\boldsymbol{A}^{\times}$ and $\psi(x)=\log x_{\infty}$ when $x=(x_{\infty}, \cdots, x_p, \cdots)\in\tilde{F}$, we get

$$\tau(G_m)=\frac{\displaystyle\int_0^{+\infty} f(\log x_{\infty})\frac{dx_{\infty}}{x_{\infty}}}{\displaystyle\int_{-\infty}^{+\infty} f(t)dt}\prod_p\int_{\boldsymbol{Z}_p^{\times}}\frac{1}{1-p^{-1}}\left|\frac{dx}{x}\right|_p=1\,.$$

Example 2. Let T be an arbitrary torus defined over $\boldsymbol{Q}$. In this case, we know the following theorem:

THEOREM 1.[3)]

$$\tau(T)=\frac{h^1(\hat{T})}{i^1(T)}\,,$$

where

$$h^1(\hat{T})=\#H^1(\boldsymbol{Q},\hat{T})\,,\qquad i^1=\#\mathrm{Ker}\left(H^1(\boldsymbol{Q},T)\longrightarrow\prod_p H^1(\boldsymbol{Q}_p,T)\right).$$

COROLLARY 1. *$\tau(T)=h^1(\hat{T})$ if T is split by a cyclic extension $K/\boldsymbol{Q}$.*

COROLLARY 2. *$\tau(T)=1$ if T is split by a finite galois extension $K/\boldsymbol{Q}$ such that $\hat{T}$ is $G(K/\boldsymbol{Q})$-projective.*

Example 3. Let $K=\boldsymbol{Q}(\sqrt{m})$, m being a square free integer $\neq 0, 1$, and

$$T=\left\{z=\begin{pmatrix}x & my\\ y & x\end{pmatrix};\ x^2-my^2=1,\ x, y\in\Omega\right\}.$$

Hence, $T(\boldsymbol{Q})=\{z\in K^{\times};\ N_{K/\boldsymbol{Q}}(z)=1\}$ with the identification:

$$z=\begin{pmatrix}x & my\\ y & x\end{pmatrix}\longleftrightarrow z=x+\sqrt{m}\,y\,,\qquad x, y\in\boldsymbol{Q}\,.$$

One can also write $T=O_2^+(f)$ with $f=x^2-my^2$. We have $\hat{T}=\langle\xi\rangle$ where $\xi\cdot\left(\begin{smallmatrix}x & my\\ y & x\end{smallmatrix}\right)=x+\sqrt{m}y$. Since $\hat{T}=\hat{T}(K)$, Corollary 1 yields

$$\tau(T)=h^1(\hat{T})=\#H^1(G(K/\boldsymbol{Q}),\hat{T})\,.$$

Call σ the generator of $G(K/\boldsymbol{Q})$. Then

$$\xi^{\sigma}\cdot\begin{pmatrix}x & my\\ y & x\end{pmatrix}=x-\sqrt{m}\,y\,.$$

Therefore,

$$(\xi+\xi^{\sigma})(z)=\xi(z)\xi^{\sigma}(z)=(x+\sqrt{m}y)(x-\sqrt{m}y)=x^2-my^2=1\ ,$$

i.e. $\xi+\xi^{\sigma}=0$, or, $\xi^{\sigma}=-\xi$. We have

$$\begin{aligned} H^1(\hat{T})\approx H^{-1}(\hat{T}) &= \{\eta\in\hat{T};\ \eta+\eta^{\sigma}=0\}/\{\eta-\eta^{\sigma};\ \eta\in\hat{T}\} \\ &= \langle\xi\rangle/\langle 2\xi\rangle\approx \boldsymbol{Z}/2\boldsymbol{Z}\ . \end{aligned}$$

Hence

$$\tau(T)=\tau(O_2^{+}(f))=2\ .$$

Remark 3. It was Tamagawa's discovery that $O_n^{+}(f)=2$ in the late fifties for any $n\geq 3$. (Siegel's theorem on the quadratic form f.) This stimulated the work of Weil (1961).[4)]

Example 4. Consider the torus $R_{K/\boldsymbol{Q}}(G_m)$ (cf. Section VI) where $K/\boldsymbol{Q}$ is a cyclic extension. The norm map defines the exact sequence:

$$0\longrightarrow T\longrightarrow R_{K/\boldsymbol{Q}}(G_m)\xrightarrow{N_{K/\boldsymbol{Q}}} G_m\longrightarrow 0\ .$$

The dual of this is:

$$\begin{array}{ccccccc} 0 & \longleftarrow & \hat{T} & \longleftarrow & \boldsymbol{Z}[\mathfrak{g}] & \longleftarrow & \boldsymbol{Z}\longleftarrow 0\ , \\ & & & & \cup & & \cup \\ & & & & z\sum_{\sigma\in\mathfrak{g}}\sigma & \longleftarrow\!\shortmid & z \end{array}$$

where $\mathfrak{g}=G(K/\boldsymbol{Q})$. Then, we have the exact sequence:

$$\begin{array}{ccccccc} H^1(\boldsymbol{Z}[\mathfrak{g}]) & \longrightarrow & H^1(\hat{T}) & \longrightarrow & H^2(\boldsymbol{Z}) & \longrightarrow & H^2(\boldsymbol{Z}[\mathfrak{g}])\ , \\ \| & & & & \| & & \| \\ 0 & & & & \boldsymbol{Z}/n\boldsymbol{Z} & & 0 \end{array}$$

$n=[K:\boldsymbol{Q}]$, and so $\tau(T)=[K:\boldsymbol{Q}]$.

Remark 4.[5)] For any galois extension $K/\boldsymbol{Q}$ and the torus $T=R^{(1)}_{K/\boldsymbol{Q}}(G_m)=\mathrm{Ker}(N_{K/\boldsymbol{Q}})$, we know that

$$i^1(T)=1 \Leftrightarrow \text{Hasse's norm theorem for } K/\boldsymbol{Q}\ .$$

Let G be a connected semi-simple algebraic group defined over $\boldsymbol{Q}$ and $\tilde{G}$ be the universal covering group of G over $\boldsymbol{Q}$. Call π the covering map which

is defined over $\boldsymbol{Q}$. Then the group $M=\operatorname{Ker}\pi$ (the fundamental group of G) is endowed with a $G(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$-module structure. Denote by $\hat{M}$ the character module $\operatorname{Hom}(M, (\bar{\boldsymbol{Q}})^{\times})$ which is a $G(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$-module, too. We have then

$$\frac{\tau(G)}{\tau(\tilde{G})}=\frac{h^0(\hat{M})}{i^1(\hat{M})},$$ [6]

where $h^0(\hat{M})=\#(\hat{M}^{\mathfrak{g}})$, $\mathfrak{g}=G(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$ and

$$i^1(\hat{M})=\#\left(\operatorname{Ker}\left(H^1(\boldsymbol{Q}, \hat{M}) \longrightarrow \prod_p H^1(\boldsymbol{Q}_p, \hat{M})\right)\right).$$

(It is known that $i^1(\hat{M})=1$ if G is simple.)

This formula determines the Tamagawa number of semi-simple groups modulo Weil's conjecture (W) (cf. Remark 1).

Example 5. Let $\tilde{G}=SL_n$ and $G=PL_n=GL_n/G_m=SL_n/W_n$ where W_n is the group of n-th roots of 1. We have $M=W_n$, $\hat{M}=\operatorname{Hom}(W_n, (\bar{\boldsymbol{Q}})^{\times})=\operatorname{Hom}(W_n, W_n)=\langle\chi\rangle$, $\chi(\zeta)=\zeta$, ζ being a primitive n-th root of 1. Since $\hat{M}^{\mathfrak{g}}=\hat{M}$, $\mathfrak{g}=G(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$, we have $h^0(\hat{M})=\#(\hat{M}^{\mathfrak{g}})=\#(\hat{M})=\#(M)=n$. Therefore

$$\frac{\tau(PL_n)}{\tau(SL_n)}=n$$

Usually, one first proves that $\tau(PL_n)=n$.[7] Then the formula implies $\tau(SL_n)=1$.

Example 6 ($n\geq 3$). $G=O_n^+(f)$, $\tilde{G}=\operatorname{Spin}_n(f)$. Since $M=\boldsymbol{Z}/2\boldsymbol{Z}$, obviously $\hat{M}^{\mathfrak{g}}=\hat{M}$. Since $\tau(O_n^+)=2$ by Siegel-Tamagawa, we have $\tau(\operatorname{Spin}_n(f))=1$.

Remark 5. We don't know yet how to use directly the "simply connectedness" of $\tilde{G}$ to prove that $\tau(\tilde{G})=1$.

Remark 6. It is desirable to extend the notion of the Tamagawa number to a more general category of algebraic varieties over $\boldsymbol{Q}$. Then $G(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$-module structure of the fundamental group and its dual of the variety should be studied.

