Fundamental Domains for Arithmetic Quotients of Reductive Algebraic Groups

Takao Watanabe

Department of Mathematics
Graduate School of Science
The University of Osaka

July 2025

To my granddaughter, Hina

Preface

The group of units of the ring of $n \times n$ matrices with integer entries is called the n-th integral unimodular group. This group acts naturally on the set of all n-variable positive definite real quadratic forms via linear transformations of variables. The description of a set of representatives for each orbit under this action is known as the reduction theory of positive definite real quadratic forms, for which different methods were proposed by Hermite, Korkine–Zolotarev, Minkowski, Voronoi, etc. ([16, Ch.2 Section v]). The reduction theory of positive definite real quadratic forms can be seen as the reduction theory of the general linear group defined over the field of rational numbers. More generally, the reduction theory of an algebraic group is a theory that describes a fundamental domain for the quotient of the group of real rational points by its arithmetic subgroup. When the base field is an algebraic number field, it is more natural to develop the reduction theory by replacing the group of real rational points with the adelic group.

A central role in Voronoi's reduction theory is played by the set of integer-component shortest vectors. When A is a positive definite real symmetric $n \times n$ matrix, the arithmetical minimum of A is defined by the minimum of ${}^t\boldsymbol{x}A\boldsymbol{x}$ for non-zero $\boldsymbol{x} \in \mathbf{Z}^n$. A vector $\boldsymbol{x} \in \mathbf{Z}^n$ attaining the arithmetical minimum is called a shortest vector of A. If $\{\boldsymbol{x}_i\}_i$ is the set of all shortest vectors of A, then the closed cone generated by $\{\boldsymbol{x}_i{}^t\boldsymbol{x}_i\}_i$ is called the Voronoi cone of A. If the Voronoi cone of A is full-dimensional in the space of real symmetric $n \times n$ matrices, then A is called a perfect form. The Voronoi fundamental domain is constructed from the Voronoi cones of finitely many perfect forms ([24, 3.1.8]). Ryshkov organized Voronoi's reduction theory from a good perspective by defining a convex polyhedron from the arithmetical minimum function on the cone of all positive definite real symmetric $n \times n$ matrices. This convex polyhedron is called the Ryshkov polyhedron. The vertices of the Ryshkov polyhedron correspond to perfect quadratic forms.

The concepts of the arithmetical minimum function, the set of shortest vectors, and the Ryshkov polyhedron can be generalized to the adelic group of an isotropic reductive algebraic group. This allowed the paper [28] to provide a method for constructing a fundamental domain for the arithmetic quotient in the adelic group of a reductive algebraic group defined over the field of rational numbers. Applying this construction to the aforementioned n-variable positive definite real quadratic forms for $n \geq 4$ yields a fundamental domain whose boundary is not a hyperplane. Therefore, we can construct a fundamental domain that differs from both the Voronoi fundamental domain and the Minkowski fundamental domain. Even when limited to this case, the concrete description of the boundary hypersurface is not simple. The motivation for constructing such a fundamental domain is related to the

Hermite–Rankin constant, which is defined as the maximum value of some arithmetical minimum function. In the paper [28], we proved that all extremal points of an arithmetical minimum function lie on the boundary hypersurface. Exploring an analogue of the Voronoi algorithm in this domain with a non-linear boundary is a future task.

This note is based on the graduate course "Topics in Number Theory II" taught during the fall and winter terms of the 2024 academic year. As preparation, Sections 1 to 5 provide an overview of the basic definitions and results of linear algebraic groups, based on [2], [4], [8], [17], [22], and others. Section 6 outlines the existence of maximal compact subgroups and the Iwasawa decomposition in reductive algebraic groups over local fields, and Section 7 outlines the definition and properties of adele groups. Section 8 introduces the theorems of Mostow–Tamagawa and Borel–Harish-Chandra concerning the compactness criterion of the arithmetic quotient, as well as Borel–Harish-Chandra's theorem stating that the Siegel set provides a fundamental set. Sections 9 to 11 introduce the results of the paper [28], including proofs.

I am grateful to Professor Hiroaki Nakamura and the Library of Mathematics staff for their invaluable help with the publication.

T. Watanabe

References

[1] E. Bombieri and W. Gubler, Heights in Diophantine Geometry, Cambridge University Press, 2006.

[2] A. Borel, Linear Algebraic Groups, 2nd Ed., Springer-Verlag, 1991.

[3] A. Borel, Intorduction aux groupes arithmetiques, Hermann, 1969.

[4] A. Borel and J. Tits, Groupes réductifs, Inst. Hautes Études Sci. Publ. Math. 27 (1965), 55 - 150.

[5] A. Borel, Some finitenes properties of adele groups over number fields, Publ. Math. Inst. Hautes Etud. Sci. 16 (1963) 5 - 30.

[6] A. Borel and Harish-Chandra, Arithmetic subgroups of algebraic groups, Ann. Math. (2) 75 (1962) 485 - 535.

[7] N. Bourbaki, Groupes et Algébres de Lie, Chapitres 4,5 et 6, Masson, 1981.

[8] C. Chevalley, Classification des groupes de Lie algébriques, Séminaire C. Chevalley 1956 - 58.

[9] C. Chevalley, Sur certain groupes simples, Tohoku Math. J. (1955) 14 - 66.

[10] C. Chevalley, Theory of Lie Groups, Princeton Univ. Press, 1946.

[11] C. Chevalley and H. Tuan, On algebraic Lie algebras, Proc. Nat. Acad. Sci. U.S.A. 31 (1945) 195- 196.

[12] M. Fujimori, A fundamental domain for the general linear group by means of successive minima, J. Lie Theory 33 (2023) 845 - 873.

[13] D. Grenier, Fundamental domains for the general linear group, Pacific J. Math. 132 (1988) 293 - 317.

[14] D. Grenier, On the shape of fundamental domains in $\mathrm{GL}(n, \mathbf{R})/\mathrm{O}(n)$, Pacific J. Math. 160 (1993) 53 - 66.

[15] R. Godement, Domaines fondamentaux des groupes arithmétiques, Séminaire N. Bourbaki, exp. n° 257 (1964) 201-225.

[16] P. M. Gruber and and C. G. Lekkerkerker, Geometry of Numbers, 2nd Ed., North-Holland, 1987.

[17] J. E. Humphreys, Linear Algebraic Groups, Springer-Verlag, 1987.

[18] J. E. Humphreys, Reflection Groups and Coxeter Groups, Cambridge Univ. Press, 1990.

[19] J. Jorgenson and S. Lang, $\mathrm{Pos}_n(\mathbf{R})$ and Eisenstein Series, Lecture Notes in Math. 1868, Springer-Verlag, 2005.

[20] J. Martinet, Perfect Lattices in Euclidean Spaces, Springer, 2003.

[21] V. Platonov and A. Rapinchuk, Algebraic Groups and Number Theory, Academic Press, 1994.

[22] I. Satake, Classification Theory of Semi-Simple Algebraic Groups, Marcel Dekker, 1971.

[23] K. Sawatani, T. Watanabe and K. Okuda, A note on the Hermite–Rankin constant, Journal de Théorie des Nombres de Bordeaux 22 (2010) 209 - 217.

[24] A. Schürmann, Computational Geometry of Positive Definite Quadratic Forms, Polyhedral Reduction Theories, Algorithms, and Applications, University Lecture Series Vol. 48, Amer. Math. Soc., 2009.

[25] A. Terras, Harmonic Analysis on Symmetric Spaces and Applications II, Springer-Verlag, 1988.

[26] J. Tits, Reductive groups over local fields, Proc. Symp. Pure Math. 33, part 1,Amer.Math. Soc., Providence, R.I., (1979) 29 - 69.

[27] B. L. van der Waerden, Gruppen von Linearen Transformationen, Ergebnisse der Mathematik und ihrer Grenzgebiete 4:2, Springer, Berlin, 1935.

[28] T. Watanabe, Ryshkov domains of reductive algebraic groups, Pacific J. Math. 270 (2014) 237 - 255.

[29] T. Watanabe, Fundamental Hermite constants of linear algebraic groups, J. Math. Soc. Japan 55 (2003) 1061 - 1080.

[30] L. T. Weng, Fundamental domains of arithmetic quotients of reductive groups over number fields, Pacific J. Math. 290 (2017) 139 - 168.

Contents

Notation

The symbols $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$ denote, respectively, the ring of integers and the fields of rational numbers, real numbers, and complex numbers. For a commutative ring R, $\mathrm{M}_{m,n}(R)$ represents the set of all $m \times n$ matrices with entries in R, and $\mathrm{M}_n(R)$ is an abbreviation for $\mathrm{M}_{n,n}(R)$. The group of all invertible elements in $\mathrm{M}_n(R)$ is denoted by $\mathrm{GL}_n(R)$. The $n \times n$ identity matrix is denoted by E_n. In text, sentences beginning with ► provide comments, remarks, or additional results for the preceding definition or theorem.

§1 Affine Algebraic Groups

Let $\mathbf{C}$ be the field of complex numbers. The following content remains the same if $\mathbf{C}$ is replaced by an algebraically closed field of characteristic 0.

1.1 Algebraic Sets

Let $\mathbf{C}[X]_N := \mathbf{C}[X_1, \ldots, X_N]$ be the polynomial ring in N variables with coefficients in $\mathbf{C}$.

Definition Let M be a subset of $\mathbf{C}[X]_N$. A subset

$$V(M) := \{z = (z_1, \ldots, z_N) \in \mathbf{C}^N \mid f(z) = 0 \quad (^\forall f \in M)\}$$

of $\mathbf{C}^N$ determined by M is called an **algebraic set**.

► Let $V = V(M)$ be an algebraic set. Then

$$I(V) := \{f \in \mathbf{C}[X]_N \mid f(z) = 0 \quad (^\forall z \in V)\}$$

is an ideal of $\mathbf{C}[X]_N$ containing M. Since $\mathbf{C}[X]_N$ is a Noetherian ring, its ideals are finitely generated. Therefore, $I(V)$ can be written as

$$I(V) = (f_1, \ldots, f_r), \qquad (^\exists f_1, \ldots, f_r \in \mathbf{C}[X]_N),$$

and

$$V = V(\{f_1, \ldots, f_r\})$$

holds.

► If $V_1 \subset \mathbf{C}^{N_1}$ and $V_2 \subset \mathbf{C}^{N_2}$ are algebraic sets with $I(V_1) \subset \mathbf{C}[X]_{N_1}$ and $I(V_2) \subset \mathbf{C}[Y]_{N_2}$, then $V_1 \times V_2$ is an algebraic set in $\mathbf{C}^{N_1+N_2}$ whose corresponding ideal is $I(V_1)\mathbf{C}[Y]_{N_2} + I(V_2)\mathbf{C}[X]_{N_1}$.

Definition Let $V \subset \mathbf{C}^N$ be an algebraic set. V is called **irreducible** if whenever $V = V_1 \cup V_2$ for non-empty algebraic sets $V_1, V_2 \subset \mathbf{C}^N$, it implies $V_1 = V$ or $V_2 = V$. V is irreducible if and only if $I(V)$ is a prime ideal.

► For any algebraic set V, there exist finitely many irreducible algebraic sets $V_j \subset V$ $(j = 1, \ldots, k)$ such that $V = V_1 \cup \cdots \cup V_k$. This representation is unique up to order. Each V_j is called an irreducible component of V.

1.2 Field of Definition for Algebraic Sets

Let F be a subfield of $\mathbf{C}$. Let $F[X]_N := F[X_1, \ldots, X_N]$ be the polynomial ring in N variables with coefficients in F.

Definition Let $V \subset \mathbf{C}^N$ be an algebraic set. If the ideal $I(V)$ can be generated by elements from $I(V) \cap F[X]_N$, i.e.,

$$^{\exists} f_1, \ldots, f_r \in I(V) \cap F[X]_N \quad \text{s.t.} \quad I(V) = \sum_{i=1}^{r} f_i \mathbf{C}[X]_N$$

then V is said to be **defined over** F, and F is called a **field of definition** for V. In this case, we set

$$V(F) := \{a = (a_1, \ldots, a_N) \in F^N \mid f_i(a) = 0 \quad (i = 1, \ldots, r)\}.$$

The elements of $V(F)$ are called the F-rational points of V.

► Let E/F be a field extension. E need not be contained in $\mathbf{C}$. If V is defined over F, then $f_i \in F[X]_N$, so we can view $f_i \in E[X]_N$, and from this, the set of E-rational points of V can be defined as

$$V(E) := \{a \in E^N \mid f_i(a) = 0 \quad (i = 1, \ldots, r)\}.$$

► Let $\overline{F} \subset \mathbf{C}$ be the algebraic closure of F, and let $\Gamma = \mathrm{Gal}(\overline{F}/F)$ be the absolute Galois group. Γ acts naturally on $\overline{F}^N$. That is,

$$\sigma((a_1, \ldots, a_N)) = (\sigma(a_1), \ldots, \sigma(a_N)) \qquad (\sigma \in \Gamma,\ (a_1, \ldots, a_N) \in \overline{F}^N).$$

For a subset $U \subset \overline{F}^N$, set $\sigma(U) = \{\sigma(a) \mid a \in U\}$. U is said to be Γ-invariant if $\sigma(U) = U$ for all $\sigma \in \Gamma$. When V is defined over $\overline{F}$, the following equivalence holds.

$$V \text{ is defined over } F \iff V(\overline{F}) \text{ is } \Gamma\text{-invariant.}$$

1.3 Polynomial Functions

Let $F \subset \mathbf{C}$ be a subfield, and let $V \subset \mathbf{C}^N$ be an algebraic set defined over F.

Definition Let $f \in F[X]_N$. The restriction of f to V, denoted by $f|_V$, is called a **polynomial function on** V **defined over** F. The set of polynomial functions on V defined over F is denoted by $F[V]$. This is an F-algebra. When $F = \mathbf{C}$, $\mathbf{C}[V]$ is isomorphic with $\mathbf{C}[X]_N/I(V)$.

Definition Let $V_1 \subset \mathbf{C}^{N_1}$ and $V_2 \subset \mathbf{C}^{N_2}$ be algebraic sets both defined over F. A map $\varphi : V_1 \longrightarrow V_2$ represented as

$$\varphi(z) = (\varphi_1(z), \ldots, \varphi_{N_2}(z))$$

is called a **polynomial map defined over** F (or F**-morphism**) if $\varphi_i \in F[V_1]$ for all i. (When $F = \mathbf{C}$ or $\overline{F}$, it is simply called a polynomial map or morphism.)

► For any ideal $J \subset \mathbf{C}[V]$, let

$$V_J := \{z \in V \mid f(z) = 0 \ \ (^\forall f \in J)\}.$$

The family of sets $\{V_J\}_J$ satisfies the axioms for closed sets, thus defining a topology on V. This topology is called the **Zariski topology**.

► According to Hilbert's Nullstellensatz, for any ideal $J \subset \mathbf{C}[V]$, we have

$$\{f \in \mathbf{C}[V] \mid f(z) = 0 \ \ (^\forall z \in V_J)\} = \sqrt{J},$$

where $\sqrt{J} := \{f \in \mathbf{C}[V] \mid {}^\exists k > 0 \ \text{ s.t. } \ f^k \in J\}$. From this, the following follow:

(1) For a proper ideal $J \subsetneq \mathbf{C}[V]$, $V_J \neq \emptyset$.

(2) For a point $z \in V$, $M_z := \{f \in \mathbf{C}[V] \mid f(z) = 0\}$ is a maximal ideal of $\mathbf{C}[V]$, and all maximal ideals of $\mathbf{C}[V]$ are of this form.

(3) A singleton set $\{z\} \subset V$ is a closed set in the Zariski topology.

► Let $V_1 \subset \mathbf{C}^{N_1}$ and $V_2 \subset \mathbf{C}^{N_2}$ be algebraic sets both defined over F. If $\varphi : V_1 \longrightarrow V_2$ is a polynomial map defined over F, then for any $f \in F[V_2]$, we have $f \circ \varphi \in F[V_1]$. Setting $\varphi^*(f) = f \circ \varphi$ defines an F-algebra homomorphism $\varphi^* : F[V_2] \longrightarrow F[V_1]$.

► Let $f, g \in F[V]$ with g not vanishing identically on each irreducible component of V. Then f/g is called a **rational function on** V **defined over** F. A map $\varphi : V_1 \longrightarrow V_2$ is called a **rational map defined over** F if its component φ_i is a rational function on V_1 defined over F for all i.

1.4 Affine Algebraic Groups

Let $F \subset \mathbf{C}$ be a subfield.

Definition A subset $G \subset \mathbf{C}^N$ is called an **affine algebraic group defined over** F or an F**-algebraic group** if it satisfies the following three conditions:

(1) G is a group.

(2) G is an algebraic set defined over F.

(3) The two maps $G \times G \longrightarrow G : (x, y) \mapsto xy$ and $G \longrightarrow G : x \mapsto x^{-1}$ are polynomial maps defined over F.

(When $F = \mathbf{C}$ or $\overline{F}$, it is simply called an algebraic group.)

► An F-algebraic group G that is irreducible as an algebraic set is called an **irreducible algebraic group** or a **connected algebraic group**. In general, if G is not irreducible, there is a unique irreducible component G° containing the identity element of G. G° is called the **identity component** (or connected component of the identity). G° itself is also an F-algebraic group. In this case, the other irreducible components can be represented as $g_1G^\circ, \ldots, g_rG^\circ$ for some $g_1, \ldots, g_r \in G$ ([2, 1.2]).

► Let G be an F-algebraic group. The set of F-rational points $G(F)$ is a group. More generally, for any field extension E/F, the set of E-rational points $G(E)$ is a group.

Examples
(1) $G = \mathbf{G}_a = \mathbf{C}$ as the additive group is a connected algebraic group. $I(G) = (0)$.

(2) $G = \mathbf{G}_m = \mathbf{C}^\times$ as the multiplicative group is a connected algebraic group. As an algebraic set, it is viewed as a subset of $\mathbf{C}^2$:

$$G = \{(z, z^{-1}) \in \mathbf{C}^2 \mid z \in \mathbf{C}^\times\} \subset \mathbf{C}^2,$$

$I(G) = (X_1X_2 - 1)$.

(3) $G = \mathrm{SL}_n = \{z = (z_{ij}) \in \mathrm{M}_n(\mathbf{C}) \mid \det z = 1\} \subset \mathbf{C}^{n^2}$ is a connected algebraic group. $I(G) = (\det(X_{ij}) - 1)$. This is called the **special linear group**.

(4) $G = \mathrm{GL}_n = \{z = (z_{ij}) \in \mathrm{M}_n(\mathbf{C}) \mid \det z \neq 0\}$ is a connected algebraic group. As an algebraic set, it is viewed as:

$$G = \{((z_{ij}), y) \in \mathrm{M}_n(\mathbf{C}) \oplus \mathbf{C} \mid \det(z_{ij})y - 1 = 0\} \subset \mathbf{C}^{n^2+1},$$

$I(G) = (\det(X_{ij})Y - 1)$. This is called the **general linear group**.

(5) The algebraic groups from (1) to (4) are all defined over $\mathbf{Q}$. Therefore, for any field extension $E/\mathbf{Q}$ (e.g., $E = \mathbf{R}, \mathbf{Q}_p$, etc.), the set of E-rational points $G(E)$ is a group.

Definition Let G be an F-algebraic group. A subset $H \subset G$ is called a **subgroup defined over** F or an F**-subgroup** of G if it satisfies:

(1) H is a subgroup.

(2) H is an algebraic subset of G defined over F.

(When $F = \mathbf{C}$ or $\overline{F}$, to distinguish from abstract subgroups, it is called a **closed subgroup**.) If H is furthermore a normal subgroup, it is called a normal F-subgroup.

► Condition (2) requires that H is a closed subset of G in the Zariski topology. In general, if H is a subgroup of G, its closure H^- in the Zariski topology is a closed subgroup of G ([2, 1.3]).

Examples
(1) SL_n is a closed subgroup of GL_n.

(2) For any F-algebraic group G, the identity component G° is a normal F-subgroup.

1.5 Homomorphisms of Algebraic Groups

Definition Let G_1 and G_2 be F-algebraic groups. A map $\varphi : G_1 \longrightarrow G_2$ is called a **homomorphism defined over** F or an F**-homomorphism** if it satisfies:

(1) φ is a group homomorphism.

(2) φ is a polynomial map defined over F.

Furthermore, if φ is bijective and the inverse map $\varphi^{-1} : G_2 \longrightarrow G_1$ is also a polynomial map defined over F, then G_1 and G_2 are said to be F**-isomorphic**, and φ is called an F**-isomorphism**.

► For an F-homomorphism $\varphi : G_1 \longrightarrow G_2$, the following hold ([2, 1.4], [17, 7.4]).

(1) $\mathrm{Ker}\,\varphi$ is a normal F-subgroup of G_1.

(2) $\mathrm{Im}\,\varphi$ is an F-subgroup of G_2. Also, $(\mathrm{Im}\,\varphi)^\circ = \varphi(G^\circ)$ holds.

► If the characteristic of F is $p > 0$ and F has inseparable extensions, then $\mathrm{Ker}\,\varphi$ is not necessarily defined over F.

► For any field extension E/F, φ naturally induces a homomorphism of (abstract) groups $\varphi_E : G_1(E) \longrightarrow G_2(E)$. If φ is injective, then φ_E is also injective. However, even if φ is surjective, φ_E is not necessarily surjective.

Example The map $\varphi : \mathbf{G}_m \longrightarrow \mathbf{G}_m : \varphi(z) = z^2$ is a surjective $\mathbf{Q}$-homomorphism, but the image of $\varphi_{\mathbf{R}} : \mathbf{G}_m(\mathbf{R}) \longrightarrow \mathbf{G}_m(\mathbf{R})$ is the set of positive real numbers, so it is not surjective.

Theorem 1 (Embedding into GL_n [2, 1.10])

Let $\boldsymbol{G}$ be an affine algebraic group. Then there exist some $\boldsymbol{n}$ and a $\mathbf{C}$-isomorphism $\boldsymbol{\varphi}$ from $\boldsymbol{G}$ into $\mathbf{GL}_{\boldsymbol{n}}$. If $\boldsymbol{G}$ is an $\boldsymbol{F}$-algebraic group, $\boldsymbol{\varphi}$ can be chosen to be an $\boldsymbol{F}$-isomorphism.

► It is clear from the definition that a closed subgroup of GL_n is an affine algebraic group. Therefore, affine algebraic groups and closed subgroups of GL_n can be considered identical.

Examples

(1) The following subgroups of GL_n are all connected $\mathbf{Q}$-subgroups.

$$\begin{aligned}
\mathrm{T}_n &:= \{(z_{ij}) \in \mathrm{GL}_n \mid z_{ij} = 0 \quad (^\forall i, j,\ i \neq j)\},\\
\mathrm{B}_n &:= \{(z_{ij}) \in \mathrm{GL}_n \mid z_{ij} = 0 \quad (^\forall i, j,\ i > j)\},\\
\mathrm{U}_n &:= \{(z_{ij}) \in \mathrm{B}_n \mid z_{11} = \ldots = z_{nn} = 1\},\\
\mathrm{Z}_n &:= \{(z_{ij}) \in \mathrm{T}_n \mid z_{11} = \ldots = z_{nn}\}.
\end{aligned}$$

T_n is the group of diagonal matrices and B_n is the group of upper triangular matrices. There are obvious $\mathbf{Q}$-isomorphisms $\mathrm{Z}_n \cong \mathbf{G}_m$ and $\mathrm{T}_n \cong \mathbf{G}_m^n$.

(2) Let G be a finite group of order n. By the regular representation $G \longrightarrow \mathrm{GL}_n(\mathbf{C})$, G is regarded as a subgroup of $\mathrm{GL}_n(\mathbf{C})$. Since a finite subset of $\mathrm{GL}_n(\mathbf{C})$ is Zariski closed, G is an algebraic group.

Definition Let G_1 and G_2 be F-algebraic groups. If there exists an F-homomorphism $\varphi : G_1 \longrightarrow G_2$ such that $\mathrm{Ker}\,\varphi$ is a finite group and $\mathrm{Im}\,\varphi = G_2$, then G_1 and G_2 are said to be **F-isogenous**, and φ is called an **F-isogeny**.

1.6 Quotient Groups

The quotient G/H of an algebraic group G by its closed subgroup H is generally not an affine algebraic set. Hereafter, let $\mathbf{P}^{N-1} = (\mathbf{C}^N - \{0\})/\mathbf{C}^\times$ denote the $(N-1)$-dimensional projective space, and let $\pi : \mathbf{C}^N - \{0\} \longrightarrow \mathbf{P}^{N-1}$ be the natural map. By considering homogeneous polynomials in the polynomial ring $\mathbf{C}[X]_N$, one can define algebraic sets in the projective space $\mathbf{P}^{N-1}$. That is, if an ideal $I \subset \mathbf{C}[X]_N$ is generated by homogeneous polynomials $f_1, \ldots, f_r$, then

$$\mathrm{P}V(I) := \{\pi(v) \in \mathrm{P}^{N-1} \mid f_1(v) = \ldots = f_r(v) = 0 \quad (v \in \mathbf{C}^N - \{0\})\}$$

is called an algebraic set in P^{N-1}. The topology on P^{N-1} for which the collection of all algebraic sets forms the closed sets is called the Zariski topology. A Zariski closed subset of P^{N-1} is called a **projective variety**, and a Zariski open subset is called a **quasi-projective variety**. Let G be an F-algebraic group and H be an F-subgroup of G. Let $\mathbf{P}^{N-1}(F) = \pi(F^N - \{0\})$. If $\varphi : G \longrightarrow \mathrm{GL}_N$ is an F-homomorphism, then G acts on $\mathbf{P}^{N-1}$ via

$$G \times \mathbf{P}^{N-1} \longrightarrow \mathbf{P}^{N-1} \ :\ g\pi(v) = \pi(\varphi(g)v) \qquad (g \in G,\ v \in \mathbf{C}^N - \{0\}).$$

Theorem 2 (Existence of Representation [2, 5.1, 6.8])

Let $\boldsymbol{G}$ be an $\boldsymbol{F}$-algebraic group and $\boldsymbol{H}$ be an $\boldsymbol{F}$-subgroup of $\boldsymbol{G}$. Then there exist some $\boldsymbol{n}$, an $\boldsymbol{F}$-homomorphism $\boldsymbol{\varphi : G \longrightarrow \mathrm{GL}_n}$, and $\boldsymbol{x_0 \in \mathbf{P}^{n-1}(F)}$ such that

$$\boldsymbol{H = \{g \in G \mid gx_0 = x_0\}}$$

and $\boldsymbol{\varphi}$ induces a bijection $\boldsymbol{G/H \cong Gx_0 \subset \mathbf{P}^{n-1}}$. Furthermore, $\boldsymbol{Gx_0 \subset \mathbf{P}^{n-1}}$ is a quasi-projective variety, and its closure $\boldsymbol{\overline{Gx_0}}$ with respect to the Zariski topology is a projective variety defined over $\boldsymbol{F}$. (Henceforth, we identify $\boldsymbol{G/H}$ with $\boldsymbol{Gx_0}$.)

If H is a normal F-subgroup, the following stronger result holds.

Theorem 3 (Existence of Quotient Group [2, 6.8])

Let $\boldsymbol{G}$ be an $\boldsymbol{F}$-algebraic group and $\boldsymbol{H}$ be a normal $\boldsymbol{F}$-subgroup of $\boldsymbol{G}$. Then there exist an $\boldsymbol{F}$-algebraic group $\boldsymbol{G^\natural}$ and a surjective $\boldsymbol{F}$-homomorphism $\boldsymbol{\varphi : G \longrightarrow G^\natural}$ satisfying the following:

(1) $\boldsymbol{\mathrm{Ker}\,\varphi = H}$.

(2) *For any $\boldsymbol{F}$-homomorphism $\boldsymbol{\psi : G \longrightarrow G'}$ such that $\boldsymbol{H \subset \mathrm{Ker}\,\psi}$, there exists a unique $\boldsymbol{F}$-homomorphism $\boldsymbol{\psi' : G^\natural \longrightarrow G'}$ such that $\boldsymbol{\psi = \psi' \circ \varphi}$.*

In particular, $\boldsymbol{G^\natural}$ is unique up to $\boldsymbol{F}$-isomorphism. (Henceforth, we view $\boldsymbol{G/H = G^\natural}$.)

► Since φ is surjective, if G is connected, then G/H is also connected.

► φ induces a homomorphism of groups of F-rational points $G(F) \longrightarrow (G/H)(F)$, but this is not necessarily surjective.

Examples

(1) The map $\mathrm{GL}_n \longrightarrow \mathrm{G}_m : g \mapsto \det g$ is a surjective $\mathbf{Q}$-homomorphism. Since $\mathrm{Ker}\,(\det) = \mathrm{SL}_n$, there is a $\mathbf{Q}$-isomorphism $\mathrm{GL}_n/\mathrm{SL}_n \cong \mathrm{G}_m$.

(2) U_n is a normal $\mathbf{Q}$-subgroup of B_n, and there is a $\mathbf{Q}$-isomorphism $\mathrm{B}_n/\mathrm{U}_n \cong \mathrm{T}_n$.

(3) Z_n is a normal $\mathbf{Q}$-subgroup of GL_n. The quotient group $\mathrm{GL}_n/\mathrm{Z}_n$ is called the **projective general linear group** and is denoted by PGL_n. Let

$$\pi : \mathrm{GL}_n \longrightarrow \mathrm{PGL}_n$$

be the natural $\mathbf{Q}$-homomorphism. Let π_1 be the restriction of π to SL_n. Then

$$\mathrm{Ker}\,\pi_1 = \mathrm{Z}_n \cap \mathrm{SL}_n = \{zE_n \mid z \in \mathbf{C},\ z^n = 1\}$$

is a finite group, and π_1 is surjective. Therefore, SL_n and PGL_n are $\mathbf{Q}$-isogenous.

§2 Reductive Algebraic Groups

Fix a subfield $F \subset \mathbf{C}$. In the following, any algebraic set V is assumed to be defined over the algebraic closure $\overline{F}$ of F, and we identify V with $V(\overline{F})$.

2.1 Solvable Algebraic Groups

For an abstract group G, let $D(G)$ denote its commutator subgroup. That is, $D(G)$ is the subgroup of G generated by $\{xyx^{-1}y^{-1} \mid x, y \in G\}$. Inductively, define

$$D^k(G) := D(D^{k-1}(G)) \qquad (k = 2, 3, \ldots).$$

Theorem 4 ([2, 2.3])

If $\boldsymbol{G}$ is a connected $\boldsymbol{F}$-algebraic group, then $\boldsymbol{D(G)}$ is a connected $\boldsymbol{F}$-subgroup. Thus, for any $\boldsymbol{k}$, $\boldsymbol{D^k(G)}$ is a connected $\boldsymbol{F}$-subgroup.

Definition A connected algebraic group G is called a **solvable algebraic group** if it satisfies $D^k(G) = \{e\}$ for some $k \geq 1$.

Example The $\mathbf{Q}$-subgroup B_n of upper triangular matrices is a solvable $\mathbf{Q}$-subgroup of GL_n.

Theorem 5 (Lie–Kolchin Theorem [2, 10.5])

If $\boldsymbol{G}$ is a connected solvable closed subgroup of $\mathbf{GL}_n$, then there exists $\boldsymbol{g \in \mathbf{GL}_n}$ such that $\boldsymbol{gGg^{-1} \subset \mathbf{B}_n}$.

► From Theorem 1 and Theorem 5, the following equivalence holds:

G is a connected solvable algebraic group

$\Longleftrightarrow$ There exists an injective $\overline{F}$-homomorphism $G \hookrightarrow \mathrm{B}_n$ for some n.

