JOURNAL
de Théorie des Nombres
de BORDEAUX
anciennement Séminaire de Théorie des Nombres de Bordeaux

Claudius HEYER

On the Decomposition of Hecke Polynomials over Parabolic Hecke Algebras

Tome 34, n° 3 (2022), p. 941-997.
https://doi.org/10.5802/jtnb.1235

Le Journal de Théorie des Nombres de Bordeaux *est membre du*
Centre Mersenne pour l'édition scientifique ouverte
http://www.centre-mersenne.org/
e-ISSN : 2118-8572

Journal de Théorie des Nombres de Bordeaux **34** (2022), 941–997

On the Decomposition of Hecke Polynomials over Parabolic Hecke Algebras

par Claudius HEYER

Résumé. On généralise un résultat classique d'Andrianov sur la décomposition des polynômes de Hecke. Pour un groupe connexe réductif $\mathbf{G}$ défini sur un corps local non-archimédien $\mathfrak{F}$, on donne un critère pour déterminer sous quelles conditions un polynôme à coefficients dans une algèbre de Hecke sphérique parahorique de $\mathbf{G}(\mathfrak{F})$ se décompose sur une algèbre de Hecke parabolique associée à un groupe parabolique *non obtus* de $\mathbf{G}$. On donne une classification des groupes paraboliques non obtus. Ceci montre alors que notre théorème de décomposition couvre tous les cas classiques dûs à Andrianov et Gritsenko. De plus, on obtient des cas nouveaux où le système de racines relatives de $\mathbf{G}$ contient des facteurs de types E_6 ou E_7.

Abstract. We generalize a classical result of Andrianov on the decomposition of Hecke polynomials. If $\mathbf{G}$ is a connected reductive group defined over a non-archimedean local field $\mathfrak{F}$, we give a criterion for when a polynomial with coefficients in the spherical parahoric Hecke algebra of $\mathbf{G}(\mathfrak{F})$ decomposes over a parabolic Hecke algebra associated with a *non-obtuse* parabolic subgroup of $\mathbf{G}$. We classify the non-obtuse parabolics. This then shows that our decomposition theorem covers all the classical cases due to Andrianov and Gritsenko. We also obtain new cases when the relative root system of $\mathbf{G}$ contains factors of types E_6 or E_7.

1. Introduction

1.1. Motivation. The problem to decompose Hecke polynomials emerged in the theory of Hecke operators acting on spaces of Siegel modular forms, see, e.g., [1, 2, 9]. One of the principal tasks is to find and study relations between Fourier coefficients of eigenforms of Hecke operators and the corresponding eigenvalues. It is instructive to work through an example to see how decomposing Hecke polynomials helps to find such relations.

Manuscrit reçu le 4 octobre 2021, révisé le 8 avril 2022, accepté le 21 mai 2022.

2020 *Mathematics Subject Classification.* 11C08, 20C08, 20G25.

Mots-clefs. Hecke Polynomials, Hecke algebras, reductive groups, Satake homomorphism, Iwasawa decomposition, Cartan decomposition.

This article constitutes part of my doctoral dissertation at the Humboldt University in Berlin. During the write-up of the article I was funded by the University of Münster and the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy EXC 2044 -390685587, Mathematics Münster: Dynamics-Geometry-Structure.

Consider the modular group $\Gamma = \mathrm{SL}_2(\mathbb{Z})$. Recall that a holomorphic function $f\colon \mathbb{H} \to \mathbb{C}$ on the upper half-plane $\mathbb{H} = \{z \in \mathbb{C} \mid \Im(z) > 0\}$ is called a *modular form of weight* k if for all $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$ and all $z \in \mathbb{H}$ it satisfies

$$f(z) = (f|\gamma)(z) \coloneqq (cz+d)^{-k} f\left(\frac{az+b}{cz+d}\right), \tag{1.1}$$

and if it admits a Fourier expansion of the form $f(z) = \sum_{j=0}^{\infty} \alpha_f(j) \cdot e^{2\pi i j z}$. Denote $\mathfrak{M}_k$ the $\mathbb{C}$-vector space of modular forms of weight k. Let S be the set of 2×2-matrices with integral entries and positive determinant. Then the algebra of Hecke operators $\mathcal{H} \coloneqq \mathcal{H}_{\mathbb{C}}(\Gamma, S)$ naturally acts on $\mathfrak{M}_k$: A double coset $(\Gamma g \Gamma) \in \mathcal{H}$ acts on f via $f|(\Gamma g \Gamma) \coloneqq \sum_{\Gamma\gamma \in \Gamma\backslash\Gamma g\Gamma} f|\gamma$. If f is a Hecke eigenform, we write $\lambda_f\colon \mathcal{H} \to \mathbb{C}$ for the corresponding eigenvalue. Then f is a Hecke eigenform if and only if $\alpha_{f|T}(j) = \lambda_f(T) \cdot \alpha_f(j)$, for all $T \in \mathcal{H}$, $j \in \mathbb{Z}_{\geq 0}$.

Fix a prime number p and consider the Hecke polynomial

$$Q_p(t) = 1 - T_1 t + pT_2 t^2, \quad \text{where } T_1 = \left(\Gamma\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)\Gamma\right),\ T_2 = (pE_2\Gamma) \in \mathcal{H},$$

where E_2 is the 2×2 identity matrix. There is a natural embedding of $\mathcal{H}$ into the parabolic Hecke algebra $\mathcal{H}^0 \coloneqq \mathcal{H}_{\mathbb{C}}(\Gamma_0, S_0)$, where Γ_0 (resp. S_0) is the subgroup of upper triangular matrices in Γ (resp. S). For example, one has $T_1 = T_1^+ + T_1^-$ in $\mathcal{H}_{\mathbb{C}}(\Gamma_0, S_0)$, where $T_1^+ = (\Gamma_0\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)\Gamma_0)$ and $T_1^- = (\Gamma_0\left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)\Gamma_0)$. Over the ring $\mathcal{H}_{\mathbb{C}}(\Gamma_0, S_0)$ the polynomial $Q_p(t)$ decomposes as

$$Q_p(t) = (1 - T_1^+ t) \cdot (1 - T_1^- t). \tag{1.2}$$

Right multiplication with the inverse power series of $1 - T_1^- t$ yields

$$Q_p(t) \cdot \sum_{l=0}^{\infty} (T_1^-)^l t^l = 1 - T_1^+ t \qquad \text{in } \mathcal{H}^0[\![t]\!]. \tag{1.3}$$

Note that $\mathcal{H}^0$ acts naturally on the space $\mathfrak{M}_k^0$ of holomorphic functions $f\colon \mathbb{H} \to \mathbb{C}$ satisfying (1.1) for all $\gamma \in \Gamma_0$ and admitting a Fourier expansion as above. Then $\mathfrak{M}_k \subseteq \mathfrak{M}_k^0$ and $\mathcal{H}^0[\![t]\!]$ acts naturally on $\mathfrak{M}_k^0[\![t]\!]$. Given $f \in \mathfrak{M}_k^0$, one computes $\alpha_{f|T_1^+}(j) = \alpha_f(j/p)$ and $\alpha_{f|T_1^-}(j) = p^{1-k}\alpha_f(pj)$, for all $j \geq 0$. (Here, we define $\alpha_f(j/p) = 0$ if $p \nmid j$.)

Let now $f \in \mathfrak{M}_k$ be a Hecke eigenform and consider the complex polynomial

$$Q_{p,f}(t) = 1 - \lambda_f(T_1) \cdot t + p \cdot \lambda_f(T_2) \cdot t^2 \in \mathbb{C}[t].$$

Letting (1.3) act on f, we obtain on the level of Fourier coefficients the relations

$$Q_{p,f}(t) \cdot \sum_{l=0}^{\infty} p^{l(1-k)} \alpha_f(p^l j) t^l = \alpha_f(j) - \alpha_f(j/p) t \quad \text{in } \mathbb{C}[\![t]\!], \text{ for each } j \geq 0.$$

This method of decomposing a Hecke polynomial over a parabolic Hecke algebra proved to be very fruitful in the more general context of Siegel modular forms. Andrianov proved a general decomposition theorem of type (1.2) in the context of Siegel modular forms, cf. [1]. In this case the modular group $\mathrm{SL}_2(\mathbb{Z})$ is replaced by $\mathrm{Sp}_{2n}(\mathbb{Z})$, for some $n \in \mathbb{Z}_{\geq 1}$, and one considers certain holomorphic functions on the Siegel upper half-space $\mathbb{H}_n$. The subgroup Γ_0 of upper triangular matrices is replaced by the "Siegel parabolic" in $\mathrm{Sp}_{2n}(\mathbb{Z})$, that is, the subgroup of matrices whose lower left quadrant is zero.

It is then natural to ask whether a decomposition of type (1.2) also holds for more general groups. Since the problem is local in nature, one may replace $\mathbb{Z}$ with the ring of integers of a non-archimedean local field $\mathfrak{F}$. In this context, Gritsenko proved a decomposition theorem for $\mathrm{GL}_n(\mathfrak{F})$ (and all parabolics) [10, 12] and for the classical groups $\mathrm{Sp}_{2n}(\mathfrak{F})$, $\mathrm{SU}_n(\mathfrak{F})$, and $\mathrm{SO}_n(\mathfrak{F})$ (for the parabolics fixing a line in the standard representation) [11].

The main result in [12] found an application in the theory of p-adic L-functions, where it was recently used by Januszewski [20] to define a projection map in order to obtain simultaneous eigenforms for certain Hecke operators. It is therefore reasonable to hope that a decomposition theorem for more general reductive groups will have applications in the theory of p-adic L-functions.

The aim of this paper is to generalize the theory developed by Andrianov [1] to the group G of $\mathfrak{F}$-rational points of a connected reductive $\mathfrak{F}$-group.

1.2. Main results. Let $\mathfrak{F}$ be a non-archimedean local field of residue characteristic $p > 0$. Let $\mathbf{G}$ be a connected reductive group over $\mathfrak{F}$, let $\mathbf{B}$ be a minimal parabolic $\mathfrak{F}$-subgroup of $\mathbf{G}$ with Levi decomposition $\mathbf{B} = \mathbf{Z}\mathbf{U}$. In this article a parabolic subgroup of $\mathbf{G}$ is a standard parabolic $\mathfrak{F}$-subgroup with respect to $\mathbf{B}$. Fix a special parahoric subgroup K of $G \coloneqq \mathbf{G}(\mathfrak{F})$ corresponding to a special point in the apartment determined by $\mathbf{Z}$. Then $G = KB$, where $B \coloneqq \mathbf{B}(\mathfrak{F})$. For any subgroup $X \subseteq G$ we put $K_X = K \cap X$. Let $\mathbf{P}$ be a parabolic subgroup of $\mathbf{G}$ and put $P \coloneqq \mathbf{P}(\mathfrak{F})$. Let R be a commutative $\mathbb{Z}[1/p]$-algebra, considered as a ring of coefficients.

The Hecke ring $\mathcal{H}_R(K_Z, Z)$, where $Z \coloneqq \mathbf{Z}(\mathfrak{F})$, identifies with the group algebra $R[Z/K_Z]$, and there are natural R-algebra embeddings $\mathcal{H}_R(K, G) \subseteq \mathcal{H}_R(K_P, P) \subseteq \mathcal{H}_R(K_B, B)$. There is a natural algebra homomorphism

$$\Theta_Z^B \colon \mathcal{H}_R(K_B, B) \longrightarrow R[Z/K_Z]$$

induced by the canonical projection map $B \to Z$. The restriction of Θ_Z^B to $\mathcal{H}_R(K_G, G)$ is called the (unnormalized) *Satake homomorphism*. It is well-known that $\mathcal{H}_R(K, G)$ is commutative. Besides $\mathcal{H}_R(K, G)$, the parabolic

Hecke algebra $\mathcal{H}_R(K_P, P)$ contains another commutative algebra C_P^-, which is constructed as the centralizer of a certain element of $\mathcal{H}_R(K_P, P)$.