IX. Class Number of Tori[1]

Let T be a torus defined over $\boldsymbol{Q}$. By the class number formula for T we

mean the equality:

$$h_T=\frac{\tau(T)\rho_T w_T\sqrt{D_T}}{R_T}\,.^{2)} \tag{1}$$

Here h_T is the class number of T, $h_T=[T(\boldsymbol{A})\colon T(\boldsymbol{Q})T(\boldsymbol{A})_\infty]$, $\tau(T)$ is the Tamagawa number of T (cf. Section VIII, Th. 1) and $w_T=\#W=\#(T(\boldsymbol{Z})\cap T(\boldsymbol{A})_K)$ (cf. Section VI, diagram). Furthermore,

$$\rho_T=\lim_{s\to 1}(s-1)^{r_{\boldsymbol{Q}}}L(s,\chi_T)\qquad\text{where}\quad r_{\boldsymbol{Q}}=\operatorname{rank}\hat{T}(\boldsymbol{Q})\,,$$

$\chi_T=$the character of the integral representation of $G(K/\boldsymbol{Q})$ on $\hat{T}$, K being a galois splitting field for T over $\boldsymbol{Q}$. It remains to define R_T and D_T.

Let $r_\infty=\operatorname{rank}\hat{T}(\boldsymbol{R})$. Choose bases ξ_i's of modules $\hat{T}(\boldsymbol{Q})$, $\hat{T}(\boldsymbol{R})$ such that

$$\hat{T}(\boldsymbol{Q})=\langle\xi_1,\cdots,\xi_{r_{\boldsymbol{Q}}}\rangle\subset\hat{T}(\boldsymbol{R})=\langle\xi_1,\cdots,\xi_{r_{\boldsymbol{Q}}},\xi_{r_{\boldsymbol{Q}}+1},\cdots,\xi_{r_\infty}\rangle\,.$$

The map $\psi_\infty\colon T(\boldsymbol{R})\to\boldsymbol{R}^{r_\infty}$ given by

$$\psi_\infty(x)=(\log|\xi_1(x)|_\infty,\cdots,\log|\xi_{r_\infty}(x)|_\infty)$$

induces isomorphisms

$$T(\boldsymbol{R})/K\approx\boldsymbol{R}^{r_\infty}\,,\qquad T(\boldsymbol{R})_1/K\approx\boldsymbol{R}^{r_\infty-r_{\boldsymbol{Q}}}\quad\text{(cf. Section VI)}\,.$$

By the unit theorem (Section VI, Th. 1), we have

$$T(\boldsymbol{Z})=E\times W\,,\qquad E\approx\boldsymbol{Z}^{r_\infty-r_{\boldsymbol{Q}}}\,.$$

Let $E=\langle e_j;\ r_{\boldsymbol{Q}}+1\le j\le r_\infty\rangle$. Since $T(\boldsymbol{Z})\subset T(\boldsymbol{R})_1$, we have

$$\psi_\infty(e_j)=(\overbrace{0,\cdots,0}^{r_{\boldsymbol{Q}}},\log|\xi_{r_{\boldsymbol{Q}}+1}(e_j)|_\infty,\cdots,\log|\xi_{r_\infty}(e_j)|_\infty)$$

for each j, $r_{\boldsymbol{Q}}+1\le j\le r_\infty$. We can now define the regulator R_T

$$R_T=|\det(\log|\xi_i(e_j)|_\infty)|\,.$$

Let ω be a gauge form on T defined over $\boldsymbol{Q}$ and ω_p be the measure on $T(\boldsymbol{Q}_p)$ induced by ω. For $p=\infty$, put

$$M_\infty=\{x\in T(\boldsymbol{R});\ 0\le|\log\xi_i(x)|_\infty<1,\ 1\le i\le r_\infty\}$$

and

$$c_T=\int_{M_\infty}\omega_\infty\prod_{p\neq\infty}\int_{T(\boldsymbol{Z}_p)}L_p(1,\chi_T)\omega_p>0\,.$$

Finally, define D_T by $D_T=1/c_T^2$.

We shall now examine those ingredients of the class number formula in case where $T=R_{k/\boldsymbol{Q}}(G_m)$, k being any finite algebraic extension of $\boldsymbol{Q}$. First, recall that $T(\boldsymbol{Q})=k$, $T(\boldsymbol{Z})=\mathfrak{o}_k^\times$, $r_\infty=r_1+r_2$, $r_{\boldsymbol{Q}}=1$. Since W is the torsion group of $k^\times$, $w_T=w_k=$the number of roots of 1 in k. Write

$$T(\boldsymbol{Z})=\mathfrak{o}_k^\times=E\times W\,,$$

$$E=\langle e_j;\ 2\leq j\leq r_1+r_2\rangle\approx\boldsymbol{Z}^{r_1+r_2-1}\,.$$

Recall also that

$$\hat{T}=\langle\eta_1,\cdots,\eta_{r_1},\eta_{r_1+1},\overline{\eta_{r_1+1}},\cdots,\eta_{r_1+r_2},\overline{\eta_{r_1+r_2}}\rangle$$

where $\eta_i(P(x))=x^{(i)}$, $P(x)$ is the regular representation of $x\in k$ and $x^{(i)}$ is the i-th conjugate of x. We have then

$$\hat{T}(\boldsymbol{Q})=\langle\eta_1+\cdots+\eta_{r_1}+(\eta_{r_1+1}+\overline{\eta_{r_1+1}})+\cdots+(\eta_{r_1+r_2}+\overline{\eta_{r_1+r_2}})\rangle$$

$$\subset\hat{T}(\boldsymbol{R})=\langle\eta_1,\cdots,\eta_{r_1},\eta_{r_1+1}+\overline{\eta_{r_1+1}},\cdots,\eta_{r_1+r_2}+\overline{\eta_{r_1+r_2}}\rangle\,.$$

Or, we can write, with

$$\xi_1=\eta_1+\cdots+\eta_{r_1}+(\eta_{r_1+1}+\overline{\eta_{r_1+1}})+(\eta_{r_1+r_2}+\overline{\eta_{r_1+r_2}})\,,$$

$$\hat{T}(\boldsymbol{Q})=\langle\xi_1\rangle\subset\hat{T}(\boldsymbol{R})=\langle\xi_1,\xi_2,\cdots,\xi_{r_1+r_2}\rangle$$

and

$$R_T=|\det(\log|\xi_i(e_j)|_\infty)|\,,$$

$2\leq i,j\leq r_1+r_2$. Therefore, we have $R_T=R_k$, the regulator of the field k.

Consider the following natural identification:

$$T(\boldsymbol{A})=J_k=\text{the idele group of}\quad k\,,$$

$$T(\boldsymbol{A})_\infty=T(\boldsymbol{R})\times\prod_{p\neq\infty}T(\boldsymbol{Z}_p)$$

$$=\prod_{v|\infty}k_v^\times\times\prod_{p\neq\infty}\prod_{\mathfrak{p}|p}\mathfrak{o}_{\mathfrak{p}}^\times$$

$$=\prod_{v|\infty}k_v^\times\times\prod_{\mathfrak{p}}\mathfrak{o}_{\mathfrak{p}}^\times\overset{\text{def}}{=}J_{k,\infty}\,,$$

$T(\boldsymbol{A})/T(\boldsymbol{Q})T(\boldsymbol{A})_\infty = J_k/k^\times J_{k,\infty} = I_k/P_k = H_k$, the ideal class group of k.

This shows that $h_T = h_k$.

Let $K/\boldsymbol{Q}$ be a galois extension such that $K \supset k$. Put $\mathfrak{g} = G(K/\boldsymbol{Q}) \supset \mathfrak{h} = G(K/k)$. Then $\mathfrak{g}$-module $\hat{T}$, $T = R_{k/\boldsymbol{Q}}(G_m)$, is induced from the trivial $\mathfrak{h}$-module $\hat{G}_m = \boldsymbol{Z}$:

$$\hat{T} = \hat{G}_m \otimes_{\boldsymbol{Z}[\mathfrak{h}]} \boldsymbol{Z}[\mathfrak{g}] .$$

Hence, $\chi_T = \chi_0^*$ where χ_0 denotes the trivial character of $\mathfrak{h}$. Then we have

$$\begin{aligned} L(s, \chi_T; K/\boldsymbol{Q}) &= L(s, \chi_0^*; K/\boldsymbol{Q}) = L(s, \chi_0; K/k) \\ &= \zeta_k(s), \quad \text{the zeta-function of} \quad k . \end{aligned}$$

Therefore we have:

$$\rho_T = \lim_{s \to 1} (s-1) L(s, \chi_T) = \lim_{s \to 1} (s-1) \zeta_k(s) = \rho_k ,$$

the residue of $\zeta_k(s)$ at $s = 1$.