B_n has a normal closed subgroup $\mathrm{U_n}$.

Definition A connected algebraic group G is called a **unipotent algebraic group** if there exists an injective $\overline{F}$-homomorphism $G \hookrightarrow \mathrm{U}_n$ for some n.

2.2 Parabolic Subgroups

Definition A maximal connected solvable closed subgroup of a connected algebraic group G is called a **Borel subgroup**. A closed subgroup of G containing a Borel subgroup is called a **parabolic subgroup**.

Theorem 6 ([2, 11.1, 11.2, 11.16])

Let $\boldsymbol{G}$ be a connected algebraic group.

(1) *A Borel subgroups of $\boldsymbol{G}$ exists uniquely up to conjugacy by elements of $\boldsymbol{G}$.*

(2) *$\boldsymbol{P}$ is a parabolic subgroup if and only if $\boldsymbol{G}/\boldsymbol{P}$ is a projective variety.*

(3) *Any parabolic subgroup $\boldsymbol{P}$ is connected. The normalizer $\boldsymbol{N_G(P)}$ of $\boldsymbol{P}$ as an abstract group coincides with $\boldsymbol{P}$.*

Example B_n is a Borel subgroup of GL_n. Any Borel subgroup of GL_n is conjugate to B_n. For $r = 1, \ldots, n-1$, let

$$\mathrm{Q}_{n,r} = \mathrm{Q}_r := \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \mathrm{GL}_n \mid a \in \mathrm{GL}_r,\ d \in \mathrm{GL}_{n-r},\ b \in \mathrm{M}_{r,n-r}(\overline{F}) \right\}.$$

Since Q_r contains B_n, it is a parabolic subgroup. Q_r is called a standard maximal parabolic subgroup. Let $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n$ be the standard basis of $\overline{F}^n$, and consider the r-dimensional subspace

$$V_r := \overline{F}\boldsymbol{e}_1 + \cdots + \overline{F}\boldsymbol{e}_r.$$

Then

$$\mathrm{Q}_r = \{ g \in \mathrm{GL}_n \mid g(V_r) = V_r \}$$

holds. Therefore,

$$\mathrm{GL}_n/\mathrm{Q}_r = \text{the set of } r\text{-dimensional subspaces of } \overline{F}^n.$$

This is called the **Grassmann variety**. In particular, $\mathrm{GL}_n/\mathrm{Q}_1 = \mathbf{P}^{n-1}$. B_n and Q_r are all defined over $\mathbf{Q}$.

▶ Let G be a connected F-algebraic group. G always has a Borel subgroup defined over $\overline{F}$, but it does not necessarily have a Borel subgroup defined over F.

2.3 Semisimple Groups and Reductive Groups

Definition Let G be a connected algebraic group. The maximal connected solvable normal closed subgroup of G is called the **radical** of G and is denoted by $R(G)$. The maximal connected unipotent normal closed subgroup of G is called the **unipotent radical** of G and is denoted by $R_u(G)$. $R_u(G) \subset R(G)$ and $R_u(G) = R_u(R(G))$ hold.

▶ Let B be a Borel subgroup of G. The identity component of $\bigcap_{g \in G} gBg^{-1}$ is $R(G)$.

Definition A connected algebraic group G is called **semisimple** if it satisfies $R(G) = \{e\}$, and **reductive** if it satisfies $R_u(G) = \{e\}$.

► For any connected algebraic group G, $G/R(G)$ is connected semisimple, and $G/R_u(G)$ is connected reductive.

Theorem 7 (Levi Decomposition [2, 11.22, 14.2])

Let $\boldsymbol{G}$ be a connected algebraic group.

(1) *There exists a maximal reductive closed subgroup $\boldsymbol{H}$ of $\boldsymbol{G}$, and $\boldsymbol{G}$ is the semidirect product of $\boldsymbol{H}$ and $\boldsymbol{R_u(G)}$. (This semidirect product is called a Levi decomposition of $\boldsymbol{G}$, and $\boldsymbol{H}$ is called a Levi subgroup.)*

(2) *If $\boldsymbol{G}$ is reductive, then $\boldsymbol{R(G)}$ is equal to the identity component $\boldsymbol{C_G^\circ}$ of the center $\boldsymbol{C_G}$ of $\boldsymbol{G}$. If $\boldsymbol{D(G)}$ is the commutator subgroup of $\boldsymbol{G}$, then the map $\boldsymbol{C_G^\circ \times D(G) \longrightarrow G : (c, h) \mapsto ch}$ is an isogeny. In particular, $\boldsymbol{C_G^\circ \cap D(G)}$ is a finite group, and $\boldsymbol{D(G)}$ is semisimple.*

► Theorem 7(1) does not hold in general for fields of characteristic $p > 0$.

► When G is a connected F-algebraic group, both $R(G)$ and $R_u(G)$ are F-subgroups of G since they are invariant by the action of the absolute Galois group $\mathrm{Gal}(\overline{F}/F)$. Mostow proved that G possesses a Levi subgroup defined over F ([4, 0.8]).

► If G is a connected reductive F-algebraic group, then the center C_G is an F-subgroup ([2, 18.2]). Therefore, C_G° is also an F-subgroup. In fact, C_G° becomes an F-torus ([2, 11.21]).

Examples

(1) $R(\mathrm{GL}_n) = \mathrm{Z}_n$. Thus GL_n is reductive. Since $\mathrm{PGL}_n = \mathrm{GL}_n/R(\mathrm{GL}_n)$, PGL_n is semisimple. SL_n, which is isogenous to PGL_n, is also semisimple.

(2) Let $\mathrm{Q}_{n,r}$ be a standard maximal parabolic subgroup of GL_n. Let

$$\mathrm{M}_{n,r} := \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \mid a \in \mathrm{GL}_r,\ d \in \mathrm{GL}_{n-r} \right\},$$

$$\mathrm{U}_{n,r} := \left\{ \begin{pmatrix} E_r & b \\ 0 & E_{n-r} \end{pmatrix} \mid b \in \mathrm{M}_{r,n-r}(\overline{F}) \right\}.$$

Then $\mathrm{U}_{n,r}$ is a normal closed subgroup of $\mathrm{Q}_{n,r}$, and $\mathrm{Q}_{n,r}$ is the semidirect product of $\mathrm{U}_{n,r}$ and $\mathrm{M}_{n,r}$. $\mathrm{M}_{n,r}$ is a Levi subgroup of $\mathrm{Q}_{n,r}$. We have $R_u(\mathrm{Q}_{n,r}) = \mathrm{U}_{n,r}$ and $R(\mathrm{Q}_{n,r}) = R(\mathrm{M}_{n,r})\mathrm{U}_{n,r}$.

(3) Since B_n is itself solvable, $R(\mathrm{B}_n) = \mathrm{B}_n$. We have $R_u(\mathrm{B}_n) = \mathrm{U}_n$.

(4) Let $D(\mathrm{GL}_n)$ be the commutator subgroup of GL_n. From Theorem 7(2),

$$\mathrm{GL}_n = \mathrm{Z}_n D(\mathrm{GL}_n) = \{zh \mid z \in \mathrm{Z}_n,\ \ h \in D(\mathrm{GL}_n)\}.$$

In particular, $\mathrm{GL}_n = \mathrm{T}_n D(\mathrm{GL}_n)$. Clearly $D(\mathrm{GL}_n) \subset \mathrm{SL}_n$. Therefore, if we set $\mathrm{T}_n^1 = \mathrm{T}_n \cap \mathrm{SL}_n$, then

$$\mathrm{SL}_n = \mathrm{T}_n^1 D(\mathrm{GL}_n)$$

holds. Now, for the case of 2x2 matrices,

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a^{-1} & 0 \\ 0 & b^{-1} \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} ab^{-1} & 0 \\ 0 & a^{-1}b \end{pmatrix} \in D(\mathrm{GL}_2).$$

Based on this, it is easy to show that $\mathrm{T}_n^1 \subset D(\mathrm{GL}_n)$ holds for any n. Thus $D(\mathrm{GL}_n) = \mathrm{SL}_n$.

(5) If G is connected semisimple, then $R(G) = \{e\}$, so Theorem 7(2) implies $G = D(G)$.

§3 Tori and Character Groups

3.1 Tori

Definition An algebraic group H is called a **torus** if it is $\overline{F}$-isomorphic to $\mathbf{G}_m^k$ for some k. If H is a torus defined over F, then H is called an F**-torus**. Furthermore, if the isomorphism $H \cong \mathbf{G}_m^k$ can be taken to be an F-isomorphism, then H is called an F**-split torus**.

► Any torus is an $\overline{F}$-split torus, but for a general F, there exist F-tori that are not F-split tori.

Definition Let G be an F-algebraic group. A maximal one among tori contained in G is called a **maximal torus** of G. A maximal one among F-split tori contained in G is called a **maximal** F**-split torus**.

Theorem 8 ([2, 11.3, 18.2, 20.9])

Let $\boldsymbol{G}$ be a connected $\boldsymbol{F}$-algebraic group.

(1) *The maximal tori in $\boldsymbol{G}$ are conjugate by elements of $\boldsymbol{G}$. Also, there exists a maximal torus defined over $\boldsymbol{F}$. (Thus, a maximal $\boldsymbol{F}$-torus is a maximal torus.)*

(2) *If $\boldsymbol{T}$ is a maximal torus of $\boldsymbol{G}$, then there exists a Borel subgroup $\boldsymbol{B}$ of $\boldsymbol{G}$ containing $\boldsymbol{T}$ such that $\boldsymbol{T}$ is a maximal torus of $\boldsymbol{B}$.*

(3) *If $\boldsymbol{G}$ is a connected reductive $\boldsymbol{F}$-algebraic group, the maximal $\boldsymbol{F}$-split tori in $\boldsymbol{G}$ are conjugate by elements of $\boldsymbol{G}(\boldsymbol{F})$. Also, there exists a maximal $\boldsymbol{F}$-torus containing a maximal $\boldsymbol{F}$-split torus.*

Definition Let G be a connected reductive F-algebraic group. Let $S \cong \mathbf{G}_m^k$ be a maximal F-split torus of G, and let $T \cong \mathbf{G}_m^\ell$ be a maximal torus of G. k is called the F**-rank** of G, and ℓ is called the **absolute rank** of G. In particular, if $k = \ell$, G is called an F**-split group**. If $k = 0$, G is called F**-anisotropic**, and if $k \geq 1$, G is called F**-isotropic**.

Examples

(1) T_n is a maximal torus of GL_n, and also a maximal $\mathbf{Q}$-split torus. The $\mathbf{Q}$-rank of GL_n is n. GL_n is a $\mathbf{Q}$-split group.

(2) SL_n is a $\mathbf{Q}$-split group. Its $\mathbf{Q}$-rank is $n - 1$.

(3) $\mathrm{SO}_{E_n} = \{g \in \mathrm{SL}_n \mid {}^t g E_n g = E_n\}$ is a $\mathbf{Q}$-subgroup of SL_n. If $n \geq 3$, it is a connected semisimple group with absolute rank $[n/2]$ and $\mathbf{Q}$-rank 0.

(4) Let $F = \mathbf{R}$ and

$$H := \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbf{C},\ a^2 + b^2 = 1 \right\}.$$

Let $\mathrm{T}_2^1 = \mathrm{T}_2 \cap \mathrm{SL}_2$. Define the map $f : H \longrightarrow \mathrm{T}_2^1$ by

$$f(g) = hgh^{-1} \qquad \text{where } h = \begin{pmatrix} -\sqrt{-1} & -1 \\ -\sqrt{-1} & 1 \end{pmatrix}.$$

Since

$$f\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\right) = \begin{pmatrix} a + b\sqrt{-1} & 0 \\ 0 & a - b\sqrt{-1} \end{pmatrix},$$

f is a $\mathbf{C}$-isomorphism. Therefore H is an $\mathbf{R}$-torus. The group of $\mathbf{R}$-rational points $H(\mathbf{R})$ is the unit circle, which is a compact group under the usual Euclidean topology. Consequently, there are no non-trivial $\mathbf{R}$-homomorphisms from $\mathbf{G}_m$ to H. Thus H is an $\mathbf{R}$-anisotropic torus.

3.2 Character Groups

Definition Let G be an algebraic group. An $\overline{F}$-homomorphism $\chi : G \longrightarrow \mathbf{G}_m$ is called a **rational character** of G. The set of all rational characters of G is denoted by $\mathrm{X}^*(G)$ and is called the **rational character group**. For $\chi_1, \chi_2 \in \mathrm{X}^*(G)$, defining

$$(\chi_1 + \chi_2)(g) := \chi_1(g)\chi_2(g), \qquad (n\chi_1)(g) := \chi_1(g)^n \qquad (g \in G,\ \ n \in \mathbf{Z})$$

makes $\mathrm{X}^*(G)$ into a $\mathbf{Z}$-module.

Definition Let G be an F-algebraic group. A rational character $\chi : G \longrightarrow \mathbf{G}_m$ that is an F-homomorphism is called an **F-rational character**. Let

$$\mathrm{X}^*(G)_F := \{\chi \in \mathrm{X}^*(G) \mid \chi \text{ is an } F\text{-rational character}\}.$$

$\mathrm{X}^*(G)_F$ is a submodule of $\mathrm{X}^*(G)$.

► A rational character of G is a polynomial function. Thus $\mathrm{X}^*(G)_F$ is a subset of $F[G]$. A $\chi \in \mathrm{X}^*(G)_F$ defines, for any field extension E/F, a group homomorphism

$$\chi_E : G(E) \longrightarrow \mathbf{G}_m(E) = E^\times.$$

► Let $\Gamma = \mathrm{Gal}(\overline{F}/F)$ be the absolute Galois group. For $\sigma \in \Gamma$ and $\chi \in \mathrm{X}^*(G)$, define ${}^\sigma\chi \in \mathrm{X}^*(G)$ by

$${}^\sigma\chi(g) := \sigma(\chi(\sigma^{-1}(g))) \qquad (g \in G = G(\overline{F})).$$

This defines an action of Γ on $\mathrm{X}^*(G)$:

$$\Gamma \times \mathrm{X}^*(G) \longrightarrow \mathrm{X}^*(G) \ : \ (\sigma, \chi) \mapsto {}^{\sigma}\chi.$$

Then, if we set

$$\mathrm{X}^*(G)^{\Gamma} := \{\chi \in \mathrm{X}^*(G) \mid {}^{\sigma}\chi = \chi \quad ({}^{\forall}\sigma \in \Gamma)\},$$

we have

$$\mathrm{X}^*(G)_F = \mathrm{X}^*(G)^{\Gamma}.$$

► If $\varphi : G_1 \longrightarrow G_2$ is an F-homomorphism, then φ induces a module homomorphism

$$\varphi^* : \mathrm{X}^*(G_2)_F \longrightarrow \mathrm{X}^*(G_1)_F : \varphi^*(\chi) = \chi \circ \varphi.$$

If φ is surjective, then φ^* is injective. In particular, an exact sequence of F-algebraic groups under F-homomorphisms

$$1 \longrightarrow H \xrightarrow{\psi} G_1 \xrightarrow{\varphi} G_2 \longrightarrow 1$$

yields the following exact sequence:

$$0 \longrightarrow \mathrm{X}^*(G_2)_F \xrightarrow{\varphi^*} \mathrm{X}^*(G_1)_F \xrightarrow{\psi^*} \mathrm{X}^*(H)_F$$

where ψ^* is not necessarily surjective.

Examples

(1) For $\mathrm{T}_n \cong \mathbf{G}_m^n$, let a diagonal matrix be

$$g = \mathrm{diag}(a_1, \ldots, a_n) = \begin{pmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_n \end{pmatrix}.$$

Define

$$\epsilon_i : T \longrightarrow \mathbf{G}_m : \epsilon_i(g) = a_i \qquad (i = 1, \ldots, n).$$

Then $\epsilon_1, \ldots, \epsilon_n$ form a $\mathbf{Z}$-basis of $\mathrm{X}^*(\mathrm{T}_n)$. Thus

$$\mathrm{X}^*(\mathrm{T}_n) = \mathbf{Z}\epsilon_1 + \cdots + \mathbf{Z}\epsilon_n \cong \mathbf{Z}^n.$$

Clearly ϵ_i are $\mathbf{Q}$-rational characters, so $\mathrm{X}^*(\mathrm{T}_n) = \mathrm{X}^*(\mathrm{T}_n)_{\mathbf{Q}}$.

(2) Similarly to (1), if T is an F-split torus with $T \cong \mathbf{G}_m^k$, then $\mathrm{X}^*(T) = \mathrm{X}^*(T)_F \cong \mathbf{Z}^k$.

(3) Since there are no polynomial homomorphisms from $\mathbf{G}_a$ to $\mathbf{G}_m$, $\mathrm{X}^*(\mathbf{G}_a) = 0$. From this, it follows that if G is a unipotent group, then $\mathrm{X}^*(G) = 0$. In particular, $\mathrm{X}^*(\mathrm{U}_n) = 0$.

(4) Since $B_n/U_n \cong T_n$, taking the exact sequence yields

$$0 \longrightarrow X^*(T_n) \longrightarrow X^*(B_n) \longrightarrow X^*(U_n) = 0.$$

So, $X^*(B_n) \cong X^*(T_n)$ and $X^*(B_n)_{\mathbf{Q}} \cong X^*(T_n)_{\mathbf{Q}}$.

(5) Any character $\chi \in X^*(GL_n)$ must satisfy $\chi(ghg^{-1}h^{-1}) = 1$, so its restriction to $D(GL_n) = SL_n$ is trivial. Therefore, from the exact sequence induced by $\det : GL_n \longrightarrow \mathbf{G}_m$:

$$1 \longrightarrow SL_n \longrightarrow GL_n \longrightarrow \mathbf{G}_m \longrightarrow 1,$$

we get

$$X^*(\mathbf{G}_m) \cong X^*(GL_n) = X^*(GL_n)_{\mathbf{Q}} = \mathbf{Z} \det.$$

(6) Let G be a connected algebraic group with Levi decomposition $G = HR_u(G)$. Since $H \cong G/R_u(G)$ and $X^*(R_u(G)) = 0$ from (3), the restriction map $\chi \mapsto \chi|_H$ yields an isomorphism $X^*(G) \cong X^*(H)$. From Theorem 7(2), $H = C_H^\circ D(H)$. For $\chi \in X^*(H)$, we have $\chi|_{D(H)} = 1$, so the restriction $\chi \mapsto \chi|_{C_H^\circ}$ yields an injection $X^*(H) \hookrightarrow X^*(C_H^\circ)$. Since $C_H^\circ = R(H)$ is a torus ([2, 11.21]), if $C_H^\circ \cong \mathbf{G}_m^k$, then $X^*(C_H^\circ) \cong \mathbf{Z}^k$. $X^*(G)$ is isomorphic to a submodule of $\mathbf{Z}^k$, thus $X^*(G)$ is also a finitely generated free abelian group. Also, if G is a connected semisimple algebraic group, then $D(G) = G$, so $X^*(G) = 0$.

3.3 Character Groups of Tori

The following holds for character groups of tori.

Theorem 9 ([2, 8.2, 8.5])

Let $\boldsymbol{T}$ be an $\boldsymbol{F}$-torus.

(1) *$\boldsymbol{T}$ is an $\boldsymbol{F}$-split torus if and only if $\mathbf{X^*(T) = X^*(T)_F}$.*

(2) *$\boldsymbol{T}$ is $\boldsymbol{F}$-anisotropic if and only if $\mathbf{X^*(T)_F = 0}$.*

(3) *If $\boldsymbol{T' \subset T}$ is a connected $\boldsymbol{F}$-subgroup, then $\boldsymbol{T'}$ and $\boldsymbol{T/T'}$ are both $\boldsymbol{F}$-tori, and the following is an exact sequence:*

$$\mathbf{0 \longrightarrow X^*(T/T')_F \longrightarrow X^*(T)_F \longrightarrow X^*(T')_F \longrightarrow 0.}$$

If $\boldsymbol{T}$ is an $\boldsymbol{F}$-split torus, then $\boldsymbol{T'}$ and $\boldsymbol{T/T'}$ are also $\boldsymbol{F}$-split tori.

(4) *Let $\boldsymbol{T_s}$ be a maximal $\boldsymbol{F}$-split torus in $\boldsymbol{T}$ and $\boldsymbol{T_a}$ be a maximal $\boldsymbol{F}$-anisotropic torus in $\boldsymbol{T}$. Then the product map $\boldsymbol{T_s \times T_a \longrightarrow T}$ is an $\boldsymbol{F}$-isogeny. Furthermore, $\mathbf{X^*(T)_F = X^*(T_s)_F}$ holds.*

► T_a in Theorem 9 (4) is given as follows:

$$T_a = \bigcap_{\chi \in \mathrm{X}^*(T)_F} \mathrm{Ker}\, \chi\,.$$

For T_s, see **3.5** below.

3.4 The Central Maximal F-split Torus of a Reductive Group

Let G be a connected reductive F-algebraic group. The maximal F-split torus contained in the center C_G of G is denoted by Z_G. Z_G is called the **central maximal F-split torus** of G.

► Since G is reductive, $R(G) = C_G^\circ$ is a torus. Thus, in the notation of Theorem 9(4), $Z_G = R(G)_s$, and $\mathrm{X}^*(R(G))_F = \mathrm{X}^*(Z_G)_F = \mathrm{X}^*(Z_G)$ holds.

Proposition 10

Let $\boldsymbol{G}$ be a connected reductive $\boldsymbol{F}$-algebraic group. Then $\boldsymbol{\mathrm{X}^*(G/Z_G)_F = 0}$, and the restriction map

$$\boldsymbol{\mathrm{X}^*(G)_F \longrightarrow \mathrm{X}^*(Z_G)_F \,:\, \chi \mapsto \chi|_{Z_G}}$$

is injective. $\boldsymbol{\mathrm{X}^*(G)_F}$ is a finite index submodule of $\boldsymbol{\mathrm{X}^*(Z_G)_F}$.

Proof. Let $R(G)_a$ be the maximal F-anisotropic torus of $R(G)$. By Theorem 9(2),(4),

$$\mathrm{X}^*(R(G)/Z_G)_F \cong \mathrm{X}^*(R(G)_a/(R(G)_a \cap Z_G))_F \subset \mathrm{X}^*(R(G)_a)_F = 0.$$

Since $G/R(G)$ is semisimple, $\mathrm{X}^*(G/R(G))_F = 0$. From the exact sequence

$$0 \longrightarrow \mathrm{X}^*(G/R(G))_F \longrightarrow \mathrm{X}^*(G/Z_G)_F \longrightarrow \mathrm{X}^*(R(G)/Z_G)_F,$$

we have $\mathrm{X}^*(G/Z_G)_F = 0$. The restriction map yields an injection $\mathrm{X}^*(G)_F \hookrightarrow \mathrm{X}^*(Z_G)_F$. From the exact sequence

$$1 \longrightarrow D(G) \longrightarrow G \longrightarrow G/D(G) \longrightarrow 1$$

and $G/D(G)$ is isomorphic to $R(G)/(D(G) \cap R(G))$, we have

$$\mathrm{X}^*(G)_F \cong \mathrm{X}^*(R(G)/(D(G) \cap R(G)))_F.$$

Since $D(G) \cap R(G)$ is a finite group, $\mathrm{X}^*(D(G) \cap R(G))_F$ is a finite abelian group. From the exact sequence

$$0 \longrightarrow \mathrm{X}^*(R(G)/(D(G) \cap R(G)))_F \longrightarrow \mathrm{X}^*(R(G))_F \longrightarrow \mathrm{X}^*(D(G) \cap R(G))_F$$

and $\mathrm{X}^*(R(G))_F = \mathrm{X}^*(Z_G)_F$, the index $[\mathrm{X}^*(Z_G)_F : \mathrm{X}^*(G)_F]$ is finite. □

Example When $G = \mathrm{GL}_n$, $Z_G = Z_n$ and we have

$$\mathrm{X}^*(\mathrm{GL}_n)_{\mathbf{Q}} = \mathbf{Z} \cdot \det, \qquad \mathrm{X}^*(Z_n)_{\mathbf{Q}} = \mathbf{Z}\epsilon_1,$$

where $\epsilon_1(z) = a$ for $z = \mathrm{diag}(a, \ldots, a) \in Z_n$. Since $\det\big|_{Z_n} = n\epsilon_1$, we have

$$[\mathrm{X}^*(Z_n)_{\mathbf{Q}} : \mathrm{X}^*(\mathrm{GL}_n)_{\mathbf{Q}}] = n.$$

The image of $\mathrm{X}^*(\mathrm{GL}_n)_{\mathbf{Q}}$ under restriction is $n\mathbf{Z}\epsilon_1 \subset \mathbf{Z}\epsilon_1$.

3.5 Cocharacter Groups of Tori

Let T be an F-torus. An F-homomorphism

$$\xi : \mathbf{G}_m \longrightarrow T$$

is called an F**-cocharacter** of T. The set of all F-cocharacters is denoted by $\mathrm{X}_*(T)_F$. Addition is defined on $\mathrm{X}_*(T)_F$ by

$$(\xi_1 + \xi_2)(x) := \xi_1(x)\xi_2(x) \qquad (\xi_1, \xi_2 \in \mathrm{X}_*(T)_F, \ \ x \in \mathbf{G}_m)$$

making $\mathrm{X}_*(T)_F$ into a $\mathbf{Z}$-module. The composition of $\chi \in \mathrm{X}^*(T)_F$ and $\xi \in \mathrm{X}_*(T)_F$

$$\chi \circ \xi : \mathbf{G}_m \longrightarrow T \longrightarrow \mathbf{G}_m$$

is an F-character of $\mathbf{G}_m$. Let ϵ_1 be the identity map of $\mathbf{G}_m$. Then $\mathrm{X}^*(\mathbf{G}_m)_F = \mathbf{Z}\epsilon_1$, so for some $k \in \mathbf{Z}$,

$$\chi \circ \xi = k\epsilon_1.$$

If we set

$$\langle \chi, \xi \rangle = k,$$

this defines a pairing

$$\langle \cdot, \cdot \rangle : \mathrm{X}^*(T)_F \times \mathrm{X}_*(T)_F \longrightarrow \mathbf{Z}.$$

This pairing is non-degenerate, and $\mathrm{X}^*(T)_F$ and $\mathrm{X}_*(T)_F$ are dual modules to each other. That is,

$$\mathrm{X}_*(T)_F \cong \mathrm{Hom}_{\mathbf{Z}}(\mathrm{X}^*(T)_F, \mathbf{Z})$$

holds. From this, $\mathrm{X}_*(T)_F$ is also a free $\mathbf{Z}$-module with the same rank as $\mathrm{X}^*(T)_F$.

► A maximal F-split torus T_s of T is given as follows:

$$T_s = \text{the closed group generated by } \bigcup_{\xi \in \mathrm{X}_*(T)_F} \mathrm{Im}\, \xi.$$

► Let $X_{\mathbf{R}} = X^*(T)_F \otimes_{\mathbf{Z}} \mathbf{R}$ and $Y_{\mathbf{R}} = X_*(T)_F \otimes_{\mathbf{Z}} \mathbf{R}$. By extending the pairing $\langle \cdot, \cdot \rangle$ $\mathbf{R}$-linearly, a non-degenerate $\mathbf{R}$-bilinear map

$$\langle \cdot, \cdot \rangle : X_{\mathbf{R}} \times Y_{\mathbf{R}} \longrightarrow \mathbf{R}$$

can be defined. Separately, given an inner product

$$(\cdot, \cdot) : X_{\mathbf{R}} \times X_{\mathbf{R}} \longrightarrow \mathbf{R}$$

on $X_{\mathbf{R}}$, a natural $\mathbf{R}$-linear map

$$X_{\mathbf{R}} \longrightarrow Y_{\mathbf{R}} : v \mapsto v^*$$

is defined by the relation

$$\langle x, v^* \rangle = (x, v) \qquad (^\forall x \in X_{\mathbf{R}}).$$

In this sense, $Y_{\mathbf{R}}$ is often identified with $X_{\mathbf{R}}$.

Example By Example (1) in **3.2**, we have

$$X^*(\mathrm{T}_n)_F = \mathbf{Z}\epsilon_1 + \cdots + \mathbf{Z}\epsilon_n \,.$$

Take the inner product of $X^*(\mathrm{T}_n)_F \otimes_{\mathbf{Z}} \mathbf{R}$ such that $\epsilon_1, \ldots, \epsilon_n$ form an orthonomal basis. For $i = 1, \ldots, n$, define $\xi_i \in X_*(\mathrm{T}_n)_F$ by

$$\xi_i(a) := \mathrm{diag}(1, \ldots, 1, \overset{i}{\breve{a}}, 1, \ldots, 1) \qquad (a \in \mathbf{G}_m).$$

Then $\xi_1, \ldots, \xi_n$ is a dual basis of $\epsilon_1, \ldots, \epsilon_n$, and hence $\epsilon_i^* = \xi_i$ for $i = 1, \ldots, n$. Let $\alpha := \epsilon_i - \epsilon_{i+1}$. Then $\alpha^* = \xi_i - \xi_{i+1}$, i.e.,

$$\alpha^*(a) = \mathrm{diag}(1, \ldots, 1, \overset{i}{\breve{a}}, a^{-1}, 1, \ldots, 1).$$

As we shall see in **4.7**, α is a simple root of A_{n-1} type root system and α^* is identified with the coroot $\alpha^\vee$ defined in **4.6**.

§4 Root Systems of Reductive Algebraic Groups

4.1 Reflections

Definition Let V be a finite-dimensional real vector space. For $0 \neq a \in V$, a linear map $f : V \longrightarrow V$ is called a **reflection** with respect to a if it satisfies:

(1) $f(a) = -a$;

(2) there exists a hyperplane $W \subset V$ such that $f(w) = w$ for all $w \in W$.

► A reflection is a linear isomorphism. If E_V is the identity map on V, then $f \circ f = E_V$. From this, we can choose an inner product $(\cdot, \cdot)$ on V that is f-invariant, i.e.,

$$(f(u), f(v)) = (u, v) \qquad (u, v \in V).$$

With respect to this inner product, W becomes the orthogonal complement of a. Furthermore, f can be expressed as

$$f(v) = v - 2\frac{(v, a)}{(a, a)}a \qquad ({}^\forall v \in V).$$

4.2 Root Systems

Let X be a free $\mathbf{Z}$-module of finite rank, and let $\mathrm{X}_{\mathbf{R}} := X \otimes_{\mathbf{Z}} \mathbf{R}$ be the real vector space.

Definition For a subset $\Phi \subset \mathrm{X}$, (X, Φ) (or simply Φ) is called an **extended root system** (or generalized root system) if it satisfies the following conditions:

(1) Φ is a finite set, $0 \notin \Phi$, and Φ contains a basis of $X_{\mathbf{R}}$;

(2) if $\alpha \in \Phi$, then $-\alpha \in \Phi$;

(3) for each $\alpha \in \Phi$, the reflection $s_\alpha : \mathrm{X}_{\mathbf{R}} \longrightarrow \mathrm{X}_{\mathbf{R}}$ with respect to α satisfies

$$s_\alpha(\Phi) = \Phi, \qquad s_\alpha(\chi) - \chi \in \mathbf{Z}\alpha \quad ({}^\forall \chi \in \mathrm{X}).$$

► If Φ satisfies the stronger condition than (2):
(2′) if $\alpha \in \Phi$, then $\mathbf{Q}\alpha \cap \Phi = \{\pm\alpha\}$,
then Φ is called a **root system**. In an extended root system, we have

$$\alpha \in \Phi \implies \mathbf{Q}\alpha \cap \Phi \subset \left\{\pm\alpha, \pm\frac{1}{2}\alpha, \pm 2\alpha\right\}.$$

► If Φ is an extended root system, let

$$\Phi_{\mathrm{nd}} = \{\alpha \in \Phi \mid \alpha/2 \notin \Phi\}.$$

Then Φ_{nd} is a root system. Φ_{nd} is called the **reduced root system** of Φ.