Consider the R-submodule $\mathscr{O}_P^- := \mathcal{H}_R(K, G).C_P^-$ of $\mathcal{H}_R(K_P, P)$. In order to develop a reasonable theory one needs to make the following assumption:

Hypothesis 1.1. *The restriction of Θ_Z^B to $\mathscr{O}_P^-$ is injective.*

It should be remarked that there is no example known where Hypothesis 1.1 fails. There is one maximal parabolic subgroup in $\mathrm{Sp}_6(\mathbb{Q}_p)$ for which we do not know whether Hypothesis 1.1 is satisfied. One can show (see Proposition 5.23) that, if Hypothesis 1.1 is satisfied for two parabolics $\mathbf{P}$ and $\mathbf{Q}$, then it is also satisfied for $\mathbf{P} \cap \mathbf{Q}$. Hence, it would suffice to verify Hypothesis 1.1 for every maximal parabolic subgroup of $\mathbf{G}$. For practical reasons we work with an equivalent form of Hypothesis 1.1, see Hypothesis 5.16 on p. 985. We prove:

Theorem (Theorem 5.24)**.** *Assume that Hypothesis 1.1 is satisfied. Let $d(t) \in \mathcal{H}_R(K, G)[t]$ be a polynomial such that $d^{\Theta_Z^B}(t)$, the polynomial obtained by applying Θ_Z^B to the coefficients of $d(t)$, decomposes in $R[Z/K_Z][t]$ as*

$$d^{\Theta_Z^B}(t) = \widetilde{f}(t) \cdot \widetilde{g}(t)$$

such that $\widetilde{g}(t)$ has coefficients in $\Theta_Z^B(C_P^-)$ with constant term 1. Then there exist polynomials $f(t), g(t) \in \mathcal{H}_R(K_P, P)[t]$ with the following properties:

- $\deg f(t) = \deg \widetilde{f}(t)$ *and* $f^{\Theta_Z^B}(t) = \widetilde{f}(t)$*;*
- $\deg g(t) = \deg \widetilde{g}(t)$ *and* $g^{\Theta_Z^B}(t) = \widetilde{g}(t)$*;*
- $d(t) = f(t) \cdot g(t)$ *in* $\mathcal{H}_R(K_P, P)[t]$*.*

The proof is merely a straightforward extension of the arguments in [1]. However, it is in general very hard to decide for which $\mathbf{P}$ Hypothesis 1.1 is satisfied. The main contribution of this paper is to single out a class of maximal parabolic subgroups in $\mathbf{G}$ for which this hypothesis holds. We make the following important definition:

Definition 1.2 (See Section 3)**.** Let $\mathbf{P}$ be a maximal parabolic subgroup of $\mathbf{G}$ with unipotent radical $\mathbf{U_P}$. Then $\mathbf{P}$ is called *non-obtuse* if any two relative roots that occur in $\mathbf{U_P}$ span a non-obtuse angle.

Our main result is then:

Theorem 1.3 (Theorem 5.17)**.** *Assume that $\mathbf{P}$ is a non-obtuse parabolic subgroup of $\mathbf{G}$. Then Hypothesis 1.1 is satisfied for $\mathbf{P}$.*

The obvious question then is whether there exist non-obtuse parabolics and if they can be classified. In Proposition 3.5 we achieve a complete classification of non-obtuse parabolic subgroups and formulate several equivalent conditions. The maximal parabolic subgroups correspond bijectively to the vertices in the Dynkin diagram of the relative root system of $\mathbf{G}$, and hence it makes sense to say when a vertex of the Dynkin diagram is non-obtuse. The classification shows that all vertices in type A_n, the terminal vertices in types B_n, C_n, and D_n, two terminal vertices in type E_6, and one terminal vertex in type E_7 are non-obtuse. It also shows that there are no non-obtuse vertices in types E_8, F_4, and G_2, cf. Figure 3.2 on p. 958.

The proof of Theorem 1.3 requires us to investigate intersections of Cartan and Iwasawa double cosets. This problem is well-known and arises, for example, in the study of the Satake homomorphism, but here it is of a different flavor. More precisely, let $z, z' \in Z$ be such that $Uz'K \cap KzK \neq \varnothing$. It is well-understood how z' and z relate. However, so far almost nothing is known about the $u \in U$ for which $uz' \in KzK$.

To state our main technical result in this direction, let φ be the point in the (adjoint) Bruhat–Tits building of G corresponding to K. By assumption, φ lies in the apartment $\mathscr{A}$ corresponding to a torus $\mathbf{T} \subseteq \mathbf{Z}$ which is maximal $\mathfrak{F}$-split in $\mathbf{G}$. By definition, φ defines valuations, denoted φ_α, on the root groups U_α. There is a canonical homomorphism $\nu\colon Z \to V$ into the underlying $\mathbb{R}$-vector space V of $\mathscr{A}$ containing the coroots with respect to $\mathbf{T}$. Fix a strictly positive element $a \in Z$ so that $\langle \alpha, \nu(a) \rangle < 0$ for all simple roots α (with respect to $\mathbf{B}$). Choose the representative z of KzK such that $z \cdot (K \cap U) \cdot z^{-1} \subseteq K \cap U$, where $U := \mathbf{U}(\mathfrak{F})$. Denote $U_P := \mathbf{U_P}(\mathfrak{F})$ the group of $\mathfrak{F}$-points of the unipotent radical of $\mathbf{P}$. We prove the following technical result, which might be of independent interest:

Theorem 1.4 (Theorem 4.4)**.** *Assume $\mathbf{P}$ is non-obtuse and that $-\nu(az)$ is a sum of simple coroots. Let $z' \in Z$ and $u \in U_P$ with $uz' \in KzK$. Then one has $az' \cdot (K \cap U_P) \cdot (az')^{-1} \subseteq K \cap U_P$ and $aua^{-1} \in K$.*

The condition $aua^{-1} \in K$ is the difficult part of the theorem and can be interpreted as follows: Write $u = u_1 \cdots u_r$, for certain $u_i \in U_{\alpha_i}$. Then $\varphi_{\alpha_i}(u_i) \geq \langle \alpha_i, \nu(a) \rangle$ for all i, that is, we obtain a lower bound for the valuations of the u_i. In order to obtain this bound, we describe an algorithm, see Section 4, which produces a sequence of left cosets $u_0 z_0 K, \ldots, u_r z_r K$ in KzK (with $u_i \in U$, $z_i \in Z$) such that $u_0 z_0 = uz'$ and $u_r = 1$ (so that $\nu(z_r)$ lies in the orbit of $\nu(z)$ under the action of the finite Weyl group). As a byproduct, by a careful analysis, we can estimate the valuations of the root group elements u_i.

Finally, it should be mentioned that there is another possible approach to study intersections of Cartan and Iwasawa double cosets, which we do not follow here. For p-adic Chevalley groups Dąbrowski describes in [8] the intersections of the form $U\tau I \cap I\sigma I$ in terms of “good subexpressions”, where I is an Iwahori subgroup and τ, σ are elements of the affine Weyl group. By adapting the methods of [21] it seems plausible that one could in this way explicitly describe the intersections $Uz'K \cap KzK$.

1.3. Structure of the paper. In Section 2 we fix notations (Section 2.1) and recall some notions about reductive groups (Sections 2.2–2.4). In Sections 2.5–2.7 we discuss positive elements, the Cartan and Iwasawa decompositions, and abstract Hecke rings.

In Section 3 we study non-obtuse parabolics. In Proposition 3.5 we classify non-obtuse parabolic subgroups and provide equivalent characterizations.

In Section 4 we present the Algorithm 4.2. Although it will not be used in the sequel it is worth to mention that it always terminates (Proposition 4.3). Our main technical result is Theorem 4.4.

Finally, in Section 5 we develop the theory leading to the decomposition Theorem 5.24. The Section 5.1 introduces parabolic Hecke algebras and defines the unnormalized version of the Satake homomorphism. In Section 5.2 we give another presentation of the twisted action due to Henniart–Vignéras [14]. Then in Section 5.3 we translate the main theorem of [14] into our context. In Section 5.4 we recall the commutative algebra C_P^+. In Section 5.5 we work out an explicit example of a parabolic Hecke algebra. We provide an explicit presentation of the parabolic Hecke algebra attached to $\mathrm{GL}_2(\mathfrak{F})$ in terms of generators and relations. The straightforward proof is given in an appendix. We also explicitly compute the Satake homomorphism for illustrative purposes. Given a strictly positive element a_P, we construct in Section 5.6 a certain Hecke polynomial $\chi_{a_P}(t)$. With Hypothesis 5.16 we impose that $(K_P a_P)$ is a “left root” of $\chi_{a_P}(t)$. This hypothesis is crucial for proving the decomposition theorem. Theorem 5.17 shows that this hypothesis is satisfied provided that the parabolic $\mathbf{P}$ is non-obtuse. Proposition 5.21 lists several conditions which are equivalent to Hypothesis 5.16. Proposition 5.23 shows that, in principle, it would suffice to verify Hypothesis 5.16 for *maximal* parabolics.

Acknowledgments. This article constitutes a part of my doctoral dissertation [16]. I want to express my deep gratitude to my advisor Elmar Große-Klönne for his support. I also thank Peter Schneider for inviting me to present these results in the Mittagsseminar at the University of Münster. My thanks also goes to the organizers of the conference “Representation Theory and D-Modules”, held in June 2019 in Rennes, for giving me the chance to present a poster about this research. Finally, I thank the anonymous referee for a careful reading of the paper and for numerous remarks, questions, and suggestions.

2. Preliminaries

2.1. Notations. We fix a locally compact non-archimedean field $\mathfrak{F}$ with residue field $\mathbb{F}_q$ of characteristic p and normalized valuation $\mathrm{val}_{\mathfrak{F}} \colon \mathfrak{F} \to \mathbb{Z} \cup \{\infty\}$.

If $\mathbf{H}$ is an algebraic group defined over $\mathfrak{F}$, we denote by the corresponding lightface letter $H := \mathbf{H}(\mathfrak{F})$ its group of $\mathfrak{F}$-rational points. The topology on $\mathfrak{F}$ makes H into a topological group.

Let $\mathbf{G}$ be a connected reductive group defined over $\mathfrak{F}$. We choose a maximal $\mathfrak{F}$-split torus $\mathbf{T}$ in $\mathbf{G}$ and write $\mathrm{X}^*(T)$ (resp. $\mathrm{X}_*(T)$) for the group of algebraic $\mathfrak{F}$-characters (resp. algebraic $\mathfrak{F}$-cocharacters) of $\mathbf{T}$.

We denote by $\mathbf{Z} := \mathbf{Z}_{\mathbf{G}}(\mathbf{T})$ the centralizer and by $\mathbf{N} := \mathbf{N}_{\mathbf{G}}(\mathbf{T})$ the normalizer of $\mathbf{T}$ in $\mathbf{G}$. We call $W_0 := N/Z$ the finite Weyl group of $\mathbf{G}$.

The (relative) root system of $(\mathbf{G}, \mathbf{T})$ is denoted by $\Phi \subseteq \mathrm{X}^*(T)$; it need not be reduced if $\mathbf{G}$ is non-split. The finite Weyl group W_0 identifies with the Weyl group of the root system Φ. We denote

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

the subroot system of reduced roots. The set of coroots is denoted $\Phi^\vee \subseteq X_*(T)$.

We consider the root group $\mathbf{U}_\alpha$ attached to $\alpha \in \Phi$. Then $\mathbf{U}_{2\alpha} \subseteq \mathbf{U}_\alpha$ whenever $\alpha, 2\alpha \in \Phi$.

We fix a minimal parabolic $\mathfrak{F}$-subgroup $\mathbf{B}$ of $\mathbf{G}$ containing $\mathbf{T}$. It then admits a Levi decomposition

$$\mathbf{B} = \mathbf{U}\mathbf{Z}.$$

This choice fixes a system of positive roots Φ^+ in Φ (resp. positive coroots $(\Phi^\vee)^+$ in $\Phi^\vee$), and the unipotent radical $\mathbf{U}$ of $\mathbf{B}$ decomposes as

$$\mathbf{U} = \prod_{\alpha \in \Phi^+_{\mathrm{red}}} \mathbf{U}_\alpha,$$

where $\Phi^+_{\mathrm{red}} = \Phi_{\mathrm{red}} \cap \Phi^+$ is the set of reduced positive roots.

All parabolic subgroups are taken to be standard with respect to $\mathbf{B}$.

2.2. The standard apartment. If $\mathbf{C}$ denotes the connected center of $\mathbf{G}$, we consider the finite-dimensional $\mathbb{R}$-vector space

$$V := \mathbb{R} \otimes_{\mathbb{Z}} \big(\mathrm{X}_*(T)/\mathrm{X}_*(C)\big).$$

We view the set of coroots $\Phi^\vee$ as a subset of V via the natural map. Note that $\Phi^\vee$ generates V as an $\mathbb{R}$-vector space. On V there is the following partial ordering: Given $v, w \in V$, we write

$$v \leq w$$

if $w - v$ is a linear combination of simple coroots with non-negative coefficients.