Finally, as for D_T, let $\omega = dx/x$ be a gauge form on G_m viewed as an algebraic group defined over k. Then,

$$c_T = \prod_{v \mid \infty} \int_{M_v} \frac{(dx)_v}{|x|_v} \prod_{\mathfrak{p}} \int_{\mathfrak{o}_\mathfrak{p}^\times} \frac{1}{1 - N\mathfrak{p}^{-1}} \cdot \frac{(dx)_\mathfrak{p}}{|x|_\mathfrak{p}}$$

where

$$\begin{aligned} M_v &= \{x \in k_v^\times ;\ 0 \leq \log |x|_v < e\} \\ &= \{x \in k_v^\times ;\ 1 \leq |x|_v < e\} . \end{aligned}$$

When v is real, then $|x|_v = |x|$ and

$$\int_{M_v} \frac{(dx)_v}{|x|_v} = 2 \int_1^e \frac{dx}{x} = 2 .$$

When v is complex, then $|x|_v = |x|^2$, $(dx)_v = i\, dx d\bar{x}$ and

$$\int_{M_v} \frac{(dx)_v}{|x|_v} = \int_0^{2\pi} \int_1^{\sqrt{e}} \frac{2r\, dr\, d\theta}{r^2} = \int_0^{2\pi} d\theta \int_1^{\sqrt{e}} \frac{2dr}{r} = 2\pi .$$

When $v = \mathfrak{p}$, finite prime, then

$$\int_{\mathfrak{o}_\mathfrak{p}^\times} \frac{N\mathfrak{p}}{N\mathfrak{p}-1}(dx)_\mathfrak{p} = \int_{\mathfrak{o}_\mathfrak{p}^\times} (dx)_\mathfrak{p} = (N\delta_\mathfrak{p})^{-1/2},$$

where $\delta_\mathfrak{p}$ is the different of $k_\mathfrak{p}$. Hence we have

$$c_T = 2^{r_1}(2\pi)^{r_2} |\Delta_k|^{-1/2}, \qquad \Delta_k = \text{discriminant of } k.$$

Then we have

$$D_T = \frac{|\Delta_k|}{(2^{r_1}(2\pi)^{r_2})^2}.$$

It is well-known that

$$\rho_k = \frac{2^{r_1}(2\pi)^{r_2} h_k R_k}{|\Delta_k|^{1/2} w_k}.$$

Comparing this with the class number formula (1) of an arbitrary torus T, we get

THEOREM 1. *For any algebraic number field k,*

$$\tau(R_{k/\boldsymbol{Q}}(G_m)) = 1.$$

We conclude this section with a formula on class numbers of isogenous tori. Let T, T' be tori over $\boldsymbol{Q}$ and

$$\lambda : T \longrightarrow T'$$

by an isogeny over $\boldsymbol{Q}$. Then λ induces the following homomorphisms:

$$\lambda(\boldsymbol{Q}_p) : T(\boldsymbol{Q}_p) \longrightarrow T'(\boldsymbol{Q}_p) \qquad (p = \infty \text{ included})$$

$$\lambda(\boldsymbol{Z}_p) : T(\boldsymbol{Z}_p) \longrightarrow T'(\boldsymbol{Z}_p)$$

$$\lambda(\boldsymbol{Z}) : T(\boldsymbol{Z}) \longrightarrow T'(\boldsymbol{Z})$$

$$\hat{\lambda}(\boldsymbol{Q}) : \hat{T}'(\boldsymbol{Q}) \longrightarrow \hat{T}(\boldsymbol{Q}).$$

In general, when $\alpha : G \to G'$ is a homomorphism of abelian groups such that groups $\operatorname{Ker}\alpha$ and $\operatorname{Cok}\alpha$ are finite, we put

$$q(\alpha) = \frac{\#(\operatorname{Cok}\alpha)}{\#(\operatorname{Ker}\alpha)}.$$

THEOREM 2. *Let $\lambda : T \to T'$ be an isogeny of tori, defined over $\boldsymbol{Q}$. Then*

$$\frac{h_T}{h_{T'}}=\frac{\tau(T)}{\tau(T')}\cdot\frac{\prod_p q(\lambda(\boldsymbol{Z}_p))}{q(\lambda(\boldsymbol{Z}))q(\hat{\lambda}(\boldsymbol{Q}))}.$$

Remark 1.[3] As for $q(\lambda(\boldsymbol{Z}_p))$, it can be shown that $q(\lambda(\boldsymbol{Z}_p))=1$ when p is unramified for $k/\boldsymbol{Q}$ and $(p, \nu(\lambda))=1$ where $\nu(\lambda)=\#(\mathrm{Ker}\,\lambda)=\#(\mathrm{Cok}\,\hat{\lambda})$ and $k/\boldsymbol{Q}$ is a common galois splitting field for T, T'. Because of this remark, the product in Theorem 2 is finite.

Remark 2. Theorem 2 is one of main theorems in Dissertation of Jih-Min Shyr (1974, The Johns Hopkins University).[4]

X. Gauss' Genus Theory Revisited

Let k be any algebraic number field of finite degree over $\boldsymbol{Q}$ and K/k be a finite galois extension. We have the exact sequence over k:

$$0\longrightarrow T_0'\longrightarrow T_0\xrightarrow{N}T_0''\longrightarrow 0$$

$$\begin{array}{c} K \\ {\scriptstyle n}\,\big| \\ k \\ {\scriptstyle n_0}\,\big| \\ \boldsymbol{Q} \end{array}$$

where $T_0=R_{K/k}(G_m)$, $T_0''=G_m$ and $N=N_{K/k}=$the norm map. With this sequence, we associate the isogeny over k:

$$\begin{array}{ccc} T_0 & \xrightarrow{n} & T_0 \\ {\scriptstyle\lambda_0}\searrow & & \nearrow{\scriptstyle\lambda_0'} \\ & T_0'\times T_0'' & \end{array}$$

where $n: x\longmapsto x^n$, $\lambda_0(x)=(x^n(Nx)^{-1}, Nx)$ and $\lambda_0'(x', x'')=x'x''$. Applying the functor $R_{k/\boldsymbol{Q}}$, we obtain the isogeny over $\boldsymbol{Q}$:

$$\lambda: T\longrightarrow T'\times T''$$

where

$$\lambda=R_{k/\boldsymbol{Q}}(\lambda_0),\ T=R_{k/\boldsymbol{Q}}(T_0)=R_{K/\boldsymbol{Q}}(G_m),\ T'=R_{k/\boldsymbol{Q}}(T_0'),\ T''=R_{k/\boldsymbol{Q}}(G_m).$$

Since

$$h_{T'\times T''}=h_{T'}\times h_{T''},\qquad \tau(T'\times T'')=\tau(T')\tau(T''),$$

Theorem 2 of Section IX yields

$$E(K/k)=\overset{\text{def}}{=}\frac{h_K}{h_k h_{T'}}=\frac{1}{\tau(T')}\,\frac{q(\lambda(\boldsymbol{R}))}{q(\lambda(\boldsymbol{Z}))q(\hat{\lambda}(\boldsymbol{Q}))}\prod_{p\neq\infty}q(\lambda(\boldsymbol{Z}_p))$$

where we used that $h_T=h_K$, $h_{T''}=h_k$ and $\tau(T)=\tau(T'')=1$ (cf. Section IX, Th. 1).
Here, $q(\hat{\lambda}(\boldsymbol{Q}))$ is the easiest one to handle.

(1) $$q(\hat{\lambda}(\boldsymbol{Q}))=q(\hat{\lambda}_0(k))=1\,.$$

Taking the dual of the exact sequence

$$\begin{array}{ccccccccc} 0 & \longrightarrow & T'_0 & \xrightarrow{\ \iota\ } & T_0 & \xrightarrow{\ N\ } & T''_0 & \longrightarrow & 0\,, \\ & & & & \| & & \| & & \\ & & & & R_{K/k}(G_m) & & G_m & & \end{array}$$

we get

$$\begin{array}{ccccccccc} 0 & \longleftarrow & \hat{T}'_0 & \xleftarrow{\ \hat{\iota}\ } & \hat{T}_0 & \xleftarrow{\ \hat{N}\ } & \hat{T}''_0 & \longleftarrow & 0 \\ & & \| & & \| & & \| & & \\ & & \boldsymbol{Z}[\mathfrak{g}]/\boldsymbol{Z}s & & \boldsymbol{Z}[\mathfrak{g}] & & \boldsymbol{Z} & & \end{array}$$

where $\mathfrak{g}=\mathrm{Gal}(K/k)$, $s=\sum_{\sigma\in\mathfrak{g}}\sigma$, $\hat{N}(z)=zs$ and $\hat{\imath}(\gamma)=\gamma \bmod \boldsymbol{Z}s$. The dual $\hat{\lambda}_0$ of the isogeny λ_0 is

$$\begin{array}{ccc} \boldsymbol{Z}[\mathfrak{g}] & \xleftarrow{\ \hat{n}=n\ } & \boldsymbol{Z}[\mathfrak{g}] \\ & {\scriptstyle\hat{\lambda}_0}\nwarrow \quad \nearrow{\scriptstyle\hat{\lambda}'_0} & \\ & \boldsymbol{Z}[\mathfrak{g}]/\boldsymbol{Z}s\times\boldsymbol{Z}\,, & \end{array}$$

where $\hat{\lambda}_0$ and $\hat{\lambda}'_0$ are injective. Since $\lambda_0(x)=(x^n(Nx)^{-1}, Nx)$, we have

$$\hat{\lambda}_0(\gamma \bmod \boldsymbol{Z}s, z)=zs+(n\gamma-S(\gamma)s)\,,$$

$$\hat{\lambda}'_0(\gamma)=(\gamma \bmod \boldsymbol{Z}s, S(\gamma))$$

where

$$S(\gamma)=\sum_{\sigma\in\mathfrak{g}}z_\sigma \qquad \text{if} \quad \gamma=\sum_{\sigma\in\mathfrak{g}}z_\sigma\cdot\sigma\,.$$