4.3 Weyl Groups

Let (X, Φ) be an extended root system. Let $\mathrm{GL}(\mathrm{X}_{\mathbf{R}})$ denote the group of all linear automorphisms of $\mathrm{X}_{\mathbf{R}}$.

Definition The subgroup of $\mathrm{GL}(\mathrm{X}_{\mathbf{R}})$ generated by $\{s_\alpha \mid \alpha \in \Phi\}$ is called the **Weyl group** of Φ and is denoted by $W(\Phi)$.

► By (3), for any $w \in W(\Phi)$, we have $w(\Phi) = \Phi$. Thus, w induces a permutation of the elements of Φ. Let $\mathrm{Sym}(\Phi)$ be the permutation group of Φ. Then there is a homomorphism $W(\Phi) \longrightarrow \mathrm{Sym}(\Phi)$. Since w is a linear map and Φ contains a basis of $\mathrm{X}_{\mathbf{R}}$, this homomorphism is injective. Therefore, $W(\Phi)$ is a finite group.

► From (3), for any $w \in W(\Phi)$, we have $w(\mathrm{X}) \subset \mathrm{X}$. Thus, w is an automorphism of X. If we let $\mathrm{GL}(X) = \{f \in \mathrm{GL}(\mathrm{X}_{\mathbf{R}}) \mid f(X) = X\}$, then $W(\Phi) \subset \mathrm{GL}(X)$.

► Since $W(\Phi)$ is a finite group, $\mathrm{X}_{\mathbf{R}}$ has a $W(\Phi)$-invariant inner product. That is, there exists an inner product such that

$$(w(u), w(v)) = (u, v) \qquad ({}^\forall u, v \in \mathrm{X}_{\mathbf{R}},\ {}^\forall w \in W(\Phi)).$$

Then s_α can be written as

$$s_\alpha(v) = v - 2\frac{(v, \alpha)}{(\alpha, \alpha)}\alpha.$$

From (3),

$$c_{\alpha,\beta} := 2\frac{(\beta, \alpha)}{(\alpha, \alpha)} \in \mathbf{Z} \qquad ({}^\forall \alpha, \beta \in \Phi).$$

These $c_{\alpha,\beta}$ are called the **Cartan integers**.

Definition Consider $\mathrm{X}_{\mathbf{R}}$ as a Euclidean space with the inner product given above. Since $\mathrm{Ker}\, s_\alpha$ is a hyperplane in $\mathrm{X}_{\mathbf{R}}$,

$$\mathrm{X}_{\mathbf{R}} - \bigcup_{\alpha \in \Phi} \mathrm{Ker}\, s_\alpha$$

is an open set. Each connected component of this open set is called a **Weyl chamber**.

► A Weyl chamber C is an open cone. Let C^- be the closure of C in $X_{\mathbf{R}}$. Then

$$X_{\mathbf{R}} = \bigcup_{w \in W(\Phi)} w(C^-), \qquad C \cap wC = \emptyset \quad (^\forall w \in W(\Phi),\ w \neq e)$$

holds ([7, Ch.VI, n°1.5]).

4.4 Positive Roots and Simple Roots

Definition Let Φ be an extended root system, and fix a Weyl chamber C. An element $\alpha \in \Phi$ is called a **positive root** (with respect to C) if

$$(v, \alpha) > 0 \qquad (^\forall v \in C)$$

and is denoted by $\alpha > 0$. The set of all positive roots is denoted by $\Phi^+(C)$ or simply Φ^+. Furthermore, a positive root α is called a **simple root** if it cannot be expressed as the sum of two positive roots. The set of all simple roots is denoted by $\Delta(C)$ or simply Δ, and is called a **fundamental system** (or base) of Φ.

► Let $\Delta = \Delta(C) = \{\alpha_1, \ldots, \alpha_n\}$. The following hold ([7, Ch.VI, n°1.5]):

(1) Let $\Phi^- := \{-\alpha \mid \alpha \in \Phi^+\}$. Then $\Phi = \Phi^+ \cup \Phi^-$;

(2) Δ is a basis of $X_{\mathbf{R}}$;

(3) any positive root $\beta \in \Phi^+$ can be expressed as

$$\beta = \sum_{i=1}^{n} k_i \alpha_i \qquad (0 \leq k_i \in \mathbf{Z});$$

(4) $C = \{v \in X_{\mathbf{R}} \mid (v, \alpha_i) > 0 \quad (i = 1, \ldots, n)\}$ holds;

(5) W is generated by $\{s_{\alpha_i} \mid i = 1, \ldots, n\}$.

► The fundamental system $\Delta \subset \Phi^+$ is uniquely determined by the set of positive roots Φ^+. Conversely, the set of positive roots is determined by the fundamental system Δ via property (3) above.

4.5 Irreducible Root Systems

Definition Let (X, Φ) be an extended root system. Φ is called **reducible** if there exist non-empty subsets $\Phi_1, \Phi_2 \subset \Phi$ such that

$$\Phi = \Phi_1 \cup \Phi_2 \quad \text{and with respect to the inner product} \quad \Phi_1 \perp \Phi_2.$$

If Φ is not reducible, it is called **irreducible**.

► The classification of irreducible root systems is well-known. They are classified by connected Dynkin diagrams into types $A_n (n \geq 1), B_n (n \geq 2), C_n (n \geq 2), D_n (n \geq 4), G_2, F_4, E_6, E_7, E_8$.

► There is only one series of irreducible extended root systems Φ that are not root systems, called type $BC_n (n \geq 2)$. In this case, the reduced root system Φ_{nd} is of type C_n.

4.6 Lattices of a Root System

Let (X, Φ) be an extended root system, and let $\Delta = \{\alpha_1, \ldots, \alpha_n\}$ be a fundamental system. Let $X_{\mathbf{Q}} := X \otimes_{\mathbf{Z}} \mathbf{Q}$.

Definition For each $\alpha \in \Phi$, the element $\alpha^\vee := 2\alpha/(\alpha, \alpha) \in X_{\mathbf{Q}}$ is called a **coroot**. The set of all coroots is denoted by $\Phi^\vee$.

► The dual lattice $X^\vee$ of X in $X_{\mathbf{Q}}$ is defined as

$$X^\vee := \{\lambda \in X_{\mathbf{Q}} \mid (\lambda, \chi) \in \mathbf{Z} \quad (^\forall \chi \in X)\}.$$

Then $\Phi^\vee \subset X^\vee$, and $(X^\vee, \Phi^\vee)$ is an extended root system. This is called the **dual root system** of (X, Φ).

Definition The $\mathbf{Z}$-module generated by Φ within $X_{\mathbf{Q}}$ is called the **root lattice** and is denoted by $(\Phi)_{\mathbf{Z}}$. Let $(\Phi^\vee)_{\mathbf{Z}}$ be the $\mathbf{Z}$-module generated by $\Phi^\vee$. The dual lattice of $(\Phi^\vee)_{\mathbf{Z}}$ in $X_{\mathbf{Q}}$ is denoted by $(\Phi^\vee)^\vee_{\mathbf{Z}}$. That is,

$$(\Phi^\vee)^\vee_{\mathbf{Z}} = \{\lambda \in X_{\mathbf{Q}} \mid (\lambda, \alpha^\vee) \in \mathbf{Z} \quad (^\forall \alpha^\vee \in \Phi^\vee)\}$$

$(\Phi^\vee)^\vee_{\mathbf{Z}}$ is called the **weight lattice**.

► From condition (3) in the definition of an extended root system, we have the inclusion relation

$$(\Phi)_{\mathbf{Z}} \subset X \subset (\Phi^\vee)^\vee_{\mathbf{Z}} \subset X_{\mathbf{Q}}.$$

Let Y be a free module such that $(\Phi)_{\mathbf{Z}} \subset Y \subset (\Phi^\vee)^\vee_{\mathbf{Z}}$. Then (Y, Φ) is an extended root system.

4.7 Root Systems of a Reductive Algebraic Group

Consider a non-commutative connected reductive F-algebraic group G. Fix a maximal F-split torus T of G and a maximal F-torus $T_{\max}$ containing T.

Definition A rational character $\alpha \in X^*(T_{\max})$ is called a **root** (of G with respect to $T_{\max}$) if there exists an injective $\overline{F}$-homomorphism

$$u_\alpha : \mathbf{G}_a \longrightarrow G$$

such that

$$tu_\alpha(x)t^{-1} = u_\alpha(\alpha(t)x) \qquad (^\forall x \in \mathbf{G}_a, \ ^\forall t \in T_{\max})$$

holds. The set of all roots is denoted by $\Phi(G, T_{\max})$ and is called the **absolute root system** (of G with respect to $T_{\max}$).

Since T is an F-split torus, $X^*(T) = X^*(T)_F$. From $T \subset T_{\max}$, a homomorphism

$$\rho : X^*(T_{\max}) \longrightarrow X^*(T) : \rho(\chi) = \chi|_T$$

can be defined. ρ is called the restriction map.

Definition The set $\rho(\Phi(G, T_{\max}))$ excluding 0 is denoted by $\Phi_F(G, T)$ or Φ_F, and is called the **relative root system** (of G with respect to T).

► If F is algebraically closed or if G is an F-split group, then $T_{\max} = T$, so in this case $\Phi(G, T) = \Phi_F(G, T)$ holds.

► Let $R(G)$ be the radical of G. $R(G) = C_G^\circ$ is a torus and $R(G) \subset T_{\max}$. If $t \in C_G^\circ$, then

$$tu_\alpha(x) = u_\alpha(x)t \qquad \text{i.e.,} \quad \alpha|_{R(G)} = 0 \qquad (^\forall \alpha \in \Phi(G, T_{\max})).$$

Thus, $\Phi(G, T_{\max})$ can be regarded as a subset of $X^*(T_{\max}/R(G))$. Similarly, let Z_G be the central maximal F-split torus of G. Then $\Phi_F(G, T)$ can be regarded as a subset of $X^*(T/Z_G)_F$.

► If G/Z_G is F-anisotropic (i.e., $T = Z_G$), then $\Phi_F(G, T) = \emptyset$.

Theorem 11 ([2, 21.6])

Let $\boldsymbol{\Phi = \Phi(G, T_{\max})}$ *and* $\boldsymbol{\Phi_F = \Phi_F(G, T)}$.

(1) $\boldsymbol{(X^*(T_{\max}/R(G)), \Phi)}$ *is a root system.*

(2) *If* $\boldsymbol{\Phi_F \neq \emptyset}$, *then* $\boldsymbol{(X^*(T/Z_G), \Phi_F)}$ *is an extended root system.*

► In general, $X^*(T_{\max})$ and $X^*(T_{\max}/R(G))$ have different ranks. In that case, the fundamental system of Φ does not form a basis for the vector space $X^*(T_{\max}) \otimes \mathbf{R}$.

Example The characters ϵ_i of T_n were defined by

$$\epsilon_i(\mathrm{diag}(a_1, \ldots, a_n)) = a_i \qquad (i = 1, \ldots, n).$$

For $1 \le i, j \le n,\ i \ne j$, let $e_{ij} \in \mathrm{M}_n(\mathbf{Q})$ be the matrix with a 1 in the (i, j) position and 0s elsewhere. Define

$$u_{ij} : \mathbf{G}_a \longrightarrow \mathrm{GL}_n : u_{ij}(x) := E_n + xe_{ij}.$$

A simple calculation shows that

$$tu_{ij}(x)t^{-1} = u_{ij}(\epsilon_i(t)\epsilon_j(t)^{-1}x) \qquad (^\forall x \in \mathbf{G}_a,\ \ ^\forall t \in \mathrm{T}_n).$$

Therefore, $\epsilon_i - \epsilon_j (= \epsilon_i\epsilon_j^{-1})$ is a $\mathbf{Q}$-root.

$$\Phi_{\mathbf{Q}}(\mathrm{GL}_n, \mathrm{T}_n) = \Phi(\mathrm{GL}_n, \mathrm{T}_n) = \{\epsilon_i - \epsilon_j \mid 1 \le i, j \le n,\ \ i \ne j\}$$

is a root system of type A_{n-1}.

$$\Delta = \{\epsilon_i - \epsilon_{i+1} \mid i = 1, \ldots, n-1\}$$

provides one fundamental system.

4.8 Classification of Connected Semisimple Split Groups

Definition Let X and X′ be free $\mathbf{Z}$-modules of the same finite rank, and let (X, Φ) and (X', Φ') be root systems. An injective homomorphism $f : \mathrm{X}' \longrightarrow \mathrm{X}$ is called a **special homomorphism** from (X', Φ') to (X, Φ) if there exists a bijection $\psi : \Phi \longrightarrow \Phi'$ such that $f(\psi(\alpha)) = \alpha$ $(^\forall \alpha \in \Phi)$.

► The definition above is for characteristic 0. Over a field of characteristic p, the condition is changed to $f(\psi(\alpha)) = q_\alpha \alpha$ (where q_α is a power of p).

► If there exists a module isomorphism $f : \mathrm{X} \longrightarrow \mathrm{X}'$ such that $f(\Phi) = \Phi'$ between two root systems (X, Φ) and (X', Φ'), we denote this by $(\mathrm{X}, \Phi) \cong (\mathrm{X}', \Phi')$.

Theorem 12 ([8, exposé 23, exposé 24])

Let $\boldsymbol{G}$ and $\boldsymbol{G'}$ be connected semisimple algebraic groups, and let $\boldsymbol{T} \subset \boldsymbol{G}$ and $\boldsymbol{T'} \subset \boldsymbol{G'}$ be maximal tori. Let $\mathbf{X} = \mathbf{X}^*(\boldsymbol{T})$, $\mathbf{X'} = \mathbf{X}^*(\boldsymbol{T'})$, and let their respective absolute root systems be $\boldsymbol{\Phi} = \boldsymbol{\Phi}(\boldsymbol{G}, \boldsymbol{T})$, $\boldsymbol{\Phi'} = \boldsymbol{\Phi}(\boldsymbol{G'}, \boldsymbol{T'})$.

(1) *(Isogeny Theorem) If a special homomorphism $\boldsymbol{f} : \mathbf{(X', \Phi')} \longrightarrow \mathbf{(X, \Phi)}$ exists, then there exists an isogeny $\boldsymbol{\varphi} : \boldsymbol{G} \longrightarrow \boldsymbol{G'}$ such that $\boldsymbol{T'} = \boldsymbol{\varphi}(\boldsymbol{T})$ and $\mathbf{(\varphi|_T)^* = f}$. Furthermore, if $\boldsymbol{\psi} : \boldsymbol{G} \longrightarrow \boldsymbol{G'}$ is another isogeny satisfying the same conditions, then there exists some $\boldsymbol{t} \in \boldsymbol{T}$ such that $\boldsymbol{\psi(g) = \varphi(tgt^{-1})}$ for all $\boldsymbol{g} \in \boldsymbol{G}$.*

(2) *(Isomorphism Theorem) If there exists an isomorphism $\boldsymbol{\varphi_T} : \boldsymbol{T} \longrightarrow \boldsymbol{T'}$ such that $\boldsymbol{\varphi_T^*}$ yields an isomorphism $\mathbf{(X', \Phi') \cong (X, \Phi)}$, then $\boldsymbol{\varphi_T}$ can be extended to an isomorphism $\boldsymbol{\varphi} : \boldsymbol{G} \longrightarrow \boldsymbol{G'}$.*

Theorem 13 (Existence Theorem [9])

Let $\mathbf{F}$ be an arbitrary field. Let $\mathbf{X}$ be a free $\mathbf{Z}$-module of finite rank, and let $(\mathbf{X}, \mathbf{\Phi})$ be a root system. Let $\mathbf{Y}$ be a free $\mathbf{Z}$-module such that $(\mathbf{\Phi})_{\mathbf{Z}} \subset \mathbf{Y} \subset (\mathbf{\Phi}^\vee)^\vee_{\mathbf{Z}}$. Then there exists a connected semisimple $\mathbf{F}$-split group $\mathbf{G}$ with a maximal $\mathbf{F}$-split torus $\mathbf{T}$ such that $(\mathbf{Y}, \mathbf{\Phi}) \cong (\mathbf{X}^*(\mathbf{T})_{\mathbf{F}}, \mathbf{\Phi}_{\mathbf{F}}(\mathbf{G}, \mathbf{T}))$, and such $\mathbf{G}$ is unique up to $\mathbf{F}$-isomorphism.

► In Theorem 13, the choice of Y is finite. The group G_{sc} corresponding to the weight lattice $(\Phi^\vee)^\vee_{\mathbf{Z}}$ is called the **simply connected group**, and the group G_{ad} corresponding to the root lattice $(\Phi)_{\mathbf{Z}}$ is called the **adjoint group**. In general, since $(\Phi)_{\mathbf{Z}} \subset Y \subset (\Phi^\vee)^\vee_{\mathbf{Z}}$, there are natural isogenies $G_{\mathrm{sc}} \longrightarrow G$ and $G \longrightarrow G_{\mathrm{ad}}$ by the Isogeny Theorem. The finite group $\pi_1(G) := (\Phi^\vee)^\vee_{\mathbf{Z}}/Y$ is called the fundamental group of G.

► An algebraic group G is said to be **almost simple** if $\{e\}$ is the only proper connected normal closed subgroup of G. If G is a connected almost simple algebraic group, then G is semisimple and its absolute root system is an irreducible root system ([2, 14.10]).

► Let G be a connected semisimple algebraic group. Then there is a finite set $\{G_1, \ldots, G_m\}$ of connected almost simple normal closed subgroup of G such that the product morphism $G_1 \times \cdots \times G_m \longrightarrow G$ is an isogeny ([2, 14.10]).

► Let G be a connected semisimple $\mathbf{Q}$-algebraic group, and let $(X, \Phi) = (X^*(T_{\max}), \Phi(G, T_{\max}))$. By Theorem 13, there exists uniquely (up to $\mathbf{Q}$-isomorphism) a connected semisimple $\mathbf{Q}$-split group G_0 and its maximal $\mathbf{Q}$-split torus T_0 such that $(X, \Phi) \cong (X^*(T_0)_{\mathbf{Q}}, \Phi_{\mathbf{Q}}(G_0, T_0))$. Over $\overline{\mathbf{Q}}$, we have $T_{\max} \cong T_0$, so by the Isomorphism Theorem, there exists a $\overline{\mathbf{Q}}$-isomorphism $G \cong G_0$. Connected semisimple $\mathbf{Q}$-split groups can be classified by their root systems (Dynkin diagrams) and fundamental groups. For a given G_0, a $\mathbf{Q}$-algebraic group G such that $G \cong G_0$ over $\overline{\mathbf{Q}}$ is called a **$\mathbf{Q}$-form** of G_0. Using Galois cohomology sets and relative root systems, $\mathbf{Q}$-forms can be classified and described.

§5 Bruhat Decomposition

Let G be a connected reductive F-algebraic group, $T \subset G$ be a maximal F-split torus, $T_{\max}$ be a maximal F-torus containing T, and let $\mathrm{X} = \mathrm{X}^*(T/Z_G)_F$. Let $\Phi = \Phi(G, T_{\max})$ and $\Phi_F = \Phi_F(G, T)$ be the absolute and relative root systems of G, respectively.

5.1 The Normalizer of T

Let $C_G(T)$ and $N_G(T)$ be the centralizer and the normalizer of T as an abstract group, respectively. Then the following holds.

Theorem 14 ([2, 8.10, 21.2])

$\boldsymbol{N_G(T)}$ is an $\boldsymbol{F}$-algebraic group. $\boldsymbol{C_G(T)}$ is a connected reductive $\boldsymbol{F}$-algebraic group and is the identity component of $\boldsymbol{N_G(T)}$. In particular, the quotient group $\boldsymbol{N_G(T)/C_G(T)}$ is a finite group. Also, a representative for each coset of $\boldsymbol{N_G(T)/C_G(T)}$ can be chosen from $\boldsymbol{N_G(T)(F)}$.

Denote the finite group $N_G(T)/C_G(T)$ by $W(G, T)$, and let the representative g of each coset $[g] = gC_G(T)$ be an element of $N_G(T)(F)$. Each $w = [g] \in W(G, T)$ yields an inner automorphism $i_w : T \longrightarrow T : i_w(t) = gtg^{-1}$. This is an F-isomorphism. From this, for $\chi \in \mathrm{X}^*(T)_F$, if we define $w\chi$ as

$$(w\chi)(t) := \chi(i_w^{-1}(t)) = \chi(g^{-1}tg) \qquad (t \in T),$$

then $w\chi \in \mathrm{X}^*(T)_F$. For $w' = [g'] \in W(G, T)$,

$$(w'w\chi)(t) = \chi((g'g)^{-1}t(g'g)) = (w\chi)(g'^{-1}tg') = \{w'(w\chi)\}(t)$$

holds, therefore

$$W(G, T) \times \mathrm{X}^*(T)_F \longrightarrow \mathrm{X}^*(T)_F : (w, \chi) \mapsto w\chi$$

provides an action of $W(G, T)$ on $\mathrm{X}^*(T)_F$. Clearly, i_w is the identity map on Z_G, so $W(G, T)$ also acts on $\mathrm{X} = \mathrm{X}^*(T/Z_G)_F$. From this, we can regard $W(G, T) \subset \mathrm{GL}(X)$.

Theorem 15 ([2, 21.2])

As a subgroup of $\mathbf{GL(X)}$, $\boldsymbol{W(G, T)}$ is equal to the Weyl group $\boldsymbol{W(\Phi_F)}$ of $\boldsymbol{\Phi_F}$.

▶ Denote the coset corresponding to $w \in W(\Phi_F)$ by $[n_w] \in W(G, T)$, $n_w \in N_G(T)(F)$.

5.2 Standard Parabolic Subgroups

From the definition of absolute roots, for each $\delta \in \Phi$, there exists a unipotent $\overline{F}$-subgroup

$$U_\delta = u_\delta(\mathbf{G}_a) \subset G.$$

Let $\rho : \Phi \longrightarrow \Phi_F \cup \{0\}$ be the restriction map. Fix a base Δ_F of Φ_F, and let Φ_F^+ be the set of positive roots. For a subset $I \subset \Delta_F$, let $(I)_{\mathbf{Z}}$ be the sub-$\mathbf{Z}$-module of X generated by I, and further define

$$[I] := (I)_{\mathbf{Z}} \cap \Phi_F,$$
$$\Phi^+(\Delta_F \setminus I) := \rho^{-1}(\Phi_F^+ - [I]) = \{\delta \in \Phi \mid \rho(\delta) \in \Phi_F^+, \ \ \rho(\delta) \notin [I]\}.$$

Define subsets T_I, M_I, U_I of G as follows.

- Since each $\alpha \in I$ is a character $\alpha : T \longrightarrow T$, its kernel $\operatorname{Ker}\alpha \subset T$ is a closed subgroup. Let the identity component of the intersection of $\operatorname{Ker}\alpha$ ($\alpha \in I$) be
$$T_I := \left(\bigcap_{\alpha \in I} \operatorname{Ker}\alpha\right)^\circ.$$
T_I becomes an F-split torus. (If $I = \emptyset$, let $T_\emptyset = T$.)
- Let the centralizer of T_I in G be $M_I := C_G(T_I)$. Then $T \subset T_{\max} \subset M_I$.
- Let $\Phi^+(\Delta_F \setminus I) = \{\delta_1, \ldots, \delta_k\}$. Define
$$U_I := \prod_{i=1}^{k} U_{\delta_i} = \{g_1 \cdots g_k \mid g_i \in U_{\delta_i} \quad (i = 1, \ldots, k)\}.$$

Theorem 16 ([2, 21.9, 21.11, 21.12])

(1) *$\boldsymbol{M_I}$ is a connected reductive $\boldsymbol{F}$-subgroup of $\boldsymbol{G}$, and its relative root system with respect to $\boldsymbol{T}$ is $\boldsymbol{\Phi_F(M_I, T) = [I]}$.*

(2) *$\boldsymbol{U_I}$ is determined independently of the numbering of the elements of $\boldsymbol{\Phi^+(\Delta_F \setminus I)}$. $\boldsymbol{U_I}$ is a unipotent $\boldsymbol{F}$-subgroup of $\boldsymbol{G}$.*

(3) *Let $\boldsymbol{P_I := M_I U_I = \{mu \mid m \in M_I, \ u \in U_I\}}$. Then $\boldsymbol{P_I}$ is a parabolic $\boldsymbol{F}$-subgroup of $\boldsymbol{G}$. $\boldsymbol{M_I}$ is a Levi subgroup of $\boldsymbol{P_I}$, and $\boldsymbol{U_I}$ is the unipotent radical of $\boldsymbol{P_I}$.*

(4) *Let $\boldsymbol{I}$ and $\boldsymbol{J}$ be two distinct subsets of $\boldsymbol{\Delta_F}$. Then $\boldsymbol{P_I \neq P_J}$ and $\boldsymbol{P_I \cap P_J = P_{I \cap J}}$ hold. In particular, $\boldsymbol{P_\Delta = G}$, and for any $\boldsymbol{I}$, $\boldsymbol{P_\emptyset \subset P_I \subset P_\Delta}$ holds.*

(5) *Let $\boldsymbol{Q \subset G}$ be an arbitrary parabolic $\boldsymbol{F}$-subgroup. Then there exist $\boldsymbol{I \subset \Delta}$ and $\boldsymbol{g \in G(F)}$ such that $\boldsymbol{Q = g^{-1} P_I g}$. $\boldsymbol{I}$ is uniquely determined by $\boldsymbol{Q}$.*

Definition Each P_I is called a **standard parabolic F-subgroup** of G. Also, $P_{\Delta_F-\{\alpha\}}$ ($\alpha \in \Delta_F$) is called a **standard maximal parabolic F-subgroup**.

► $P_\emptyset$ and its conjugates are minimal among the parabolic F-subgroups of G, and are thus called **minimal parabolic F-subgroups**. If F is an algebraically closed field or G is an F-split group, then $P_\emptyset$ is a Borel subgroup of G.

► If $I = \Delta$, then

$$T_\Delta = \left(\bigcap_{\alpha\in\Delta} \mathrm{Ker}\,\alpha\right)^\circ = Z_G$$

holds. Therefore, $M_I = C_G(Z_G) = G$.

Example Consider the base of the root system $\Phi = \Phi_{\mathbf{Q}} = \Phi_{\mathbf{Q}}(\mathrm{GL}_n, \mathrm{T}_n)$ of GL_n:

$$\Delta = \{\alpha_i = \epsilon_i - \epsilon_{i+1} \mid i = 1, \ldots, n-1\}.$$

Fix α_r, and let $I = \Delta - \{\alpha_r\}$. Then

$$T_I = \left(\bigcap_{i\neq r} \mathrm{Ker}\,\alpha_i\right)^\circ = \left\{\begin{pmatrix} aE_r & 0 \\ 0 & dE_{n-r}\end{pmatrix} \mid a, d \in \mathbf{G}_m\right\}.$$

Therefore

$$M_I = \left\{\begin{pmatrix} A & 0 \\ 0 & D\end{pmatrix} \mid A \in \mathrm{GL}_r,\ D \in \mathrm{GL}_{n-r}\right\}.$$

The set of positive roots of Φ is

$$\begin{aligned}\Phi^+ &= \{\epsilon_i - \epsilon_j \mid 1 \le i < j \le n\} \\ &= \{\alpha_i + \cdots + \alpha_{i+k} \mid 1 \le i \le n-1,\ 0 \le k \le n-i-1\}.\end{aligned}$$

Thus

$$\begin{aligned}\Phi^+(\Delta \setminus I) &= \{\alpha_i + \cdots + \alpha_{i+k} \mid 1 \le i \le r,\ r-i \le k \le n-i-1\} \\ &= \{\epsilon_i - \epsilon_j \mid 1 \le i \le r,\ r+1 \le j \le n\}.\end{aligned}$$

Hence

$$U_I = \left\{\begin{pmatrix} E_r & B \\ 0 & E_{n-r}\end{pmatrix} \mid B \in \mathrm{M}_{r,n-r}(\overline{\mathbf{Q}})\right\}.$$

From this

$$P_I = \left\{\begin{pmatrix} A & B \\ 0 & D\end{pmatrix} \mid A \in \mathrm{GL}_r,\ D \in \mathrm{GL}_{n-r},\ B \in \mathrm{M}_{r,n-r}(\overline{\mathbf{Q}})\right\} = \mathrm{Q}_{n,r}$$

is obtained.

► Let $P = MU$ be a Levi decomposition of a parabolic F-subgroup P. Then, for the group of F-rational points,

$$P(F) = M(F)U(F), \qquad (G/P)(F) = G(F)/P(F)$$

holds([2, Proposition 20.5]).

5.3 Bruhat Decomposition

Let $W_F = W(\Phi_F) = \{[n_w] \in W(G,T)\}$ be the Weyl group of Φ_F. For each $\alpha \in \Phi_F$, there is a reflection $s_\alpha \in W_F$, and W_F is generated by $\{s_\alpha\}_{\alpha\in\Delta_F}$. For a subset $I \subset \Delta_F$, denote the subgroup of W_F generated by $\{s_\alpha\}_{\alpha\in I}$ as $W_F(I)$. (However, if $I = \emptyset$, let $W_F(\emptyset) = \{e\}$.) For two subsets $I, J \subset \Delta_F$, denote an element of the double cosets $W_F(I)\backslash W_F/W_F(J)$ as $[w]_{I,J} = W_F(I)wW_F(J)$. Let $P = P_\emptyset$ be the standard minimal parabolic F-subgroup of G.

Theorem 17 (Bruhat Decomposition [2, 21.15, 21.16])

For the group of $\boldsymbol{F}$*-rational points* $\boldsymbol{G(F)}$*,*

$$\boldsymbol{G(F) = \bigsqcup_{w\in W_F} P(F)n_wP(F) = \bigsqcup_{[w]_{I,J}\in W_F(I)\backslash W_F/W_F(J)} P_I(F)n_wP_J(F)}$$

holds, where each union of double cosets is a disjoint union.

▶ Let $M = M_\emptyset$ and $U = U_\emptyset$. Then, since $T_\emptyset = T$, we have $M = C_G(T)$. Since $C_G(T)$ is a normal subgroup of $N_G(T)$, for $n_w \in N_G(T)(F)$, $n_wM(F) = M(F)n_w$ holds. Therefore, we have

$$P(F)n_wP(F) = U(F)n_wP(F) = P(F)n_wU(F).$$

Example In the case of GL_n, $W_{\mathbf{Q}} \cong S_n$ (the n-th symmetric group), and the representatives of $W(\mathrm{GL}_n, \mathrm{T}_n)$ can be taken as follows. Let e_i be the i-th column of the identity matrix E_n. For $\sigma \in S_n$ as a permutation of $\{1, 2, \ldots, n\}$, define the matrix

$$n_\sigma = (e_{\sigma(1)}, e_{\sigma(2)}, \ldots, e_{\sigma(n)}) \in \mathrm{GL}_n(\mathbf{Q}).$$

Then,

$$W(\mathrm{GL}_n, \mathrm{T}_n) = \{[n_\sigma] \mid \sigma \in S_n\}.$$

Therefore, the Bruhat decomposition of GL_n is

$$\mathrm{GL}_n(\mathbf{Q}) = \bigsqcup_{\sigma\in S_n} \mathrm{B}_n(\mathbf{Q})n_\sigma\mathrm{B}_n(\mathbf{Q})$$

where B_n is the standard Borel subgroup of upper triangular matrices.