The conjugation action of W_0 on $\mathbf{T}$ induces an action on V such that the natural pairing

$$\langle \cdot\,, \cdot \rangle \colon V^* \times V \longrightarrow \mathbb{R}$$

is non-degenerate and W_0-equivariant. Here, $V^* = \mathrm{Hom}_{\mathbb{R}}(V, \mathbb{R})$ denotes the $\mathbb{R}$-linear dual of V. We view Φ as a generating subset of V^*. We fix a W_0-invariant scalar product $(\cdot\,,\cdot)$ on V so that V becomes a Euclidean vector space. We denote $\|\cdot\|$ the norm induced by $(\cdot\,,\cdot)$. The scalar product $(\cdot\,,\cdot)$ induces a W_0-invariant scalar product on V^* which we again denote $(\cdot\,,\cdot)$.

By [6, 1.1.13] the tuple $(Z, (U_\alpha)_{\alpha\in\Phi})$ is a generating root group datum of G in the sense of [5, (6.1.1)]. In particular, this means that the root groups U_α satisfy the following condition:

(DR2) For all $\alpha, \beta \in \Phi$, the commutator group $[U_\alpha, U_\beta]$ is contained in the group generated by the $U_{n\alpha+m\beta}$, where $n, m \in \mathbb{Z}_{>0}$ are such that $n\alpha + m\beta \in \Phi$.

The standard apartment $\mathscr{A}$ in the adjoint building $\mathscr{B}(G)$ of G is an affine space under V consisting of certain valuations [5, (6.2.1)] of $(Z, (U_\alpha)_{\alpha\in\Phi})$. Since valuations will be instrumental later on, we will recall their definition. For the moment let L_α, for $\alpha \in \Phi$, be the subgroup generated by U_α, Z, and $U_{-\alpha}$, and put

$$M_\alpha \coloneqq \left\{ x \in L_\alpha \;\middle|\; xU_\alpha x^{-1} = U_{-\alpha} \text{ and } xU_{-\alpha}x^{-1} = U_\alpha \right\} \subseteq N. \tag{2.1}$$

Then M_α is a left and right coset under Z with image $\{s_\alpha\}$ in W_0. We record the following useful lemma:

Lemma 2.1 ([5, (6.1.2) (2)]). *Let $\alpha \in \Phi$ and $u \in U_\alpha^* \coloneqq U_\alpha \smallsetminus \{1\}$. Then there exists a unique triple $(u', m(u), u'') \in U_{-\alpha} \times G \times U_{-\alpha}$ such that $u = u'm(u)u''$, $m(u)U_{-\alpha}m(u)^{-1} = U_\alpha$, and $m(u)U_\alpha m(u)^{-1} = U_{-\alpha}$. Moreover, one has $m(u) \in M_\alpha$ and $u', u'' \neq 1$.*

Definition 2.2 ([5, (6.2.1)]). A *valuation* on $(Z, (U_\alpha)_{\alpha\in\Phi})$ is a tuple $\psi = (\psi_\alpha)_{\alpha\in\Phi}$ of functions $\psi_\alpha\colon U_\alpha \to \mathbb{R}\cup\{\infty\}$ satisfying the following conditions:

(V0) The image of ψ_α contains at least three elements;

(V1) For each $\alpha \in \Phi$ and $r \in \mathbb{R} \cup \{\infty\}$ the set $U_{\alpha,r} = \psi_\alpha^{-1}([r, \infty])$ is a subgroup of U_α, and $U_{\alpha,\infty} = \{1\}$;

(V2) For each $\alpha \in \Phi$ and each $m \in M_\alpha$ the function

$$U_{-\alpha}^* = U_{-\alpha} \smallsetminus \{1\} \longrightarrow \mathbb{R}, \quad u \longmapsto \psi_{-\alpha}(u) - \psi_\alpha(mum^{-1})$$

is constant.

(V3) Given $\alpha, \beta \in \Phi$ with $\beta \notin \mathbb{R}_{<0}\alpha$, and $r, s \in \mathbb{R}$, the commutator group $[U_{\alpha,r}, U_{\beta,s}]$ is contained in the group generated by the groups $U_{n\alpha+m\beta,nr+ms}$, for $n, m \in \mathbb{Z}_{>0}$ such that $n\alpha + m\beta \in \Phi$;

(V4) If $\alpha, 2\alpha \in \Phi$, then $\psi_{2\alpha}$ is the restriction of $2\psi_\alpha$ to $U_{2\alpha} \subseteq U_\alpha$;

(V5) Given $\alpha \in \Phi$, $u \in U_\alpha$, and $u', u'' \in U_{-\alpha}$ such that $u'uu'' \in M_\alpha$, one has $\psi_{-\alpha}(u') = \psi_{-\alpha}(u'') = -\psi_\alpha(u)$.

The space of valuations on $(Z, (U_\alpha)_{\alpha\in\Phi})$ admits the following two actions [5, (6.2.5)]:

- Given a valuation $\psi = (\psi_\alpha)_{\alpha\in\Phi}$ and $v \in V$, the tuple
$$\psi + v = \big(\psi_\alpha + \langle \alpha, v\rangle\big)_{\alpha\in\Phi}$$
is again a valuation.
- Let $\psi = (\psi_\alpha)_{\alpha\in\Phi}$ be a valuation and $n \in N$. Denote w the image of n under the canonical projection $N \to N/Z = W_0$. We obtain a new valuation $n.\psi = ((n.\psi)_\alpha)_{\alpha\in\Phi}$ defined by
$$(n.\psi)_\alpha(u) = \psi_{w^{-1}(\alpha)}(n^{-1}un), \qquad \text{for all } u \in U_\alpha.$$
In this way, the group N acts on the space of valuations.

By [6, 5.1.20 Thm. and 5.1.23 Prop.] there exists a valuation
$$\varphi = (\varphi_\alpha\colon U_\alpha \to \mathbb{R}\cup\{\infty\})_{\alpha\in\Phi} \quad \text{of } (Z, (U_\alpha)_{\alpha\in\Phi})$$
which is discrete [5, (6.2.21)], special [5, (6.2.13)] and compatible with the valuation $\mathrm{val}_{\mathfrak{F}}$ [6, 4.2.8 Déf.]. The standard apartment $\mathscr{A}$ is the Euclidean affine space under V given by
$$\mathscr{A} = \{\varphi + v \mid v \in V\}\,.$$
The action of N restricts to an action on $\mathscr{A}$ by Euclidean affine automorphisms and the subgroup Z acts by translations [5, (6.2.10)]. More concretely, it follows from (V2) that there exists a unique group homomorphism $\nu\colon Z \to V$ such that $z.\varphi = \varphi + \nu(z)$, that is,
$$\varphi_\alpha(z^{-1}uz) = \varphi_\alpha(u) + \langle \alpha, \nu(z)\rangle, \qquad \text{for all } u \in U_\alpha, \text{ all } \alpha \in \Phi. \tag{2.2}$$
The fact that φ is compatible with $\mathrm{val}_{\mathfrak{F}}$ then expresses the condition that $\langle \chi|_{\mathbf{T}}, \nu(z)\rangle = -\mathrm{val}_{\mathfrak{F}}(\chi(z))$, for all $\chi \in \mathrm{X}^*(Z)$.

The affine action of N on $\mathscr{A}$ induces a linear action of $W_0 = N/Z$ on V, obtained by composing the action map $N \to \mathrm{Aff}(\mathscr{A})$ (where $\mathrm{Aff}(\mathscr{A})$ denotes the group of affine automorphisms of $\mathscr{A}$) with the canonical projection $\mathrm{Aff}(\mathscr{A}) \to \mathrm{GL}_{\mathbb{R}}(V)$. This action coincides with the natural action of W_0 on V.

Given $\alpha \in V^*$ and $r \in \mathbb{R}$, we consider the hyperplane
$$H_{\alpha,r} \coloneqq \{\varphi + v \in \mathscr{A} \mid \langle \alpha, v\rangle + r = 0\}$$
and put
$$\mathfrak{H} \coloneqq \{H_{\alpha,r} \mid \alpha \in \Phi_{\mathrm{red}} \text{ and } r \in \varphi_\alpha(U_\alpha^*)\}\,.$$
Then N acts on $\mathfrak{H}$ via
$$n.H_{\alpha,r} = H_{w(\alpha), r - \langle w(\alpha), n.\varphi - \varphi\rangle}, \quad \text{for } n \in N \text{ with image } w \in W_0.$$
The groups $U_{\alpha,r} = \varphi_\alpha^{-1}([r,\infty])$, for $r \in \mathbb{R}$, are a neighborhood basis of $1 \in U_\alpha$ consisting of compact open subgroups, and we have
$$nU_{\alpha,r}n^{-1} = U_{w(\alpha), r - \langle w(\alpha), n.\varphi - \varphi\rangle}, \quad \text{for } n \in N \text{ with image } w \in W_0.$$

2.3. The associated reduced root system. We denote by $S(\mathfrak{H})$ the set of orthogonal reflections s_H through $H \in \mathfrak{H}$. Conversely, we denote H_s the hyperplane in $\mathscr{A}$ fixed by $s \in S(\mathfrak{H})$. This exhibits a canonical bijection $\mathfrak{H} \cong S(\mathfrak{H})$.

The group W^{aff} generated by $S(\mathfrak{H})$ (inside the group of affine automorphisms of $\mathscr{A}$) is called the *affine Weyl group* of G. The stabilizer of φ in W^{aff} identifies with W_0, since φ is special. This yields a semidirect product decomposition

$$W^{\mathrm{aff}} = (W^{\mathrm{aff}} \cap V) \rtimes W_0,$$

and $W^{\mathrm{aff}} \cap V$ is generated by the translations $r\alpha^\vee$, for $\alpha \in \Phi_{\mathrm{red}}$ and $r \in \varphi_\alpha(U_\alpha^*)$ [5, (6.2.19)]. In particular, $W^{\mathrm{aff}} \cap V$ is a lattice of rank $\dim_{\mathbb{R}} V$ in V. Now, [4, Ch. VI, §2, no. 5, Prop. 8] shows that there exists a unique reduced root system

$$\Sigma \subseteq V^*$$

such that W^{aff} is the affine Weyl group of Σ. This means that W^{aff} coincides with the group generated by the reflections $s_{\alpha,k}$, for $(\alpha, k) \in \Sigma^{\mathrm{aff}} := \Sigma \times \mathbb{Z}$, defined by

$$s_{\alpha,k}(x) = x - (\langle \alpha, x - \varphi \rangle + k) \cdot \alpha^\vee, \qquad \text{for } x \in \mathscr{A}.$$

We write simply s_α instead of $s_{\alpha,0}$ and view it as an element of W_0.

By [25, Lem. I.2.10],

$$\varphi_\alpha(U_\alpha^*) = \epsilon_\alpha^{-1}\mathbb{Z}, \qquad \text{for } \alpha \in \Phi,$$

is a group, where $\epsilon_\alpha \in \mathbb{Z}_{>0}$ is a natural number which is even whenever $2\alpha \in \Phi$. We obtain a surjective map

$$\Phi \twoheadrightarrow \Sigma, \quad \alpha \longmapsto \epsilon_\alpha \alpha$$

which induces a bijection $\Phi_{\mathrm{red}} \cong \Sigma$.

Under this bijection, Φ^+ corresponds to a system of positive roots in Σ, which we denote Σ^+.

For each $\alpha = \epsilon_\beta \beta$ in Σ, where $\beta \in \Phi_{\mathrm{red}}$, we put $U_\alpha := U_\beta$ and

$$U_{(\alpha,k)} := U_{\beta, \epsilon_\beta^{-1} k}, \qquad \text{for all } k \in \mathbb{Z}.$$

This defines a $\mathbb{Z}$-indexed descending filtration on U_α by compact open subgroups which is separated and exhaustive. If $n \in N$ with image w in W_0, we have

$$nU_{(\alpha,k)}n^{-1} = U_{(w(\alpha), k - \langle w(\alpha), n.\varphi - \varphi \rangle)}. \tag{2.3}$$

2.4. The Iwahori–Weyl group. Let K be the special parahoric subgroup of G associated with φ [6, 5.2.6]. If $X \subseteq G$ is a subgroup, we write

$$K_X \coloneqq K \cap X.$$

We note the following properties:

- the special point φ is fixed by K under the natural action of G on $\mathscr{B}(G)$;
- the group $K \cap N$ contains a set of representatives of W_0;
- for all $\alpha \in \Sigma$ we have $K \cap U_\alpha = U_{(\alpha,0)}$ [28, (51)];
- if $\mathbf{P} = \mathbf{U_P M}$ is a parabolic subgroup of $\mathbf{G}$ with Levi $\mathbf{M}$ and unipotent radical $\mathbf{U_P}$, then K_M is a special parahoric subgroup of M [13, Lem. 4.1.1]. In particular, since Z is anisotropic, K_Z is the unique parahoric subgroup of Z;

Since K_Z is the unique parahoric subgroup of Z, it is normalized by N. We call

$$W \coloneqq N/K_Z$$

the *Iwahori–Weyl group*. The subgroup

$$\Lambda \coloneqq Z/K_Z \subseteq W$$

is a finitely generated abelian group with finite torsion and the same rank as $X_*(T)$ [13, Thm. 1.0.1]. We therefore denote it additively. When we view Λ as a subgroup of W, we employ an exponential notation, that is, we write $e^\lambda \in W$ for $\lambda \in \Lambda$. The natural exact sequence

$$0 \longrightarrow \Lambda \longrightarrow W \longrightarrow W_0 \longrightarrow 1$$

splits, that is, W decomposes as the semidirect product

$$W \cong \Lambda \rtimes W_0,$$

and W_0 acts on Λ by $e^{w(\lambda)} \coloneqq we^\lambda w^{-1}$. We note that the map $\nu\colon Z \to V$ (2.2) factors through Λ and induces a W_0-equivariant map

$$\nu\colon \Lambda \longrightarrow V.$$

2.5. The positive monoid. We define

$$\Lambda^+ \coloneqq \Lambda^{+,G} \coloneqq \left\{ \lambda \in \Lambda \,\middle|\, \langle \alpha, \nu(\lambda) \rangle \leq 0 \text{ for all } \alpha \in \Sigma^+ \right\}$$

and denote Z^+ (or $Z^{+,G}$ if we want to emphasize the dependence on G) the preimage of Λ^+ under the projection $Z \twoheadrightarrow \Lambda$. We refer to Z^+ as the *positive monoid*. The *negative monoid* is defined as $Z^- \coloneqq (Z^+)^{-1}$. We also write $\Lambda^- \coloneqq -\Lambda^+$.