Note that $\hat{n}(\gamma)=n\gamma$ ($\hat{n}=n$) and $\hat{\lambda}_0\hat{\lambda}'_0=n$. Taking $\mathfrak{g}$-invariant parts of the last diagram we have

$$\begin{array}{ccc} Zs & \xleftarrow{\ n\ } & Zs \\ & {\scriptstyle \hat{\lambda}_0(k)} \searrow \quad \swarrow {\scriptstyle \hat{\lambda}'_0(k)} & \\ & Z & \end{array}$$

because $Z[\mathfrak{g}]^{\mathfrak{g}} = Zs$, $(Z[\mathfrak{g}]/Zs)^{\mathfrak{g}} = \{0\}$, $Z^{\mathfrak{g}} = Z$. Since $\hat{\lambda}_0$ is injective,

$$q(\hat{\lambda}_0(k)) = \frac{\#\operatorname{Cok}(\hat{\lambda}_0(k))}{\#\operatorname{Ker}(\hat{\lambda}_0(k))} = \#\operatorname{Cok}\hat{\lambda}_0(k)\,.$$

On the other hand,

$$\hat{\lambda}'_0(k)(zs) = (zs \bmod Zs,\ S(zs)) = (0,\ nz) = nz$$

and hence

$$n = \#\operatorname{Cok}\hat{\lambda}'_0(k)\,\#\operatorname{Cok}\hat{\lambda}_0(k) = n\,\#\operatorname{Cok}\hat{\lambda}_0(k)\,,$$

or $\#\operatorname{Cok}\hat{\lambda}_0(k) = 1$, which proves our assertion (1).

From now on we assume that k contains a primitive n-th root of 1.

$$q(\lambda(\boldsymbol{R})) = \prod_{v|\infty} q(\lambda_0(k_v)) = n^{(1-n)r_2}\,. \tag{2}$$

Let v be an infinite place of k.

Case 1. $k_v = \boldsymbol{C}$. We claim that $q(\lambda_0(k_v)) = n^{1-n}$. Since

$$T_0(k_v) = R_{K/k}(G_m)(k_v) = \prod_{V|v} K_V^{\times} = \underbrace{\boldsymbol{C}^{\times} \times \cdots \times \boldsymbol{C}^{\times}}_{n}\,,$$

$$T''_0(k_v) = k_v^{\times} = \boldsymbol{C}^{\times}\,,$$

$$Nx = x_1 \cdots x_n \qquad \text{if} \quad x = (x_1, \cdots, x_n) \in (\boldsymbol{C}^{\times})^n\,,$$

$$T'_0(k_v) = \{x \in (\boldsymbol{C}^{\times})^n : x_1 \cdots x_n = 1\}\,,$$

the isogeny $\lambda_0(k_v)$ is just the map:

$$\lambda_0(k_v) : x \longmapsto \left(\left(\frac{x_1^n}{x_1 \cdots x_n}, \cdots, \frac{x_n^n}{x_1 \cdots x_n}\right), x_1 \cdots x_n\right).$$

If x belongs to $\operatorname{Ker}\lambda_0(k_v)$, then $x_1 \cdots x_n = 1$ and $x_1^n = \cdots = x_n^n = 1$. Then, it follows that $\#\operatorname{Ker}\lambda_0(k_v) = n^{n-1}$. On the other hand, take any $(u, v) \in T'_0(k_v) \times T''_0(k_v)$ with $u_1 \cdots u_n = 1$, $u = (u_1, \cdots, u_n)$. Find x_i such that $x_1^n = u_1 v, \cdots,$

$x_n^n = u_n v$. Then, $x_1^n \cdots x_n^n = u_1 \cdots u_n v^n = v^n$ and $x_1 \cdots x_n = wv$ with $w^n = 1$. Put $x_n^* = x_n w^{-1}$. Then, $x_1 \cdots x_{n-1} x_n^* = v$. Now put

$$x = (x_1, \cdots, x_{n-1}, x_n^*) \in T_0(k_v) .$$

Then we have

$$\begin{aligned} \lambda_0(k_v)(x) &= ((x_1^n, \cdots, x_{n-1}^n, x_n^n)/((x_1 \cdots x_{n-1} x_n^*), x_1 \cdots x_{n-1} x_n^*) \\ &= ((u_1 v, \cdots, u_{n-1} v, u_n v)/v, v) = (u, v) \end{aligned}$$

which shows that $\# \operatorname{Cok} \lambda_0(k_v) = 1$. Hence we have $q(\lambda_0(k_v)) = n^{1-n}$.

Case 2. $k_v = \boldsymbol{R}$, $K_v = \boldsymbol{R}$ for any $V \mid v$. Our assumption implies that $n = 2$. Since

$$\begin{aligned} &T_0(k_v) = \boldsymbol{R}^\times \times \boldsymbol{R}^\times , \\ &T_0''(k_v) = \boldsymbol{R}^\times , \\ &Nx = x_1 x_2 \quad \text{and} \\ &T_0'(k_v) = \{x = (x_1, x_2);\ x_1 x_2 = 1\} , \end{aligned}$$

the isogeny $\lambda_0(k_v)$ is just the map:

$$\lambda_0(k_v) \colon x = (x_1, x_2) \longmapsto \left(\left(\frac{x_1^2}{x_1 x_2}, \frac{x_2^2}{x_1 x_2} \right), x_1 x_2 \right) = \left(\left(\frac{x_1}{x_2}, \frac{x_2}{x_1} \right), x_1 x_2 \right).$$

It is easy to see that $\operatorname{Ker} \lambda_0(k_v) = \{(1, 1), (-1, -1)\}$ and so $\# \operatorname{Ker} \lambda_0(k_v) = 2$. On the other hand, we have an isomorphism

$$T_0'(k_v) \times T_0''(k_v) \approx \boldsymbol{R}^\times \times \boldsymbol{R}^\times$$

by the correspondence

$$((u_1, u_2), v) \longleftrightarrow (u_1, v) \qquad \text{where} \quad u_1 u_2 = 1$$

and one sees easily that $\operatorname{Im}(\lambda_0(k_v)) \approx \{(u_1, v);\ u_1 v > 0\}$, which proves that $\# \operatorname{Cok} \lambda_0(k_v) = 2$. Hence $q(\lambda_0(k_v)) = 1$.

Case 3. $k_v = \boldsymbol{R}$, $K_v = \boldsymbol{C}$ for any $V \mid v$. Again our assumption implies that $n = 2$. Since

$$T_0(k_v) = (R_{K/k}(G_m))(k_v) = \prod_{V \mid v} K_V^\times = \boldsymbol{C}^\times ,$$

$$T_0''(k_v)=\boldsymbol{R}^{\times},$$

$$Nx=x\bar{x} \quad \text{and}$$

$$T_0'(k_v)=\{x\in\boldsymbol{C}^{\times};\ Nx=x\bar{x}=1\}\overset{\text{def}}{=}\boldsymbol{C}^{(1)},$$

the isogeny $\lambda_0(k_v)$ is just the map:

$$\lambda_0(k_v)\colon x\longmapsto(x^2/Nx,\ Nx)=(x/\bar{x},\ x\bar{x}).$$

In this case, one verifies again that $\#\operatorname{Ker}\lambda_0(k_v)=\#\operatorname{Cok}\lambda_0(k_v)=2$. Hence $q(\lambda_0(k_v))=1$.

Summarizing 3 cases, we have

$$q(\lambda(\boldsymbol{R}))=\prod_{v|\infty}q(\lambda_0(k_v))=n^{(1-n)r_2}$$

where r_2 denotes the number of complex places of k.

$$q(\lambda(\boldsymbol{Z}_p))=\prod_{\mathfrak{p}|p}q(\lambda_0(\mathfrak{o}_\mathfrak{p}))=\prod_{\mathfrak{p}|p}e_\mathfrak{p}(K/k)(N\mathfrak{p})^{(n-1)v_\mathfrak{p}(n)}. \tag{3}$$