§6 Algebraic Groups over Local Fields

6.1 Locally Compact Groups

Definition Let L be a group. L is called a **locally compact group** if it satisfies the conditions:

(1) L is a locally compact Hausdorff topological space;

(2) the map $L \times L \longrightarrow L : (x, y) \mapsto xy^{-1}$ is continuous.

Furthermore, if L is a real analytic (or complex analytic) manifold and the map in (2) is real analytic (or complex analytic), then L is called a **Lie group** (or **complex Lie group**).

Examples
(1) (**p-adic field**) Fix a prime number p. For any $0 \neq n \in \mathbf{Z}$, if $n = p^k n'$ where $p \nmid n'$, define

$$|n|_p := p^{-k}$$

and furthermore, for any rational number $n/m \in \mathbf{Q}$, define

$$|n/m|_p := |n|_p |m|_p^{-1}, \qquad |0|_p = 0.$$

This defines the norm $|\cdot|_p : \mathbf{Q} \longrightarrow \mathbf{R}$. Then

$$d_p : \mathbf{Q} \times \mathbf{Q} \longrightarrow \mathbf{R} : d_p(x, y) = |x - y|_p$$

becomes a metric. Let R_p be the set of all Cauchy sequences in $\mathbf{Q}$ with respect to d_p. Define addition and multiplication on R_p by

$$\{a_i\} + \{b_i\} = \{a_i + b_i\}, \quad \{a_i\} \cdot \{b_i\} = \{a_i b_i\} \qquad (\{a_i\}, \{b_i\} \in R_p).$$

Then R_p becomes a commutative ring. Furthermore, let

$$I_p := \{\{a_i\} \in R_p \mid \lim_{i \to \infty} a_i = 0\}.$$

Then I_p is a maximal ideal. Therefore, R_p/I_p is a field. We denote this by $\mathbf{Q}_p = R_p/I_p$ and call it the p-adic field. $\mathbf{Q}_p$ is the completion of $\mathbf{Q}$ with respect to d_p. Any $a \in \mathbf{Q}_p$ has the following unique representation:

$$a = \sum_{i=k}^{\infty} a_i p^i, \qquad a_i \in \{0, 1, \ldots, p-1\}.$$

By defining $|a|_p = p^{-k}$ in this case, the norm can be extended to $\mathbf{Q}_p$. Let $\mathbf{Z}_p$ be the closure of $\mathbf{Z}$ in $\mathbf{Q}_p$. Then $\mathbf{Z}_p = \{a \in \mathbf{Q}_p \mid |a|_p \leq 1\}$, and $\mathbf{Z}_p$ is an open and compact subring. The group of units of $\mathbf{Z}_p$ is

$$\mathbf{Z}_p^\times = \{a \in \mathbf{Z}_p \mid |a|_p = 1\} = \mathbf{Z}_p - p\mathbf{Z}_p$$

and $p\mathbf{Z}_p = \{a \in \mathbf{Z}_p \,|\, |a|_p < 1\}$ is the unique maximal ideal of $\mathbf{Z}_p$. Also, we have

$$\mathbf{Q}_p^\times = p^{\mathbf{Z}} \cdot \mathbf{Z}_p^\times = \{p^k u \,|\, k \in \mathbf{Z},\ u \in \mathbf{Z}_p^\times\}.$$

$\{p^n \mathbf{Z}_p\}_{n\in\mathbf{Z}}$ provides a fundamental system of neighborhoods of 0 in $\mathbf{Q}_p$. In particular, $\mathbf{Q}_p$ becomes a locally compact topological field, and the multiplicative group $\mathbf{Q}_p^\times$ becomes a locally compact topological group.

(2) Let $\mathcal{P}_f$ be the set of all prime numbers, consider the symbol ∞ formally, and let $\mathcal{P} = \mathcal{P}_f \cup \{\infty\}$. The elements of $\mathcal{P}$ are called the primes (or **places**) of $\mathbf{Q}$. Hereafter, when we write $q \in \mathcal{P}$ or $q \leq \infty$, it means q is a prime number or ∞. We define $\mathbf{Q}_q$ as the p-adic field if $q = p$ is a prime number, and $\mathbf{Q}_\infty = \mathbf{R}$ if $q = \infty$. $\mathbf{Q}_q$ is called a **local field**. $\mathbf{Q}_q$ is a locally compact field. By the product topology, $\mathrm{M}_n(\mathbf{Q}_q) = \mathbf{Q}_q^{n^2}$ also becomes a locally compact topological space. By endowing $\mathrm{GL}_n(\mathbf{Q}_q) \subset \mathrm{M}_n(\mathbf{Q}_q)$ with the relative topology, $\mathrm{GL}_n(\mathbf{Q}_q)$ becomes a locally compact topological group. To distinguish it from the Zariski topology, we call the topology of the locally compact group $\mathrm{GL}_n(\mathbf{Q}_q)$ the **q-topology**. If $L \subset \mathrm{GL}_n(\mathbf{Q}_q)$ is a closed subgroup with respect to the q-topology, then L is also a locally compact group.

(3) Let $G \subset \mathrm{GL}_n$ be a closed subgroup defined over $\mathbf{Q}$. Since G is given as the zero set of a finite number of polynomials with $\mathbf{Q}$ coefficients, for any $q \in \mathcal{P}$, $G(\mathbf{Q}_q)$ is a closed set of $\mathrm{GL}_n(\mathbf{Q}_q)$ with respect to the q-topology. Given that the group operation is defined by polynomial maps defined over $\mathbf{Q}$, it is continuous in the q-topology. Therefore, the set of $\mathbf{Q}_q$-rational points $G(\mathbf{Q}_q)$ of a $\mathbf{Q}$-algebraic group G becomes a locally compact group with respect to the q-topology.

► If G is a $\mathbf{Q}$-algebraic group and p is a prime number, then $G(\mathbf{Q}_p)$ is **totally disconnected** with respect to the p-topology. That is, for any neighborhood U of the identity element in $G(\mathbf{Q}_p)$, there exists an open compact subgroup L such that $L \subset U$.

► Even if G is a connected $\mathbf{Q}$-algebraic group, $G(\mathbf{Q}_\infty)$ is not necessarily connected with respect to the ∞-topology.

► If $G \subset \mathrm{GL}_n$ is a connected algebraic group, then $G = G(\mathbf{C})$ is a connected complex Lie group with respect to the topology induced from the complex Lie group $\mathrm{GL}_n(\mathbf{C})$. Conversely, if G is a connected complex Lie group and $\mathfrak{g}$ is its Lie algebra, then

G is an algebraic group $\iff$ the replica of any element of $\mathfrak{g}$ is contained in $\mathfrak{g}$

holds (Chevalley-Tuan theorem, [11]).

► If L is a compact Lie group, then there exists an algebraic group G defined over $\mathbf{R}$ such that $L = G(\mathbf{R})$ (Chevalley's version of **Tannaka duality** [10, Chapter VI]).

Theorem 18 (Existence of Invariant Measures)

*Let $\boldsymbol{L}$ be a locally compact group, and let $\boldsymbol{\mathcal{B}}$ be the Borel $\boldsymbol{\sigma}$-algebra of $\boldsymbol{L}$ (i.e., the smallest $\boldsymbol{\sigma}$-algebra containing all open sets of $\boldsymbol{L}$). There exists a measure $\boldsymbol{\mu_\ell : \mathcal{B} \longrightarrow [0,\infty]}$ on $\boldsymbol{L}$, unique up to a positive constant factor, such that $\boldsymbol{\mu_\ell(gB) = \mu_\ell(B)}$ for all $\boldsymbol{B \in \mathcal{B}}$ and $\boldsymbol{g \in L}$, and $\boldsymbol{\mu_\ell(U) > 0}$ for any open set $\boldsymbol{U}$. ($\boldsymbol{\mu_\ell}$ is called a **left invariant measure** on $\boldsymbol{L}$.)*

► Theorem 18 is well-known. Invariant measures are also called Haar measures. We can paraphrase left as right, i.e., a locally compact group has a non-trivial right invariant measure uniquely up to a positive constant factor.

► For $g \in L$, if we define $\mu_{\ell,g}(B) = \mu_\ell(Bg)$ ($B \in \mathcal{B}$), then $\mu_{\ell,g}$ is also a left invariant measure. By uniqueness, there exists a positive constant $\Delta(g) > 0$ such that $\mu_{\ell,g} = \Delta(g)\mu_\ell$. $\Delta : L \longrightarrow (0,\infty)$ is a continuous homomorphism. This Δ is called the **modular character** (or modular function). When $\Delta = 1$, μ_ℓ is also a right invariant measure. Such an L is called a **unimodular group**.

► Let L be a compact group. In this case, $\Delta(L) \subset (0,\infty)$ is compact, so $\Delta(L) = \{1\}$ holds. Therefore, compact groups are unimodular.

6.2 Maximal Compact Subgroups

Definition Let L be a locally compact group. A non-trivial subgroup K of L is called a **maximal compact subgroup** if K is compact and there exists no compact subgroup that properly contains K.

► If the only compact subgroup of L is $\{e\}$, or if L has an infinite ascending chain of compact subgroups, then L is said to have no maximal compact subgroup.

Theorem 19 ([21, Propositions 3.10, 3.15 and 3.16, Theorem 3.1])

Fix $\boldsymbol{q \in \mathcal{P}}$. Let $\boldsymbol{G}$ be a connected $\mathbf{Q}_q$-algebraic group, and let $\boldsymbol{G(\mathbf{Q}_q)}$ be a locally compact group.

(1) *$\boldsymbol{G(\mathbf{Q}_q)}$ has a maximal compact subgroup if and only if $\boldsymbol{G}$ is reductive.*

(2) *If $\boldsymbol{G}$ is reductive and $\boldsymbol{K \subset G(\mathbf{Q}_q)}$ is a compact subgroup, then there exists a maximal compact subgroup containing $\boldsymbol{K}$.*

(3) *If $\boldsymbol{G}$ is reductive and $\boldsymbol{q = \infty}$, then all maximal compact subgroups of $\boldsymbol{G(\mathbf{R})}$ are conjugate by elements of $\boldsymbol{G(\mathbf{R})}$.*

(4) *$\boldsymbol{G(\mathbf{Q}_q)}$ is compact if and only if $\boldsymbol{G}$ is reductive and $\mathbf{Q}_q$-anisotropic.*

► If G is reductive and $q = p$ is a prime number, the conjugacy classes of maximal compact subgroups of $G(\mathbf{Q}_p)$ under conjugation by elements of $G(\mathbf{Q}_p)$ are generally not unique. Therefore, there may exist multiple non-conjugate maximal compact subgroups.

Examples

(1) Let the group consisting of all orthogonal matrices be

$$\mathrm{O}_n(\mathbf{R}) := \{g \in \mathrm{GL}_n(\mathbf{R}) \mid {}^t g g = E_n\}.$$

This is a maximal compact subgroup of $\mathrm{GL}_n(\mathbf{R})$.

(2) Denote the group of units of the matrix ring $\mathrm{M}_n(\mathbf{Z}_p)$ by $\mathrm{GL}_n(\mathbf{Z}_p)$. That is,

$$\mathrm{GL}_n(\mathbf{Z}_p) := \{g \in \mathrm{M}_n(\mathbf{Z}_p) \mid g^{-1} \in \mathrm{M}_n(\mathbf{Z}_p)\}.$$

This coincides with the stabilizer of $\mathbf{Z}_p^n$ in $\mathrm{GL}_n(\mathbf{Q}_p)$. Namely,

$$\mathrm{GL}_n(\mathbf{Z}_p) = \{g \in \mathrm{GL}_n(\mathbf{Q}_p) \mid g\mathbf{Z}_p^n = \mathbf{Z}_p^n\}.$$

$\mathrm{GL}_n(\mathbf{Z}_p)$ is a unique (up to conjugation) maximal compact subgroup of $\mathrm{GL}_n(\mathbf{Q}_p)$.

6.3 Iwasawa Decomposition

Fix $q \in \mathcal{P}$, and let G be a connected reductive $\mathbf{Q}_q$-algebraic group. Fix a maximal $\mathbf{Q}_q$-split torus T, and let $P_\emptyset$ be the standard minimal parabolic $\mathbf{Q}_q$-subgroup. Let $M_\emptyset U_\emptyset$ be a Levi decomposition of $P_\emptyset$, where $M_\emptyset = C_G(T)$.

Theorem 20 (Iwasawa Decomposition [21, Theorem 3.9], [26, 3.3.2])

There exists a maximal compact subgroup $\boldsymbol{K}$ of $\boldsymbol{G(\mathbf{Q}_q)}$ such that

$$\boldsymbol{G(\mathbf{Q}_q) = KT(\mathbf{Q}_q)U_\emptyset(\mathbf{Q}_q) = U_\emptyset(\mathbf{Q}_q)T(\mathbf{Q}_q)K}$$

holds. That is, any $\boldsymbol{g \in G(\mathbf{Q}_q)}$ can be represented as

$$\boldsymbol{g = kau = u'a'k' \qquad (k, k' \in K,\ a, a' \in T(\mathbf{Q}_q),\ u, u' \in U_\emptyset(\mathbf{Q}_q)).}$$

► The elements k, a, u in the representation of g are generally not unique.

► In the case $q = \infty$, let $T(\mathbf{Q}_\infty)^+$ be the identity component of $T(\mathbf{Q}_\infty)$ with respect to the ∞-topology. Then the map

$$K \times T(\mathbf{Q}_\infty)^+ \times U_\emptyset(\mathbf{Q}_\infty) \longrightarrow G(\mathbf{Q}_\infty) \ : \ (k, a, u) \mapsto kau$$

is a diffeomorphism, and in particular, it is a bijection.

Corollary 21

Let $\boldsymbol{K \subset G(\mathbf{Q}_q)}$ *be a maximal compact subgroup for which the Iwasawa decomposition holds. Let* $\boldsymbol{K_1}$ *be a maximal compact subgroup conjugate to* $\boldsymbol{K}$*, and let* $\boldsymbol{P}$ *be a parabolic* $\mathbf{Q}_q$*-subgroup of* $\boldsymbol{G}$*. Then*

$$\boldsymbol{G(\mathbf{Q}_q) = K_1 P(\mathbf{Q}_q) = P(\mathbf{Q}_q) K_1}$$

holds.

Proof. By assumption, $G(\mathbf{Q}_q) = KP_\emptyset(\mathbf{Q}_q)$ holds. Therefore, for any standard parabolic $\mathbf{Q}_q$-subgroup P_I, we have $G(\mathbf{Q}_q) = KP_I(\mathbf{Q}_q)$. P is conjugate to some P_I by an element of $G(\mathbf{Q}_q)$ (Theorem 16, (5)). Thus, there exists $g \in G(\mathbf{Q}_q)$ such that $P = gP_Ig^{-1}$. Since $G(\mathbf{Q}_q) = KP_I(\mathbf{Q}_q)$, we can write $g = kh$ for some $k \in K$ and $h \in P_I(\mathbf{Q}_q)$. Then $P = khP_I(kh)^{-1} = khP_Ih^{-1}k^{-1} = kP_Ik^{-1}$. So,

$$G(\mathbf{Q}_q) = kG(\mathbf{Q}_q)k^{-1} = k(KP_I(\mathbf{Q}_q))k^{-1} = (kKk^{-1})(kP_I(\mathbf{Q}_q)k^{-1}) = KP(\mathbf{Q}_q)$$

holds. The bijecton $g \mapsto g^{-1}$ yields $G(\mathbf{Q}_q) = P(\mathbf{Q}_q)K$. K_1 is conjugate to K, so we can write $K_1 = \gamma K\gamma^{-1}$ for some $\gamma \in G(\mathbf{Q}_q)$. From the decomposition $G(\mathbf{Q}_q) = P(\mathbf{Q}_q)K$, γ can be taken in $P(\mathbf{Q}_q)$. Therefore,

$$G(\mathbf{Q}_q) = \gamma G(\mathbf{Q}_q)\gamma^{-1} = \gamma(KP(\mathbf{Q}_q))\gamma^{-1} = (\gamma K\gamma^{-1})(\gamma P(\mathbf{Q}_q)\gamma^{-1}) = K_1P(\mathbf{Q}_q)$$

holds. □

§7 Adele Groups

7.1 Adelization of GL_n

For a finite subset $S \subset \mathcal{P}_f$, let

$$\mathrm{GL}_n(\mathbf{A}_S) := \prod_{p \in S} \mathrm{GL}_n(\mathbf{Q}_p) \times \prod_{p \in \mathcal{P}_f - S} \mathrm{GL}_n(\mathbf{Z}_p).$$

We equip $\mathrm{GL}_n(\mathbf{A}_S)$ with the product topology of the p-adic topologies, making it a locally compact group. Clearly, if $S \subset S'$, then $\mathrm{GL}_n(\mathbf{A}_S) \subset \mathrm{GL}_n(\mathbf{A}_{S'})$. The inductive limit with respect to this inclusion relation is denoted by

$$\mathrm{GL}_n(\mathbf{A}_f) := \varinjlim \mathrm{GL}_n(\mathbf{A}_S) = \bigcup_{S \subset \mathcal{P}_f} \mathrm{GL}_n(\mathbf{A}_S).$$

Here, S runs over all finite subsets of $\mathcal{P}_f$. The topology of $\mathrm{GL}_n(\mathbf{A}_f)$ is defined as follows:

$$O \text{ is an open set } \overset{\text{def}}{\iff} \text{ for any } S,\ O \cap \mathrm{GL}_n(\mathbf{A}_S) \text{ is an open set in } \mathrm{GL}_n(\mathbf{A}_S).$$

This makes $\mathrm{GL}_n(\mathbf{A}_f)$ a locally compact group. Furthermore, we set

$$\mathrm{GL}_n(\mathbf{A}) := \mathrm{GL}_n(\mathbf{Q}_\infty) \times \mathrm{GL}_n(\mathbf{A}_f).$$

With the product topology, $\mathrm{GL}_n(\mathbf{A})$ becomes a locally compact group. $\mathrm{GL}_n(\mathbf{A})$ is called the **adele group** of GL_n.

7.2 Adelization of an Algebraic Group

Let $G \subset \mathrm{GL}_n$ be a $\mathbf{Q}$-subgroup. For $p \in \mathcal{P}_f$, set

$$G_{\mathbf{Z}_p} := G(\mathbf{Q}_p) \cap \mathrm{GL}_n(\mathbf{Z}_p).$$

$G_{\mathbf{Z}_p}$ is a compact group. For a finite subset $S \subset \mathcal{P}_f$, let

$$G(\mathbf{A}_S) := \prod_{p \in S} G(\mathbf{Q}_p) \times \prod_{p \in \mathcal{P}_f - S} G_{\mathbf{Z}_p}$$

and endow it with the product topology. Similar to the case of GL_n, take the inductive limit

$$G(\mathbf{A}_f) := \varinjlim G(\mathbf{A}_S) = \bigcup_{S \subset \mathcal{P}_f} G(\mathbf{A}_S)$$

and define the topology similarly to the GL_n case, making $G(\mathbf{A}_f)$ a locally compact group. Furthermore, set

$$G(\mathbf{A}) := G(\mathbf{Q}_\infty) \times G(\mathbf{A}_f).$$

With the product topology, $G(\mathbf{A})$ becomes a locally compact group. $G(\mathbf{A})$ is called the **adele group of** G.

► Clearly,

$$G(\mathbf{A}) \subset \prod_{q \in \mathcal{P}} G(\mathbf{Q}_q)$$

but the topology is different from the relative topology induced by the product topology on the right-hand side. On the other hand, $G(\mathbf{A}) \subset \mathrm{GL}_n(\mathbf{A})$ is also clear, and the topology of $G(\mathbf{A})$ coincides with the relative topology induced from $\mathrm{GL}_n(\mathbf{A})$. More generally, if $H \subset G$ is a $\mathbf{Q}$-subgroup, then, by definition, one has

$$H(\mathbf{A}) = G(\mathbf{A}) \cap \prod_{q \in \mathcal{P}} H(\mathbf{Q}_q).$$

Thus, $H(\mathbf{A})$ is a subgroup of $G(\mathbf{A})$, and the topology on $H(\mathbf{A})$ coincides with the relative topology induced from $G(\mathbf{A})$ ([21, Lemma 5.4]).

► $G(\mathbf{A}_f)$ is a totally disconnected locally compact group. $G(\mathbf{A}_f)$ is sometimes called the **finite adele group of** G.

Examples

(1) In the case of $\mathbf{G}_a$, we have

$$\mathbf{G}_a(\mathbf{A}_S) = \prod_{p \in S} \mathbf{Q}_p \times \prod_{p \in \mathcal{P}_f - S} \mathbf{Z}_p, \qquad \mathbf{G}_a(\mathbf{A}_f) = \bigcup_{S \subset \mathcal{P}_f} \mathbf{G}_a(\mathbf{A}_S).$$

$\mathbf{G}_a(\mathbf{A}) = \mathbf{Q}_\infty \times \mathbf{G}_a(\mathbf{A}_f)$ is called the **adele ring** of $\mathbf{Q}$.

(2) Let us look at the case $\mathbf{G}_m = \mathrm{GL}_1$. Since $\mathrm{GL}_1(\mathbf{Z}_p) = \mathbf{Z}_p^\times$, we have

$$\mathbf{G}_m(\mathbf{A}_S) = \prod_{p \in S} \mathbf{Q}_p^\times \times \prod_{p \in \mathcal{P}_f - S} \mathbf{Z}_p^\times, \qquad \mathbf{G}_m(\mathbf{A}_f) = \bigcup_{S \subset \mathcal{P}_f} \mathbf{G}_m(\mathbf{A}_S).$$

$\mathbf{G}_m(\mathbf{A}) = \mathbf{G}_m(\mathbf{Q}_\infty) \times \mathbf{G}_m(\mathbf{A}_f)$ is specifically called the group of **ideles**. For $x = (x_\infty, x_f) \in \mathbf{G}_m(\mathbf{A})$, where $x_f = (x_p) \in \mathbf{G}_m(\mathbf{A}_S)$, we define

$$|x|_{\mathbf{A}} := \prod_{q \in \mathcal{P}} |x_q|_q = |x_\infty|_\infty \prod_{p \in S} |x_p|_p \in \mathbf{R}_{>0},$$

where $|\cdot|_\infty$ denotes the usual absolute value of $\mathbf{R}$. The map

$$|\cdot|_{\mathbf{A}} : \mathbf{G}_m(\mathbf{A}) \longrightarrow \mathbf{R}_{>0}$$

is a continuous homomorphism. This is called the **idele norm**. Let the diagonal embedding be

$$\iota : \mathbf{G}_m(\mathbf{Q}) \longrightarrow \mathbf{G}_m(\mathbf{A}) : \iota(a) = (a, a, a, \ldots).$$

Then, for any $a \in \mathbf{G}_m(\mathbf{Q})$, $|\iota(a)|_{\mathbf{A}} = 1$ holds.

Proposition 22

For $g \in G(\mathbf{Q})$, there exists a finite set $S \subset \mathcal{P}_f$ such that $g \in G_{\mathbf{Z}_p}$ for all $p \in \mathcal{P}_f - S$. In particular, via the natural diagonal embedding

$$\iota : G(\mathbf{Q}) \hookrightarrow \prod_{q \in \mathcal{P}} G(\mathbf{Q}_q) \ : \ \iota(g) = (g, g, g, \ldots)$$

we have $\iota(G(\mathbf{Q})) \subset G(\mathbf{A})$. Furthermore, $\iota(G(\mathbf{Q}))$ is discrete in $G(\mathbf{A})$.

Proof. It suffices to show this for $G = \mathrm{GL}_n$. Let $g = (g_{ij}) \in \mathrm{GL}_n(\mathbf{Q})$. Let

$$S' = \{p \in \mathcal{P}_f \mid |\det g|_p = 1, \ \ |g_{ij}|_p \leq 1 \ \ (\text{for all } i, j)\}.$$

Then $S = \mathcal{P}_f - S'$ is a finite set, and for $p \in S'$, we have $g \in \mathrm{GL}_n(\mathbf{Z}_p)$. From this, $\iota(g) \in \mathrm{GL}_n(\mathbf{Q}_\infty) \times \mathrm{GL}_n(\mathbf{A}_S)$. Since such an S can be chosen for each g, we have $\iota(\mathrm{GL}_n(\mathbf{Q})) \subset \mathrm{GL}_n(\mathbf{A})$. For the empty set $\emptyset$,

$$\mathrm{GL}_n(\mathbf{A}_\emptyset) = \prod_{p \in \mathcal{P}_f} \mathrm{GL}_n(\mathbf{Z}_p)$$

is an open subgroup of $\mathrm{GL}_n(\mathbf{A}_f)$. Since

$$\iota(\mathrm{GL}_n(\mathbf{Q})) \cap (\mathrm{GL}_n(\mathbf{Q}_\infty) \times \mathrm{GL}_n(\mathbf{A}_\emptyset)) = \iota(\mathrm{GL}_n(\mathbf{Z})),$$

if we let

$$O_\infty = \{(g_{ij}) \in \mathrm{GL}_n(\mathbf{Q}_\infty) \mid |g_{ij}| < 1/2 \ (i \neq j), \ \ |g_{ii} - 1| < 1/2 \ (\text{for all } i)\}$$

then

$$\iota(\mathrm{GL}_n(\mathbf{Q})) \cap (O_\infty \times \mathrm{GL}_n(\mathbf{A}_\emptyset)) = \{\iota(E_n)\}.$$

Therefore, $\iota(\mathrm{GL}_n(\mathbf{Q}))$ is discrete in $\mathrm{GL}_n(\mathbf{A})$. □

► Hereafter, we omit the embedding map ι and consider $G(\mathbf{Q}) \subset G(\mathbf{A})$.

7.3 Fundamental Results on Adele Groups

Let G and G' be $\mathbf{Q}$-algebraic groups, and let $f : G \longrightarrow G'$ be a $\mathbf{Q}$-homomorphism. For each $q \in \mathcal{P}$, f induces a homomorphism $f_q : G(\mathbf{Q}_q) \longrightarrow G'(\mathbf{Q}_q)$ which is continuous with respect to the q-adic topology. Let the product map be

$$\prod f_q : \prod_{q \in \mathcal{P}} G(\mathbf{Q}_q) \longrightarrow \prod_{q \in \mathcal{P}} G'(\mathbf{Q}_q).$$

The restiction of this product map to $G(\mathbf{A})$ is denoted by $f_{\mathbf{A}}$, i.e.,

$$f_{\mathbf{A}} = \left(\prod_q f_q\right)\Big|_{G(\mathbf{A})} : G(\mathbf{A}) \longrightarrow \prod_{q\in\mathcal{P}} G'(\mathbf{Q}_q).$$

Definition Let $f : G \longrightarrow G'$ be a $\mathbf{Q}$-homomorphism. We say that f has a **local section** if for each $y \in G'$, there exist a Zariski open neighborhood O_y of y and a $\mathbf{Q}$-rational map $g_y : O_y \longrightarrow G$ such that $f \circ g_y$ is the identity map of O_y.

Theorem 23 ([21, Lemma 5.2, Propositions 5.2 and 5.3])

Let $\boldsymbol{f : G \longrightarrow G'}$ be a $\mathbf{Q}$-homomorphism.

(1) *$\boldsymbol{f_{\mathbf{A}}}$ yields a continuous homomorphism $\boldsymbol{f_{\mathbf{A}} : G(\mathbf{A}) \longrightarrow G'(\mathbf{A})}$.*

(2) *If $\boldsymbol{f}$ is injective, then $\boldsymbol{f_{\mathbf{A}}}$ is also injective.*

(3) *If $\boldsymbol{f}$ has a local section, then $\boldsymbol{f_{\mathbf{A}}}$ is surjective. In particular, if $\boldsymbol{f}$ is a $\mathbf{Q}$-isomorphism, then $\boldsymbol{f_{\mathbf{A}}}$ is also an isomorphism.*

► In general, even if f is surjective, f_q and $f_{\mathbf{A}}$ are not necessarily surjective. For example, let $f : \mathbf{G}_m \longrightarrow \mathbf{G}_m$ be $f(x) = x^2$. Then f is surjective (over an algebraically closed field), but $f_\infty : \mathbf{R}^\times \to \mathbf{R}^\times$ is not surjective.

► If $N \subset G$ is a normal $\mathbf{Q}$-subgroup, then $N(\mathbf{A})$ is a normal subgroup of $G(\mathbf{A})$. The quotient group G/N is also a $\mathbf{Q}$-algebraic group, so $(G/N)(\mathbf{A})$ can be defined. The natural map $\pi : G \longrightarrow G/N$ induces $\pi_{\mathbf{A}} : G(\mathbf{A}) \longrightarrow (G/N)(\mathbf{A})$, which is not necessarily surjective, so $G(\mathbf{A})/N(\mathbf{A})$ and $(G/N)(\mathbf{A})$ may not be isomorphic.

► The identity component G° of G is a normal $\mathbf{Q}$-subgroup. The group $G(\mathbf{A})/G^\circ(\mathbf{A})$ is compact ([5, 1.9]).

► Let $H \subset G$ be a $\mathbf{Q}$-subgroup and $N \subset G$ be a normal $\mathbf{Q}$-subgroup such that G is a semidirect product of H and N. In this case, for the natural map $\pi : G \longrightarrow G/N \cong H$, the map $G/N \cong H \hookrightarrow G$ yields a local section, so $\pi_{\mathbf{A}}$ is surjective. $G(\mathbf{A})$ is a semidirect product of $H(\mathbf{A})$ and $N(\mathbf{A})$ ([5, 1.6]).

► Let G be a connected reductive $\mathbf{Q}$-algebraic group, and let $P \subset G$ be a parabolic $\mathbf{Q}$-subgroup. If $P = MU$ is a Levi decomposition, then by the above remark, $P(\mathbf{A}) = M(\mathbf{A})U(\mathbf{A})$ is a semidirect product.

7.4 Iwasawa Decomposition of Adele Groups

Let $G \subset \mathrm{GL}_n$ be a connected reductive $\mathbf{Q}$-algebraic group.

Theorem 24 ([26, 3.9.1])

If the finite set $S \subset \mathcal{P}_f$ is taken sufficiently large, then for any $p \in \mathcal{P}_f - S$, $G_{\mathbf{Z}_p} = G(\mathbf{Q}_p) \cap \mathrm{GL}_n(\mathbf{Z}_p)$ is a maximal compact subgroup of $G(\mathbf{Q}_p)$, and the Iwasawa decomposition holds for $G_{\mathbf{Z}_p}$.

For $p \in \mathcal{P}_f - S$, let $K_p = G_{\mathbf{Z}_p}$. For $q \in S \cup \{\infty\}$, let $K_q \subset G(\mathbf{Q}_q)$ be a maximal compact subgroup for which the Iwasawa decomposition holds. Then set

$$K := \prod_{q \in \mathcal{P}} K_q.$$

Proposition 25

K is a maximal compact subgroup of $G(\mathbf{A})$. If $P \subset G$ is a parabolic $\mathbf{Q}$-subgroup, then

$$G(\mathbf{A}) = KP(\mathbf{A}) = P(\mathbf{A})K$$

holds.