An element $\lambda \in \Lambda^+$ is called *strictly positive* if $\langle \alpha, \nu(\lambda) \rangle < 0$, for all $\alpha \in \Sigma^+$. Note that if λ is strictly positive, the group Λ is generated as a monoid by Λ^+ and $-\lambda$.

More generally, let $\mathbf{P} = \mathbf{U_P M}$ be a parabolic subgroup of $\mathbf{G}$. We denote

$$M^+ := \left\{ m \in M \;\middle|\; m K_{U_P} m^{-1} \subseteq K_{U_P} \right\}$$

the *monoid of M-positive elements.* Note that $K_M \subseteq M^+ \cap (M^+)^{-1}$. We define

$$\mu_{U_P}(m) := [K_{U_P} : K_{U_P} \cap m^{-1} K_{U_P} m] \in q^{\mathbb{Z}_{\geq 0}}. \tag{2.4}$$

Clearly, $m \in M$ is M-positive if and only if $\mu_{U_P}(m) = 1$. The integers $\mu_{U_P}(m)$ have been studied in [18, §3.4].

An element $\lambda \in \Lambda$ is called *strictly M-positive* if $\langle \Sigma_M, \nu(\lambda) \rangle = 0$ and $\langle \alpha, \nu(\lambda) \rangle < 0$ for all $\alpha \in \Sigma^+ \smallsetminus \Sigma_M$. Note that by (2.3), the monoid

$$\Lambda_{M^+} := \left\{ \lambda \in \Lambda \;\middle|\; \langle \alpha, \nu(\lambda) \rangle \leq 0 \text{ for all } \alpha \in \Sigma^+ \smallsetminus \Sigma_M \right\} \tag{2.5}$$

coincides with the image of $Z \cap M^+$ in Λ.

We call $a \in Z$ *strictly M-positive* if a lies in the center of M and $aK_Z \in \Lambda$ is strictly M-positive. We remark that by [7, (6.14)] there exist strictly M-positive elements.

2.6. Double coset decompositions. We recall here the Cartan and the Iwasawa decomposition of G. In Section 4 we will study intersections between Cartan and Iwasawa double cosets.

Cartan decomposition 2.3 ([13, Thm. 1.0.3])**.** *The inclusion $Z \subseteq G$ induces a bijection*

$$\Lambda / W_0 \cong K \backslash G / K.$$

Remark 2.4.

(a) The monoids Λ^+ and Λ^- are representatives for the W_0-orbits of Λ [14, 6.3 Lem.]. Therefore, the inclusion $Z \subseteq G$ induces bijections $\Lambda^+ \cong K\backslash G/K$ and $\Lambda^- \cong K\backslash G/K$. These are also referred to as the Cartan decomposition.
(b) The Cartan decomposition implies that if $KzK = Kz'K$, for some $z, z' \in Z$, then there exists $w \in W_0$ such that $w(zK_Z) = z'K_Z$ (and hence also $w.\nu(z) = \nu(z')$).

Iwasawa decomposition 2.5. *The inclusion $Z \subseteq G$ induces a bijection*

$$\Lambda \cong U \backslash G / K.$$

This decomposition is often written as $G = BK = UZK = ZUK$.

Remark 2.6. It is of general interest to study intersections of Cartan and Iwasawa double cosets. We recall some well-known results. Let $z \in Z^-$ and $z' \in Z$ such that $Uz'K \cap KzK \neq \varnothing$. Then:

(a) $\nu(z') \leq \nu(z)$, see [13, Lem. 10.2.1] or [14, 6.10 Prop.].
(b) If $\nu(z) = \nu(z')$, then $zK_Z = z'K_Z$, see [14, 6.10 Prop.].

(c) $w.\nu(z') \leq \nu(z)$, for all $w \in W_0$. This follows from properties of the Satake homomorphism as in [24, Lem. 2.1] but using [14, 7.13 Thm.]. This argument is also spelled out in Remark 5.8.

This inequality is equivalent to saying that $\nu(z')$ lies inside the convex polytope spanned by the W_0-orbit of $\nu(z)$, cf. [23, (2.6.2)].

In Section 4 we give an algorithm which yields also information about the $u \in U$ with $uz' \in KzK$.

2.7. Abstract Hecke rings. We briefly discuss abstract Hecke rings. The references below refer to, and details can be found in, [3, Ch. 3, §1].

Let G be a topological group and $\Gamma \subseteq G$ a compact open subgroup. Let $\Gamma \subseteq S \subseteq G$ be a submonoid. The pair (Γ, S) is called a *Hecke pair*. Let

$$\mathbb{Z}[\Gamma\backslash S] = \bigoplus_{\Gamma s \in \Gamma\backslash S} \mathbb{Z}.(\Gamma s)$$

be the free $\mathbb{Z}$-module on the set of right cosets $\Gamma\backslash S$. It admits a natural right S-action by $(\Gamma s) \cdot s' = (\Gamma s s')$, for $s, s' \in S$. Clearly, $\mathbb{Z}[\Gamma\backslash S]$ is a left module under the ring

$$\mathcal{H}(\Gamma, S) \coloneqq \mathrm{End}_S(\mathbb{Z}[\Gamma\backslash S]).$$

We usually make the identification

$$\mathcal{H}(\Gamma, S) \xrightarrow{\cong} \mathbb{Z}[\Gamma\backslash S]^\Gamma,$$
$$T \longmapsto T((\Gamma)).$$

The submodule $\mathbb{Z}[\Gamma\backslash S]^\Gamma$ of Γ-invariants is a free $\mathbb{Z}$-module on the set of double cosets $\Gamma\backslash S/\Gamma$. Concretely, it admits $\{(s)_\Gamma \mid \Gamma s \Gamma \in \Gamma\backslash S/\Gamma\}$ as a basis, where

$$(s)_\Gamma \coloneqq \sum_{\Gamma s' \subseteq \Gamma s \Gamma} (\Gamma s').$$

The sum runs through all right cosets contained in $\Gamma s \Gamma$. Note that the sum is finite, because Γ is compact open, so that the set $(\Gamma \cap s^{-1}\Gamma s)\backslash\Gamma$ is finite, and the map

$$(\Gamma \cap s^{-1}\Gamma s)\backslash\Gamma \xrightarrow{\cong} \Gamma\backslash\Gamma s\Gamma, \tag{2.6}$$
$$(\Gamma \cap s^{-1}\Gamma s)\gamma \longmapsto \Gamma s\gamma$$

is bijective. The multiplication on $\mathbb{Z}[\Gamma\backslash S]^\Gamma$ is concretely given by

$$\left(\sum_i n_i \cdot (\Gamma s_i)\right) \cdot \left(\sum_j m_j \cdot (\Gamma t_j)\right) = \sum_{i,j} n_i m_j \cdot (\Gamma s_i t_j).$$

For an explicit description of the multiplication in terms of double cosets, see [3, Lem. 1.5].

The following two results are frequently useful:

Proposition 2.7 ([3, Prop. 1.9]). *Let* (Γ, S) *and* (Γ_0, S_0) *be two Hecke pairs satisfying*

$$\Gamma_0 \subseteq \Gamma, \quad S \subseteq \Gamma S_0, \quad \text{and} \quad \Gamma \cap S_0 \cdot S_0^{-1} \subseteq \Gamma_0. \tag{2.7}$$

Then the map

$$\begin{aligned} \varepsilon\colon \mathcal{H}(\Gamma, S) &\hookrightarrow \mathcal{H}(\Gamma_0, S_0), \\ \sum_i n_i \cdot (\Gamma s_i) &\longmapsto \sum_i n_i \cdot (\Gamma_0 s_i), \end{aligned}$$

where the s_i *are chosen in* S_0*, is an injective ring homomorphism.*

Proposition 2.8 ([3, Prop. 1.11]). *Let* (Γ, S) *be a Hecke pair. Then* (Γ, S^{-1}) *is also a Hecke pair, and the map*

$$\begin{aligned} \zeta_S\colon \mathcal{H}(\Gamma, S) &\longrightarrow \mathcal{H}(\Gamma, S^{-1}), \\ (s)_\Gamma &\longmapsto (s^{-1})_\Gamma \end{aligned} \tag{2.8}$$

is an anti-isomorphism of rings.

Lemma 2.9 ([3, Lem. 1.13]). *Let* (Γ, S) *and* (Γ_0, S_0) *be two Hecke pairs satisfying* (2.7) *such that* (Γ, S^{-1}) *and* (Γ_0, S_0^{-1}) *also satisfy* (2.7)*. Then the following diagram is commutative:*

$$\begin{array}{ccc} \mathcal{H}(\Gamma, S) & \xrightarrow{\ \varepsilon\ } & \mathcal{H}(\Gamma_0, S_0) \\ {\scriptstyle \zeta_S}\downarrow & & \downarrow{\scriptstyle \zeta_{S_0}} \\ \mathcal{H}(\Gamma, S^{-1}) & \xrightarrow[\ \varepsilon\ ]{} & \mathcal{H}(\Gamma_0, S_0^{-1}). \end{array}$$

If R is a commutative ring with 1, we put

$$\mathcal{H}_R(\Gamma, S) \coloneqq R \otimes_{\mathbb{Z}} \mathcal{H}(\Gamma, S).$$

It is clear that Propositions 2.7 and 2.8 and Lemma 2.9 remain valid for Hecke rings over R.

3. Non-obtuse parabolics

We fix a maximal parabolic subgroup $\mathbf{P} = \mathbf{U_P M}$ of $\mathbf{G}$. Recall from Section 2.2 the Euclidean vector space $(V^*, (\,\cdot\,,\cdot\,))$, on which the finite Weyl group W_0 acts, and the special point $\varphi \in \mathscr{A}$ from Section 2.2. We view φ as a valuation on the root group datum $(Z, (U_\alpha)_{\alpha\in\Phi})$. Also recall from Section 2.3 the reduced root system $\Sigma \subseteq V^*$. The system Σ^+ of positive roots determines a unique basis Δ of Σ. Since $\mathbf{M}$ is reductive, all these objects have an analogue for $\mathbf{M}$, and we denote them by adding the subscript 'M'. For example, we write Σ_M, $W_{0,M}$, Δ_M etc.

Definition 3.1. The parabolic $\mathbf{P}$ is called *non-obtuse* if

$$\langle \alpha, \beta^\vee \rangle \geq 0, \qquad \text{for all } \alpha, \beta \in \Sigma^+ \smallsetminus \Sigma_M.$$

Remark 3.2. For $\mathbf{P}$ to be non-obtuse it is equivalent to say that

$$(\alpha, \beta) \geq 0, \qquad \text{for all } \alpha, \beta \in \Sigma^+ \smallsetminus \Sigma_M.$$

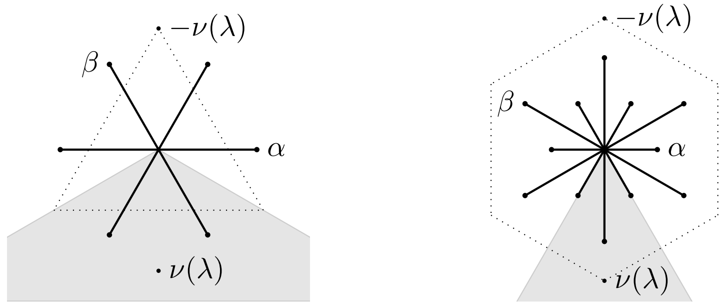
This more geometric definition explains the term “non-obtuse”: It means that any two roots in $\Sigma^+ \smallsetminus \Sigma_M$ span a non-obtuse angle.