Let $\mathfrak{P}$ be a prime factor of $\mathfrak{p}$ in K. We use the standard notation $e=e_\mathfrak{p}=e_\mathfrak{p}(K/k)$, $f=f_\mathfrak{p}=f_\mathfrak{p}(K/k)$, $g=g_\mathfrak{p}=g_\mathfrak{p}(K/k)$. We have $n=efg$. Since $T_0(\mathfrak{o}_\mathfrak{p})=\prod_{\mathfrak{P}|\mathfrak{p}}\mathfrak{o}_\mathfrak{P}^{\times}$, $T_0''(\mathfrak{o}_\mathfrak{p})=\mathfrak{o}_\mathfrak{p}^{\times}$ and $N(x)=N_\mathfrak{p}(x_1)\cdots N_\mathfrak{p}(x_g)$ when $x=(x_1,\cdots,x_g)\in T_0(\mathfrak{o}_\mathfrak{p})$,[1] the isogeny $\lambda_0(\mathfrak{o}_\mathfrak{p})$ is the map:

$$\lambda_0(\mathfrak{o}_\mathfrak{p})\colon \Gamma\longrightarrow\Gamma^{(1)}\times\mathfrak{o}_\mathfrak{p}^{\times}$$

where $\Gamma=\prod_{\mathfrak{P}|\mathfrak{p}}\mathfrak{o}_\mathfrak{P}^{\times}$, $\Gamma^{(1)}=\{x\in\Gamma;\ Nx=1\}$, given by

$$\lambda_0(\mathfrak{o}_\mathfrak{p})(x)=(x^n(Nx)^{-1},\ Nx).$$

First we claim that $\#\operatorname{Ker}\lambda_0(\mathfrak{o}_\mathfrak{p})=(ef)n^{g-1}=g^{-1}n^g$. So suppose that $(x^n(Nx)^{-1},\ Nx)=(1,\ 1)$. Then, $Nx=1$ and $x^n=(x_1^n,\cdots,x_g^n)=1$, i.e. $x_1^n=\cdots=x_g^n=1$, or $x_i=\zeta^{a_i}$. Now, we have

$$1=Nx=\prod_{i=1}^{g}(N\zeta)^{a_i}=\prod_{i=1}^{g}\zeta^{efa_i}=\zeta^{ef\sum_{i=1}^{g}a_i}$$

$$\Longleftrightarrow ef\sum_{i=1}^{g}a_i\equiv 0\ (\text{mod. } n)\Longleftrightarrow\sum_{i=1}^{g}a_i\equiv 0\ (\text{mod. } g).$$

This implies that

$$\operatorname{Ker}\lambda_0(\mathfrak{o}_\mathfrak{p})=\left\{x=(\zeta^{a_1},\cdots,\zeta^{a_g});\ \sum_{i=1}^{g} a_i\equiv 0\ (\text{mod. } g)\right\}.$$

Since a_g is uniquely determined mod. g by

$$a_g\equiv -\sum_{i=1}^{g-1} a_i \quad (\text{mod. } g)\,,$$

there are $g^{-1}n=ef$ choices of a_g mod. n and we get

$$\#\operatorname{Ker}\lambda_0(\mathfrak{o}_\mathfrak{p})=g^{-1}n^g\,.$$

Before computing $\operatorname{Cok}\lambda_0(\mathfrak{o}_\mathfrak{p})$ we state a simple lemma which will also be needed later on.

LEMMA 1. *Let $\phi: A\to A'$ be a homomorphism of abelian groups and ψ be the restriction of ϕ on a subgroup B of A.*

$$\begin{array}{ccc} A & \xrightarrow{\ \phi\ } & A' \\ \cup & & \\ B & \xrightarrow{\ \psi\ } & \end{array}$$

Assuming all indices are finite, we get

$$[A:B]=[\operatorname{Im}\phi:\operatorname{Im}\psi][\operatorname{Ker}\phi:\operatorname{Ker}\psi]\,.$$

We apply the lemma to the following situation:

$$\begin{array}{ccc} \Gamma^{(1)}\times\mathfrak{o}_\mathfrak{p}^{\times} & \xrightarrow{\ \phi\ } & \Gamma^{(1)}\mathfrak{o}_\mathfrak{p}^{\times} \\ \cup & & \cup \\ \operatorname{Im}\lambda_0(\mathfrak{o}_\mathfrak{p}) & \xrightarrow{\ \psi\ } & \Gamma^{n}\,. \end{array} \qquad \phi(x,y)=xy$$

Obviously, ϕ is onto. The same is true for ψ, because for any x we have $\psi(u,v)=uv=x^n$ with $u=x^n(Nx)^{-1}$, $v=Nx$. Now,

$$\begin{aligned}\operatorname{Ker}\phi\ni(x,y)&\Longleftrightarrow x=y^{-1}\in\Gamma^{(1)}\cap\mathfrak{o}_\mathfrak{p}^{\times}\\ &\Longleftrightarrow x=y^{-1},\ 1=Ny=(y^{ef})^g=y^n\,.\end{aligned}$$

Hence $\#\operatorname{Ker}\phi=\#(\Gamma^{(1)}\cap\mathfrak{o}_\mathfrak{p}^{\times})=n$. Next,

$$\begin{aligned}\operatorname{Ker}\psi\ni(u,v)&\Longleftrightarrow u=v^{-1}\in\Gamma^{(1)}\cap\mathfrak{o}_\mathfrak{p}^{\times}\\ &\Longleftrightarrow u=v^{-1},\ v^n=1\,.\end{aligned}$$

This time, however, $u=x^n(Nx)^{-1}$, $v=Nx$ for some $x\in\Gamma$. From $u=v^{-1}$ it follows that $x^n(Nx)^{-1}=(Nx)^{-1}$, i.e. $x^n=1$ or $x_1^n=\cdots=x_g^n=1$. Since k contains all n-th roots of 1, all x_i belong to k and so $Nx=x_1^{ef}\cdots x_g^{ef}=v$. Therefore $v^g=x_1^n\cdots x_g^n=1$. Conversely, $v^g=1\Rightarrow v^n=1\Rightarrow v=\zeta^N$ for some $N\Rightarrow n \mid gN\Rightarrow ef \mid N\Rightarrow v=\zeta^{efh}$. So, if we put $x=(\zeta^h, 1, \cdots, 1)$, then $Nx=(\zeta^h)^{ef}=v$ and $u=v^{-1}=x^n(Nx)^{-1}$, which shows that $(u, v)\in\operatorname{Ker}\psi$. Thus, we have seen that $\#\operatorname{Ker}\psi=g$. By Lemma 1, we have

$$\begin{aligned}\#\operatorname{Cok}\lambda_0(\mathfrak{o}_\mathfrak{p}) &= [\Gamma^{(1)}\times\mathfrak{o}_\mathfrak{p}^\times : \operatorname{Im}\lambda_0(\mathfrak{o}_\mathfrak{p})]\\ &= [\operatorname{Im}\phi : \operatorname{Im}\psi][\operatorname{Ker}\phi : \operatorname{Ker}\psi]\\ &= [\Gamma^{(1)}\mathfrak{o}_\mathfrak{p}^\times : \Gamma^n]\cdot n/g\\ &= \frac{n}{g}\cdot\frac{[\Gamma:\Gamma^n]}{[\Gamma:\Gamma^{(1)}\mathfrak{o}_\mathfrak{p}^\times]}.\end{aligned}$$

Applying Lemma 1 to the situation:

$$\begin{array}{ccc}\Gamma & \xrightarrow{N} & \mathfrak{o}_\mathfrak{p}^\times\\ \cup & & \cup\\ \Gamma^{(1)}\mathfrak{o}_\mathfrak{p}^\times & \longrightarrow & (\mathfrak{o}_\mathfrak{p}^\times)^n\end{array}$$

we have

$$\begin{aligned}[\Gamma:\Gamma^{(1)}\mathfrak{o}_\mathfrak{p}^\times] &= [N\Gamma:(\mathfrak{o}_\mathfrak{p}^\times)^n][\Gamma^{(1)}:\Gamma^{(1)}]\\ &= [N\Gamma:(\mathfrak{o}_\mathfrak{p}^\times)^n].\end{aligned}$$

Hence,

$$\#\operatorname{Cok}\lambda_0(\mathfrak{o}_\mathfrak{p})=\frac{n}{g}\cdot\frac{[\Gamma:\Gamma^n]}{[N\Gamma:(\mathfrak{o}_\mathfrak{p}^\times)^n]}.$$

Therefore,

$$q(\lambda_0(\mathfrak{o}_\mathfrak{p}))=\frac{1}{n^{g-1}}\cdot\frac{[\Gamma:\Gamma^n]}{[N\Gamma:(\mathfrak{o}_\mathfrak{p}^\times)^n]}.$$

Note that $N\Gamma=N_\mathfrak{p}\mathfrak{o}_\mathfrak{P}^\times$ where $\mathfrak{P}$ is any prime factor of $\mathfrak{p}$ in K and $N_\mathfrak{p}$ on the right means the norm for $K_\mathfrak{P}/k_\mathfrak{p}$. From local class field theory, we have

$$\#H^0(\mathfrak{o}_\mathfrak{P}^\times)=[\mathfrak{o}_\mathfrak{p}^\times : N_\mathfrak{p}\mathfrak{o}_\mathfrak{P}^\times]=e_\mathfrak{p},^{2)}$$

and so

$$q(\lambda_0(\mathfrak{o}_\mathfrak{p}))=\frac{e_\mathfrak{p}}{n^{g_\mathfrak{p}-1}}\cdot\frac{[\mathfrak{o}_\mathfrak{P}^\times:(\mathfrak{o}_\mathfrak{P}^\times)^n]^{g_\mathfrak{p}}}{[\mathfrak{o}_\mathfrak{p}^\times:(\mathfrak{o}_\mathfrak{p}^\times)^n]}.$$