Proof. We can write $K = K_\infty \times K_f$, where

$$K_f = \prod_{p \in \mathcal{P}_f} K_p.$$

It suffices to show that $K_f \subset G(\mathbf{A}_f)$ is a maximal compact subgroup. Take a compact subgroup L such that $K_f \subset L \subset G(\mathbf{A}_f)$. Since K_f is an open subgroup, L/K_f is a finite set. Let

$$L = g_1 K_f \cup \cdots \cup g_n K_f.$$

Choose a finite set $S \subset \mathcal{P}_f$ such that if $p \in \mathcal{P} - S$, then $g_{ip} \in G_{\mathbf{Z}_p}$ for $i = 1, \ldots, n$ and $K_p = G_{\mathbf{Z}_p}$ holds. Then

$$K_f \subset L \subset G(\mathbf{A}_S) = \prod_{p \in S} G(\mathbf{Q}_p) \times \prod_{p \in \mathcal{P}_f - S} K_p.$$

Thus, we can write

$$L = L_S \times \prod_{p \in \mathcal{P}_f - S} K_p, \qquad L_S \subset \prod_{p \in S} G(\mathbf{Q}_p).$$

Since

$$K_S = \prod_{p \in S} K_p \subset \prod_{p \in S} G(\mathbf{Q}_p)$$

is a maximal compact subgroup, we must have $K_S = L_S$. Therefore $K_f = L$, and $K_f \subset G(\mathbf{A}_f)$ is a maximal compact subgroup. From Corollary 21, $G(\mathbf{A}) = KP(\mathbf{A})$ follows easily. □

7.5 Unit Adele Groups

Let $G \subset \mathrm{GL}_n$ be a connected $\mathbf{Q}$-algebraic group, and let $\mathrm{X}^*(G)_{\mathbf{Q}}$ be the group of $\mathbf{Q}$-rational characters of G. By Theorem 23(1), each $\chi \in \mathrm{X}^*(G)_{\mathbf{Q}}$ yields a continuous homomorphism

$$\chi_{\mathbf{A}} \,:\, G(\mathbf{A}) \longrightarrow \mathbf{G}_m(\mathbf{A}).$$

Let $|\chi|_{\mathbf{A}}$ denote the composition of $\chi_{\mathbf{A}}$ and the idele norm. That is,

$$|\chi|_{\mathbf{A}} \,:\, G(\mathbf{A}) \longrightarrow \mathbf{R}_{>0} \,:\, |\chi|_{\mathbf{A}}(g) = |\chi_{\mathbf{A}}(g)|_{\mathbf{A}}.$$

Let

$$G(\mathbf{A})^1 := \left\{ g \in G(\mathbf{A}) \mid |\chi|_{\mathbf{A}}(g) = 1 \ \text{ for all } \chi \in \mathrm{X}^*(G)_{\mathbf{Q}} \right\}.$$

We will call $G(\mathbf{A})^1$ the **unit adele group** of G for convenience. Let $\chi_1, \ldots, \chi_r$ be a $\mathbf{Z}$-basis of $\mathrm{X}^*(G)_{\mathbf{Q}}$. Define ϑ_G by

$$\vartheta_G \,:\, G(\mathbf{A}) \longrightarrow (\mathbf{R}_{>0})^r \,:\, \vartheta_G(g) = \left(|\chi_1|_{\mathbf{A}}(g), \ldots, |\chi_r|_{\mathbf{A}}(g)\right).$$

Then

$$G(\mathbf{A})^1 = \mathrm{Ker}\, \vartheta_G.$$

Thus, $G(\mathbf{A})^1$ is a normal subgroup of $G(\mathbf{A})$. Clearly, $G(\mathbf{Q}) \subset G(\mathbf{A})^1$.

Examples

(1) In the case of GL_n,

$$\mathrm{X}^*(\mathrm{GL}_n)_{\mathbf{Q}} = \mathbf{Z} \det$$

so

$$\mathrm{GL}_n(\mathbf{A})^1 = \left\{ g \in \mathrm{GL}_n(\mathbf{A}) \mid |\det(g)|_{\mathbf{A}} = 1 \right\}.$$

Let Z_n be the center of GL_n, and let $Z_n(\mathbf{Q}_\infty)^+$ be the connected component of the identity of $Z_n(\mathbf{Q}_\infty)$ with respect to the ∞-topology. That is,

$$Z_n(\mathbf{Q}_\infty)^+ = \left\{ aE_n \mid a \in \mathbf{R}_{>0} \right\}.$$

Via the natural injection

$$\mathrm{GL}_n(\mathbf{Q}_\infty) \hookrightarrow \mathrm{GL}_n(\mathbf{A}) = \mathrm{GL}_n(\mathbf{Q}_\infty) \times \mathrm{GL}_n(\mathbf{A}_f) \,:\, g \mapsto (g, e)$$

we regard $Z_n(\mathbf{Q}_\infty)^+ \subset \mathrm{GL}_n(\mathbf{A})$. Then we have a direct product decomposition

$$\mathrm{GL}_n(\mathbf{A}) = Z_n(\mathbf{Q}_\infty)^+ \cdot \mathrm{GL}_n(\mathbf{A})^1.$$

(2) Let G be a connected reductive $\mathbf{Q}$-algebraic group, and let Z_G be the maximal central $\mathbf{Q}$-split torus of G. From Proposition 10, $X^*(G)_\mathbf{Q}$ is a subgroup of finite index in $X^*(Z_G)_\mathbf{Q}$. Let $Z_G(\mathbf{Q}_\infty)^+$ be the connected component of the identity of $Z_G(\mathbf{Q}_\infty)$ with respect to the ∞-topology, and naturally regard $Z_G(\mathbf{Q}_\infty)^+ \subset G(\mathbf{Q}_\infty)$ as a subgroup of $G(\mathbf{A})$. Then $G(\mathbf{A})$ has a direct product decomposition

$$G(\mathbf{A}) = Z_G(\mathbf{Q}_\infty)^+ \cdot G(\mathbf{A})^1.$$

(3) Let $Q_r = Q_{n,r} \subset \mathrm{GL}_n$ be the standard maximal parabolic subgroup. If $Q_r = M_r U_r$ is a Levi decomposition, then $M_r \cong \mathrm{GL}_r \times \mathrm{GL}_{n-r}$. From $X^*(Q_r)_\mathbf{Q} = X^*(M_r)_\mathbf{Q}$, we get

$$Q_r(\mathbf{A})^1 = M_r(\mathbf{A})^1 U_r(\mathbf{A}), \qquad M_r(\mathbf{A})^1 \cong \mathrm{GL}_r(\mathbf{A})^1 \times \mathrm{GL}_{n-r}(\mathbf{A})^1.$$

(4) Let G be a connected reductive $\mathbf{Q}$-algebraic group. If G is $\mathbf{Q}$-anisotropic or if G is semisimple, then $X^*(G)_\mathbf{Q} = 0$, so in this case $G(\mathbf{A})^1 = G(\mathbf{A})$.

► In general, $G(\mathbf{A})$ is not a unimodular group, but $G(\mathbf{A})^1$ is a unimodular group.

§8 Arithmetic Quotients of Adele Groups

8.1 Fundamental Domains

Let Γ be an abstract group acting on a Hausdorff topological space V. Denote the action by

$$\Gamma \times V \longrightarrow V \ : \ (\gamma, v) \mapsto \gamma \cdot v.$$

If there exists an open set $\Omega \subset V$ satisfying the conditions:

(1) if Ω^- denotes the closure of Ω, then $V = \Gamma\Omega^-$;

(2) $\{\gamma \in \Gamma \mid \gamma\Omega^- \cap \Omega \neq \emptyset\} = \{e\}$,

then such Ω is called an **open fundamental domain** for $\Gamma\backslash V$. A set F such that $\Omega \subset F \subset \Omega^-$ is called a **fundamental domain** for $\Gamma\backslash V$.

Theorem 26 (Baer–Levi [27, Section 10])

If the action of $\boldsymbol{\Gamma}$ *on* $\boldsymbol{V}$ *is free and properly discontinuous, then an open fundamental domain for* $\boldsymbol{\Gamma\backslash V}$ *exists.*

▶ The action of Γ is said to be **free** if

$$\{\gamma \in \Gamma \mid \gamma v = v\} = \{e\} \qquad (\text{for all } v \in V)$$

holds. The action of Γ is said to be **properly discontinuous** if for any $v \in V$, there exists a neighborhood O_v of v such that

$$\sharp\{\gamma \in \Gamma \mid \gamma O_v \cap O_v \neq \emptyset\} < \infty$$

holds.

▶ If the condition (2) for an open fundamental domain is replaced by

(2′) $\sharp\{\gamma \in \Gamma \mid \gamma\Omega^- \cap \Omega \neq \emptyset\} < \infty$,

then a set F such that $\Omega \subset F \subset \Omega^-$ is called a **fundamental set**. The condition (2′) is called the **Siegel property** for Γ ([3, 9.6])

Example Let G be a connected $\mathbf{Q}$-algebraic group. The natural action of $G(\mathbf{Q})$

$$G(\mathbf{Q}) \times G(\mathbf{A})^1 \longrightarrow G(\mathbf{A})^1 \ : \ (\gamma, g) \mapsto \gamma g$$

is clearly free. For any $g \in G(\mathbf{A})^1$, let O_g be a compact neighborhood of g. Then $O_g \cdot O_g^{-1}$ is a compact subset of $G(\mathbf{A})^1$, and since $G(\mathbf{Q}) \subset G(\mathbf{A})^1$ is discrete,

$$\sharp\left(O_g \cdot O_g^{-1} \cap G(\mathbf{Q})\right) < \infty$$

holds. Therefore, the action of $G(\mathbf{Q})$ is properly discontinuous. From this, an open fundamental domain $\Omega \subset G(\mathbf{A})^1$ for $G(\mathbf{Q})\backslash G(\mathbf{A})^1$ exists. The quotient space $G(\mathbf{Q})\backslash G(\mathbf{A})^1$ (or $G(\mathbf{Q})\backslash G(\mathbf{A})$) is called the **arithmetic quotient** of G.

▶ From proper discontinuity, the natural map $\pi : G(\mathbf{A})^1 \longrightarrow G(\mathbf{Q})\backslash G(\mathbf{A})^1$ is a local homeomorphism. That is, for any $g \in G(\mathbf{A})^1$, there exists a neighborhood O_g such that π restricted to O_g is a homeomorphism.

8.2 Compactness Criterion

Theorem 27 (Mostow–Tamagawa, Borel–Harish-Chandra [5, 5.8])

For a connected $\mathbf{Q}$*-algebraic group* $\boldsymbol{G}$*,* $\boldsymbol{G(\mathbf{Q})\backslash G(\mathbf{A})^1}$ *is compact if and only if* $\boldsymbol{G/R(G)}$ *is* $\mathbf{Q}$*-anisotropic. Here* $\boldsymbol{R(G)}$ *is the radical of* $\boldsymbol{G}$*.*

Examples

(1) If T is a $\mathbf{Q}$-torus, then $R(T) = T$, so $T(\mathbf{Q})\backslash T(\mathbf{A})^1$ is compact. Let Z_T be the maximal $\mathbf{Q}$-split torus in T. Since $T(\mathbf{A}) = Z_T(\mathbf{Q}_\infty)^+ T(\mathbf{A})^1$ and $T(\mathbf{Q})\backslash T(\mathbf{A}) = Z_T(\mathbf{Q}_\infty)^+ \cdot (T(\mathbf{Q})\backslash T(\mathbf{A})^1)$, it follows that

$$T(\mathbf{Q})\backslash T(\mathbf{A}) \text{ is compact } \iff Z_T = \{e\}, \text{ i.e., } T \text{ is } \mathbf{Q}\text{-anisotropic.}$$

In particular, for the ideles $\mathbf{G}_m(\mathbf{A})$, $\mathbf{G}_m(\mathbf{Q})\backslash \mathbf{G}_m(\mathbf{A})^1$ is compact, but $\mathbf{G}_m(\mathbf{Q})\backslash \mathbf{G}_m(\mathbf{A})$ is not compact.

(2) If G is a connected reductive $\mathbf{Q}$-algebraic group, since $G(\mathbf{A}) = Z_G(\mathbf{Q}_\infty)^+ G(\mathbf{A})^1$ and $G(\mathbf{Q})\backslash G(\mathbf{A}) = Z_G(\mathbf{Q}_\infty)^+ \cdot (G(\mathbf{Q})\backslash G(\mathbf{A})^1)$, the following are equivalent:

$$G(\mathbf{Q})\backslash G(\mathbf{A}) \text{ is compact } \iff Z_G = \{e\} \text{ and } G/R(G) \text{ is } \mathbf{Q}\text{-anisotropic.}$$

8.3 Siegel Sets

Let G be a connected reductive $\mathbf{Q}$-algebraic group, let $T \subset G$ be a maximal $\mathbf{Q}$-split torus, and let $T \subset T_{\max} \subset G$ be a maximal $\mathbf{Q}$-torus. Assume the relative root system $\Phi_{\mathbf{Q}} = \Phi_{\mathbf{Q}}(G, T) \neq \emptyset$, and fix a fundamental system $\Delta_{\mathbf{Q}} \subset \Phi_{\mathbf{Q}}$. Let $P = P_\emptyset$ be the standard minimal $\mathbf{Q}$-parabolic subgroup, let M_P be its Levi subgroup and U_P its unipotent radical. Since T is a maximal $\mathbf{Q}$-split torus of M_P and $R(M_P) = Z_{M_P} = T$, the quotient $M_P/R(M_P) = P/R(P)$ is $\mathbf{Q}$-anisotropic, so $P(\mathbf{Q})\backslash P(\mathbf{A})^1$ is compact by Theorem 27. Therefore, there exists an open and relatively compact subset $\omega \subset P(\mathbf{A})^1$ such that

$$P(\mathbf{A})^1 = P(\mathbf{Q})\omega.$$

Let $K \subset G(\mathbf{A})$ be the maximal compact subgroup given in Proposition 25. Then the Iwasawa decomposition holds:

$$G(\mathbf{A}) = P(\mathbf{A})K.$$

For a constant $c > 0$, set

$$T(\mathbf{A})_c := \{t \in T(\mathbf{A}) \mid |\beta|_{\mathbf{A}}(t) \geq c \quad (\text{for all } \beta \in \Delta_{\mathbf{Q}})\}.$$

Then let

$$\mathfrak{S}_{\omega,c} := \omega T(\mathbf{A})_c K.$$

$\mathfrak{S}_{\omega,c}$ is called a **Siegel set**.

► Since $T(\mathbf{A}) = Z_T(\mathbf{Q}_\infty)^+ \cdot T(\mathbf{A})^1$, if we set

$$Z_T(\mathbf{Q}_\infty)_c^+ := Z_T(\mathbf{Q}_\infty)^+ \cap T(\mathbf{A})_c$$

then $T(\mathbf{A})_c = Z_T(\mathbf{Q}_\infty)_c^+ \cdot T(\mathbf{A})^1$.

Theorem 28 (Borel–Harish-Chandra [15, Théorèm 7])

For some $\boldsymbol{c > 0}$, $\mathfrak{S}_{\omega,c}$ is a fundamental set for $\boldsymbol{G(\mathbf{Q})\backslash G(\mathbf{A})}$. That is,

$$\boldsymbol{G(\mathbf{A}) = G(\mathbf{Q})\mathfrak{S}_{\omega,c}} \quad \textit{and} \quad \boldsymbol{\sharp\{\gamma \in G(\mathbf{Q}) \mid \gamma\mathfrak{S}_{\omega,c} \cap \mathfrak{S}_{\omega,c} \neq \emptyset\} < \infty}$$

holds.

► It should be noted that there are two different methods to construct fundamental sets by using Siegel sets. [5, Theorem 4.5] is using a Siegel set of GL_n and is different from [15, Théorèm 7]. See also [3, Sections 9 and 13].

As an application of this theorem, the following can be proved.

Corollary 29 ([5, 5.8])

Let $\boldsymbol{G}$ be a connected $\mathbf{Q}$-algebraic group. Then the volume of $\boldsymbol{G(\mathbf{Q})\backslash G(\mathbf{A})^1}$ by an invariant measure on $\boldsymbol{G(\mathbf{A})^1}$ is finite.

► Every Siegel set has a finite volume if $Z_G = \{e\}$ ([3, Lemma 12.5]).

Corollary 30 ([21, Theorem 4.2])

Let $\boldsymbol{G \subset \mathrm{GL}_n}$ be a connected $\mathbf{Q}$-algebraic group. Then $\boldsymbol{G_{\mathbf{Z}} = G(\mathbf{Q}) \cap \mathrm{GL}_n(\mathbf{Z})}$ is finitely generated and is presented by a finite number of defining relations.

§9 Arithmetical Minimum Functions

9.1 Setting and Preparation

• Let G be a connected reductive $\mathbf{Q}$-algebraic group, $T \subset G$ a maximal $\mathbf{Q}$-split torus, and $T \subset T_{\max} \subset G$ a maximal $\mathbf{Q}$-torus.

• We assume the relative root system $\Phi_{\mathbf{Q}} = \Phi_{\mathbf{Q}}(G,T)$ is non-empty, and fix a fundamental system $\Delta_{\mathbf{Q}} \subset \Phi_{\mathbf{Q}}$. $\Delta_{\mathbf{Q}}$ forms a basis of the real vector space $\mathrm{X}_{\mathbf{R}} = \mathrm{X}^*(T/Z_G) \otimes_{\mathbf{Z}} \mathbf{R}$.

• Let $W_G = W(G,T) = W(\Phi_{\mathbf{Q}})$ be the Weyl group. W_G is generated by the reflections $\{s_\beta\}_{\beta\in\Delta_{\mathbf{Q}}}$ of $\mathrm{X}_{\mathbf{R}}$, and acts on both $\mathrm{X}^*(T)$ and $\mathrm{X}^*(T/Z_G)$, (see **5.1**).

• We fix a simple root $\alpha \in \Delta_{\mathbf{Q}}$, and let $Q = P_{\Delta_{\mathbf{Q}}-\{\alpha\}}$ be the standard maximal parabolic $\mathbf{Q}$-subgroup. Let $M = M_{\Delta_{\mathbf{Q}}-\{\alpha\}}$ and $U = U_{\Delta_{\mathbf{Q}}-\{\alpha\}}$. Let Z_G and Z_M be the maximal central $\mathbf{Q}$-split tori of G and M, respectively. We have

$$Z_G \subset Z_M \subset T$$

and

$$Z_G = \left(\bigcap_{\beta\in\Delta_{\mathbf{Q}}} \mathrm{Ker}\,\beta\right)^\circ, \qquad Z_M = \left(\bigcap_{\beta\in\Delta_{\mathbf{Q}}-\{\alpha\}} \mathrm{Ker}\,\beta\right)^\circ.$$

• From the exact sequence

$$1 \longrightarrow Z_M/Z_G \longrightarrow T/Z_G \longrightarrow T/Z_M \longrightarrow 1,$$

we have the exact sequence

$$0 \longrightarrow \mathrm{X}^*(T/Z_M) \longrightarrow \mathrm{X}^*(T/Z_G) \longrightarrow \mathrm{X}^*(Z_M/Z_G) \longrightarrow 0.$$

Thus, $\mathrm{X}^*(Z_M/Z_G) \otimes \mathbf{Q}$ is a one-dimensional vector space with basis $\alpha\big|_{Z_M}$, and $\mathrm{X}^*(Z_M/Z_G)$ is a free $\mathbf{Z}$-module of rank 1. From Proposition 10, $\mathrm{X}^*(M/Z_M)_{\mathbf{Q}} = 0$. Therefore

$$\mathrm{X}^*(M/Z_G)_{\mathbf{Q}} \subset \mathrm{X}^*(Z_M/Z_G)_{\mathbf{Q}} = \mathrm{X}^*(Z_M/Z_G),$$

and $\mathrm{X}^*(M/Z_G)_{\mathbf{Q}}$ is also a free $\mathbf{Z}$-module of rank 1.

• Choose a $\mathbf{Z}$-basis $\widehat{\alpha} \in \mathrm{X}^*(M/Z_G)_{\mathbf{Q}}$ such that $\widehat{\alpha}\big|_{Z_M} \in \mathbf{Q}_{>0}\left(\alpha\big|_{Z_M}\right)$.

Example In the case $G = \mathrm{GL}_n$, $Q = Q_r = Q_{n,r}$, we have

$$M = M_r = \left\{\mathrm{diag}(a,d) = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \mid a \in \mathrm{GL}_r, \;\; d \in \mathrm{GL}_{n-r}\right\}, \qquad Z_G = Z_n.$$

Thus, for $(k,\ell) \in \mathbf{Z}^2$, let

$$\chi_{k,\ell} : M_r \longrightarrow \mathbf{G}_m : \chi_{k,\ell}(\mathrm{diag}(a,d)) = (\det a)^k (\det d)^\ell.$$

Then $X^*(M_r)_{\mathbf{Q}} = \{\chi_{k,\ell} \mid (k,\ell) \in \mathbf{Z}^2\}$. Since

$$\chi_{k,\ell}\big|_{Z_n} = 0 \iff rk + (n-r)\ell = 0,$$

letting $\gcd(r, n-r) = r'$, we have

$$X^*(M_r/Z_n)_{\mathbf{Q}} = \mathbf{Z}\chi_{(n-r)/r',-r/r'} = \mathbf{Z}\chi_{-(n-r)/r',r/r'}.$$

Since $\alpha = \alpha_r = \epsilon_r - \epsilon_{r+1}$, we have

$$\left(\chi_{(n-r)/r',-r/r'}\right)\Big|_{Z_M} = \frac{r(n-r)}{r'}\left(\alpha_r\big|_{Z_M}\right) \in \mathbf{Q}_{>0}\left(\alpha_r\big|_{Z_M}\right).$$

Thus we can take $\widehat{\alpha} = \chi_{(n-r)/r',-r/r'}$.

► When $\widehat{\alpha}$ is regarded as a rational character of M, it becomes trivial on the commutator subgroup $D(M)$ of M. The identity connected component $(T \cap D(M))^\circ$ of $T \cap D(M)$ is a maximal $\mathbf{Q}$-split torus of $D(M)$, and $\Delta_{\mathbf{Q}} - \{\alpha\}$ is a base of the relative root system $\Phi_{\mathbf{Q}}(D(M), (T \cap D(M))^\circ)$. From this, the restriction $\widehat{\alpha}\big|_T$ of $\widehat{\alpha}$ to T satisfies

$$(\widehat{\alpha}\big|_T, \beta^\vee) = 0 \quad ({}^\forall\beta \in \Delta_{\mathbf{Q}} - \{\alpha\}), \qquad (\widehat{\alpha}\big|_T, \alpha^\vee) > 0.$$

Here, $\beta^\vee$ is the coroot corresponding to β. As noted in **3.5**, $\beta^\vee$ is regarded as an element of $X_*(T)_F \otimes_{\mathbf{Z}} \mathbf{R}$, and in fact, $\beta^\vee$ is contained in $X_*((T \cap D(M))^\circ)_F$ if $\beta \neq \alpha$. This is the reason for $(\widehat{\alpha}\big|_T, \beta^\vee) = 0$. In particular, $\widehat{\alpha}\big|_T$ is located in the boundary of the Weyl chamber

$$C := \{v \in X_{\mathbf{R}} \mid (v, \beta^\vee) > 0 \quad ({}^\forall\beta \in \Delta_{\mathbf{Q}})\}.$$

Proposition 31

Let $\boldsymbol{W_\alpha}$ be the subgroup of $\boldsymbol{W_G}$ generated by $\{\boldsymbol{s_\beta}\}_{\boldsymbol{\beta \in \Delta_Q - \{\alpha\}}}$. Then

$$\boldsymbol{W_\alpha = \left\{w \in W_G \mid w\widehat{\alpha}\big|_T = \widehat{\alpha}\big|_T\right\}}$$

holds.

Proof. Let W' denote the group on the right-hand side. By Theorem 16(1), $\Phi_{\mathbf{Q}}(M,T) = [\Delta_{\mathbf{Q}} - \{\alpha\}]$, so $\Phi_{\mathbf{Q}}(M,T)$ is an extended root system with base $\Delta_{\mathbf{Q}} - \{\alpha\}$. Thus $W_\alpha = W(\Phi_{\mathbf{Q}}(M,T))$, and a representative n_w of $w = [n_w] \in W_\alpha$ can be taken from $M(\mathbf{Q})$. Since $\widehat{\alpha}$ is a rational character of M, we have

$$w\widehat{\alpha}\big|_T(t) = \widehat{\alpha}(n_w^{-1} t n_w) = \widehat{\alpha}(n_w)^{-1}\widehat{\alpha}(t)\widehat{\alpha}(n_w) = \widehat{\alpha}\big|_T(t) \qquad ({}^\forall t \in T, {}^\forall w \in W_\alpha).$$

Therefore $W_\alpha \subset W'$, and

$$\{s_\beta\}_{\beta\in\Delta_{\mathbf{Q}}-\{\alpha\}} \subset W' \cap \{s_\beta\}_{\beta\in\Delta_{\mathbf{Q}}}.$$

By the previous remark and the general theory of Coxeter groups ([17, 1.12 Theorem (a)]), W' is generated by $W' \cap \{s_\beta\}_{\beta\in\Delta_{\mathbf{Q}}}$. Since $\widehat{\alpha}\big|_{Z_M} \in \mathbf{Q}_{>0}\alpha\big|_{Z_M}$, we have $s_\alpha \notin W'$. Thus

$$\{s_\beta\}_{\beta\in\Delta_{\mathbf{Q}}-\{\alpha\}} = W' \cap \{s_\beta\}_{\beta\in\Delta_{\mathbf{Q}}}$$

must hold, so $W_\alpha = W'$. □

► From the Bruhat decomposition of $G(\mathbf{Q})$, it follows

$$G(\mathbf{Q}) = \bigsqcup_{[w]\in W_\alpha\backslash W_G/W_\alpha} Q(\mathbf{Q})n_wQ(\mathbf{Q}).$$

Fix a maximal compact subgroup $K \subset G(\mathbf{A})$ which admits an Iwasawa decomposition. Since $G(\mathbf{A}) = Q(\mathbf{A})K$, we can write $g \in G(\mathbf{A})$ as

$$g = umh \qquad (u \in U(\mathbf{A}), m \in M(\mathbf{A}), h \in K).$$

Define

$$z_Q(g) := Z_G(\mathbf{A})M(\mathbf{A})^1 m \in Z_G(\mathbf{A})M(\mathbf{A})^1\backslash M(\mathbf{A}).$$

Proposition 32

The map $\boldsymbol{z_Q : G(\mathbf{A}) \longrightarrow Z_G(\mathbf{A})M(\mathbf{A})^1\backslash M(\mathbf{A})}$ *is well-defined, and*

$$\boldsymbol{z_Q(g'g) = z_Q(g) \qquad (^\forall g' \in Z_G(\mathbf{A})Q(\mathbf{A})^1, {}^\forall g \in G(\mathbf{A}))}$$

holds. Thus z_Q *induces a map*

$$\boldsymbol{z_Q : Z_G(\mathbf{A})Q(\mathbf{A})^1\backslash G(\mathbf{A}) \longrightarrow Z_G(\mathbf{A})M(\mathbf{A})^1\backslash M(\mathbf{A}).}$$

Proof. Let $g = u'm'h'$ $(u' \in U(\mathbf{A}), m' \in M(\mathbf{A}), h' \in K)$ be another decomposition of g. Since

$$h'h^{-1} \in Q(\mathbf{A}) \cap K \subset Q(\mathbf{A})^1 = U(\mathbf{A})M(\mathbf{A})^1,$$

we can write

$$h' = u_1m_1h \qquad (u_1 \in U(\mathbf{A}), m_1 \in M(\mathbf{A})^1).$$

Thus

$$umh = u'm'u_1m_1h, \quad \text{so} \quad m = m_2m', \qquad (m_2 = m'm_1(m')^{-1} \in M(\mathbf{A})^1).$$

Therefore $Z_G(\mathbf{A})M(\mathbf{A})^1m = Z_G(\mathbf{A})M(\mathbf{A})^1m'$. The latter half is trivial. □

Proposition 33

The natural map

$$\boldsymbol{Q(\mathbf{A})^1\backslash G(\mathbf{A})^1 \longrightarrow Z_G(\mathbf{A})Q(\mathbf{A})^1\backslash G(\mathbf{A})}$$

is bijective.

Proof. Since $G(\mathbf{A}) = Z_G(\mathbf{R})^+G(\mathbf{A})^1$, surjectivity is clear. For $g \in G(\mathbf{A})^1$, it suffices to show that if $g \in Z_G(\mathbf{A})Q(\mathbf{A})^1$, then $g \in Q(\mathbf{A})^1$. Let

$$g = zh, \qquad (z \in Z_G(\mathbf{A}),\ h \in Q(\mathbf{A})^1).$$

Then

$$z = gh^{-1} \in G(\mathbf{A})^1.$$

Since $X^*(G) \subset X^*(Z_G)$ has finite index, $Z_G(\mathbf{A})^1 = Z_G(\mathbf{A}) \cap G(\mathbf{A})^1$. Thus $z \in Z_G(\mathbf{A})^1$. From the exact sequence

$$0 \longrightarrow X^*(Z_M/Z_G) \longrightarrow X^*(Z_M) \longrightarrow X^*(Z_G) \longrightarrow 0$$

and elementary divisor theory, we have $Z_G(\mathbf{A})^1 \subset Z_M(\mathbf{A})^1$. Thus $Z_G(\mathbf{A})^1 \subset M(\mathbf{A})^1 \subset Q(\mathbf{A})^1$, so $g = zh \in Q(\mathbf{A})^1$. □

9.2 Height Functions

$\widehat{\alpha}$ defines a continuous homomorphism

$$\widehat{\alpha}_{\mathbf{A}} \ : \ Z_G(\mathbf{A})M(\mathbf{A})^1\backslash M(\mathbf{A}) \longrightarrow \mathbf{G}_m(\mathbf{A}).$$

The composition of z_Q and $\widehat{\alpha}_{\mathbf{A}}$ yields the map

$$\widehat{\alpha}_{\mathbf{A}} \circ z_Q \ : \ G(\mathbf{A}) \longrightarrow Z_G(\mathbf{A})M(\mathbf{A})^1\backslash M(\mathbf{A}) \longrightarrow \mathbf{G}_m(\mathbf{A}).$$

Composing this with the idele norm, define

$$H_Q \ : \ G(\mathbf{A}) \longrightarrow \mathbf{R}_{>0} \ : \ H_Q(g) := |\widehat{\alpha}_{\mathbf{A}} \circ z_Q(g)|_{\mathbf{A}}^{-1}.$$

Letting $\mathcal{Y} := Q(\mathbf{A})^1\backslash G(\mathbf{A})^1 = Z_G(\mathbf{A})Q(\mathbf{A})^1\backslash G(\mathbf{A})$, H_Q yields a continuous function on $\mathcal{Y}$:

$$H_Q \ : \ \mathcal{Y} \longrightarrow \mathbf{R}_{>0}.$$

By definition, for any $u \in U(\mathbf{A}), m \in M(\mathbf{A}), g \in G(\mathbf{A})^1$,

$$H_Q(umg) = |\widehat{\alpha}_{\mathbf{A}}(m)|_{\mathbf{A}}^{-1}H_Q(g)$$

holds. Then, from the Iwasawa decomposition $G(\mathbf{A}) = Q(\mathbf{A})K$,

$$\sup_{y \in \mathcal{Y}} \frac{H_Q(yg)}{H_Q(y)} = \sup_{h \in K} H_Q(hg) = \max_{h \in K} H_Q(hg)$$

holds. We denote this by

$$\|g\| := \max_{h \in K} H_Q(hg)$$

and call this the norm of g. The following is easily verified.

Proposition 34

The norm $\|\cdot\| : G(\mathbf{A})^1 \longrightarrow \mathbf{R}_{>0}$ *is continuous and satisfies the following:*

(1) $\|g_1 g_2\| \leq \|g_1\| \cdot \|g_2\|$ $\quad (^\forall g_1, g_2 \in G(\mathbf{A})^1)$;

(2) $\|h_1 g h_2\| = \|g\|$ $\quad (^\forall h_1, h_2 \in K, \ ^\forall g \in G(\mathbf{A})^1)$;

(3) $\|h\| = 1$ $\quad (^\forall h \in K)$.