During the whole section we assume that $\mathbf{P}$ is non-obtuse. The main result of this section is a complete classification of the non-obtuse parabolic subgroups of $\mathbf{G}$. First, we prove an important technical result which explains our interest in non-obtuse parabolics.

Lemma 3.3. *Let $\lambda, \mu \in \Lambda$ such that λ is strictly M-positive. Assume that $\nu(w(\mu)) \leq \nu(-\lambda)$ for all $w \in W_0$. Then one has*

$$\langle \alpha, \nu(\lambda + \mu) \rangle \leq 0, \qquad \text{for all } \alpha \in \Sigma^+ \smallsetminus \Sigma_M.$$

Example 3.4. Before giving the proof, let us look at the two examples in Figure 3.1. Example (A) explains why Lemma 3.3 should be expected to hold true for non-obtuse parabolics, while (B) explains why Lemma 3.3 fails otherwise.



(A) Type A_2: The translate of the dotted region by $\nu(\lambda)$ fits into the shaded area. Lemma 3.3 holds in this case.

(B) Type G_2: The translate of the dotted region by $\nu(\lambda)$ does not fit into the shaded area. Lemma 3.3 fails.

FIGURE 3.1. In both examples we choose $\Sigma_M = \{\pm\alpha\}$, and $\nu(\mu)$ can lie anywhere in the dotted region.

Proof of Lemma 3.3. Recall that $\mathbf{P}$ is non-obtuse so that $\langle \alpha, \beta^\vee \rangle \geq 0$ for all $\alpha, \beta \in \Sigma^+ \smallsetminus \Sigma_M$. We proceed in two steps.

Step 1. Assume $\mu = w(-\lambda)$, for some $w \in W_0$. We do an induction on the length $\ell(w)$ of w. If $\ell(w) = 1$, we write $w = s_\beta$ for some simple root $\beta \in \Delta$.

For each $\alpha \in \Sigma^+ \smallsetminus \Sigma_M$ we compute

$$\begin{aligned}\langle \alpha, \nu(\lambda + s_\beta(-\lambda)) \rangle &= \langle \alpha, \nu(\lambda) - s_\beta(\nu(\lambda)) \rangle \\ &= \langle \alpha, \langle \beta, \nu(\lambda) \rangle \cdot \beta^\vee \rangle \\ &= \langle \beta, \nu(\lambda) \rangle \cdot \langle \alpha, \beta^\vee \rangle \\ &\leq 0,\end{aligned}$$

where in the last step we have used $\langle \beta, \nu(\lambda) \rangle < 0$ and that $\mathbf{P}$ is non-obtuse. Now assume $\ell(w) > 1$, and let $\beta \in \Delta$ with $\ell(s_\beta w) < \ell(w)$. We write

$$\nu(\lambda + w(-\lambda)) = \nu(\lambda + s_\beta(-\lambda)) + s_\beta(\nu(\lambda + s_\beta w(-\lambda))). \tag{3.1}$$

We distinguish two cases:

- If $\beta \in \Delta_M$, then we have $s_\beta(\Sigma^+ \smallsetminus \Sigma_M) = \Sigma^+ \smallsetminus \Sigma_M$. For each $\alpha \in \Sigma^+ \smallsetminus \Sigma_M$, the induction hypothesis (applied to $s_\beta w$) yields:

  $$\langle \alpha, s_\beta(\nu(\lambda + s_\beta w(-\lambda))) \rangle = \langle s_\beta(\alpha), \nu(\lambda + s_\beta w(-\lambda)) \rangle \leq 0.$$

  Together with (3.1) and the base case the statement follows.
- If $\beta \in \Delta \smallsetminus \Delta_M$, then we compute for each $\alpha \in \Sigma^+ \smallsetminus \Sigma_M$:

  $$\begin{aligned}&\langle \alpha, \nu(\lambda + w(-\lambda)) \rangle \\ &\quad = \langle \alpha, \nu(\lambda + s_\beta(-\lambda)) \rangle + \langle \alpha, s_\beta(\nu(\lambda + s_\beta w(-\lambda))) \rangle \\ &\quad = \langle \alpha, \langle \beta, \nu(\lambda) \rangle \cdot \beta^\vee \rangle + \langle s_\beta(\alpha), \nu(\lambda + s_\beta w(-\lambda)) \rangle \\ &\quad = \langle \beta, \nu(\lambda) \rangle \cdot \langle \alpha, \beta^\vee \rangle + \langle \alpha - \langle \alpha, \beta^\vee \rangle \cdot \beta, \nu(\lambda + s_\beta w(-\lambda)) \rangle \\ &\quad = \langle \alpha, \nu(\lambda + s_\beta w(-\lambda)) \rangle - \langle \alpha, \beta^\vee \rangle \cdot \langle \beta, \nu(s_\beta w(-\lambda)) \rangle \\ &\quad = \langle \alpha, \nu(\lambda + s_\beta w(-\lambda)) \rangle + \langle \alpha, \beta^\vee \rangle \cdot \langle (s_\beta w)^{-1}(\beta), \nu(\lambda) \rangle \\ &\quad \leq 0,\end{aligned}$$

  where the last step uses the induction hypothesis and $(s_\beta w)^{-1}(\beta) \in \Sigma^+$, which in turn follows from $\ell((s_\beta w)^{-1} s_\beta) > \ell((s_\beta w)^{-1})$ (see, e.g., [19, 1.6 Lem.]).

This finishes the induction step.

Step 2. Let μ be general. Take an arbitrary $\alpha \in \Sigma^+ \smallsetminus \Sigma_M$. Let $\alpha_0 = w(\alpha)$ be a root of maximal height in the W_0-orbit of α. (If we write $\alpha_0 = \sum_{\beta \in \Delta} n_\beta \beta$, the *height* of α_0 is $\sum_{\beta \in \Delta} n_\beta$.) Then we have $\langle \alpha_0, \beta^\vee \rangle \geq 0$, for all $\beta \in \Sigma^+$, since otherwise $s_\beta(\alpha_0) = \alpha_0 - \langle \alpha_0, \beta^\vee \rangle \cdot \beta$ would have greater height than α_0. By the hypothesis, $\nu(-\lambda) - \nu(w(\mu))$ is a linear combination of simple coroots with non-negative coefficients. Therefore,

$$\begin{aligned}\langle \alpha, \nu(w^{-1}(\lambda) + \mu) \rangle &= \langle w(\alpha), \nu(\lambda + w(\mu)) \rangle \\ &= -\langle \alpha_0, \nu(-\lambda) - \nu(w(\mu)) \rangle \leq 0.\end{aligned} \tag{3.2}$$

By Step 1 we have

$$\langle \alpha, \nu(\lambda + w^{-1}(-\lambda)) \rangle \leq 0. \tag{3.3}$$

Finally, (3.2) and (3.3) imply

$$\langle \alpha, \nu(\lambda + \mu) \rangle = \langle \alpha, \nu(\lambda + w^{-1}(-\lambda)) \rangle + \langle \alpha, \nu(w^{-1}(\lambda) + \mu) \rangle \leq 0. \qquad \square$$

We now turn to the classification of non-obtuse parabolics. Since $\mathbf{P}$ is assumed to be maximal, the roots in $\Sigma^+ \smallsetminus \Sigma_M$ are contained in an irreducible component of Σ. Without loss of generality we may therefore assume that Σ is irreducible.

The maximal parabolics of $\mathbf{G}$ are in one-to-one correspondence with the elements of the basis Δ of Σ. We write $\Delta = \{\alpha_1, \ldots, \alpha_n\}$ and denote $s_r := s_{\alpha_r}$ the simple reflection attached to α_r. Let $\mathbf{P}_r = \mathbf{U}_{\mathbf{P}_r}\mathbf{M}_r$ be the maximal parabolic subgroup corresponding to α_r so that $\Delta_{M_r} = \Delta \smallsetminus \{\alpha_r\}$. We put

$$\Sigma_{U_{P_r}} := \Sigma^+ \smallsetminus \Sigma_{M_r}.$$

Then α_r is the unique element in $\Sigma_{U_{P_r}} \cap \Delta$. We say that α_r is *non-obtuse* if $\mathbf{P}_r$ is.

Proposition 3.5. *The classification of non-obtuse parabolic subgroups of* $\mathbf{G}$ *is given in terms of the Dynkin diagram of* Σ *in Figure 3.2. Moreover, the following conditions are equivalent:*

- (i) α_r *is non-obtuse.*
- (ii) $\langle \alpha_r, \beta^\vee \rangle \geq 0$ *for all* $\beta \in \Sigma_{U_{P_r}}$.
- (iii) *The Weyl group* W_{0,M_r} *acts transitively on the roots in* $\Sigma_{U_{P_r}}$ *of the same length.*
- (iv) *In the notation of* (3.4) *below we have* $c_r(\alpha_0^r) = 1$, *where* α_0^r *is the highest root of the same length as* α_r.

Proof. We consider each type separately. The equivalences of (i)–(iv) are obtained along the way. For the concrete description of the roots systems we follow [4, Planches I–IX].

As usual we denote $e_1, \ldots, e_n$ the standard basis of $\mathbb{R}^n$, endowed with the canonical scalar product $(\cdot\,,\cdot)$. Given a root $\beta \in \Sigma$, we write

$$\beta = \sum_{i=1}^{n} c_i(\beta) \cdot \alpha_i. \tag{3.4}$$

Observe that $c_i(s_j(\beta)) = c_i(\beta)$, for $i \neq j$. In particular, the action of W_{0,M_r} does not affect $c_r(\beta)$. Observe that $\Sigma_{U_{P_r}}$ consists of those $\beta \in \Sigma^+$ with $c_r(\beta) > 0$.

(A_n). Inside $V = \{(x_1, \ldots, x_{n+1}) \in \mathbb{R}^{n+1} \mid \sum_{i=1}^{n+1} x_i = 0\}$ the root system of type A_n is

$$\Sigma = \{\pm(e_i - e_j) \,|\, 1 \leq i < j \leq n+1\}.$$

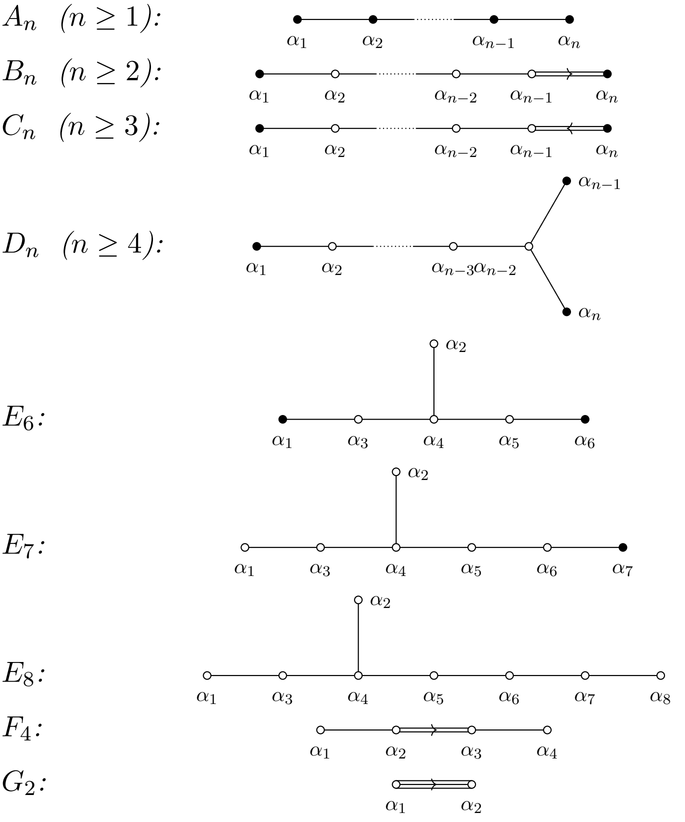


Figure 3.2. The black vertices are precisely the non-obtuse simple roots. Note that in types E_8, F_4, and G_2 there are no non-obtuse parabolics, while in type A_n all maximal parabolics are non-obtuse.