Since

$$[\mathfrak{o}_\mathfrak{p}^\times:(\mathfrak{o}_\mathfrak{p}^\times)^n]=n(N\mathfrak{p})^{v_\mathfrak{p}(n)},\qquad [\mathfrak{o}_\mathfrak{P}^\times:(\mathfrak{o}_\mathfrak{P}^\times)^n]=n(N\mathfrak{P})^{v_\mathfrak{P}(n)}=n(N\mathfrak{p})^{e_\mathfrak{p}f_\mathfrak{p}v_\mathfrak{p}(n)},$$

we see that

$$q(\lambda_0(\mathfrak{o}_\mathfrak{p}))=e_\mathfrak{p}(N\mathfrak{p})^{(n-1)v_\mathfrak{p}(n)}$$

and that

$$q(\lambda(\boldsymbol{Z}_p))=\prod_{\mathfrak{p}|p}e_\mathfrak{p}\cdot\prod_{\mathfrak{p}|p}(N\mathfrak{p})^{(n-1)v_\mathfrak{p}(n)}.$$

Multiplying this for all $p(\neq\infty)$, we get

$$\prod_{p\neq\infty}q(\lambda(\boldsymbol{Z}_p))=\left(\prod_\mathfrak{p}e_\mathfrak{p}\right)n^{n_0(n-1)}. \tag{4}$$

From now on we assume that $\mathfrak{g}=\mathrm{Gal}(K/k)$ is cyclic of degree n.

$$q(\lambda(\boldsymbol{Z}))=n^{r_K-r_k-1}\cdot 2^\rho\cdot\#H^1(\mathfrak{o}_K^\times).^{3)} \tag{5}$$

The isogeny λ_0 induces the map

$$\begin{array}{ccccc}\lambda_0(\mathfrak{o}_k):\ T_0(\mathfrak{o}_k) & \longrightarrow & T_0'(\mathfrak{o}_k) & \times & T_0''(\mathfrak{o}_k)\\ \| & & \| & & \|\\ \mathfrak{o}_K^\times & & \mathfrak{o}_K^{(1)} & & \mathfrak{o}_k^\times\end{array}$$

where $\mathfrak{o}_K^{(1)}=\{x\in\mathfrak{o}_K^\times;\ Nx=1\}$. Since $\zeta\in k$, one sees easily that $\#\operatorname{Ker}\lambda_0(\mathfrak{o}_k)=n$. To determine $\#\operatorname{Cok}\lambda_0(\mathfrak{o}_k)$, apply Lemma 1 to the situation:

$$\begin{array}{ccc}\mathfrak{o}_K^{(1)}\times\mathfrak{o}_k^\times & \xrightarrow{\phi} & \mathfrak{o}_K^{(1)}\cdot\mathfrak{o}_k^\times\\ \cup & & \cup\\ \operatorname{Im}\lambda_0(\mathfrak{o}_k) & \xrightarrow{\psi} & (\mathfrak{o}_k^\times)^n.\end{array}\qquad \phi(x,y)=xy$$

We get

$$\#\operatorname{Cok}\lambda_0(\mathfrak{o}_k)=[\operatorname{Im}\phi:\operatorname{Im}\psi][\operatorname{Ker}\phi:\operatorname{Ker}\psi]=[\mathfrak{o}_K^{(1)}\cdot\mathfrak{o}_k^\times:(\mathfrak{o}_K^\times)^n]\cdot n,$$

because one verifies immediately that $\operatorname{Ker}\phi\approx\mathfrak{o}_K^{(1)}\cap\mathfrak{o}_k^\times=\langle\zeta\rangle$ and $\operatorname{Ker}\psi=1$.

We have therefore

$$\#\mathrm{Cok}\,\lambda_0(\mathfrak{o}_k)=n\frac{[\mathfrak{o}_K^{\times}:(\mathfrak{o}_K^{\times})^n]}{[\mathfrak{o}_K^{\times}:\mathfrak{o}_K^{(1)}\cdot\mathfrak{o}_k^{\times}]}\,.$$

Applying again Lemma 1 to the situation:

$$\begin{array}{ccc}\mathfrak{o}_K^{\times} & \xrightarrow{N} & \mathfrak{o}_k^{\times}\\ \cup & & \cup\\ \mathfrak{o}_K^{(1)}\cdot\mathfrak{o}_k^{\times} & \longrightarrow & (\mathfrak{o}_k^{\times})^n\end{array}$$

we get $[\mathfrak{o}_K^{\times}:\mathfrak{o}_K^{(1)}\mathfrak{o}_k^{\times}]=[N\mathfrak{o}_K^{\times}:(\mathfrak{o}_k^{\times})^n][\mathfrak{o}_K^{(1)}:\mathfrak{o}_K^{(1)}]=[N\mathfrak{o}_K^{\times}:(\mathfrak{o}_k^{\times})^n]$ and so

$$q(\lambda(\boldsymbol{Z}))=\frac{[\mathfrak{o}_K^{\times}:(\mathfrak{o}_K^{\times})^n]}{[N\mathfrak{o}_K^{\times}:(\mathfrak{o}_k^{\times})^n]}\,.$$

In general, for a $\mathfrak{g}=\langle\sigma\rangle$-module A, the Herbrand quotient is defined by

$$Q(A)=\frac{\#H^0(A)}{\#H^{-1}(A)}=\frac{\#H^0(A)}{\#H^1(A)}\,.$$

It is known in class field theory that

$$Q(\mathfrak{o}_K^{\times})=\frac{[\mathfrak{o}_k^{\times}:N\mathfrak{o}_K^{\times}]}{[\mathfrak{o}_K^{(1)}:(\mathfrak{o}_K^{\times})^{1-\sigma}]}=\frac{2^{\rho}}{n}$$ [4)]

where ρ is the number of real places in k which ramify for K/k. [i.e. $2^{\rho}=\prod_{v|\infty}e_v(K/k)$]. As for the group of units, write

$$\mathfrak{o}_k^{\times}=W_k\times\boldsymbol{Z}^{r_k}\,,\qquad r_k=r_1+r_2-1\,,$$

$$\mathfrak{o}_K^{\times}=W_K\times\boldsymbol{Z}^{r_K}\,,\qquad r_K=R_1+R_2-1\,.$$

Since one verifies easily that $[W_K:W_K^n]=[W_k:W_k^n]$, we have

$$\frac{[\mathfrak{o}_K^{\times}:(\mathfrak{o}_K^{\times})^n]}{[\mathfrak{o}_k^{\times}:(\mathfrak{o}_k^{\times})^n]}=n^{r_K-r_k}\,.$$

Since

$$[N\mathfrak{o}_K^{\times}:(\mathfrak{o}_k^{\times})^n]=\frac{[\mathfrak{o}_k^{\times}:(\mathfrak{o}_k^{\times})^n]}{[\mathfrak{o}_k^{\times}:N\mathfrak{o}_K^{\times}]}=\frac{[\mathfrak{o}_k^{\times}:(\mathfrak{o}_k^{\times})^n]}{Q(\mathfrak{o}_K^{\times})}\cdot\frac{1}{\#H^1(\mathfrak{o}_K^{\times})}\,,$$

we get finally

$$q(\lambda(\boldsymbol{Z}))=n^{r_K-r_k-1}\cdot 2^{\rho}\cdot \# H^1(\mathfrak{o}_k^{\times})\,.$$

Before combining (1), $\cdots$, (5), note the following relations,

$$(6)\qquad \begin{cases} nn_0=R_1+2R_2 \\ n_0=r_1+2r_2 \\ r_1=\sigma+\rho\,, & \sigma \text{ being the number of real places of } k \text{ unramified for } K/k\,, \\ R_1=n\sigma \\ R_2=(n/2)\rho+nr_2\,. \end{cases}$$

Note that $\rho=0$ if $n\geq 3$ because $\zeta\in k$. Note also that our assumption K/k yields $\tau(T')=n$ (Section VIII, Th. 1, Cor. 1).[5]

We are now ready to determine

$$(7)\qquad E(K/k)=\frac{h_K}{h_k h_{T'}}=\frac{1}{\tau(T')}\,\frac{q(\lambda(\boldsymbol{R}))}{q(\lambda(\boldsymbol{Z}))q(\hat{\lambda}(\boldsymbol{Q}))}\prod_{p\neq\infty} q(\lambda(\boldsymbol{Z}_p))\,.$$

By (1), $\cdots$, (7), we get

$$(8)\qquad E(K/k)=\frac{n^{n\rho/2}}{2^{\rho}}\cdot\frac{\prod_{\mathfrak{p}} e_{\mathfrak{p}}(K/k)}{\# H^1(\mathfrak{o}_K^{\times})}\,.$$

If $n=2$, we have $(n^{n\rho/2})/2^{\rho}=1$. If $n\geq 3$, since $\rho=0$ in this case, we have $(n^{n\rho/2})/2^{\rho}=1$ again. Hence, we get

$$(9)\qquad E(K/k)=\frac{\prod_{\mathfrak{p}} e_{\mathfrak{p}}(K/k)}{\# H^1(\mathfrak{o}_K^{\times})}\,,\qquad K/k=\text{cyclic kummer}\,.$$