Let $\mathcal{X} := Q(\mathbf{Q})\backslash G(\mathbf{Q})$. Since $G(\mathbf{Q}) \cap Q(\mathbf{A})^1 = Q(\mathbf{Q})$, there is a natural injection

$$\mathcal{X} \hookrightarrow \mathcal{Y}.$$

For each $g \in G(\mathbf{A})^1$, we have

$$\mathcal{X}g \subset \mathcal{Y}.$$

For $\lambda > 0$, let

$$B_\lambda := \{y \in \mathcal{Y} \mid H_Q(y) \leq \lambda\}.$$

This is a closed subset of $\mathcal{Y}$.

Proposition 35

For any $\lambda > 0$ *and* $g \in G(\mathbf{A})^1$, $\mathcal{X}g \cap B_\lambda$ *is a finite set.*

Proof. Fix λ and g. For $y \in B_\lambda$,

$$H_Q(yg^{-1}) \leq H_Q(y)\|g^{-1}\| \leq \lambda \|g^{-1}\|.$$

Let $\mu = \lambda\|g^{-1}\|$. Then $B_\lambda g^{-1} \subset B_\mu$. It suffices to show that $\mathcal{X} \cap B_\mu$ is a finite set. Since Q is a parabolic subgroup, $Q\backslash G$ can be embedded into a projective space. By using the existence of a **strongly Q-rational representation**([4, Section 12]), we can construct an embedding $\varphi : Q\backslash G \hookrightarrow \mathbf{P}^N$ defined over $\mathbf{Q}$ satisfying the following ([28, Section 3]):

- There exists a constant μ', depending on μ, such that

$$\varphi(\mathcal{X} \cap B_\mu) \subset \{v \in \mathbf{P}^N(\mathbf{Q}) \mid H_{\mathbf{P}^N}(v) \leq \mu'\},$$

  where $H_{\mathbf{P}^N}$ denotes the Weil height on $\mathbf{P}^N$.

By Northcott's theorem ([1, Theorem 2.4.9]), the right-hand side is a finite set. Therefore, $\mathcal{X} \cap B_\mu$ is also a finite set. □

► In [4, Section 12], G is assumed to be semisimple. When G is reductive, it is easy to extend a strongly $\mathbf{Q}$-rational representation of $D(G)$ to G. See [3, 14.4].

Let $\mathbf{G}_m(\mathbf{A})_{>1} := \{a \in \mathbf{G}_m(\mathbf{A}) \mid |a|_{\mathbf{A}} > 1\}$.

Proposition 36

Let $\sigma = [n_\sigma]$ and $\tau = [n_\tau] \in W_G$ be elements such that $\sigma^{-1}W_\alpha \neq \tau^{-1}W_\alpha$. Then there exists a $\mathbf{Q}$-cocharacter $\xi = \xi_{\sigma,\tau} \in \mathrm{X}_*(T)_{\mathbf{Q}}$ of T such that

$$H_Q(n_\sigma \xi(a) n_\sigma^{-1}) > H_Q(n_\tau \xi(a) n_\tau^{-1}) \qquad ({}^\forall a \in \mathbf{G}_m(\mathbf{A})_{>1}).$$

Proof. By Proposition 31, $\sigma^{-1}\widehat{\alpha}\big|_T \neq \tau^{-1}\widehat{\alpha}\big|_T$. Thus, by the nondegenerate pairing

$$\langle \cdot, \cdot \rangle \ : \ \mathrm{X}^*(T)_{\mathbf{Q}} \times \mathrm{X}_*(T)_{\mathbf{Q}} \longrightarrow \mathbf{Z},$$

there exists $\xi \in \mathrm{X}_*(T)_{\mathbf{Q}}$ such that

$$\ell := \langle \sigma^{-1}\widehat{\alpha}\big|_T - \tau^{-1}\widehat{\alpha}\big|_T \ , \ \xi \rangle < 0.$$

Then we can write

$$\widehat{\alpha}(n_\sigma \xi(x) n_\sigma^{-1}) \cdot \widehat{\alpha}(n_\tau \xi(x) n_\tau^{-1})^{-1} = x^\ell \qquad ({}^\forall x \in \mathbf{G}_m).$$

Therefore, if $a \in \mathbf{G}_m(\mathbf{A})_{>1}$, then

$$H_Q(n_\sigma \xi(a) n_\sigma^{-1})^{-1} \cdot H_Q(n_\tau \xi(a) n_\tau^{-1}) = |a|_{\mathbf{A}}^\ell < 1$$

holds. □

9.3 Arithmetical Minimum Functions

By Proposition 35, for $g \in G(\mathbf{A})^1$, the following minimum exists:

$$m_Q(g) := \min_{x \in \mathcal{X}} H_Q(xg).$$

We call m_Q the **arithmetical minimum function** defined by H_Q. Let

$$\pi : G(\mathbf{Q}) \longrightarrow \mathcal{X} = Q(\mathbf{Q})\backslash G(\mathbf{Q})$$

be the natural map, and let $\bar{e} = \pi(e) \in \mathcal{X}$. Clearly,

$$m_Q(g) \leq H_Q(\bar{e}g) = H_Q(g).$$

Proposition 37

The function $\boldsymbol{m_Q : G(\mathbf{A})^1 \longrightarrow \mathbf{R}_{>0}}$ *is continuous.*

Proof. Let O be a compact neighborhood of $g_0 \in G(\mathbf{A})^1$. Since H_Q and the norm are continuous, there exist

$$\lambda = \max_{g \in O} H_Q(g), \qquad c = \max_{g \in O} \|g^{-1}\|.$$

Letting $\mu = c\lambda$, as in the proof of Proposition 35, we have

$$\bar{e} \in \mathcal{X} \cap B_\lambda g^{-1} \subset \mathcal{X} \cap B_\mu \qquad (^\forall g \in O).$$

Since $\mathcal{X} \cap B_\mu$ is a finite set, let $\mathcal{X} \cap B_\mu = \{x_1, \ldots, x_\ell\}$. Then

$$m_Q(g) = \min_{1 \leq i \leq \ell} H_Q(x_i g) \qquad (^\forall g \in O).$$

Thus m_Q is continuous on O. □

► By definition,

$$m_Q(\gamma g h) = m_Q(g) \qquad (\gamma \in G(\mathbf{Q}), g \in G(\mathbf{A})^1, h \in K),$$

so

$$m_Q : G(\mathbf{Q})\backslash G(\mathbf{A})^1 / K \longrightarrow \mathbf{R}_{>0}.$$

§10 Fundamental Domains for Arithmetic Quotients

The setting is the same as in Section 9.

10.1 Minimal Points

For $g \in G(\mathbf{A})^1$, define

$$X_Q(g) := \{x \in \mathcal{X} \mid m_Q(g) = H_Q(xg)\}.$$

This is a finite set by Proposition 35. Clearly,

$$X_Q(\gamma g h) = X_Q(g)\gamma^{-1} \qquad (\gamma \in G(\mathbf{Q}), g \in G(\mathbf{A})^1, h \in K)$$

holds. An element of $X_Q(g)$ is called a **minimal point** of g

Proposition 38

For each $\boldsymbol{g_0 \in G(\mathbf{A})^1}$, there exists a neighborhood $\boldsymbol{O}$ of $\boldsymbol{g_0}$ such that $\boldsymbol{X_Q(g) \subset X_Q(g_0)}$ holds for all $\boldsymbol{g \in O}$.

Proof. For g_0, let

$$c = \min_{x \in \mathcal{X} - X_Q(g_0)} H_Q(xg_0).$$

Then $m_Q(g_0) < c$. Choose a constant δ such that $1 < \delta < c/m_Q(g_0)$, and let

$$O_e := \left\{ u \in G(\mathbf{A})^1 \mid \|u^{-1}\| < \frac{c}{\delta m_Q(g_0)} \text{ and } \frac{m_Q(g_0 u)}{m_Q(g_0)} < \delta \right\}.$$

By the continuity of m_Q, O_e is a neighborhood of the identity element e. We will show that $X_Q(g_0u) \subset X_Q(g_0)$ for any $u \in O_e$. By the definition of the norm, for any $y \in \mathcal{Y}$ and $u \in O_e$, we have

$$\frac{H_Q(yuu^{-1})}{H_Q(yu)} \leq \|u^{-1}\|.$$

Let $y = xg_0$ with $x \in X_Q(g_0u)$. Then

$$\frac{H_Q(xg_0)}{\|u^{-1}\|} \leq H_Q(xg_0u) = m_Q(g_0u).$$

If $x \notin X_Q(g_0)$, then $c \leq H_Q(xg_0)$, so

$$\delta m_Q(g_0) \leq \delta m_Q(g_0)\frac{H_Q(xg_0)}{c} < \frac{H_Q(xg_0)}{\|u^{-1}\|} \leq m_Q(g_0u) < \delta m_Q(g_0),$$

which is a contradiction. Therefore $x \in X_Q(g_0)$. □

► A neighborhood O with the property of Proposition 38 will be called a **stable neighborhood** of g_0.

10.2 Ryshkov Domains

For m_Q, define the closed subset of $G(\mathbf{A})^1$ as follows:

$$R = R_Q := \{g \in G(\mathbf{A})^1 \mid m_Q(g) = H_Q(g)\} = \{g \in G(\mathbf{A})^1 \mid \bar{e} \in X_Q(g)\},$$

which is called the **Ryshkov domain** defined by m_Q.

Proposition 39

The following hold:

(1) $\boldsymbol{R = Q(\mathbf{Q})RK}$.

(2) $\boldsymbol{G(\mathbf{A})^1 = G(\mathbf{Q})R}$.

(3) *For* $\boldsymbol{g \in G(\mathbf{A})^1}$, $\boldsymbol{X_Q(g) = \{\pi(\gamma) \mid \gamma \in G(\mathbf{Q}),\ \gamma g \in R\}}$.

(4) *For* $\boldsymbol{\gamma \in G(\mathbf{Q})}$, $\boldsymbol{\gamma R \subset R}$ *if and only if* $\boldsymbol{\gamma \in Q(\mathbf{Q})}$.

Proof. (1) is clear. Let $g \in G(\mathbf{A})^1$ and $x = \pi(\gamma) \in \mathcal{X}$. From

$$x \in X_Q(g) \iff H_Q(xg) = m_Q(g) = m_Q(\gamma g) \iff \gamma g \in R,$$

both (2) and (3) follow. Suppose $\gamma R \subset R$. Then for any $g \in R$, $\gamma g \in R$, so by (3), $x = \pi(\gamma) \in X_Q(g)$. Thus

$$x \in \bigcap_{g \in R} X_Q(g).$$

Since $\gamma Q(\mathbf{Q})R = \gamma R \subset R$, the same argument implies

$$\pi(\gamma Q(\mathbf{Q})) \subset \bigcap_{g \in R} X_Q(g).$$

If $\gamma \notin Q(\mathbf{Q})$, then $\pi(\gamma Q(\mathbf{Q})) \subset \mathcal{X}$ is an infinite set by the Bruhat decomposition. □

For each $g \in G(\mathbf{A})^1$, denote the number of elements in $X_Q(g)$ by $n_Q(g)$.

Proposition 40

Let $\boldsymbol{g_0 \in R}$ *be such that* $\boldsymbol{n_Q(g_0) \geq 2}$, *and let* $\boldsymbol{x_0 \in X_Q(g_0)}$ *be arbitrary. Then any neighborhood* $\boldsymbol{O}$ *of* $\boldsymbol{g_0}$ *contains an element* $\boldsymbol{g \in O}$ *such that* $\boldsymbol{X_Q(g) \subset X_Q(g_0)}$ *and* $\boldsymbol{x_0 \notin X_Q(g)}$.

Proof. We may assume that O is a stable neighborhood of g_0. Since $n_Q(g_0) \geq 2$, we can take $\bar{e} \neq y \in X_Q(g_0)$. This y can be written as

$$y = \pi(n_\sigma \gamma), \qquad (\gamma \in Q(\mathbf{Q}),\ \sigma = [n_\sigma] \in W_G - W_\alpha).$$

By Proposition 36, there exists a cocharacter $\xi = \xi_{\sigma,e} \in \mathrm{X}_*(T)_{\mathbf{Q}}$ such that

$$H_Q(n_\sigma \xi(a) n_\sigma^{-1}) > H_Q(\xi(a)) \qquad ({}^\forall a \in \mathbf{G}_m(\mathbf{A})_{>1}).$$

Take a sufficiently close to the identity so that $g_a := \gamma^{-1}\xi(a)\gamma g_0 \in O$. Then

$$\begin{aligned} H_Q(g_a) &= H_Q(\xi(a)\gamma g_0) = H_Q(\xi(a)) H_Q(g_0) \\ &= H_Q(\xi(a)) m_Q(g_0), \\ H_Q(y g_a) &= H_Q(n_\sigma \xi(a) \gamma g_0) = H_Q(n_\sigma \xi(a) n_\sigma^{-1}) H_Q(n_\sigma \gamma g_0) \\ &= H_Q(n_\sigma \xi(a) n_\sigma^{-1}) m_Q(g_0) \end{aligned}$$

hold. Therefore

$$\begin{cases} H_Q(g_a) < H_Q(y g_a) & (a \in \mathbf{G}_m(\mathbf{A})_{>1}), \\ H_Q(g_a) > H_Q(y g_a) & (a^{-1} \in \mathbf{G}_m(\mathbf{A})_{>1}). \end{cases}$$

We consider the cases for $x_0 \in X_Q(g_0)$.
If $x_0 = \bar{e}$, then taking $a^{-1} \in \mathbf{G}_m(\mathbf{A})_{>1}$, we have

$$m_Q(g_a) \leq H_Q(y g_a) < H_Q(g_a),$$

so $x_0 \notin X_Q(g_a)$.
If $x_0 \neq \bar{e}$, we can take $y = x_0$. Taking $a \in \mathbf{G}_m(\mathbf{A})_{>1}$, we have

$$m_Q(g_a) \leq H_Q(g_a) < H_Q(x_0 g_a),$$

so $x_0 \notin X_Q(g_a)$. □

Corollary 41

$\min_{g \in R} n_Q(g) = 1$.

Proof. Take $g_0 \in R$ such that $n_Q(g_0) = \min_{g \in R} n_Q(g)$. If $n_Q(g_0) \geq 2$, then by Proposition 40, there exists $g_1 \in G(\mathbf{A})^1$ such that $n_Q(g_1) < n_Q(g_0)$. By Proposition 39 (2), there exists $\gamma \in G(\mathbf{Q})$ such that $\gamma g_1 \in R$. Since $X_Q(\gamma g_1) = X_Q(g_1)\gamma^{-1}$, we have $n_Q(\gamma g_1) = n_Q(g_1) < n_Q(g_0)$, which contradicts the minimality of $n_Q(g_0)$. □

10.3 Interior of R

Let R° be the interior of R in $G(\mathbf{A})^1$. Define

$$R_1 := \{g \in R \mid n_Q(g) = 1\} = \{g \in G(\mathbf{A})^1 \mid X_Q(g) = \{\overline{e}\}\}.$$

Clearly $Q(\mathbf{Q})R_1 = R_1$ and

$$G(\mathbf{Q})R_1 = \{g \in G(\mathbf{A})^1 \mid n_Q(g) = 1\}.$$

Proposition 42

The following hold:

(1) $\boldsymbol{R^\circ = R_1}$.

(2) $\boldsymbol{G(\mathbf{Q})R_1}$ *is open and dense in* $\boldsymbol{G(\mathbf{A})^1}$.

(3) *For* $\boldsymbol{\gamma \in G(\mathbf{Q})}$, $\boldsymbol{R_1 \cap \gamma R \neq \emptyset}$ *if and only if* $\boldsymbol{\gamma \in Q(\mathbf{Q})}$.

(4) *Let* $\boldsymbol{R_1^-}$ *be the closure of* $\boldsymbol{R_1}$ *in* $\boldsymbol{G(\mathbf{A})^1}$. *Then* $\boldsymbol{G(\mathbf{A})^1 = G(\mathbf{Q})R_1^-}$.

Proof. (1) Let $g \in R_1$ and $\mathcal{O}$ be a stable neighborhood of g. Then $\mathcal{O} \subset R_1$, so R_1 is open. Thus $R_1 \subset R^\circ$. If $R_1 \neq R^\circ$, there exists $g_0 \in R^\circ$ such that $n_Q(g_0) \geq 2$. By Proposition 40, R° contains $g \in R^\circ$ such that $\overline{e} \notin X_Q(g)$, which contradicts the definition of R.

(2) Since R_1 is open, $G(\mathbf{Q})R_1$ is also open. We show by contradiction that $G(\mathbf{A})^1 - G(\mathbf{Q})R_1$ has no interior points. Suppose there exists an interior point $g_0 \in G(\mathbf{A})^1 - G(\mathbf{Q})R_1$. Then there exists a neighborhood $\mathcal{O}$ of g_0 such that $\mathcal{O} \cap G(\mathbf{Q})R_1 = \emptyset$. There exists $\gamma_0 \in G(\mathbf{Q})$ such that $\gamma_0 g_0 \in R$. Since $n_Q(g_0) = n_Q(\gamma_0 g_0) \geq 2$, by Proposition 40, there exists $g_1 \in \gamma_0 \mathcal{O}$ such that $n_Q(g_1) < n_Q(g_0)$. There exists $\gamma_1 \in G(\mathbf{Q})$ such that $\gamma_1 g_1 \in R$. If $n_Q(g_1) \geq 2$, there exist $g_2 \in \gamma_1\gamma_0\mathcal{O}$ and $\gamma_2 \in G(\mathbf{Q})$ such that $n_Q(g_2) < n_Q(g_1)$ and $\gamma_2 g_2 \in R$. Repeating this process, we find $g_\ell \in \gamma_{\ell-1}\cdots\gamma_1\mathcal{O}$ such that $n_Q(g_\ell) = 1$. Then $(\gamma_{\ell-1}\cdots\gamma_1)^{-1} g_\ell \in \mathcal{O} \cap G(\mathbf{Q})R_1$, which is a contradiction.

(3) If there exists $g \in R_1 \cap \gamma R$, then by Proposition 39 (3),

$$\pi(\gamma^{-1}) \in X_Q(g) = \{\overline{e}\},$$

so $\gamma \in Q(\mathbf{Q})$.

(4) Let $g \in G(\mathbf{A})^1$ be arbitrary, and let $\mathcal{O}$ be a stable neighborhood of g. By (2), there exists a sequence $\{g_n\} \subset \mathcal{O} \cap G(\mathbf{Q})R^1$ converging to g. Since $n_Q(g_n) = 1$, we have $X_Q(g_n) = \{x_n\}$. Since $x_n \in X_Q(g)$ for all n, there exists a subsequence $\{g_{n_j}\}$ such that $x_{n_j} = x$ for all j. Let $x = \pi(\gamma)$, $\gamma \in G(\mathbf{Q})$. Then $\{g_{n_j}\} \subset \gamma^{-1}R_1$, and $g \in \gamma^{-1}R_1^-$. □

► The arithmetical minimum function m_Q has the maximum value $\max m_Q$. ([29, Proposition 1]). This is proved by using Borel–Harish-Chandra's Theorem (Theorem 28). By Proposition 42 (4), we have

$$\max m_Q = \max_{g \in G(\mathbf{A})^1} m_Q(g) = \max_{g \in R_1^-} m_Q(g).$$

If $g_0 \in R_1^-$ attains $\max m_Q$, then g_0 must be in the boundary of R_1^-. This is proved as follows. The height function H_Q yields an isomorphism from $Z_G(\mathbf{A})Z_M(\mathbf{A})^1 \backslash Z_M(\mathbf{A})$ onto $\mathbf{R}_{>0}$. Let $g_0 \in R_1$ and $z \in Z_M(\mathbf{A})$. If z is sufficiently close to the identity element, then $zg_0 \in R_1$ since R_1 is open, and we have

$$m_Q(zg_0) = H_Q(zg_0) = H_Q(z)H_Q(g_0) = H_Q(z)m_Q(g_0).$$

Since $H_Q(z)$ can vary in a neighborhood of 1, $m_Q(g_0)$ cannot be a maximum.

10.4 Fundamental Domains

Since $Q(\mathbf{Q})R_1^- = R_1^-$, $Q(\mathbf{Q})$ acts freely and properly discontinuously on R_1^-. Let Ω be an open fundamental domain for $Q(\mathbf{Q})\backslash R_1^-$. Denote the interior and closure of Ω in $G(\mathbf{A})^1$ by Ω° and Ω^-, respectively.

Proposition 43

$\Omega^\circ = \Omega \cap R_1$ *and* **$\Omega^- = (\Omega^\circ)^-$**.

Proof. $\Omega^\circ \subset R_1$. Indeed, if there exists $g_0 \in \Omega^\circ \cap (R_1^- - R_1)$, then $n_Q(g_0) \geq 2$. Let $\mathcal{O} \subset \Omega^\circ$ be a neighborhood of g_0. Then by Proposition 40, there exists $g \in \mathcal{O} \subset R_1^-$ such that $\bar{e} \notin X_Q(g)$, which is a contradiction. Thus $\Omega^\circ \subset \Omega \cap R_1$. Since Ω is open in the relative topology of R_1^-, there exists an open set U in $G(\mathbf{A})^1$ such that $\Omega = R_1^- \cap U$. Therefore $\Omega \cap R_1 = R_1 \cap U$ is open in $G(\mathbf{A})^1$, so $\Omega \cap R_1 \subset \Omega^\circ$. For the latter half, it suffices to show that $\Omega \subset (\Omega^\circ)^-$. Let $g \in \Omega$, and let $\mathcal{O}$ be any neighborhood of g in $G(\mathbf{A})^1$. Since $g \in R_1^-$, we have $\mathcal{O} \cap R_1 \neq \emptyset$. Thus $g \in (\Omega \cap R_1)^-$. □

Theorem 44

Ω° *is an open fundamental domain for* **$G(\mathbf{Q})\backslash G(\mathbf{A})^1$**.

Proof. By the choice of Ω, we have $R_1^- = Q(\mathbf{Q})\Omega^-$. By Proposition 42 (4), $G(\mathbf{A})^1 = G(\mathbf{Q})R_1^- = G(\mathbf{Q})\Omega^-$. Let $\gamma \in G(\mathbf{Q})$ be such that $\Omega^\circ \cap \gamma\Omega^- \neq \emptyset$. By Proposition 42 (3), $\gamma \in Q(\mathbf{Q})$. Since Ω is an open fundamental domain for the action of $Q(\mathbf{Q})$, we have $\gamma = e$. □

10.5 Class Numbers

We prepare a result that will be needed in the next section. We have fixed a maximal compact subgroup K of $G(\mathbf{A})$, which we express as

$$K = K_\infty \times K_f, \qquad K_f := \prod_{p \in \mathcal{P}_f} K_p.$$

We define the following notation:

$$G_{\mathbf{A},\infty} := G(\mathbf{Q}_\infty) \times K_f, \quad G^1_{\mathbf{A},\infty} := G_{\mathbf{A},\infty} \cap G(\mathbf{A})^1, \quad G_{\mathbf{Z}} := G(\mathbf{Q}) \cap G_{\mathbf{A},\infty}.$$

The number of elements in the double coset space $G(\mathbf{Q})\backslash G(\mathbf{A})/G_{\mathbf{A},\infty}$ is denoted by

$$n(G) := \sharp\left(G(\mathbf{Q})\backslash G(\mathbf{A})/G_{\mathbf{A},\infty}\right),$$

which is called the **class number** of G.

Theorem 45 ([5, 5.1])

***n*(*G*)** *is finite.*

Examples

(1) $n(\mathrm{GL}_n) = 1$. In particular, $n(\mathbf{G}_m) = 1$, and hence $n(T) = 1$ if T is a $\mathbf{Q}$-split torus.

(2) Let G be a connected simply connected almost simple $\mathbf{Q}$-group. If G is $\mathbf{Q}$-isotropic, then $n(G) = 1$. This is a consequence of the strong approximation property of G ([21, Theorem 7.12]). In particular, $n(\mathrm{SL}_n) = 1$.

(3) The class number can be defined for a general connected $\mathbf{Q}$-algebraic group, not necessarily reductive. The class number of a unipotent group equals to 1 ([5, 2.5]). In general, the class number of a connected $\mathbf{Q}$-algebraic group is less than or equal to the class number of its Levi subgroup ([5, 2.7]).

► If $n(G) = 1$, then clearly $G(\mathbf{A}) = G(\mathbf{Q})G_{\mathbf{A},\infty}$. From this, $G(\mathbf{A})^1 = G(\mathbf{Q})G^1_{\mathbf{A},\infty}$.

► Let k be an algebraic number field of finite degree. The class number $n_{\mathrm{k}}(G)$ is defined as

$$n_{\mathrm{k}}(G) := \sharp\left(G(\mathrm{k})\backslash G(\mathbf{A}_{\mathrm{k}})/G_{\mathbf{A}_{\mathrm{k}},\infty}\right),$$

where $\mathbf{A}_{\mathrm{k}} = \mathbf{A} \otimes_{\mathbf{Q}} \mathrm{k}$ denotes the adele ring of k. The class number $n_{\mathrm{k}}(\mathrm{GL}_n)$ coincides with the ideal class number of k ([5, 2.2]).

Theorem 46 ([5, 7.5])

Let ***P*** *be a parabolic* $\mathbf{Q}$*-subgroup of* ***G***. *Then the number of elements in the double coset space* $\boldsymbol{P(Q)\backslash G(Q)/G_{\mathbf{Z}}}$ *is equal to the class number of a Levi subgroup of* ***P***.

Example In the case $G = \mathrm{GL}_n$, we can take $K_\infty = \mathrm{O}_n(\mathbf{R})$ and $K_p = \mathrm{GL}_n(\mathbf{Z}_p)$. In this case,

$$G_{\mathbf{Z}} = \mathrm{GL}_n(\mathbf{Q}) \cap \left(\mathrm{GL}_n(\mathbf{R}) \times \prod_p \mathrm{GL}_n(\mathbf{Z}_p) \right) = \mathrm{GL}_n(\mathbf{Z}).$$

Since the class number of T_n is equal to 1, we have

$$\mathrm{GL}_n(\mathbf{Q}) = \mathrm{B}_n(\mathbf{Q})\mathrm{GL}_n(\mathbf{Z}).$$

In particular, for the standard maximal parabolic subgroup $\mathrm{Q} = \mathrm{Q}_{n,k}$,

$$\mathrm{GL}_n(\mathbf{Q}) = \mathrm{Q}(\mathbf{Q})\mathrm{GL}_n(\mathbf{Z}).$$

This equality can be shown elementarily without using the result of class number 1. Let $\mathcal{X} = Q(\mathbf{Q})\backslash\mathrm{GL}_n(\mathbf{Q})$, and let $\pi : \mathrm{GL}_n(\mathbf{Q}) \longrightarrow \mathcal{X}$ be the natural map. Then $\pi(\mathrm{GL}_n(\mathbf{Z})) = \mathcal{X}$. Let $Q_{\mathbf{Z}} = Q(\mathbf{Q}) \cap \mathrm{GL}_n(\mathbf{Z})$. Then π induces a bijection $Q_{\mathbf{Z}}\backslash\mathrm{GL}_n(\mathbf{Z}) \cong \mathcal{X}$.

§11 Fundamental Domains in the Case of Class Number 1

We use the same notation as in Section 10.

11.1 ∞ Components

In this section, **we assume** $n(G) = n(M) = 1$. Thus

$$G(\mathbf{Q}) = Q(\mathbf{Q})G_{\mathbf{Z}}, \qquad G(\mathbf{A})^1 = G(\mathbf{Q})G^1_{\mathbf{A},\infty} = Q(\mathbf{Q})G^1_{\mathbf{A},\infty}$$

hold. From $G(\mathbf{A}) = G(\mathbf{Q}_\infty) \times G(\mathbf{A}_f)$, we regard $G(\mathbf{Q}_\infty)$ as a subgroup of $G(\mathbf{A})$ and set $G(\mathbf{Q}_\infty)^1 := G(\mathbf{Q}_\infty) \cap G(\mathbf{A})^1$, i.e.,

$$G(\mathbf{Q}_\infty)^1 = \{umh \mid u \in U(\mathbf{Q}_\infty),\ m \in M(\mathbf{Q}_\infty),\ h \in K_\infty,\ |\widehat{\alpha}(m)|_\infty = 1\}.$$

Clearly, $G^1_{\mathbf{A},\infty} = G(\mathbf{Q}_\infty)^1 \times K_f$. Also, for $g_\infty \in G(\mathbf{Q}_\infty)^1$, by the class number 1 assumption,

$$m_Q(g_\infty) = \min_{x \in \mathcal{X}} H_Q(xg_\infty) = \min_{\delta \in G_{\mathbf{Z}}} H_Q(\delta g_\infty).$$

► Since $\delta g_\infty = (\delta g_\infty, \delta) \in G(\mathbf{Q}_\infty)^1 \times K_f$ as an element of $G(\mathbf{A})^1_{\mathbf{A},\infty}$, the finite adele component is contained in K_f. In the decomposition $G(\mathbf{Q}_\infty) = U(\mathbf{Q}_\infty)M(\mathbf{Q}_\infty)K_\infty$ which follows from the Iwasawa decomposition, let $(\delta g_\infty)_M$ denote the $M(\mathbf{Q}_\infty)$ component of δg_∞. Then

$$H_Q(\delta g_\infty) = |\widehat{\alpha}((\delta g_\infty)_M)|^{-1}_\infty.$$

Therefore, $H_Q(\delta g_\infty)$, and hence $m_Q(g_\infty)$, are determined only by the infinite place component.

We define the Ryshkov domain at the infinite place by

$$R_\infty := \{g_\infty \in G(\mathbf{Q}_\infty)^1 \mid m_Q(g_\infty) = H_Q(g_\infty)\}.$$

By the class number 1 assumption, i.e., $G(\mathbf{A})^1 = Q(\mathbf{Q})G^1_{\mathbf{A},\infty}$, we have

$$R = Q(\mathbf{Q}) \cdot (R_\infty \times K_f).$$

Define the subgroup $Q_{\mathbf{Z}}$ of $Q(\mathbf{Q})$ by

$$Q_{\mathbf{Z}} := Q(\mathbf{Q}) \cap G_{\mathbf{A},\infty} = Q(\mathbf{Q}) \cap G_{\mathbf{Z}}.$$

The closed set $R_\infty \times K_f$ is $Q_{\mathbf{Z}}$-invariant, i.e.,

$$Q_{\mathbf{Z}} \cdot (R_\infty \times K_f) = R_\infty \times K_f.$$

Proposition 47

For $g \in Q(\mathbf{Q})$, $g(R_\infty \times K_f) \cap (R_\infty \times K_f) \neq \emptyset$ if and only if $g \in Q_{\mathbf{Z}}$.

Proof. If there exists $h \in R_\infty \times K_f$ such that $gh \in R_\infty \times K_f$, then

$$g \in (R_\infty \times K_f)h^{-1} \subset G_{\mathbf{A},\infty},$$

so $g \in Q_{\mathbf{Z}}$. The converse is clear. □

Let $\{\gamma_j\}$ be a complete set of representatives for $Q(\mathbf{Q})/Q_{\mathbf{Z}}$. By Proposition 47,

$$R = \bigsqcup_j \gamma_j(R_\infty \times K_f) \qquad \text{(disjoint union)}.$$

Let R_∞° be the interior of R_∞ in $G(\mathbf{Q}_\infty)^1$. Denote the closure of R_∞° by R_∞^*. Since the above decomposition of R is disjoint,

$$R^\circ = \bigsqcup_j \gamma_j(R_\infty^\circ \times K_f), \qquad R_1^- = \bigsqcup_j \gamma_j(R_\infty^* \times K_f).$$

Let

$$R_{\infty,1} = \{g_\infty \in G(\mathbf{Q}_\infty)^1 \mid n_Q(g_\infty) = 1\}.$$

Then $R_\infty^\circ = R_{\infty,1}$ by Proposition 42.