The simple roots are given by $\alpha_i = e_i - e_{i+1}$, for $i = 1, \dots, n$, and the roots $e_i - e_j = \sum_{k=i}^{j-1} \alpha_k$, for $1 \leq i < j \leq n+1$, are positive. The Weyl group W_0 is the symmetric group $\mathfrak{S}_{n+1}$ acting on $e_1, \dots, e_{n+1}$. Fix $1 \leq r \leq n$. Then we have

$$\Sigma_{U_{P_r}} = \{e_i - e_j \mid 1 \leq i \leq r < j \leq n+1\}\,.$$

If $e_i - e_j, e_a - e_b \in \Sigma_{U_{P_r}}$, then we have $a \neq j$ and $i \neq b$. Hence, $(e_i - e_j, e_a - e_b) = \delta_{ia} + \delta_{jb} \geq 0$ and α_r is non-obtuse. The Weyl group W_{0,M_r} identifies with $\mathfrak{S}_r \times \mathfrak{S}_{n+1-r}$ with the first factor acting on $\{e_1, \dots, e_r\}$ and the second on $\{e_{r+1}, \dots, e_{n+1}\}$. It clearly acts transitively on $\Sigma_{U_{P_r}}$.

(B_n). Inside $V = \mathbb{R}^n$ the root system of type B_n is

$$\Sigma = \{\pm e_i \mid 1 \leq i \leq n\} \cup \{\pm e_i \pm e_j \mid 1 \leq i < j \leq n\}\,.$$

A basis is given by $\alpha_i = e_i - e_{i+1}$, for $1 \leq i < n$, and $\alpha_n = e_n$. The positive roots are

$$\begin{cases} e_i = \sum_{k=i}^{n} \alpha_k, & \text{for } 1 \leq i \leq n; \\ e_i - e_j = \sum_{k=i}^{j-1} \alpha_k, & \text{for } 1 \leq i < j \leq n; \\ e_i + e_j = \sum_{k=i}^{j-1} \alpha_k + 2\sum_{k=j}^{n} \alpha_k, & \text{for } 1 \leq i < j \leq n. \end{cases}$$

The Weyl group W_0 identifies with $(\mathbb{Z}/2\mathbb{Z})^n \rtimes \mathfrak{S}_n$ with $\mathfrak{S}_n$ permuting the e_i, and $(\mathbb{Z}/2\mathbb{Z})^n$ acting by changing the signs of the e_i. Consider three cases:

- Assume $r = 1$. Then

$$\Sigma_{U_{P_1}} = \{e_1\} \cup \{e_1 \pm e_i \,|\, 2 \leq i \leq n\}.$$

  Given $e_1 + \varepsilon_1 e_i, e_1 + \varepsilon_2 e_j \in \Sigma_{U_{P_1}}$, with $\varepsilon_1, \varepsilon_2 \in \{-1, 0, 1\}$, we compute

$$(e_1 + \varepsilon_1 e_i, e_1 + \varepsilon_2 e_j) = 1 + \varepsilon_1 \varepsilon_2 \delta_{ij} \geq 0.$$

  Hence, α_1 is non-obtuse. The Weyl group W_{0,M_1} identifies with $(\mathbb{Z}/2\mathbb{Z})^{n-1} \rtimes \mathfrak{S}_{n-1}$ with both groups acting on $\{\pm e_2, \ldots, \pm e_n\}$, leaving e_1 fixed. It acts transitively on $\{e_1 \pm e_i \,|\, 2 \leq i \leq n\}$ (and on $\{e_1\}$).
- Assume $r = n$. Then

$$\Sigma_{U_{P_n}} = \{e_i \,|\, 1 \leq i \leq n\} \cup \{e_i + e_j \,|\, 1 \leq i < j \leq n\}.$$

  It is obvious that α_n is non-obtuse. The Weyl group W_{0,M_n} identifies with $\mathfrak{S}_n$ acting on $e_1, \ldots, e_n$. It clearly acts transitively on both $\{e_1, \ldots, e_n\}$ and $\{e_i + e_j \,|\, 1 \leq i < j \leq n\}$.
- Assume $1 < r < n$; in particular, $n \geq 3$. Note that both $\alpha_r = e_r - e_{r+1}$ and $e_{r-1} + e_{r+1}$ lie in $\Sigma_{U_{P_r}}$ and satisfy $(e_r - e_{r+1}, e_{r-1} + e_{r+1}) = -1$. Hence, α_r is not non-obtuse. The highest root is $\alpha_0 = e_1 + e_2 = \alpha_1 + 2\sum_{k=2}^{n} \alpha_k$. Notice that α_0 and α_r both lie in $\Sigma_{U_{P_r}}$ and have the same length. But since $c_r(\alpha_0) = 2 \neq 1 = c_r(\alpha_r)$, it follows that α_0 does not lie in the W_{0,M_r}-orbit of α_r.

(C_n). Inside $V = \mathbb{R}^n$ the root system of type C_n is

$$\Sigma = \{\pm 2e_i \,|\, 1 \leq i \leq n\} \cup \{\pm e_i \pm e_j \,|\, 1 \leq i < j \leq n\}.$$

A basis is given by $\alpha_i = e_i - e_{i+1}$, for $1 \leq i < n$, and $\alpha_n = 2e_n$. The positive roots are

$$\begin{cases} e_i - e_j = \sum_{k=i}^{j-1} \alpha_k, & \text{for } 1 \leq i < j \leq n; \\ e_i + e_j = \sum_{k=i}^{j-1} \alpha_k + 2\sum_{k=j}^{n-1} \alpha_k + \alpha_n, & \text{for } 1 \leq i < j \leq n; \\ 2e_i = 2\sum_{k=i}^{n-1} \alpha_k + \alpha_n, & \text{for } 1 \leq i \leq n. \end{cases}$$

The Weyl group W_0 identifies with $(\mathbb{Z}/2\mathbb{Z})^n \rtimes \mathfrak{S}_n$ as for type B_n. Consider three cases:

- Assume $r=1$. Then
$$\Sigma_{U_{P_1}} = \{2e_1\} \cup \{e_1 \pm e_i \mid 2 \leq i \leq n\}.$$
Given $e_1+\varepsilon_1 e_i, e_1+\varepsilon_2 e_j \in \Sigma_{U_{P_1}}$, with $i,j \neq 1$ and $\varepsilon_1, \varepsilon_2 \in \{\pm 1\}$, we compute
$$(e_1+\varepsilon_1 e_i, e_1+\varepsilon_2 e_j) = 1+\varepsilon_1\varepsilon_2\delta_{ij} \geq 0.$$
Since also $(2e_1, e_1 \pm e_i) = 2 \geq 0$ (for $i \neq 1$), the root α_1 is non-obtuse. The Weyl group W_{0,M_1} identifies with $(\mathbb{Z}/2\mathbb{Z})^{n-1} \rtimes \mathfrak{S}_{n-1}$ with both groups acting on $\{\pm e_2, \ldots, \pm e_n\}$ leaving e_1 fixed. It clearly acts transitively on $\{e_1 \pm e_i \mid 2 \leq i \leq n\}$ (and on $\{2e_1\}$).
- Assume $r=n$. Then
$$\Sigma_{U_{P_n}} = \{2e_i \mid 1 \leq i \leq n\} \cup \{e_i+e_j \mid 1 \leq i < j \leq n\}.$$
It is obvious that α_n is non-obtuse. The Weyl group W_{0,M_n} identifies with $\mathfrak{S}_n$ acting on $e_1, \ldots, e_n$. It clearly acts transitively on $\{2e_1, \ldots, 2e_n\}$ and on $\{e_i+e_j \mid 1 \leq i < j \leq n\}$.
- Assume $1 < r < n$; in particular, $n \geq 3$. Note that both $\alpha_r = e_r - e_{r+1}$ and $e_{r-1}+e_{r+1}$ lie in $\Sigma_{U_{P_r}}$ and satisfy $(e_r - e_{r+1}, e_{r-1}+e_{r+1}) = -1$. Hence, α_r is not non-obtuse. Consider the root $\alpha_0^r = e_1+e_2 = \alpha_1 + 2\sum_{k=2}^{n-1}\alpha_k + \alpha_n$. Then α_0^r and α_r both lie in $\Sigma_{U_{P_r}}$ and have the same length. But since $c_r(\alpha_0^r) = 2 \neq 1 = c_r(\alpha_r)$, it follows that α_0^r does not lie in the W_{0,M_r}-orbit of α_r.

(D_n). Inside $V=\mathbb{R}^n$ the root system of type D_n is
$$\Sigma = \{\pm e_i \pm e_j \mid 1 \leq i < j \leq n\}.$$
A basis is given by $\alpha_i = e_i - e_{i+1}$, for $1 \leq i < n$, and $\alpha_n = e_{n-1}+e_n$. The positive roots are
$$\begin{cases} e_i - e_j = \sum_{k=i}^{j-1}\alpha_k, & \text{for } 1 \leq i < j \leq n; \\ e_i + e_n = \sum_{k=i}^{n-2}\alpha_k + \alpha_n, & \text{for } 1 \leq i < n; \\ e_i + e_j = \sum_{k=i}^{j-1}\alpha_k + 2\sum_{k=j}^{n-2}\alpha_k + \alpha_{n-1} + \alpha_n, & \text{for } 1 \leq i < j < n. \end{cases}$$
The Weyl group W_0 identifies with $\Gamma \rtimes \mathfrak{S}_n$, where Γ is the kernel of the map $(\mathbb{Z}/2\mathbb{Z})^n \to \mathbb{Z}/2\mathbb{Z}$, $(x_i)_i \mapsto \sum_{i=1}^n x_i$. We distinguish the following cases:

- Assume $r=1$. Then
$$\Sigma_{U_{P_1}} = \{e_1 \pm e_i \mid 2 \leq i \leq n\}.$$
The same computation as in (B_n) shows that α_1 is non-obtuse. The Weyl group W_{0,M_1} identifies with $\Gamma_1 \rtimes \mathfrak{S}_{n-1}$, where $\mathfrak{S}_{n-1}$ permutes $e_2, \ldots, e_n$ and $\Gamma_1 \subseteq \Gamma$ is the subgroup of elements $(x_i)_i$ with $x_1 = 0$. It is easy to check that W_{0,M_1} acts transitively on $\Sigma_{U_{P_1}}$.

- Assume $r = n-1$ or $r = n$. By the symmetry of the Dynkin diagram it suffices to consider the case $r = n$. Then
$$\Sigma_{U_{P_n}} = \{e_i + e_j \mid 1 \le i < j \le n\}.$$
It is obvious that α_n is non-obtuse. The Weyl group W_{0,M_n} identifies with $\mathfrak{S}_n$ which acts by permuting the $e_1, \dots, e_n$. It clearly acts transitively on $\Sigma_{U_{P_n}}$.
- Assume $1 < r < n-1$. Both $\alpha_r = e_r - e_{r+1}$ and $e_{r-1} + e_{r+1}$ lie in $\Sigma_{U_{P_r}}$ and satisfy $(e_r - e_{r+1}, e_{r-1} + e_{r+1}) = -1$. Hence, α_r is not non-obtuse. The highest root is $\alpha_0 = e_1 + e_2 = \alpha_1 + 2\sum_{k=2}^{n-2} \alpha_k + \alpha_{n-1} + \alpha_n$. Then α_0 and α_r both lie in $\Sigma_{U_{P_r}}$ and have the same length. But since $c_r(\alpha_0) = 2 \ne 1 = c_r(\alpha_r)$, it follows that α_0 does not lie in the W_{0,M_r}-orbit of α_r.