If, in particular, $n=l$ a prime number, we have

$$(10)\qquad \prod_{\mathfrak{p}} e_{\mathfrak{p}}(K/k)=l^{t(K/k)}\,,$$

where $t(K/k)$ means the number of prime ideals of k ramified for K/k. We also have

$$(11)\qquad H^1(\mathfrak{o}_K^{\times})=(\boldsymbol{Z}/l\boldsymbol{Z})^{e(K/k)}\ 6)$$

for some integer $e(K/k)\geq 0$. Hence, in this case,

$$E(K/k)=l^{t(K/k)-e(K/k)}. \tag{12}$$

Suppose now that $k=\boldsymbol{Q}$ and $l=2$. As $h_{\boldsymbol{Q}}=1$ and $T=O_2^+(f_{\mathfrak{o}_K}), f_{\mathfrak{o}_K}=N(x+y\omega)$ (see Sections I, II, III), we have $h_T=h_K^*$ and so

$$E(K/\boldsymbol{Q})=h_K/h_K^*=2^{t(K/\boldsymbol{Q})-e(K/\boldsymbol{Q})}. \tag{13}$$

Let σ be the generator of galois group $G(K/\boldsymbol{Q})$. Then

$$H^1(\mathfrak{o}_K^\times)\approx H^{-1}(\mathfrak{o}_K^\times)=\mathfrak{o}_K^{(1)}/(\mathfrak{o}_K^\times)^{1-\sigma}.$$

From this, one finds easily that

$$e(K/\boldsymbol{Q})=\begin{cases}1, & \Delta_K<0 \quad \text{or} \quad \Delta_K>0, \quad \exists\varepsilon\in\mathfrak{o}_K^\times, \quad N\varepsilon=-1\\ 2, & \Delta_K>0, \quad N\varepsilon=1 \quad \forall\varepsilon\in\mathfrak{o}_K^\times.\end{cases}$$

and so

$$h_K^+/h_K^*=2^{t(K/\boldsymbol{Q})-1}, \tag{14}$$

which is the Theorem of Gauss (Section II, Th. 6).

Remark 1. Let $K=\boldsymbol{Q}(e^{2\pi i/p})$, $p=a$ prime ≥ 3, and let k be the maximal real subfield of K: $k=\boldsymbol{Q}(\zeta+\zeta^{-1})$, $\zeta=e^{2\pi i/p}$. Applying (12) to this quadratic extension, we can prove that

$$E(K/k)=1.^{7)}$$

Remark 2. The number $E(K/k)$ makes sense for any finite extension K/k.

Added in Proof. Recently, we obtained for any galois extension K/k the following formula which generalizes (8):

$$E(K/k)=\frac{\#\mathrm{Ker}(H^0(\mathfrak{g}, K^\times)\to H^0(\mathfrak{g}, K_A^\times))\prod_v \#H^0(\mathfrak{g}_v, \mathfrak{o}_V^\times)}{[K':k]\,\#H^0(\mathfrak{g}, \mathfrak{o}_K^\times)}$$

where K'/k is the maximal abelian subextension of K/k, $K_A^\times$ is the idele group of K, $\mathfrak{o}_V=\mathfrak{o}_{\mathfrak{P}}$ or $\boldsymbol{R}$ or $\boldsymbol{C}$ for $V\mid v$ and $\mathfrak{g}_v$ is the galois group of K_V/k_v.

Notes

I.

1) Prequisites on quadratic forms and quadratic fields are found in [5] and [7]. Some classics are: [17], [18], [32] and [35].
2) $N\alpha=\alpha\alpha'$, the norm of $\alpha\in K$.
3) $f>0$ means that the quadratic form f is positive definite. Note that for f in $Q(\Delta_K)$ one has $(a,b,c)=1$.
4) cf. [14] Sec. V, art. 234–art. 249.
5) cf. [13] Supplement XI, Über die Theorie der ganzen algebraischen Zahlen.
6) See, e.g. [21] p. 79, Theorem 27.

II.

1) See, e.g. [5] p. 70, Theorem 2.
2) cf. [14] Sec. V, art. 230–art. 233.
3) See [5] Chapter 1, [7] Chapter 3 and [30] Chapter III for proofs of properties of Hilbert symbols.
4) See [7] Chapter 8.
5) I used Tables in [6]. I want to take this opportunity to mention a perhaps novel invariant p_K of an imaginary quadratic field $K=\boldsymbol{Q}(\sqrt{m})$. Notation being as in Section I, put $l=N\omega$ and consider the polynomial

$$P_K(x)=N(x+\omega)=\begin{cases}x^2+l\,, & m\equiv 2,3 \pmod 4\,,\\ x^2+x+l\,, & m\equiv 1 \pmod 4\,.\end{cases}$$

For a natural number v, denote by $\deg v$ the number of its prime factors counted with multiplicity. Now put

$$p_K=\max_{0\leqq x\leqq l-2}\deg(P_K(x))\,.$$

This invariant of K is closely connected with the structure of H_K. For example, we have

$$p_K=1\Longleftrightarrow h_K=1 \text{ ([29])}\,,$$

$$p_K=2\Longleftrightarrow h_K=2 \text{ (R. Sasaki, cf. [34])}\,.$$

But, $p_K=3<h_K=4$ if $m=-21$. Sasaki also proved that $p_K\leqq h_K$ always (cf. [34]). I have a conjectural inequality

$$(*)\qquad h_K\leqq 2^{p_K}\,.$$

H. Wada informed me, using computer, that $(*)$ is true for $-m\leqq 8173$. See, e.g. [16] more about recent progresses on class numbers of imaginary quadratic fields.

III.

1) Prerequisites on algebraic groups are found in [2], [19]. Some classics are: [9], [10], [11], [12].
2) An algebraically closed field Ω that has an infinite transcendence degree over the prime field is called a universal domain.
3) We followed the proof in [7] pp 113–114.
4) The definition of $G(A)$ for any linear algebraic group G was given by [23], but its intrinsic

character, i.e. the invariance under algebraic isomorphisms over $\boldsymbol{Q}$ was proved by [37], 1.2. Weil's lectures [37] have played an important role in the development of the arithmetic of algebraic groups and Tamagawa numbers. cf. [28] for a survey of the history of the arithmetic theory of algebraic groups.

5) cf. [1].

IV.

1) $\boldsymbol{A}$ means the adele ring of $\boldsymbol{Q}$.
2) $\boldsymbol{A}^\times$ = the idele group of $\boldsymbol{Q}$, $\boldsymbol{A}_\infty^\times = \boldsymbol{R}^\times \times \prod_{p \neq \infty} \boldsymbol{Z}_p$.

V.

1) cf. [1], [3].
2) cf. [1], [15].
3) At this moment, ω_∞ (resp. $\omega_{\boldsymbol{A}}$) simply means any Haar measure of the unimodular group $G(R)_1$ (resp. $G(\boldsymbol{A})_1$).

VI.

1) cf. [3].
2) cf. [4] Proposition 5.1.
3) cf. [24] Theorem 4.
4) cf. [37], 1.3. Because of its importance, we reproduce here the definition of the functor: Let K/k be a finite separable extension of degree d. Let V, W be varieties defined over K, k, respectively. Let $p: W \to V$ a map defined over K. Let $\Sigma = \{\sigma_1, \cdots, \sigma_d\}$ be the set of all distinct isomorphisms of K into $\bar{k}$. We can then define $p^\sigma: W \to V^\sigma$, and also $(p^{\sigma_1}, \cdots, p^{\sigma_d}): W \to V^{\sigma_1} \times \cdots \times V^{\sigma_d}$, this being the mapping $w \longmapsto (p^\sigma(w))_{\sigma \in \Sigma}$. If the latter map gives an isomorphism, we call W (actually the pair $\{W, p\}$) the variety obtained form V by the restriction of the field of definition from K to k and write $\{W, p\} = R_{K/k}(V)$, or by abuse of language, $W = R_{K/k}(V)$.

VII.

1) cf. [25] (1.2.6).
2) cf. [11].
3) cf. [33].

VIII.

1) cf. [37], Chapter II and Appendix by Ono. See also [22].
2) See the end of Section IV.
3) cf. [26].
4) cf. [37].
5) cf. [26], Theorem 6.1.1.
6) cf. [27].
7) cf. [37], Chapter III.

IX.

1) Although the notation of the Tamagawa number $\tau(G)$ is intrinsic, i.e. independent of the matrix embedding $G \subset GL_n$, things like $G(\boldsymbol{Z}_p)$, $p \neq \infty$, $G(\boldsymbol{Z})$, $G(\boldsymbol{A})_\infty$, h_G, etc. depend on how we realize G as a matrix group. Fortunately, however, as far as tori are concerned, it is customary to adopt the following intrinsic definition. (cf. [25], 2.1) Namely, for a torus T over $\boldsymbol{Q}$, we define $T(\boldsymbol{Z}_p)$ as the unique maximal compact subgroup of $T(\boldsymbol{Q}_p)$:

$$T(\boldsymbol{Z}_p) \overset{\text{def}}{=} \{x \in T(\boldsymbol{Q}_p);\ |\xi(x)|_p = 1,\ \forall \xi \in \hat{T}(\boldsymbol{Q}_p)\}\ .$$

[When $p=\infty$, this is the group $K \subset T(\boldsymbol{R})$ in Section VI.]
We then put

$$T(\boldsymbol{A})_\infty \overset{\text{def}}{=} T(\boldsymbol{R}) \times \prod_{p \neq \infty} T(\boldsymbol{Z}_p)\ , \qquad T(\boldsymbol{Z}) \overset{\text{def}}{=} T(\boldsymbol{Q}) \cap T(\boldsymbol{A})_\infty\ ,$$

$$h_T \overset{\text{def}}{=} \#(T(\boldsymbol{Q})\backslash T(\boldsymbol{A})/T(\boldsymbol{A})_\infty)\ .$$

in Sections IX and X, we shall follow this shift of definition for tori.