Theorem 48

Let $\boldsymbol{\Omega_\infty}$ be an open fundamental domain for $\boldsymbol{Q_{\mathbf{Z}}\backslash R_\infty^*}$. Then $\boldsymbol{\Omega = \Omega_\infty \times K_f}$ is an open fundamental domain for $\boldsymbol{Q(\mathbf{Q})\backslash R_1^-}$.

Proof. Let Ω_∞^* be the closure of Ω_∞ in $G(\mathbf{Q}_\infty)^1$. Then $\Omega^- = \Omega_\infty^* \times K_f$ and

$$Q(\mathbf{Q})\Omega^- = Q(\mathbf{Q})(\Omega_\infty^* \times K_f) = \bigcup_j \gamma_j Q_{\mathbf{Z}}(\Omega_\infty^* \times K_f) = \bigcup_j \gamma_j(R_\infty^* \times K_f) = R_1^-.$$

Suppose

$$\emptyset \neq \Omega \cap g\Omega^- = (\Omega_\infty \times K_f) \cap g(\Omega_\infty^* \times K_f)$$

for $g \in Q(\mathbf{Q})$. Then $g = \gamma_j\delta$ for some j and $\delta \in Q_{\mathbf{Z}}$. Since $\delta\Omega_\infty^* \subset R_\infty$,

$$\emptyset \neq (R_\infty \times K_f) \cap \gamma_j(R_\infty \times K_f).$$

By Proposition 47, $\gamma_j = e$, so $g = \delta$. Furthermore,

$$\emptyset \neq \Omega_\infty \cap \delta\Omega_\infty^*$$

implies $\delta = e$. □

► Let Ω_∞° be the interior of Ω_∞ in $G(\mathbf{Q}_\infty)^1$. By Theorem 44, $\Omega_\infty^\circ \times K_f$ provides an open fundamental domain for $G(\mathbf{Q})\backslash G(\mathbf{A})^1$.

► A simple argument shows that Ω_∞° is an open fundamental domain for $G_{\mathbf{Z}}\backslash G(\mathbf{Q}_\infty)^1$.

► As noted below Proposition 42, the maximum of m_Q is attained on the boundary of R_∞^*.

► The cases where the class number is not equal to 1, as well as the cases where the field of definition is an algebraic number field, were studied by Lee Tim Weng ([30]). Fujimori ([12]) studied the case GL_n defined over an algebraic number field.

11.2 The Case of GL_n

Let $G = \mathrm{GL}_n$, fix $k \in \{1, \ldots, n-1\}$, and let $Q = Q_k = Q_{n,k}$. Take the maximal compact subgroup K of $G(\mathbf{A})$ as

$$K_\infty = \mathrm{O}_n(\mathbf{R}), \qquad K_p = \mathrm{GL}_n(\mathbf{Z}_p) \quad ({}^\forall p \in \mathcal{P}_f).$$

By definition,

$$G(\mathbf{Q}_\infty)^1 = \{g_\infty \in \mathrm{GL}_n(\mathbf{R}) \mid |\det g|_\infty = 1\}.$$

Also,

$$G_{\mathbf{Z}} = G(\mathbf{Q}) \cap G_{\mathbf{A},\infty} = \mathrm{GL}_n(\mathbf{Z}), \qquad Q_{\mathbf{Z}} = Q(\mathbf{Q}) \cap \mathrm{GL}_n(\mathbf{Z}).$$

Let

$$\mathrm{P}_n := \{A \in \mathrm{M}_n(\mathbf{R}) \mid {}^t A = A,\ A \text{ is positive definite}\}, \qquad \mathrm{P}_n^1 := \mathrm{P}_n \cap \mathrm{SL}_n(\mathbf{R}).$$

Then the map

$$f\ :\ G(\mathbf{Q}_\infty) = \mathrm{GL}_n(\mathbf{R}) \longrightarrow \mathrm{P}_n\ :\ f(g_\infty) = {}^t g_\infty^{-1} g_\infty^{-1}$$

yields homeomorphisms

$$G(\mathbf{Q}_\infty)/K_\infty \cong \mathrm{P}_n, \qquad G(\mathbf{Q}_\infty)^1/K_\infty \cong \mathrm{P}_n^1.$$

Any $A \in \mathrm{P}_n$ has a unique Jacobi decomposition

$$A = \begin{pmatrix} E_k & 0 \\ {}^t u & E_{n-k} \end{pmatrix} \begin{pmatrix} v & 0 \\ 0 & w \end{pmatrix} \begin{pmatrix} E_k & u \\ 0 & E_{n-k} \end{pmatrix} \qquad (u \in \mathrm{M}_{k,n-k}(\mathbf{R}),\ v \in \mathrm{P}_k,\ w \in \mathrm{P}_{n-k}).$$

We write

$$u = u_A, \qquad v = A^{[k]}, \qquad w = A_{[n-k]}.$$

• Description of H_Q

Let

$$V^{n,k} = \bigwedge^k \mathbf{Q}^n, \qquad V_q^{n,k} = \bigwedge^k \mathbf{Q}_q^n \quad (q \in \mathcal{P}).$$

Let $e_1, \ldots, e_n$ be the standard basis of $\mathbf{Q}^n$. For a subset $I = \{i_1 < \cdots < i_k\}$ of $\{1, \ldots, n\}$ with k elements, let $e_I = e_{i_1} \wedge \cdots \wedge e_{i_k}$. Then $\{e_I\}_I$ is a basis of $V^{n,k}$ and $V_q^{n,k}$. Define the local height $H_q : V_q^{n,k} \longrightarrow \mathbf{R}_{>0}$ by

$$H_\infty\left(\sum_I a_I e_I\right) = \left(\sum_I |a_I|_\infty^2\right)^{1/2},$$

$$H_p\left(\sum_I a_I e_I\right) = \sup_I |a_I|_p \qquad (p \in \mathcal{P}_f).$$

Define the function $H_{n,k} : \mathrm{GL}_n(\mathbf{A}) \longrightarrow \mathbf{R}_{>0}$ by

$$H_{n,k}(g) = \prod_{q \in \mathcal{P}} H_q(g_q e_1 \wedge \cdots \wedge g_q e_k).$$

A simple calculation shows that

$$H_{n,k}\left(h\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} u\right) = |\det a|_{\mathbf{A}}, \quad (h \in K,\ a \in \mathrm{GL}_k(\mathbf{A}),\ d \in \mathrm{GL}_{n-k}(\mathbf{A}), u \in U_{n,k}(\mathbf{A})),$$

so

$$H_Q(g) = H_{n,k}(g^{-1})^{n/\ell} \qquad (g \in G(\mathbf{A})^1, \quad \ell = \gcd(n,k)).$$

Consider the case $g = \gamma g_\infty$ ($\gamma \in G_{\mathbf{Z}}, g_\infty \in G(\mathbf{Q}_\infty)^1$). For each $p \in \mathcal{P}_f$, $g_p = \gamma \in \mathrm{GL}_n(\mathbf{Z}) \subset K_p$, so

$$H_p(g_p e_1 \wedge \cdots \wedge g_p e_k) = 1.$$

Thus

$$H_Q(\gamma g_\infty) = H_\infty(g_\infty^{-1}\gamma^{-1} e_1 \wedge \cdots \wedge g_\infty^{-1}\gamma^{-1} e_k)^{n/\ell}.$$

From this formula, it is also clear that if $\gamma \in Q_{\mathbf{Z}}$, then $H_Q(\gamma g_\infty) = H_Q(g_\infty)$. Let $E_{n,k}$ be the $n \times k$ matrix consisting of the first k columns of the identity matrix E_n. By Binet's formula ([1, Proposition 2.8.8]),

$$H_Q(\gamma g_\infty) = \det({}^t(\gamma^{-1}E_{n,k}) f(g_\infty)(\gamma^{-1}E_{n,k}))^{n/2\ell}.$$

Let

$$\gamma_{(k)} = \gamma E_{n,k}, \qquad \Gamma_{n,k} := \{\gamma_{(k)} \mid \gamma \in \mathrm{GL}_n(\mathbf{Z})\}.$$

Then

$$m_Q(g_\infty) = \min_{\gamma_{(k)} \in \Gamma_{n,k}} \det({}^t\gamma_{(k)} f(g_\infty)\gamma_{(k)})^{n/2\ell}.$$

Since $H_Q(g_\infty) = \det({}^tE_{n,k} f(g_\infty) E_{n,k})^{n/2\ell}$,

$$\begin{aligned} R_\infty &= \{g_\infty \in G(\mathbf{Q}_\infty)^1 \mid m_Q(g_\infty) = H_Q(g_\infty)\} \\ &= \{g_\infty \in G(\mathbf{Q}_\infty)^1 \mid \det({}^tE_{n,k} f(g_\infty) E_{n,k}) \le \det({}^t\gamma_{(k)} f(g_\infty) \gamma_{(k)}) \quad ({}^\forall\gamma_{(k)})\}. \end{aligned}$$

Since $R_\infty^\circ = R_{\infty,1}$,

$$R_\infty^\circ = \{g_\infty \in G(\mathbf{Q}_\infty)^1 \mid \det({}^tE_{n,k} f(g_\infty) E_{n,k}) < \det({}^t\gamma_{(k)} f(g_\infty) \gamma_{(k)}) \quad ({}^\forall\gamma_{(k)} \notin Q_{\mathbf{Z}} E_{n,k})\}.$$

• Description of a fundamental domain

$\mathrm{GL}_k(\mathbf{Z})$ acts naturally on $\Gamma_{n,k}$ by multiplication from the right. Let $S_{n,k}$ be a complete set of representatives for $\Gamma_{n,k}/\mathrm{GL}_k(\mathbf{Z})$, and assume $E_{n,k} \in S_{n,k}$. For any nonempty subset $S \subset \Gamma_{n,k}$, define the closed subset $\mathrm{R}(S)$ of P_n by

$$\mathrm{R}(S) := \{A \in \mathrm{P}_n \mid \det A^{[k]} \le \det({}^tXAX) \quad ({}^\forall X \in S)\}.$$

In particular, let

$$\mathrm{R}_{n,k} := \{A \in \mathrm{P}_n \mid \det A^{[k]} \le \det({}^tXAX) \quad ({}^\forall X \in \Gamma_{n,k})\}.$$

Then $\mathrm{R}_{n,k} = \mathrm{R}(S_{n,k})$. The interior of $\mathrm{R}_{n,k}$ is given by

$$\mathrm{R}_{n,k}^\circ := \{A \in \mathrm{P}_n \mid \det A^{[k]} < \det({}^tXAX) \quad ({}^\forall X \in S_{n,k} - \{E_{n,k}\})\}.$$

Then

$$R_\infty^\circ / K_\infty \cong f(R_\infty^\circ) = \mathrm{R}_{n,k}^\circ \cap \mathrm{P}_n^1.$$

Define the right action of $G_{\mathbf{Z}}$ on P_n by

$$\mathrm{P}_n \times G_{\mathbf{Z}} \longrightarrow \mathrm{P}_n \ : \ (A, \gamma) \mapsto A[\gamma] := {}^t\gamma A \gamma.$$

Then

$$Q_{\mathbf{Z}} \backslash R_\infty^\circ / K_\infty \cong (\mathrm{R}_{n,k}^\circ \cap \mathrm{P}_n^1)/Q_{\mathbf{Z}}.$$

If $\gamma \in Q_{\mathbf{Z}}$ is of the form

$$\gamma = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \qquad (a \in \mathrm{GL}_k(\mathbf{Z}), d \in \mathrm{GL}_{n-k}(\mathbf{Z}), b \in \mathrm{M}_{k,n-k}(\mathbf{Z})),$$

then for $A \in \mathrm{P}_n$,

$$u_{A[\gamma]} = a^{-1}(u_A d + b), \qquad A[\gamma]^{[k]} = {}^taA^{[k]}a, \qquad A[\gamma]_{[n-k]} = {}^tdA_{[n-k]}d.$$

Let $\mathcal{D}$ be a closed fundamental domain for $\mathrm{P}_k/\mathrm{GL}_k(\mathbf{Z})$, and let $\mathcal{E}$ be a closed fundamental domain for $\mathrm{P}_{n-k}/\mathrm{GL}_{n-k}(\mathbf{Z})$. Let

$$\mathrm{M}_{k,n-k}(\mathbf{R})_{1/2} := \{(u_{ij}) \in \mathrm{M}_{k,n-k}(\mathbf{R}) \mid |u_{ij}| \le 1/2 \quad ({}^\forall i, j), \quad u_{11} \ge 0\}.$$

Define

$$\mathrm{F}(\mathcal{D},\mathcal{E}) := \left\{A \in \mathrm{P}_n \mid A^{[k]} \in \mathcal{D},\ A_{[n-k]} \in \mathcal{E},\ u_A \in \mathrm{M}_{k,n-k}(\mathbf{R})_{1/2}\right\}.$$

Let $\mathrm{R}^*_{n,k}$ be the closure of $\mathrm{R}^\circ_{n,k}$ in P_n. Then

$$\mathrm{R}^*_{n,k} \cap \mathrm{F}(\mathcal{D},\mathcal{E})$$

is a closed fundamental domain for $Q_{\mathbf{Z}}$ in $\mathrm{R}^*_{n,k}$. Therefore, the pullback $f^{-1}(\mathrm{R}^*_{n,k} \cap \mathrm{F}(\mathcal{D},\mathcal{E}) \cap \mathrm{P}^1_n)$ is a closed fundamental domain for $R^*_\infty/Q_{\mathbf{Z}}$. By Theorem 48,

$$f^{-1}(\mathrm{R}^*_{n,k} \cap \mathrm{F}(\mathcal{D},\mathcal{E}) \cap \mathrm{P}^1_n) \times K_f$$

is a closed fundamental domain for $G(\mathbf{Q})\backslash G(\mathbf{A})^1$.

► $\mathrm{R}^*_{n,k} \cap \mathrm{F}(\mathcal{D},\mathcal{E})$ is a closed fundamental domain for $\mathrm{P}_n/\mathrm{GL}_n(\mathbf{Z})$. Since the interior of $\mathrm{R}^*_{n,k}$ coincides with the interior of $\mathrm{R}_{n,k}$,

$$\mathrm{R}_{n,k} \cap \mathrm{F}(\mathcal{D},\mathcal{E}) - \mathrm{R}^*_{n,k} \cap \mathrm{F}(\mathcal{D},\mathcal{E}) \subset \partial \mathrm{R}_{n,k}.$$

We weaken the boundary condition in the definition of a fundamental domain and call a closed subset $\Omega \subset \mathrm{P}_n$ an almost fundamental domain (AFD) if it satisfies the following two conditions:

(1) $\mathrm{P}_n = \bigcup_{\gamma \in \mathrm{GL}_n(\mathbf{Z})} {}^t\gamma\Omega\gamma.$

(2) If $B = A[\gamma]$ for $A, B \in \Omega$ and some $\gamma \in \mathrm{GL}_n(\mathbf{Z})$, $\gamma \neq \pm E_n$, then $A \in \partial\Omega$.

Thus, $\mathrm{R}_{n,k} \cap F(\mathcal{D},\mathcal{E})$ is an AFD for $\mathrm{P}_n/\mathrm{GL}_n(\mathbf{Z})$. For $k = 1$, an AFD can be constructed inductively on n as follows. For $n = 2$,

$$\Omega_2 = \mathrm{R}_{2,1} \cap \mathrm{F}(\mathrm{P}_1, \mathrm{P}_1)$$

is an AFD for $\mathrm{P}_2/\mathrm{GL}_2(\mathbf{Z})$. Then

$$\Omega_3 = \mathrm{R}_{3,1} \cap \mathrm{F}(\mathrm{P}_1, \Omega_2)$$

provides an AFD for $\mathrm{P}_3/\mathrm{GL}_3(\mathbf{Z})$. Similarly,

$$\Omega_n = \mathrm{R}_{n,1} \cap \mathrm{F}(\mathrm{P}_1, \Omega_{n-1})$$

provides an AFD for $\mathrm{P}_n/\mathrm{GL}_n(\mathbf{Z})$. This construction coincides with the Korkine-Zolotareff-Grenier construction ([13, Theorem 1], [25, Theorem 2]). The first Ω_2 coincides with Minkowski's fundamental domain.

► Based on the methods described in Sections 9 through 11, Fujimori defined a kind of successive minima derived from a height function and then constructed a fundamental domain for $\mathrm{GL}_n(\mathbf{Q})\backslash\mathrm{GL}_n(\mathbf{A})$. Fujimori's fundamental domain is contained in a Siegel set of $\mathrm{GL}_n(\mathbf{A})$ ([12, Corollary 3.3]).

► Grenier constructed the **Satake compactification** of $\mathrm{P}_n^1/\mathrm{GL}_n(\mathbf{Z})$ by using Ω_n ([14, Section 4] or [19, Chapter 1, Section 4]). If we put $\Omega_n^1 = \Omega_n \cap \mathrm{P}_n^1$, then this compactification is described as $\Omega_n^1 \cup \Omega_{n-1}^1 \cup \cdots \cup \Omega_1^1$.

11.3 Remaining Problems

Since the number of inequalities defining $\mathrm{R}_{n,k} = \mathrm{R}(S_{n,k})$ is infinite, the finiteness of the boundary of $\mathrm{R}_{n,k} \cap \mathrm{F}(\mathcal{D}, \mathcal{E})$ is not obvious. The finiteness of the boundary of Ω_n constructed above was shown in [13]. That is, there exists a finite subset $S^{(n)} \subset \Gamma_{n,1}$ such that

$$\mathrm{R}_{n,1} \cap \mathrm{F}(\mathrm{P}_1, \Omega_{n-1}) = \mathrm{R}(S^{(n)}) \cap \mathrm{F}(\mathrm{P}_1, \Omega_{n-1}).$$

It is not known whether a similar result holds for general $\mathrm{R}_{n,k} \cap \mathrm{F}(\mathcal{D}, \mathcal{E})$. There is no restriction on the choice of $\mathcal{D}$ and $\mathcal{E}$, but to make the problem concrete, let M_n be Minkowski's fundamental domain for $\mathrm{P}_n/\mathrm{GL}_n(\mathbf{Z})$ and take $\mathcal{D} = \mathrm{M}_k$, $\mathcal{E} = \mathrm{M}_{n-k}$.

Problem

- *Does there exist a finite subset* $\boldsymbol{S_0 \subset S_{n,k}}$ *such that* $\boldsymbol{\mathrm{R}_{n,k} \cap \mathrm{F}(\mathrm{M}_k, \mathrm{M}_{n-k}) = \mathrm{R}(S_0) \cap \mathrm{F}(\mathrm{M}_k, \mathrm{M}_{n-k})}$*?*
- *Give an exact* $\boldsymbol{S_0}$ *for small* $\boldsymbol{n}$ *if there exists such a finite subset* $\boldsymbol{S_0}$*.*
- *Give a reduction algorithm for* $\boldsymbol{\mathrm{R}_{n,k} \cap \mathrm{F}(\mathrm{M}_k, \mathrm{M}_{n-k})}$*. Namely, give an algorithm to find* $\boldsymbol{\gamma \in \mathrm{GL}_n(\mathbf{Z})}$ *for a given* $\boldsymbol{A \in \mathrm{P}_n}$ *such that* $\boldsymbol{A[\gamma] \in \mathrm{R}_{n,k} \cap \mathrm{F}(\mathrm{M}_k, \mathrm{M}_{n-k})}$*.*

► **Minkowski's fundamental domain** M_n for $\mathrm{P}_n/\mathrm{GL}_n(\mathbf{Z})$ is defined as follows:

$$\mathrm{M}_n := \left\{ A = (a_{ij}) \in \mathrm{P}_n \;\middle|\; \begin{array}{l} A[z] \geq a_{jj} \text{ if } z = {}^t(z_1, \ldots, z_n) \in \mathbf{Z}^n \text{ with } \gcd(z_j, \ldots, z_n) = 1 \\ \text{and } a_{j,j+1} \geq 0 \text{ for all } j \end{array} \right\}.$$

See [25, Section 4.4.2]. When $n = 2$, one has

$$\mathrm{M}_2 = \left\{ \begin{pmatrix} a_{11} & a_{12} \\ a_{12} & a_{22} \end{pmatrix} \in \mathrm{P}_2 \;\middle|\; 0 \leq 2a_{12} \leq a_{11} \leq a_{22} \right\}.$$

► Let $\mathrm{M}_n(\mathbf{Z})^* := \mathrm{GL}_n(\mathbf{Q}) \cap \mathrm{M}_n(\mathbf{Z})$. The **Hermite–Rankin constant** $\gamma_{n,k}$ is defined as follows:

$$\gamma_{n,k} := \max_{A \in \mathrm{P}_n} \left\{ \frac{\min_{\gamma \in \mathrm{M}_n(\mathbf{Z})^*} \det({}^t(\gamma E_{n,k}) A (\gamma E_{n,K}))}{(\det A)^{k/n}} \right\} = \max_{g \in \mathrm{GL}_n(\mathbf{Q}_\infty)^1} \min_{\delta \in \mathrm{M}_n(\mathbf{Z})^*} \det({}^t E_{n,k} {}^t\delta {}^t g_\infty g_\infty \delta E_{n,k}).$$

See [20, Section 2.8] for the Hermite–Rankin constant. For $\delta \in \mathrm{M}_n(\mathbf{Z})^*$, $\delta E_{n,k}$ has the elementary divisors $e_1, \ldots, e_k$, and there are $\gamma \in \mathrm{GL}_n(\mathbf{Z})$ and $\gamma' \in \mathrm{GL}_k(\mathbf{Z})$ such that

$$\delta E_{n,k} = \gamma \begin{pmatrix} e_1 & & 0 \\ & \ddots & \\ 0 & & e_k \\ 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{pmatrix} \gamma' = \gamma E_{n,k} \begin{pmatrix} e_1 & & 0 \\ & \ddots & \\ 0 & & e_k \end{pmatrix} \gamma'.$$

Then one has

$$\det({}^t E_{n,k}\, {}^t\delta^t g_\infty g_\infty \delta E_{n,k}) = (e_1 \cdots e_k)^2 \det({}^t E_{n,k}\, {}^t\gamma^t g_\infty g_\infty \gamma E_{n,k}),$$

and as a consequence

$$\min_{\delta \in \mathrm{M}_n(\mathbf{Z})^*} \det({}^t E_{n,k}\, {}^t\delta^t g_\infty g_\infty \delta E_{n,k}) = \min_{\gamma \in \mathrm{GL}_n(\mathbf{Z})} \det({}^t E_{n,k}\, {}^t\gamma^t g_\infty g_\infty \gamma E_{n,k}) = m_Q(g_\infty^{-1})^{2\ell/n},$$

where ℓ denotes $\gcd(n,k)$. Therefore, we obtain

$$\gamma_{n,k} = \max_{g_\infty \in \mathrm{GL}_n(\mathbf{Q}_\infty)^1} m_Q(g_\infty)^{2\ell/n} = \max_{[g_\infty] \in \mathrm{GL}_n(\mathbf{Z}) \backslash \mathrm{GL}_n(\mathbf{Q}_\infty)^1 / K_\infty} m_Q(g_\infty)^{2\ell/n}.$$

As remarked in **10.3**, the maximum of m_Q is attained on the boundary of $R_{n,k}$. The following is a table of known values of $\gamma_{n,k}$ and ciritical points ([23]).

$\gamma_{4,2}$	$\gamma_{6,2}$	$\gamma_{8,2}$	$\gamma_{8,3}$	$\gamma_{8,4}$
3/2	$3^{2/3}$	3	4	4
D_4	E_6	E_8	E_8	E_8

The value of $\gamma_{4,2}$ was determined by Rankin. Here positive definite symmetric matrices D_4, E_6, E_8 are given as follows:

$$D_4 = \begin{pmatrix} 2 & 1 & 1 & 1 \\ 1 & 2 & 1 & 0 \\ 1 & 1 & 2 & 1 \\ 1 & 0 & 1 & 2 \end{pmatrix}, \quad E_6 = \begin{pmatrix} 2 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 1 & 0 & 1 & 1 \\ 1 & 1 & 2 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 & 0 & 1 \\ 1 & 1 & 1 & 0 & 2 & 1 \\ 1 & 1 & 1 & 1 & 1 & 2 \end{pmatrix}, \quad E_8 = \begin{pmatrix} 2 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 2 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 2 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 2 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 2 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 2 \end{pmatrix}.$$

These are LLL reduced Gram matrices corresponding to D_4, E_6, E_8 root lattices, respectively ([20, Section 14.2]).

► A compactification of $\mathrm{R}_{n,k} \cap \mathrm{F}(\mathrm{M}_k, \mathrm{M}_{n-k}) \cap \mathrm{P}^1_n$ is another problem to be considered.

Appendix. Numerical Computations of Minimal k tuples

We fix positive integers n and k with $2 \le k \le n-1$. Let $\Gamma_n = \mathrm{GL}_n(\mathbf{Z})$ and $\mathrm{M}_n(\mathbf{Z})^* = \mathrm{M}_n(\mathbf{Z}) \cap \mathrm{GL}_n(\mathbf{Q})$. Let $E_{n,k}$ be the $n \times k$ matrix consisting of the first k columns of the $n \times n$ identity matrix E_n. We set

$$\Gamma_{n,k} := \{\gamma E_{n,k} \mid \gamma \in \Gamma_n\} \quad \text{and} \quad \mathrm{M}_{n,k}(\mathbf{Z})^* := \{XE_{n,k} \mid X \in \mathrm{M}_n(\mathbf{Z})^*\}.$$

Let $\mathcal{L}$ denote the space of all full-rank lattices in $\mathbf{R}^n$ and P_n denote the cone of positive definite real symmetric $n \times n$ matrices. For $A \in \mathrm{P}_n$, define

$$\mathsf{m}_k(A) := \min_{X \in \mathrm{M}_{n,k}} \det A[X] = \min_{X \in \Gamma_{n,k}} \det A[X],$$

where $A[X] = {}^tXAX$, and

$$S_k(A) := \{X \in \mathrm{M}_{n,k}(\mathbf{Z})^* \mid \det A[X] = \mathsf{m}_k(A)\}.$$

An element of $S_k(A)$ is called a **minimal k-tuple** of A. By Proposition 35(or Propositons A1 and A2 in Appendix), the cardinality of $S_k(A)/\Gamma_k$ is finite.

A 1 $\mathcal{L}$ and P_n

For $g \in \mathrm{GL}_n(\mathbf{R})$, define $L_g := g\mathbf{Z}^n$. If $\gamma \in \Gamma_n$, then $L_{g\gamma} = L_g$, which means each coset $g\Gamma_n \in \mathrm{GL}_n(\mathbf{R})/\Gamma_n$ corresponds to a lattice $L_g = L_{g\Gamma_n}$. This provides a bijection $\mathrm{GL}_n(\mathbf{R})/\Gamma_n \cong \mathcal{L}$. Two lattices L and L' are said to be isometric if there exists $h \in \mathrm{O}_n(\mathbf{R})$ such that $hL = L'$. We denote the isometric class of L by $[L]$. Let $\mathcal{L}_{\mathrm{iso}}$ be the set of all isometric classes. If $L = L_{g\Gamma_n}$, then

$$[L_{g\Gamma_n}] = \mathrm{O}_n(\mathbf{R})L_{g\Gamma_n} = \{L_{hg\Gamma_n} \mid h \in \mathrm{O}_n(\mathbf{R})\}.$$

Thus the mapping $\mathrm{O}_n(\mathbf{R})g\Gamma_n \mapsto [L_{g\Gamma_n}]$ yields a bijection

$$\mathrm{O}_n(\mathbf{R})\backslash\mathrm{GL}_n(\mathbf{R})/\Gamma_n \cong \mathcal{L}_{\mathrm{iso}}.$$

For $g \in \mathrm{GL}_n(\mathbf{R})$, define $A_g := {}^tgg \in \mathrm{P}_n$. The Γ_n-orbit of A_g is denoted by $[A_g]$, i.e.,

$$[A_g] = A_g[\Gamma_n] = \{A_{g\gamma} \mid \gamma \in \Gamma_n\}.$$

Since $A_{hg} = A_g$ for $h \in \mathrm{O}_n(\mathbf{R})$, the mapping $[L_{g\Gamma_n}] \mapsto [A_g]$ yields a bijection $\mathcal{L}_{\mathrm{iso}} \cong \mathrm{P}_n/\Gamma_n$.

A 2 Minimal-equivalence classes

Let $L \in \mathcal{L}$. We denote by $L^{(k)}$ the set of all k-tuples $(X_1, \ldots, X_k)$ consisting of k linearly independent elements $X_1, \ldots, X_k$ in L, i.e.,

$$L^{(k)} = \{(X_1, \ldots, X_k) \in \mathrm{GL}_n(\mathbf{R})E_{n,k} \mid X_i \in L \ \text{ for all } i\}.$$

$\Gamma_k = \mathrm{GL}_k(\mathbf{Z})$ naturally acts on $L^{(k)}$ from the right. For $X = (X_1, \ldots, X_k) \in L^{(k)}$, define $\delta(X)$ by $\det({}^tXX)$. This $\delta(X)$ depends only on the Γ_k-orbit of X since $\delta(X\gamma) = (\det\gamma)^2\delta(X) = \delta(X)$ for any $\gamma \in \Gamma_k$. We write $[X]$ for the Γ_k-orbit $X\Gamma_k$ of X. Define $\delta(L)$ and $S_k(L)$ as follows:

$$\delta(L) := \min_{[X]\in L^{(k)}/\Gamma_k} \delta(X)$$

and

$$S_k(L) := \{[X] \in L^{(k)}/\Gamma_k \mid \delta(X) = \delta(L)\}.$$

When $L = L_{g\Gamma_n}$, every element $x \in L$ is of the form $x = gz$ with $z \in \mathbf{Z}^n$, so $L^{(k)} = g\mathrm{M}_{n,k}(\mathbf{Z})^*$. Then, for $X = gZ \in L^{(k)}$ with $Z \in \mathrm{M}_{n,k}(\mathbf{Z})^*$, we have

$$\delta(X) = \det({}^tZ^tggZ) = \det({}^tZA_gZ) = \det A_g[Z],$$

and hence

$$\delta(L_{g\Gamma_n}) = \min_{Z\in \mathrm{M}_{n,k}(\mathbf{Z})^*} \det A_g[Z] = \mathsf{m}_k(A_g).$$

Since $A_{hg} = A_g$ for $h \in \mathrm{O}_n(\mathbf{R})$, $\delta(L)$ depends only on the isometric class of L. The following are immediately proved:

(1) $S_k(L_{g\Gamma_n}) = gS_k(A_g)/\Gamma_k$;

(2) $S_k(A_{g\gamma})/\Gamma_k = \gamma^{-1}S_k(A_g)/\Gamma_k$ for every $\gamma \in \Gamma_n$;

(3) $S_k(hL) = hS_k(L)$ for every $h \in \mathrm{O}_n(\mathbf{R})$.