(E_6). Inside $V = \big\{(x_1, \dots, x_8) \in \mathbb{R}^8 \,\big|\, x_6 = x_7 = -x_8\big\}$ the root system of type E_6 is

$$\begin{aligned}\Sigma &= \{\pm e_i \pm e_j \mid 1 \le i < j \le 5\} \\ &\cup \left\{ \pm\frac{1}{2}\left(e_8 - e_7 - e_6 + \sum_{i=1}^{5} (-1)^{\nu(i)} e_i\right) \,\middle|\, \nu(i) \in \mathbb{Z}/2\mathbb{Z},\ \sum_{i=1}^{5} \nu(i) = 0 \right\}.\end{aligned}$$

A basis is given by $\alpha_1 = \frac{1}{2}(e_1 + e_8) - \frac{1}{2}(e_2 + e_3 + \dots + e_7)$, $\alpha_2 = e_2 + e_1$, and $\alpha_i = e_{i-1} - e_{i-2}$, for $3 \le i \le 6$. We distinguish the following cases:

- Assume $r = 1$ or $r = 6$. By the symmetry of the Dynkin diagram for E_6 it suffices to consider the case $r = 1$. We have
$$\Sigma_{U_{P_1}} = \left\{ \frac{1}{2}\left(e_8 - e_7 - e_6 + \sum_{i=1}^{5} (-1)^{\nu(i)} e_i\right) \,\middle|\, \nu(i) \in \mathbb{Z}/2\mathbb{Z},\ \sum_{i=1}^{5} \nu(i) = 0 \right\}.$$
We write $\alpha_\nu := \frac{1}{2}(e_8 - e_7 - e_6 + \sum_{i=1}^{5} (-1)^{\nu(i)} e_i)$, for each $\nu = (\nu(i))_i \in (\mathbb{Z}/2\mathbb{Z})^5$, to ease the notation. Let $\nu, \mu \in (\mathbb{Z}/2\mathbb{Z})^5$ such that $\sum_{i=1}^{5} \nu(i) = \sum_{i=1}^{5} \mu(i) = 0$. Since $\sum_{i=1}^{5} (\nu(i) + \mu(i)) = 0$, we observe that the cardinality of the set $\{1 \le i \le 5 \mid \nu(i) \ne \mu(i)\}$ is even, hence equals 0, 2, or 4. But then $|\{1 \le i \le 5 \mid \nu(i) = \mu(i)\}|$ is either 1, 3, or 5. Thus, we compute
$$(\alpha_\nu, \alpha_\mu) = \frac{1}{4}(3 + |\{i \mid \nu(i) = \mu(i)\}| - |\{i \mid \nu(i) \ne \mu(i)\}|) \ge 0.$$
Therefore, α_1 is non-obtuse. The Weyl group W_{0,M_1} is the group $\Gamma \rtimes \mathfrak{S}_5$ of type D_5 described in (D_n); it acts on $e_1, \dots, e_5$, leaving e_6, e_7, and e_8 fixed. Given $\nu, \mu \in (\mathbb{Z}/2\mathbb{Z})^5$ with $\alpha_\nu, \alpha_\mu \in \Sigma_{U_{P_1}}$, we may view $\mu - \nu$ as an element of Γ which maps α_ν to α_μ. Therefore, W_{0,M_1} acts transitively on $\Sigma_{U_{P_1}}$.

- Assume $1 < r < 6$. The roots $\beta_1 = \sum_{k=1}^5 \alpha_k = \frac{1}{2}(e_8 - e_7 - e_6 + e_1 + e_2 - e_3 + e_4 - e_5)$ and $\beta_2 = \alpha_2 + \alpha_3 + 2\alpha_4 + \alpha_5 + \alpha_6 = e_5 + e_3$ both lie in $\Sigma_{U_{P_r}}$ and satisfy $(\beta_1, \beta_2) = -1$. Hence, α_r is not non-obtuse. Notice that $\beta_1 = w_r(\alpha_r)$, where $w_r \in W_{0,M_r}$ is given by

$$\begin{aligned} w_2 &= s_5 s_1 s_3 s_4, \\ w_3 &= s_5 s_1 s_2 s_4, \\ w_4 &= s_5 s_1 s_3 s_2, \\ w_5 &= s_1 s_2 s_3 s_4. \end{aligned}$$

Clearly, $w_r^{-1}(\beta_2) \in \Sigma_{U_{P_r}}$ and $(\alpha_r, w_r^{-1}(\beta_2)) = (\beta_1, \beta_2) = -1$.

The highest root is $\alpha_0 = \frac{1}{2}(e_8 - e_7 - e_6 + e_1 + e_2 + e_3 + e_4 + e_5) = \alpha_1 + 2\alpha_2 + 2\alpha_3 + 3\alpha_4 + 2\alpha_5 + \alpha_6$. Then α_0 and α_r both lie in $\Sigma_{U_{P_r}}$ and have the same length. But since $c_r(\alpha_0) > 1 = c_r(\alpha_r)$, it follows that α_0 does not lie in the W_{0,M_r}-orbit of α_r.

(E_7). Inside $V = \{(x_1, \dots, x_8) \in \mathbb{R}^8 \,|\, x_7 = -x_8\}$ the root system of type E_7 is

$$\begin{aligned} \Sigma = &\{\pm e_i \pm e_j \,|\, 1 \le i < j \le 6\} \cup \{\pm(e_8 - e_7)\} \\ &\cup \left\{ \pm\frac{1}{2}\left(e_8 - e_7 + \sum_{i=1}^{6} (-1)^{\nu(i)} e_i \right) \,\middle|\, \nu(i) \in \mathbb{Z}/2\mathbb{Z},\ \sum_{i=1}^{6} \nu(i) \neq 0 \right\}. \end{aligned}$$

A basis is given by $\alpha_1 = \frac{1}{2}(e_1 + e_8) - \frac{1}{2}(e_2 + e_3 + \cdots + e_7)$, $\alpha_2 = e_2 + e_1$, and $\alpha_i = e_{i-1} - e_{i-2}$, for $3 \le i \le 7$. We distinguish the following cases:

- Assume $r = 7$. Then

$$\begin{aligned} \Sigma_{U_{P_7}} = &\{e_6 \pm e_i \,|\, 1 \le i \le 5\} \cup \{e_8 - e_7\} \\ &\cup \left\{ \frac{1}{2}\left(e_8 - e_7 + e_6 + \sum_{i=1}^{5} (-1)^{\nu(i)} e_i \right) \,\middle|\, \nu(i) \in \mathbb{Z}/2\mathbb{Z},\ \sum_{i=1}^{5} \nu(i) \neq 0 \right\}. \end{aligned}$$

(These are all the positive roots not lying in the subroot system of type E_6.) To ease the notation we write $\alpha_\nu := \frac{1}{2}(e_8 - e_7 + \sum_{i=1}^6 (-1)^{\nu(i)} e_i)$, for each $\nu = (\nu(i))_i \in (\mathbb{Z}/2\mathbb{Z})^6$. For all $1 \le i, j \le 5$ and $\nu \in (\mathbb{Z}/2\mathbb{Z})^6$ with $\alpha_\nu \in \Sigma_{U_{P_7}}$ we compute

$$\begin{aligned} (e_6 \pm e_i, e_6 \pm e_j) &= 1 \pm \delta_{ij} \ge 0, \\ (e_6 \pm e_i, e_8 - e_7) &= 0, \\ (e_6 \pm e_i, \alpha_\nu) &= \frac{1}{2}(1 \pm (-1)^{\nu(i)}) \ge 0, \\ (e_8 - e_7, \alpha_\nu) &= 1. \end{aligned}$$

Let now $\nu, \mu \in (\mathbb{Z}/2\mathbb{Z})^6$ with $\nu(6) = \mu(6) = 0$ and $\sum_{i=1}^5 \nu(i) = \sum_{i=1}^5 \mu(i) \neq 0$. As $\sum_{i=1}^5 (\nu(i) + \mu(i)) = 0$, we observe that the cardinality of the set $\{1 \leq i \leq 6 \,|\, \nu(i) \neq \mu(i)\}$ is even, but not 6, hence equals 0, 2, or 4. But then $|\{1 \leq i \leq 6 \,|\, \nu(i) = \mu(i)\}|$ is either 2, 4, or 6. Thus, we compute

$$(\alpha_\nu, \alpha_\mu) = \frac{1}{4}(2 + |\{i \,|\, \nu(i) = \mu(i)\}| - |\{i \,|\, \nu(i) \neq \mu(i)\}|) \geq 0.$$

Therefore, α_7 is non-obtuse. The Weyl group W_{0,M_7} is the group generated by s_1 and the group $\Gamma \rtimes \mathfrak{S}_5$ of type D_5 (acting on $\{\pm e_1, \dots, \pm e_5\}$ while leaving e_6, e_7, and e_8 fixed). Given $\nu, \mu \in \Sigma_{U_{P_7}}$, we may view $\mu - \nu$ as an element of Γ (by forgetting the last entry) which maps α_ν to α_μ. Moreover, $\Gamma \rtimes \mathfrak{S}_5$ clearly acts transitively on $\{e_6 \pm e_i \,|\, 1 \leq i \leq 5\}$. Together with

$$s_1(e_6 - e_1) = e_6 - e_1 + \alpha_{(0,1,1,1,1,1)} = \alpha_{(1,1,1,1,1,0)},$$

$$\text{and} \quad s_1(\alpha_{(1,0,0,0,0,0)}) = \alpha_{(1,0,0,0,0,0)} + \alpha_{(0,1,1,1,1,1)} = e_8 - e_7,$$

and the fact that Γ acts transitively on the set of those α_ν with $\sum_{i=1}^5 \nu(i) \neq 0$ and $\nu(6) = 0$, it follows that $\Sigma_{U_{P_7}}$ is the W_{0,M_7}-orbit of α_7. Hence, W_{0,M_7} acts transitively on $\Sigma_{U_{P_7}}$.

- Assume $1 \leq r < 7$. The roots $\beta_1 = \sum_{k=1}^6 \alpha_k = \alpha_{(0,0,1,1,0,1)}$ and $\beta_2 = \alpha_1 + \alpha_2 + 2\alpha_3 + 3\alpha_4 + 2\alpha_5 + \alpha_6 + \alpha_7 = \alpha_{(1,1,0,0,1,0)}$ both lie in $\Sigma_{U_{P_r}}$ and satisfy $(\beta_1, \beta_2) = -1$. Hence, α_r is not non-obtuse. Note that $\beta_1 = w_r(\alpha_r)$, where $w_r \in W_{0,M_r}$ is given by

$$w_1 = s_6 s_5 s_2 s_4 s_3, \qquad w_2 = s_6 s_5 s_1 s_3 s_4, \qquad w_3 = s_6 s_5 s_2 s_4 s_1,$$
$$w_4 = s_6 s_5 s_1 s_3 s_2, \qquad w_5 = s_6 s_1 s_3 s_2 s_4, \qquad w_6 = s_1 s_2 s_3 s_4 s_5.$$

  Clearly, $w_r^{-1}(\beta_2) \in \Sigma_{U_{P_r}}$ and $(\alpha_r, w_r^{-1}(\beta_2)) = (\beta_1, \beta_2) = -1$.

  The highest root is $\alpha_0 = e_8 - e_7 = 2\alpha_1 + 2\alpha_2 + 3\alpha_3 + 4\alpha_4 + 3\alpha_5 + 2\alpha_6 + \alpha_7$. Then α_0 and α_r both lie in $\Sigma_{U_{P_r}}$ and have the same length. But since $c_r(\alpha_0) > 1 = c_r(\alpha_r)$, it follows that α_0 does not lie in the W_{0,M_r}-orbit of α_r.

(E_8). Inside $V = \mathbb{R}^8$ the root system of type E_8 is

$$\Sigma = \{\pm e_i \pm e_j \,|\, 1 \leq i < j \leq 8\} \cup \left\{ \pm\frac{1}{2}\Big(e_8 + \sum_{i=1}^7 (-1)^{\nu(i)} e_i\Big) \,\middle|\, \nu(i) \in \mathbb{Z}/2\mathbb{Z},\ \sum_{i=1}^7 \nu(i) = 0 \right\}.$$

A basis is given by $\alpha_1 = \frac{1}{2}(e_1 + e_8) - \frac{1}{2}(e_2 + e_3 + \cdots + e_7)$, $\alpha_2 = e_2 + e_1$, and $\alpha_i = e_{i-1} - e_{i-2}$, for $3 \leq i \leq 8$.

Let $1 \leq r \leq 8$. The roots $\beta_1 = \sum_{k=1}^8 \alpha_k = \frac{1}{2}(e_8 + e_7 - e_6 + e_1 + e_2 - e_3 - e_4 - e_5)$ and $\beta_2 = \alpha_1 + 2\alpha_2 + 3\alpha_3 + 5\alpha_4 + 4\alpha_5 + 3\alpha_6 + 2\alpha_7 + \alpha_8 =$

$\frac{1}{2}(e_8+e_7+e_6-e_1-e_2+e_3+e_4+e_5)$ both lie in $\Sigma_{U_{P_r}}$ and satisfy $(\beta_1,\beta_2)=-1$. Hence, α_r is not non-obtuse. Note that $\beta_1=w_r(\alpha_r)$, where $w_r\in W_{0,M_r}$ is given by

$$\begin{aligned} w_1 &= s_8s_7s_6s_5s_2s_4s_3, & w_2 &= s_8s_7s_6s_5s_1s_3s_4,\\ w_3 &= s_8s_7s_6s_5s_2s_4s_1, & w_4 &= s_8s_7s_6s_5s_1s_3s_2,\\ w_5 &= s_8s_7s_6s_2s_1s_3s_4, & w_6 &= s_8s_7s_2s_1s_3s_4s_5,\\ w_7 &= s_8s_2s_1s_3s_4s_5s_6, & w_8 &= s_2s_1s_3s_4s_5s_6s_7. \end{aligned}$$

Clearly, $w_r^{-1}(\beta_2)\in\Sigma_{U_{P_r}}$ and $(\alpha_r,w_r^{-1}(\beta_2))=(\beta_1,\beta_2)=-1$.