2) The formula (1) is implicit in [25], explicit in [31] and is obtained by following Tate's computations of various measures in idele groups (cf. [36]).
3) cf. [25], Theorem 2.3.1.
4) cf. [31], Theorem 3.1.1.

X.

1) $N_{\mathfrak{p}}(\alpha)$ means the $K_{\mathfrak{P}}/k_{\mathfrak{p}}$-norm of $\alpha \in K_{\mathfrak{P}}$.
2) [20], p. 188, Lemma 4.
3) r_K, r_k, ρ will be explained soon.
4) [20], p. 192, Corollary 2.
5) Actually, Section VIII, Th. 1, Cor. 1 is not enough unless $k=\boldsymbol{Q}$. For a general k, $\tau(T')=\tau_k(T'_0)=n$ follows from [26], p. 69, Cor.
6) See e.g. [8], p. 105, Corollary 1 and Corollary 2.
7) [31], p. 53.

Bibliography

[1] A. Borel, Some finiteness properties of adele groups over number fields, *IHES Publ.*, **16** (1963), 5–30.
[2] A. Borel, *Linear Algebraic Groups*, Benjamin, New York, 1969.
[3] A. Borel and Harish-Chandra, Arithmetic subgroups of algebraic groups, *Ann. of Math.*, **75** (1962), 485–535.
[4] A. Borel and J.-P. Serre, Théorèmes de finitude en cohomologie galoisienne, *Comm. Math. Helv.*, **39** (1964), 111–164.
[5] Z. I. Borevich and I. R. Shafarevich, *Number Theory* (translated from Russian), Academic Press, New York, 1966.
[6] J. Brillhart, D. H. Lehmer, J. L. Selfridge, B. Tuckerman and S. S. Wagstaff, Factorizations of $b^n \pm 1$, $b=2$, 3,5, 6, 7, 10, 11, 12 and up to high powers, *Contemporary Mathematics*, *AMS*, **22** (1983).
[7] J. W. S. Cassels, *Rational Quadratic Forms*, Academic Press, New York, 1978.
[8] J. W. S. Cassels and A. Fröhlich, Algebraic Number Theory, Proceedings of the Brighton Conference, Academic Press, 1968.
[9] C. Chevalley, *Théorie des Groupes de Lie*, Tome II, Groupes algébriques, Hermann, Paris, 1951.
[10] C. Chevalley, *Théorie des Groupes de Lie*, Tome III, Théorèmes généraux sur les algèbres de Lie, Hermann, Paris, 1955.

[11] C. Chevalley, Sur certains groupes simples, *Tôhoku Math. J.*, **7** (1955), 14–66.
[12] C. Chevalley, Séminaire sur la classification des groupes de Lie algébriques, *Ecole Norm. Sup., Paris*, (1956–58).
[13] P. G. L. Dirichlet, *Vorlesungen über Zahlentheorie*, 2nd ed., Braunschweig, 1871.
[14] C. F. Gauss, *Disquisitiones arithmeticae*, 1801, Werke, Bd. I. (English translation: Yale University Press, 1966).
[15] R. Godement, Domaines fondamentaux des groupes arithmétiques, *Sém. Bourbaki*, **15** (1962–63), Exp. 257.
[16] D. Goldfeld, Gauss' class number problem for imaginary quadratic fields, *Bull. AMS*, **13** (1985), 23–37.
[17] H. Hasse, *Vorlesungen über Zahlentheorie*, Springer-Verlag, Berlin, 1950.
[18] E. Hecke, *Vorlesungen über die Theorie der algebraischen Zahlen*, Chelsea Pub. Co., New York, 1948.
[19] J. E. Humphreys, *Linear Algebraic Groups*, Springer-Verlag, New York, 1975.
[20] S. Lang, *Algebraic Number Theory*, Addison-Wesley, Reading, Mass., 1971.
[21] D. Marcus, *Number Fields*, Springer-Verlag, New York, 1977.
[22] J. Oesterlé, Nombres de Tamagawa et groupes unipotents en caractéristique p, *Invent. Math.*, **78** (1984), 13–88.
[23] T. Ono, Sur une propriété arithmétique des groupes algébriques commutatifs, *Bull. Soc. Math. France*, **85** (1957), 307–323.
[24] T. Ono, On some arithmetic properties of linear algebraic groups, *Ann. of Math.*, **70** (1959), 266–290.
[25] T. Ono, Arithmetic of algebraic tori, *Ann. of Math.*, **74** (1961), 101–139.
[26] T. Ono, On the Tamagawa number of algebraic tori, *Ann. of Math.*, **78** (1963), 47–73.
[27] T. Ono, On the relative theory of Tamagawa numbers, *Ann. of Math.*, **82** (1965), 88–111.
[28] V. P. Platonov, The arithmetic theory of algebraic groups, *Russian Math. Surveys*, **37**: 3 (1982), 1–62.
[29] G. Rabinovitch, Eindeutigkeit der Zerlegung in quadratischen Zahlkörpern, *J. Reine Angew Math.*, **142** (1913), 153–164.
[30] J.-P. Serre, *A Course in Arithmetic*, Springer-Verlag, New York, 1970.
[31] Jih-Min Shyr, Class number formula of algebraic tori with applications to relative class numbers of certain relative quadratic extensions of algebraic number fields, Thesis, The Johns Hopkins Univ., Baltimore, Maryland, 1974.
[32] C. L. Siegel, Analytische Zahlentheorie, II, Lecture Notes at Göttingen Univ., 1963/64.
[33] R. Steinberg, Variations on a theme of Chevalley, *Pacific J. Math.*, **9** (1959), 875–891.
[34] J. B. Svirsky, On the class numbers of imaginary quadratic fields, Thesis, The Johns Hopkins Univ., Baltimore, Maryland, 1985.
[35] T. Takagi, *Lectures on Elementary Number Theory*, (in Japanese), Kyoritsu Pub. Co., Tokyo, 1953.
[36] J. Tate, Fourier analysis in number fields and Hecke's zeta-functions, Thesis, Princeton Univ., Princeton, New Jersey, 1950.
[37] A. Weil, Adeles and algebraic groups, notes by M. Demazure and T. Ono, Progress in Math., 23, Birkhäuser, Boston, 1982.

あとがき

1985年4月5日から7月4日迄，立教大学国際学術交流制度による招聘研究員として，Johns Hopkins大学教授小野孝先生をお迎えした。招聘期間中，立教大学に於ては，小野先生による10回の連続講義・公式のセミナー・2回にわたって行われた公開講演の他，先生を中心とした非公式のセミナーも毎週行われた。セミナーには立教大学のほか，東大・都立大・早稲田大など都内の多くの大学から，特に若手の代数群や整数論の研究者が多勢出席し，盛況であった。

また招聘期間後もほぼ一ケ月近く滞在され，北海道から大阪・神戸まで各地の大学の談話会などで講演され，多くの数学者に影響を与えた。7月末金沢大学で行われた代数学シンポジュームに於ても，講演後若手研究者と熱心に検討されている小野先生の姿が印象的であった。

この報告書は，立教大学に於ける連続講義をもとに，小野先生自身により若干の手直しを行い引用文献等をつけ加えたものである。小野先生の講義は，周到に準備された主テーマがさりげない形で導入部に現われ，それをもととして深い理論が展開され，最後にまた主テーマが内容を豊かにして再び現われるという，クラシックの交響曲を聞くようなすばらしいものであった。

講演の内容はこの報告書をお読みいただければ明らかであるので，解説などはさしひかえたいが，小野先生の話は明解で，また大切なことはくり返して指摘されるなど大変教育的でもあった。

数学者の頭脳流出が云われて久しいが，今でもまだ日本の国全体としては有効な手立てが打たれているとはいえない状態にある。しかし時宜を得て優秀な研究者を招聘すれば，国内の若手研究者には大いなるはげましが与えられることも証明されたといえる。このような機会を与えてくれた立教大学の国際学術交流制度が今後とも充実し，更に発展してゆくことを期待したい。

なお小野先生の招聘に際して，東京大学教授藤崎源二郎先生ならびに慶応大学教授伊藤雄二先生にたいへんお世話になった。最後になったが，ここに感謝の意を記しておきたい。

1985年8月

立教大学理学部数学教室
遠藤幹彦

立教大学国際学術交流報告書　第六輯
代数群の整数論とその応用

1986 年 3 月 20 日

著 者 小 野 孝
発行者 高 橋 健 人

発行所 立 教 大 学
〒171 東京都豊島区西池袋 3 丁目
電話 03-985-2208

印刷所 (株) 国際文献印刷社

ISSN 0388-5305