If we change a representative g to $g\gamma$ with $\gamma \in \Gamma_n$, then by (1) and (2),

$$S_k(L_{g\gamma\Gamma_n}) = g\gamma S_k(A_{g\gamma})/\Gamma_k = g\gamma(\gamma^{-1}S_k(A_g)/\Gamma_k) = gS_k(A_g)/\Gamma_k = S_k(L_{g\Gamma_n}).$$

For $u \in \mathrm{GL}_n(\mathbf{R})$, $S_k(uL)$ is not necessarily equal to $uS_k(L)$. It is clear that $S_k(uL) = uS_k(L)$ if and only if $S_k(A_{ug})/\Gamma_k = S_k(A_g)/\Gamma_k$. Two lattices L and L' are said to be **minimal-equivalent** if there exists $u \in \mathrm{GL}_n(\mathbf{R})$ such that $L' = uL$ and $S_k(L') = uS_k(L)$. This defines an equivalence relation on $\mathcal{L}$. We denote the minimal-equivalence class of L by $[L]_\mathrm{m}$ and the set of minimal-equivalence classes by $\mathcal{L}_\mathrm{min}$. If L and L' are isometric, then they are minimal-equivalent by (3). Therefore, there is a natural surjection from $\mathcal{L}_\mathrm{iso}$ onto $\mathcal{L}_\mathrm{min}$. By $\mathcal{L}_\mathrm{iso} \cong \mathbf{P}_n/\Gamma_n$, the minimal-equivalence relation is transformed into an equivalence relation on $\mathbf{P}_n/\Gamma_n$. Two positive definite symmetric matrices A and A' are said to be minimal-equivalent if there exists $\gamma \in \Gamma_n$ such that $\gamma S_k(A')/\Gamma_k = S_k(A)/\Gamma_k$. In this case, we write $A \sim_\mathrm{m} A'$. For every $\gamma \in \Gamma_n$, we have $A \sim_\mathrm{m} A[\gamma]$ because of $\gamma S_k(A[\gamma])/\Gamma_k = S_k(A)/\Gamma_k$ by (2). We show the following:

(4) $[L_{g\Gamma_n}]_\mathrm{m} = [L_{g'\Gamma_n}]_\mathrm{m}$ if and only if $A_g \sim_\mathrm{m} A_{g'}$.

Proof. If $[L_{g\Gamma_n}]_{\mathrm{m}} = [L_{g'\Gamma_n}]_{\mathrm{m}}$, then there exists $u \in \mathrm{GL}_n(\mathbf{R})$ such that $L_{g'\Gamma_n} = uL_{g\Gamma_n}$ and $S_k(L_{g'\Gamma_n}) = uS_k(L_{g\Gamma_n})$. Since $g'\Gamma_n = ug\Gamma_n$, we can take $\gamma \in \Gamma_n$ such that $g' = ug\gamma$. By (1), we have

$$ugS_k(A_g)/\Gamma_k = uS_k(L_{g\Gamma_n}) = S_k(L_{g'\Gamma_n}) = g'S_k(A_{g'})/\Gamma_k = ug\gamma S_k(A_{g'})/\Gamma_k,$$

and hence,

$$S_k(A_g)/\Gamma_k = \gamma S_k(A_{g'})/\Gamma_k.$$

Conversely, assume $A_g \sim_{\mathrm{m}} A_{g'}$ and take $\gamma \in \Gamma_n$ such that $\gamma S_k(A_{g'})/\Gamma_k = S_k(A_g)/\Gamma_k$. If we set $u = g'\gamma^{-1}g^{-1}$, then $uL_{g\Gamma_n} = L_{ug\Gamma_n} = L_{g'\Gamma_n}$ and

$$uS_k(L_{g\Gamma_n}) = ugS_k(A_g)/\Gamma_k = g'\gamma^{-1}S_k(A_g)/\Gamma_k = g'S_k(A_{g'})/\Gamma_k = S_k(L_{g'\Gamma_n}).$$

□

As a consequence, we obtain $\mathcal{L}_{\min} \cong \mathrm{P}_n/\sim_{\mathrm{m}} = (\mathrm{P}_n/\Gamma_n)/\sim_{\mathrm{m}}$. Coulangeon proved that the cardinal number $\ell := \sharp\mathcal{L}_{\min}$ is finite ([A1, Proposition 2.7]). We can take a complete set $\{A_1, \ldots, A_\ell\}$ of representatives for $\mathrm{P}_n/\sim_{\mathrm{m}}$. Then, for every $A \in \mathrm{P}_n$, there exist a unique A_i and a $\gamma \in \Gamma_n$ such that $\gamma S_k(A)/\Gamma_k = S_k(A_i)/\Gamma_k$. Let $\mathrm{R}_{n,k} \subset \mathrm{P}_n$ be the Ryshkov domain defined in **11.2** and let $\Omega \subset \mathrm{R}_{n,k}$ be a fundamental domain for $\mathrm{P}_{\mathrm{n}}/\Gamma_n$. Then we can take $\{A_1, \ldots, A_\ell\}$ as a subset of Ω and assume $A_1 \in \mathrm{R}^{\circ}_{n,k}$. It is clear by definiton that

$$\bigcup_{A \in \mathrm{R}^{\circ}_{n,k}} S_k(A)/\Gamma_k = \{E_{n,k}\Gamma_k\} = S_k(A_1)/\Gamma_k$$

is a singleton set. In general, for a given subset $\mathcal{O} \subset \mathrm{P}_n$, define $S_{\Gamma_k}(\mathcal{O}) \subset \Gamma_{n,k}/\Gamma_k$ as follows:

$$S_{\Gamma_k}(\mathcal{O}) := \bigcup_{A \in \mathcal{O}} S_k(A)/\Gamma_k.$$

It is a question whether the set $S_{\Gamma_k}(\Omega)$ is finite. In particular, whether the cardinal number $\sharp S_{\Gamma_k}(\mathrm{R}_{n,k} \cap \mathrm{F}(\mathrm{M}_k, \mathrm{M}_{n-k}))$ is finite or not would be related to Problem in **11.3**.

A 3 k-Perfection

Let us define k-perfection. For $X = (X_1, \ldots, X_k) \in \mathrm{M}_{n,k}(\mathbf{R})$ of rank k, let $\Phi_X = (Y_1, \ldots, Y_k)$ denote the Gram–Schmidt orthogonalization of X with respect to the standard inner product of $\mathbf{R}^n$. Namely $(Y_1, \ldots, Y_k)$ satisfies that

- the subspace spanned by $Y_1, \ldots, Y_i$ equals the subspace spanned by $X_1, \ldots, X_i$ for each $i = 1, \ldots, k$, and
- ${}^tY_i \cdot Y_j = \delta_{ij}$ for $1 \leq i, j \leq k$.

For $A = A_g \in \mathrm{P}_n$, fix a complete system $\{X^{(j)}\}_j$ of representatives of $S_k(A)/\Gamma_k$. Then A is said to be k**-perfect** if $\{\Phi_{gX^{(j)}} \cdot {}^t\Phi_{gX^{(j)}}\}_j$ spanns the whole space of real symmetric $n \times n$ matrices. It is easy to see that this definition does not depend on the choice of both g and $\{X^{(j)}\}_j$. In particular, if A is k-perfect, then the cardinality $\sharp S_k(A)/\Gamma_k$ is greater than or equal to $n(n+1)/2$. The k**-perfect rank** of A is defined to be the dimension of the real linear space spanned by $\{\Phi_{gX^{(j)}} \cdot {}^t\Phi_{gX^{(j)}}\}_j$.

A 4 A Finite Set Containing a System of Representatives

We fix an $A \in \mathrm{P}_n$ and consider the mapping $q_A : X \mapsto A[X]$ from $\Gamma_{n,k}$ to P_k. Since $A[X\gamma] = A[X][\gamma] = {}^t\gamma A[X]\gamma$ for $\gamma \in \Gamma_k$, q_A is regarded as a mapping from $\Gamma_{n,k}/\Gamma_k$ to P_k/Γ_k. Let M_k denote Minkowski's fundamental domain for P_k/Γ_k. If $B = (b_{ij}) \in \mathrm{M}_k$, then its entries satisfy the following inequalities:

(a) $b_{11} \leq b_{22} \leq \cdots \leq b_{kk}$;

(b) $b_{11}b_{22}\cdots b_{kk} \leq C_k \det B$;

(c) $0 \leq 2b_{1j} \leq b_{11}$ for $j = 2, \ldots, k$.

where C_k is a positive constant, (see [A7, Lectures XI and XIII] for example). The best possible value of C_k is known for $k \leq 5$ as follows:

$$C_2 = \frac{4}{3}, \qquad C_3 = 2, \qquad C_4 = 4\,, \qquad C_5 = 8$$

(see [A2, Supplement to Chapter 2, v.5]). For $k \geq 6$, one can choose

$$C_k = \left(\frac{4}{\pi}\right)^k \left(\frac{5}{4}\right)^{\frac{(k-3)(k-4)}{2}} \left(\Gamma\left(\frac{k}{2}+1\right)\right)^2$$

by Remak's estimate ([A5], see also [A8]). We fix a constant $\lambda \geq \mathsf{m}_k(A)$, and set

$$S_k(A,\lambda) := \{X \in \Gamma_{n,k} \mid q_A(X) \in \mathrm{M}_k \text{ and } \det q_A(X) \leq \lambda\}$$

and

$$T_k(A,\lambda) := \left\{ X \in \Gamma_{n,k} \mid A[X_i] \leq \left(\frac{\lambda C_k}{\mathsf{m}_1(A)^{i-1}}\right)^{1/(k-i+1)} \text{ for } i = 1, \ldots, k \right\}.$$

Proposition A1

$S_k(A,\lambda)$ is a subset of $T_k(A,\lambda)$ and $T_k(A,\lambda)$ is a finite subset of $\Gamma_{n,k}$.

Proof. For $X = (X_1, \dots, X_k) \in \Gamma_{n,k}$, the i-th diagonal entry of $q_A(X)$ equals $A[X_i]$ for $i = 1, \dots, k$. If $X \in S_k(A, \lambda)$, then by (b)

$$A[X_1]A[X_2] \cdots A[X_k] \le C_k \det q_A(X) \le \lambda C_k .$$

By $\mathsf{m}_1(A) \le A[X_1]$ and (a), we obtain

$$m_1(A)^{i-1} A[X_i]^{k-i+1} \le A[X_1]A[X_2] \cdots A[X_k],$$

and hence

$$A[X_i] \le \left(\frac{\lambda C_k}{\mathsf{m}_1(A)^{i-1}} \right)^{1/(k-i+1)}$$

for $i = 1, \dots, k$. Therefore, $S_k(A, \lambda)$ is a subset of $T_k(A, \lambda)$. The finiteness of the cardinality of $T_k(A, \lambda)$ is trivial. □

Proposition A2

$S_k(A, \lambda)$ *contains a complete system of representatives of* ***$S_k(A)/\Gamma_k$***.

Proof. Let X be an arbitrary element in $S_k(A)$. Then $\det q_A(X) = \mathsf{m}_k(A) \le \lambda$. Since M_k is a fundamental domain for P_k/Γ_k, there exists $\gamma \in \Gamma_k$ such that $q_A(X)[\gamma] \in \mathrm{M}_k$. Then $X\gamma \in S_k(A, \lambda)$, i.e., $S_k(A, \lambda)$ contains a representative of the class $X\Gamma_k$. □

When $\lambda = \mathsf{m}_k(A)$, we can slightly improve the estimate of $A[X_i]$. Let $\{\lambda_i(A)\}_i$ denote the successive minima of the gauge function $x \mapsto A[x]^{1/2}$ on $\mathbf{R}^n$ defined by A.

Proposition A3

If $\boldsymbol{X = (X_1, \dots, X_k) \in S_k(A, \mathsf{m}_k(A))}$, *then*

$$\boldsymbol{A[X_i]^{k-i+1} \le \{\lambda_i(A) \cdots \lambda_k(A)\}^2 C_k}$$

holds for each $\boldsymbol{i = 1, \dots, k}$.

Proof. By Hadamard's inequality, we have

$$\mathsf{m}_k(A) \le \det A[X] \le A[X_1]A[X_2] \cdots A[X_k]$$

for all $X \in \mathrm{M}_{n,k}(\mathbf{Z})^*$. This implies

$$\mathsf{m}_k(A) \le \{\lambda_1(A)\lambda_2(A) \cdots \lambda_k(A)\}^2 \le A[X_1]A[X_2] \cdots A[X_k]$$

for $X \in \mathrm{M}_{n,k}(\mathbf{Z})^*$. If $q_A(X) \in \mathrm{M}_k$, then

$$\{\lambda_1(A)\cdots\lambda_{i-1}(A)\}^2 \le A[X_1]\cdots A[X_{i-1}]$$

holds for all $i = 2, \ldots, k$. Therefore, if $X \in S_k(A, \mathsf{m}_k(A))$, then

$$A[X_i]^{k-i+1} \le \frac{\mathsf{m}_k(A)C_k}{\{\lambda_1(A)\cdots\lambda_{i-1}(A)\}^2} \le \{\lambda_i(A)\cdots\lambda_k(A)\}^2 C_k\,.$$

□

A 5 Algorithm to Computing $S_k(A)/\Gamma_k$

By Propositions A1 and A2, the following algorithm computes $S_k(A)/\Gamma_k$.

Input: $A \in \mathrm{P}_n$.

Output: A complete system of representatives of $S_k(A)/\Gamma_k$.

Step 1 For each $i = 1, \ldots, k$, compute the set

$$T_{\lambda,i} := \left\{ 0 \ne Y_i \in \mathbf{Z}^n \mid A[Y_i] \le \left(\frac{\lambda C_k}{\mathsf{m}_1(A)^{i-1}} \right)^{1/(k-i+1)} \right\}.$$

Step 2 Compose possible $Y = (Y_1, \ldots, Y_k) \in T_{\lambda,1} \times \cdots \times T_{\lambda,k}$, and select all $Y^{(j)} \in T_{\lambda,1} \times \cdots \times T_{\lambda,k}$ such that the rank of $q_A(Y^{(j)})$ equals k.

Step 3 Select $Y^{(j')} \in \{Y^{(j)}\}$ such that $\det q_A(Y^{(j')}) = \min_j \det q_A(Y^{(j)})$. Such $Y^{(j')}$s are automatically contained in $S_k(A)$.

Step 4 Check Γ_k equivalence among $Y^{(j')}$s.

There are several choices of λ for A. One is $\lambda = \det A[E_{n,k}]$. Another is

$$\lambda = \gamma_n^k (\det A)^{k/n} \quad \text{or} \quad \left(\frac{4}{\pi} \Gamma\left(1 + \frac{n}{2}\right)^{2/n} (\det A)^{1/n} \right)^k$$

(see [A3, Theorems 2.6.8 and 2.7.4]). Here γ_n denotes Hermite's constant. If the diagonal elements of $A = (a_{ij})$ satisfy $a_{11} \le a_{22} \le \cdots \le a_{nn}$, then one has $\lambda_i(A)^2 \le a_{ii}$ for $i = 1, \ldots, n$. In this case, by Proposition A3, we can replace $T_{\lambda,i}$ with

$$T_i := \left\{ 0 \ne Y_i \in \mathbf{Z}^n \mid A[Y_i] \le (a_{ii}\cdots a_{kk} C_k)^{1/(k-i+1)} \right\}.$$

Since $\det A[E_{n,k}] \le a_{11}a_{22}\cdots a_{kk}$ by Hadamard's inequality, T_i is not necessarily better than $T_{i,\lambda}$ of $\lambda = \det A[E_{n,k}]$. To reduce the size of the set $\{Y^{(j)}\}$ of Step 2, we can replace $T_{\lambda,j}$ with its half subset $T_{\lambda,j} \mod \{\pm E_k\}$ since $S_k(A)$ is Γ_k invariant. If we want to compute $S_k(A, \lambda)$, we cannot use such reduction, because that $S_k(A, \lambda)$ is not invariant by $\{\mathrm{diag}(\epsilon_1, \ldots, \epsilon_k) : \epsilon_i \in \{\pm 1\}\}$. In this case, we can impose the condition (c) to select $Y^{(j)}$. On Step 4, we note that two elements $X, X' \in \Gamma_{n,k}$ are Γ_k-equivalent if and only if $X_1 \wedge \cdots \wedge X_k = \pm X'_1 \wedge \cdots \wedge X'_k$.

A 6 Examples

We give some numerical examples. These examples were computed by using Pari/GP in Step 1 and Mathematica in Steps 2, 3 and 4. In the following, we use the standard labeling of the irreducible root lattices, i.e., A_n, D_n, E_6, E_7 and E_8. The Watson lattices of dimension n ($3 \leq n \leq 7$) are denoted by W_n ([A1, Section 5]). Equivalence classes of n dimensional perfect lattices are classified in $n \leq 8$. We use Martinet's labeling of perfect lattices in dimension ≤ 7 ([A3, Section 14.1] and [A4]). The similar equivalence class (i.e., $\mathbf{R}^\times \cdot \mathrm{GL}_n(\mathbf{Z})$ orbit in P_n) of a Gram matrix of one of these lattices is expressed by the same label as the lattice in question. For an orbit $[[A]] = A[\mathbf{R}^\times \cdot \mathrm{GL}_n(\mathbf{Z})]$, we denote by $[[A]]^*$ the dual of $[[A]]$, i.e., $[[A]]^* = [[A^{-1}]]$. Although we do not display an explicit form of a matrix A representing a given label, the values $\det A$ and $\mathsf{m}_k(A)$ depend only on the equivalence class $A[\mathrm{GL}_n(\mathbf{Z})]$, and the values $\mathsf{hr}_k(A) = \mathsf{m}_k(A)/(\det A)^{k/n}$, $\sharp S_k(A)/\Gamma_k$ and k-perfect rank depend only on the similar equivalence class $[[A]]$. The number of the similar equivalent classes of k-parfect elements in P_n is finite ([A1, Thèoréme 4.5]). For irreducible root lattices A_n, D_n, E_6, E_7, E_8 ($n \geq 3$) and Watson lattices W_n, Coulangeon computed $\sharp S_2(A)/\Gamma_2$, and proved that

(d) all of these lattices are 2-perfect except only A_3, and moreover

(e) irreducible root lattices of dimension n are k-eutactic if $k \leq n$,

([A1, Thèoréme 5.1.1 and Proposition 5.2.1]). Thus Table 1 follows from [A1] and Tables 2, 3, 5, 7 contain a part of Coulangeon's computation.

• $(n, k) = (4, 2)$

$[A]$	$\det A$	$\mathsf{m}_2(A)$	$\mathsf{hr}_2(A)$	$\sharp S_2(A)/\Gamma_2$	2-perfect rank
$P_4^1 = D_4$	4	3	1.5	16	10
$P_4^2 = A_4$	5	3	1.3416...	10	10
A_4^*	125	15	1.3416...	10	10
W_4	32	8	1.4142...	15	10
W_4^*	128	16	1.4142...	15	10

Table 1

Gram matrices of D_4, A_4 and W_4 are given as follows:

$$D_4 = \begin{pmatrix} 2 & 1 & 1 & 1 \\ 1 & 2 & 1 & 0 \\ 1 & 1 & 2 & 1 \\ 1 & 0 & 1 & 2 \end{pmatrix}, \quad A_4 = \begin{pmatrix} 2 & 1 & 1 & 1 \\ 1 & 2 & 1 & 1 \\ 1 & 1 & 2 & 1 \\ 1 & 1 & 1 & 2 \end{pmatrix}, \quad W_4 = \begin{pmatrix} 3 & -1 & -1 & -1 \\ -1 & 3 & -1 & 1 \\ -1 & -1 & 3 & -1 \\ -1 & 1 & -1 & 3 \end{pmatrix}.$$

Only in these cases, we show representatives of minimal 2-tuples.

Representatives of $S_2(D_4)/\Gamma_2$:

$$\begin{pmatrix} -1 & 0 \\ 1 & 0 \\ 0 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} -1 & -1 \\ 1 & 0 \\ 0 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 1 & 1 \\ 0 & -1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} -1 & -1 \\ 1 & 1 \\ 0 & -1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 0 & 0 \\ 0 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \\ 0 & -1 \\ 1 & 1 \end{pmatrix},$$
$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & -1 \\ 0 & 1 \\ 0 & -1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 0 \\ 0 & -1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 1 \\ -1 & -1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \\ -1 & -1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 1 & 0 \\ -1 & -1 \\ 1 & 1 \end{pmatrix},$$
$$\begin{pmatrix} 0 & -1 \\ 0 & 0 \\ 1 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & -1 \\ 1 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \\ 1 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Representatives of $S_2(A_4)/\Gamma_2$:

$$\begin{pmatrix} 0 & -1 \\ 0 & 0 \\ 0 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & -1 \\ 0 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \\ 0 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 0 \\ 0 & -1 \\ 1 & 1 \end{pmatrix},$$
$$\begin{pmatrix} 0 & 0 \\ -1 & 0 \\ 0 & -1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 0 & 0 \\ 1 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & -1 \\ 1 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \\ 1 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Representatives of $S_2(W_4)/\Gamma_2$:

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \\ 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \\ 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \\ 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 0 \\ 1 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 1 \\ 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \\ 0 & 0 \\ 1 & 0 \end{pmatrix},$$
$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \\ 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 1 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \\ 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \\ 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \\ 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \\ 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

There are 2 equivalence classes P_4^1, P_4^2 of 4 dimensional perfect lattices. We note that W_4 (and hence W_4^*) is not 2-eutacitc. This is immediately checked by using the data $S_2(W_4)/\Gamma_2$.

• $(n, k) = (5, 2)$

$[A]$	$\det A$	$\mathsf{m}_2(A)$	$\mathsf{hr}_2(A)$	$\sharp S_2(A)/\Gamma_2$	2-perfect rank
$P_5^1 = D_5$	4	3	1.7230...	40	15
$P_5^2 = W_5^*$	162	12	1.5681...	15	10
$P_5^3 = A_5$	6	3	1.4650...	20	15
A_5^*	1296	24	1.3651...	15	15
D_5^*	256	16	1.7411...	50	15
W_5	48	8	1.7005...	45	15

Table 2

There are 3 equivalence classes P_5^1, P_5^2, P_5^3 of 5 dimensional perfect lattices. By (d) and (e), both A_5 and D_5 are 2-extreme. By duality ([A1, Proposition 4.6]) and (e), A_5^* and D_5^* are 2-eutactic, and hence, by Table 2, both A_5^* and D_5^* are 2-extreme .

• $(n, k) = (6, 2)$

$[A]$	$\det A$	$\mathsf{m}_2(A)$	$\mathsf{hr}_2(A)$	$\sharp S_2(A)/\Gamma_2$	2-perfect rank
$P_6^1 = E_6$	3	3	2.0800...	120	21
$P_6^2 = E_6^*$	243	12	1.9229...	45	21
$P_6^3 = D_6$	4	3	1.8898...	80	21
P_6^4	324	12	1.7471...	30	21
P_6^5	343	12	1.7142...	28	21
P_6^6	351	12	1.7011...	27	19
$P_6^7 = A_6$	7	3	1.5682...	35	21
A_6^*	16807	35	1.3663...	21	21
D_6^*	16	4	1.5874...	15	6
W_6	64	8	2	120	21
W_6^*	64	8	2	120	21

Table3

• $(n, k) = (6, 3)$

$[A]$	$\det A$	$\mathsf{m}_3(A)$	$\mathsf{hr}_3(A)$	$\sharp S_3(A)/\Gamma_3$	3-perfect rank
$P_6^1 = E_6$	3	4	2.3094	270	21
$P_6^2 = E_6^*$	243	36	2.3094	270	21
$P_6^3 = D_6$	4	4	2	140	21
P_6^4	324	32	1.77778	9	9
P_6^5	343	32	1.7278...	14	13
P_6^6	351	32	1.7080...	8	7
$P_6^7 = A_6$	7	4	1.5118...	35	21
W_6	64	16	2	60	16

Table 4

There are 7 equivalence classes $P_6^1, \ldots, P_6^7$ of 6 dimensional perfect lattices. By (d) and (e), A_6, D_6, E_6 are 2-extreme. By duality and (e), A_6^*, D_6^* and E_6^* are 2-eutactic, and hence, Table 3 shows both A_6^* and E_6^* are 2-extreme, but not D_6^*. It is known that $\mathsf{hr}_2(E_6) = 3^{2/3}$ attains the maximum of the function hr_2 on P_6 ([A6]). By (e) and Table4, A_6, D_6, E_6 (and hence A_6^*, D_6^*, E_6^*) are 3-extreme.

• $(n,k) = (7,2)$

$[A]$	$\det A$	$\mathsf{m}_2(A)$	$\mathsf{hr}_2(A)$	$\sharp S_2(A)/\Gamma_2$	2-perfect rank
$P_7^1 = E_7 = W_7^*$	2	3	2.4610...	336	28
$P_7^2 = E_7^* = W_7$	64	8	2.4380...	378	28
P_7^3	486	12	2.0491...	72	28
$P_7^4 = D_7$	4	3	2.0188...	140	28
P_7^5	512	12	2.0188...	84	28
P_7^6	9216	27	1.9890...	50	26
P_7^7	540	12	1.9883...	69	28
P_7^8	576	12	1.9520...	58	28
P_7^9	356720	75	1.9439...	34	25
P_7^{10}	588	12	1.9405...	61	28
P_7^{11}	10080	27	1.9387...	48	28
P_7^{12}	10240	27	1.9300...	30	20
P_7^{13}	76880	48	1.9288...	35	25
P_7^{14}	10336	27	1.9248...	42	28
P_7^{15}	77618	48	1.9235...	35	27
P_7^{16}	10368	27	1.9231...	46	28
P_7^{17}	10528	27	1.9147...	37	28
P_7^{18}	78880	48	1.9147...	37	28
P_7^{19}	10584	27	1.9118...	42	27
P_7^{20}	10658	27	1.9080...	39	27
P_7^{21}	10752	27	1.9033...	40	28
P_7^{22}	630	12	1.9026...	49	28
P_7^{23}	10780	27	1.9018...	38	28
P_7^{24}	10808	27	1.9004...	39	28
P_7^{25}	11008	27	1.8905...	38	28
P_7^{26}	648	12	1.8874...	52	28
P_7^{27}	648	12	1.8874...	48	28
P_7^{28}	648	12	1.8874...	51	28
P_7^{29}	684	12	1.8585...	47	28
P_7^{30}	686	12	1.8569...	42	28
P_7^{31}	720	12	1.8314...	43	28
P_7^{32}	756	12	1.8061...	45	28
$P_7^{33} = A_7$	8	3	1.6561...	56	28
A_7^*	262144	48	1.3585...	28	28
D_7^*	4096	16	1.4859...	21	7

Table 5

There are 33 equivalence classes $P_7^1, \ldots, P_7^{33}$ of 7 dimensional perfect lattices. By (d) and (e), A_7, D_7, E_7 are 2-extreme. By duality and (e), A_7^*, D_7^* and E_7^* are 2-eutactic, and hence, Table 5 shows A_7^* and E_7^* are 2-extreme, but not D_7^*.

• $(n,k) = (7,3)$

$[A]$	$\det A$	$\mathsf{m}_3(A)$	$\mathsf{hr}_3(A)$	$\sharp S_3(A)/\Gamma_3$	3-perfect rank
$P_7^1 = E_7 = W_7^*$	2	4	2.9719...	1260	28
$P_7^2 = E_7^* = W_7$	64	16	2.6918...	315	28
P_7^3	486	32	2.2580...	27	19
$P_7^4 = D_7$	4	4	2.2081...	315	28
P_7^5	512	32	2.2081...	104	28
P_7^6	9216	108	2.1594...	8	8
P_7^7	540	32	2.1583...	58	28
P_7^8	576	32	2.0994...	36	28
P_7^9	356720	500	2.0864...	8	8
P_7^{10}	588	32	2.0810...	52	28
P_7^{11}	10080	108	2.0780...	27	25
P_7^{12}	10240	120	2.2934...	135	27
P_7^{13}	76880	256	2.0621...	5	5
P_7^{14}	10336	108	2.0558...	14	14
P_7^{15}	77618	256	2.0537...	7	7
P_7^{16}	10368	108	2.0531...	18	16
P_7^{17}	10528	108	2.0396...	9	9
P_7^{18}	78880	256	2.0395...	9	9
P_7^{19}	10584	108	2.0350...	27	20
P_7^{20}	10658	108	2.0289...	18	18
P_7^{21}	10752	108	2.0213...	17	15
P_7^{22}	630	32	2.0203...	22	20
P_7^{23}	10780	108	2.0191...	14	14
P_7^{24}	10808	108	2.0168...	15	15
P_7^{25}	11008	108	2.0010...	10	10
P_7^{26}	648	32	1.9961...	33	25
P_7^{27}	648	32	1.9961...	17	12
P_7^{28}	648	32	1.9961...	32	28
P_7^{29}	684	32	1.9504...	25	20
P_7^{30}	686	32	1.9479...	21	20
P_7^{31}	720	32	1.9080...	21	17
P_7^{32}	756	32	1.8685...	28	20
$P_7^{33} = A_7$	8	4	1.6406...	70	28
A_7^*	262144	320	1.5237...	56	28
D_7^*	4096	64	1.8114...	35	7

Table 6

By (e), duality and Table 6, $A_7, D_7, E_7, A_7^*, E_7^*$ are 3-extreme.

• $(n,k) = (8,2), (8,3)$ and $(8,4)$

$[A]$	$\det A$	$\mathsf{m}_2(A)$	$\sharp S_2(A)/\Gamma_2$	$\mathsf{m}_3(A)$	$\sharp S_3(A)/\Gamma_3$	$\mathsf{m}_4(A)$	$\sharp S_4(A)/\Gamma_4$
E_8	1	3	1120	4	7560	4	3150

Table 7

$\sharp S_4(E_8)/\Gamma_4 = 3150$ was computed as follows. If we put $C_4 = 4$ and $\lambda = \det E_8[E_{8,4}] = 4$, then one has $T_{\lambda,1} = T_{\lambda,2} = T_{\lambda,3} = T_{\lambda,4}$ and $T_{\lambda,1}$ consists of 240 minimal vectors of E_8. We fix a set M of 120 representatives of $T_{\lambda,1}/\{\pm 1\}$. Elements of M are ordered as $Y_1, Y_2, \ldots, Y_{120}$. Then, as an initial set of Step 2, one can take

$$T := \{(Y_{i_1}, Y_{i_2}, Y_{i_3}, Y_{i_4}) \in \mathrm{M}_{8,4}(\mathbf{Z}) \mid 1 \le i_1 < i_2 < i_3 < i_4 \le 120\}.$$

The cardinality of T equals 8214570. Since $\mathsf{m}_4(E_8) = 4$ is known, we select $Y^{(j)} \in T$ with $\det E_8[Y^{(j)}] = 4$. The cardinality of $\{Y^{(j)}\}$ equals 982800. Finally, we make a set $\{Y_1^{(j)} \wedge Y_2^{(j)} \wedge Y_3^{(j)} \wedge Y_4^{(j)}\}$ modulo $\{\pm 1\}$, and count elements of this set.

References

[A1] R. Coulangeon, *Réseaux k-extrêmes*, Proc. London Math. Soc. 73 (1996), 555-574.

[A2] P. M. Gruber and C. G. Lekkerkerker, Geometry of Numbers, 2nd edition, North-Holland, 1987.

[A3] J. Martinet, Perfect Lattices in Euclidean Spaces, Springer-Verlag 2003.

[A4] J. Martinet, Perfect lattices in dimensions 2 to 7, A database in J. Martinet's homepage.

[A5] R. Remak, *Uber die Minkowskische Reduktion der definiten quadratischen Formen*, Compositio Math. 5 (1938), 368-391.

[A6] K. Sawatani, T. Watanabe and K. Okuda, *A note on the Hermite–Rankin constant*, J. Th. Nombres Bordeaux 22 (2010) 209-217.

[A7] C. L. Siegel, Lectures on the Geometry of Numbers, Notes by B. Friedman, Rewritten by Komaravolu Chandrasekharan with the Assistance of Rudolf Suter, Springer-Verlag, 1989.

[A8] B. L. van der Waerden, *Die Reduktionstheorie der positiven quadratischen Formen*, Acta Math. 96 (1956) 265-309.

Index