The highest root is $\alpha_0=e_8+e_7=2\alpha_1+3\alpha_2+4\alpha_3+6\alpha_4+5\alpha_5+4\alpha_6+3\alpha_7+2\alpha_8$. Then α_r and α_0 both lie in $\Sigma_{U_{P_r}}$ and have the same length. But since $c_r(\alpha_0)>1=c_r(\alpha_r)$, it follows that α_0 does not lie in the W_{0,M_r}-orbit of α_r.

(F_4). Inside $V=\mathbb{R}^4$ the root system of type F_4 is

$$\Sigma=\{\pm e_i\,|\,1\le i\le 4\}\cup\{\pm e_i\pm e_j\,|\,1\le i<j\le 4\}\cup\{\tfrac{1}{2}(\pm e_1\pm e_2\pm e_3\pm e_4)\}.$$

A basis is given by $\alpha_1=e_2-e_3$, $\alpha_2=e_3-e_4$, $\alpha_3=e_4$, and $\alpha_4=\frac{1}{2}(e_1-e_2-e_3-e_4)$. We have

$$\begin{aligned} (\alpha_1,\alpha_1+3\alpha_2+4\alpha_3+2\alpha_4) &= (e_2-e_3,e_1+e_3)=-1,\\ (\alpha_2,\alpha_1+\alpha_2+2\alpha_3+2\alpha_4) &= (e_3-e_4,e_1-e_3)=-1,\\ (\alpha_3,\alpha_1+2\alpha_2+2\alpha_3+2\alpha_4) &= (e_4,e_1-e_4)=-1,\\ (\alpha_4,\alpha_1+2\alpha_2+3\alpha_3+\alpha_4) &= \frac{1}{4}\cdot(e_1-e_2-e_3-e_4,e_1+e_2+e_3+e_4)\\ &= -\frac{1}{2}. \end{aligned}$$

Hence, none of the $\alpha_1,\dots,\alpha_4$ is non-obtuse. Consider the following cases:

- Assume $r=1$ or $r=2$. The highest root is $\alpha_0=e_1+e_2=2\alpha_1+3\alpha_2+4\alpha_3+2\alpha_4$. Then both α_0 and α_r lie in $\Sigma_{U_{P_r}}$ and have the same length. But since $c_r(\alpha_0)>1=c_r(\alpha_r)$, it follows that α_0 does not lie in the W_{0,M_r}-orbit of α_r.
- Assume $r=3$ or $r=4$. The highest short root is $\alpha_0^r=e_1=\alpha_1+2\alpha_2+3\alpha_3+2\alpha_4$. Then α_0^r and α_r both lie in $\Sigma_{U_{P_r}}$ and have the same length. But since $c_r(\alpha_0^r)>1=c_r(\alpha_r)$, it follows that α_0^r does not lie in the W_{0,M_r}-orbit of α_r.

(G_2). Inside $V=\{(x,y,z)\in\mathbb{R}^3\,|\,x+y+z=0\}$ the root system of type G_2 is

$$\Sigma=\pm\{e_1-e_2,e_2-e_3,e_1-e_3,2e_1-e_2-e_3,2e_2-e_1-e_3,2e_3-e_1-e_2\}.$$

A basis is given by $\alpha_1 = e_1 - e_2$ and $\alpha_2 = -2e_1 + e_2 + e_3$. Since

$$\begin{aligned} &(\alpha_1, \alpha_1 + \alpha_2) = (e_1 - e_2, e_3 - e_1) = -1 \\ \text{and} \quad &(\alpha_2, 3\alpha_1 + \alpha_2) = (-2e_1 + e_2 + e_3, e_1 - 2e_2 + e_3) = -3, \end{aligned}$$

neither α_1 nor α_2 are non-obtuse.

The highest root is $\alpha_0 = 3\alpha_1 + 2\alpha_2 = -e_1 - e_2 + 2e_3$. Then both α_0 and α_2 lie in $\Sigma_{U_{P_2}}$ and have the same length. But since $c_2(\alpha_0) = 2 \neq 1 = c_2(\alpha_2)$, it follows that α_0 does not lie in the W_{0,M_2}-orbit of α_2.

Similarly, the highest short root is $\alpha_0^1 = 2\alpha_1 + \alpha_2 = e_3 - e_2$, and both α_0^1 and α_1 lie in $\Sigma_{U_{P_1}}$ and have the same length. But since $c_1(\beta) = 2 \neq 1 = c_1(\alpha_1)$, it follows that α_0^1 does not lie in the W_{0,M_1}-orbit of α_1. □

We end this section by applying the previous analysis to prove a result on the ordering of positive roots that will become useful later. First, we need a preliminary lemma which also appeared in [22, Lem. (2.1.1)]. For the convenience of the reader we supply the simple proof.

We make the following convention: If Δ' is a basis of Σ, we denote by $\Sigma^+_{\Delta'}$ (resp. $\Sigma^-_{\Delta'}$) the system of positive (resp. negative) roots with respect to Δ'.

Recall, [4, Ch. VI, §1.6, Cor. 3 of Prop. 17], that there exists a unique longest element $w_0 \in W_0$. It satisfies $w_0^2 = 1$ and $\ell(ww_0) = \ell(w_0) - \ell(w)$, for all $w \in W_0$.

Lemma 3.6. *Let $w_0 = s_{i_1} \cdots s_{i_r}$ be a reduced decomposition and put $\beta_j := s_{i_1} \cdots s_{i_{j-1}}(\alpha_{i_j})$, for $j = 1, \ldots, r$. Then one has, for all $0 \leq j \leq r$,*

$$\Sigma^+_{s_{i_1} \cdots s_{i_j}(\Delta)} = \{\beta_{j+1}, \beta_{j+2}, \ldots, \beta_r, -\beta_1, -\beta_2, \ldots, -\beta_j\}.$$

Proof. Write $w_j = s_{i_1} \cdots s_{i_j}$. Applying [4, Ch. VI, §1.6, Cor. 2 of Prop. 17] to $w_j^{-1} = s_{i_j} \cdots s_{i_1}$ yields

$$\Sigma^+_\Delta \cap \Sigma^-_{w_j(\Delta)} = \Sigma^+_\Delta \cap w_j \Sigma^-_\Delta = \{\beta_1, \beta_2, \ldots, \beta_j\}.$$

Note that $\Sigma^+_\Delta = \Sigma^+_\Delta \cap \Sigma^-_{w_0(\Delta)} = \{\beta_1, \beta_2, \ldots, \beta_r\}$. Hence, the assertion follows from

$$\begin{aligned} \Sigma^+_{w_j(\Delta)} &= (\Sigma^-_\Delta \cap \Sigma^+_{w_j(\Delta)}) \sqcup (\Sigma^+_\Delta \cap \Sigma^+_{w_j(\Delta)}) \\ &= -(\Sigma^+_\Delta \cap \Sigma^-_{w_j(\Delta)}) \sqcup (\Sigma^+_\Delta \smallsetminus \Sigma^-_{w_j(\Delta)}). \end{aligned}$$ □

Example 3.7. It is instructive to visualize an example. The orderings of the positive roots in Σ^+ obtained in Lemma 3.6 generalize the "circular orderings" one has for root systems of rank 2. Assume Σ is of type G_2 with basis $\{\alpha_1, \alpha_2\}$ such that α_2 is the long root. The ordering of Σ^+ corresponding to the reduced decomposition $w_0 = s_1 s_2 s_1 s_2 s_1 s_2$ is shown in Figure 3.3.

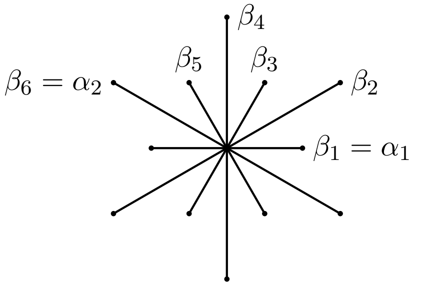


Figure 3.3. The circular ordering in type G_2

Corollary 3.8. *Let $\alpha_i \in \Delta = \{\alpha_1, \dots, \alpha_n\}$ be a non-obtuse simple root, and let $\alpha \in \Sigma_{U_{P_i}}$ such that α and α_i have the same length. There exists a reduced decomposition $w_0 = s_{i_1} \cdots s_{i_r}$ such that, if we put $\beta_j := s_{i_1} \cdots s_{i_{j-1}}(\alpha_{i_j})$, there exists $0 \le l < r$ with $\beta_1, \dots, \beta_l \in \Sigma_{M_i}$ and $\beta_{l+1} = \alpha$. In particular,*

$$\Sigma_{U_{P_i}} \smallsetminus \{\alpha\} \subseteq \Sigma^+_{s_{i_1} \cdots s_{i_{l+1}}(\Delta)} = \{\beta_{l+2}, \dots, \beta_r, -\beta_1, \dots, -\beta_l, -\alpha\}.$$

Remark 3.9. Corollary 3.8 says geometrically that, for non-obtuse α_i, the roots of length $\|\alpha_i\|$ are extremal in the cone generated by $\Sigma_{U_{P_i}}$.

The statement of Corollary 3.8 is generally false if α_i is not non-obtuse, see Figure 3.3.

Proof of Corollary 3.8. Denote w_{0,M_i} the longest element in W_{0,M_i}. Since α_i is non-obtuse, we find by Proposition 3.5 (iii) an element $w \in W_{0,M_i}$ with $w(\alpha_i) = \alpha$. Choose reduced decompositions

$$w = s_{i_1} \cdots s_{i_l} \qquad \text{and} \qquad w_{0,M_i} w_0 = s_{i_{l+1}} \cdots s_{i_{r'}}.$$

For each $v \in W_{0,M_i}$ we compute

$$\begin{aligned} \ell(v w_{0,M_i} w_0) &= \ell(w_0) - \ell(v w_{0,M_i}) \\ &= \ell(w_0) - \ell(w_{0,M_i}) + \ell(v) = \ell(v) + \ell(w_{0,M_i} w_0). \end{aligned} \tag{3.5}$$

In particular, $w w_{0,M_i} w_0 = s_{i_1} \cdots s_{i_{r'}}$ is a reduced decomposition. We further observe $s_{i_{l+1}} = s_i$, for otherwise we would have $s_{i_{l+1}} \in W_{0,M_i}$ and $\ell(s_{i_{l+1}} w_{0,M_i} w_0) < \ell(w_{0,M_i} w_0)$, contradicting (3.5) for $v = s_{i_{l+1}}$. Now, if we pick a reduced decomposition $(w w_{0,M_i} w_0)^{-1} w_0 = s_{i_{r'+1}} \cdots s_{i_r}$, then it is clear that we obtain a reduced decomposition $w_0 = s_{i_1} \cdots s_{i_r}$. From the construction it is clear that $\beta_1, \dots, \beta_l \in \Sigma_{M_i}$ and $\beta_{l+1} = \alpha$. The last statement is a consequence of Lemma 3.6. $\square$

4. The algorithm

Recall the special parahoric subgroup K of G associated with φ. Given $z \in Z^-$ and $z' \in Z$, it is of general interest to understand the intersection of the Iwasawa double coset $Uz'K$ and the Cartan double coset KzK. For example, it is well-known that $\nu(z') \leq \nu(z)$ provided $Uz'K \cap KzK \neq \varnothing$, see Section 2.6.

There is, however, very little known about the $u \in U$ such that $uz' \in KzK$. One of the main goals of this article is to study the following question: If $uz' \in KzK$ and if we write $u = u_{\gamma_1} \cdots u_{\gamma_r}$, with $u_{\gamma_i} \in U_{\gamma_i}$, what can be said about the valuations $\varphi_{\gamma_i}(u_{\gamma_i})$? We will prove that for each strictly positive element $a \in Z$ with $\nu(z) \leq \nu(a^{-1})$, the valuation $\varphi_{\gamma_i}(u_{\gamma_i})$ is bounded below by $\langle \gamma_i, \nu(a) \rangle$, see Theorem 4.4.

In this section we present an algorithm that gives information about the $\varphi_{\gamma_i}(u_{\gamma_i})$. First, we need to set up some notation. We fix a reduced decomposition $w_0 = s_{i_1} \cdots s_{i_r}$ of the longest element w_0 of W_0.

Notation 4.1. Recall the reduced root system Σ associated with Φ. Let $\Delta = \{\alpha_1, \ldots, \alpha_n\}$ be the fixed basis of Σ.

(a) Put $\beta_j := s_{i_1} \cdots s_{i_{j-1}}(\alpha_{i_j})$ and $\Delta^{(j)} = s_{i_1} \cdots s_{i_j}(\Delta)$, for $1 \leq j \leq r$. Thanks to Lemma 3.6 we have

$$\Sigma^{(j)} := \Sigma^+_{\Delta^{(j)}} = \{\beta_{j+1}, \beta_{j+2}, \ldots, \beta_r, -\beta_1, -\beta_2, \ldots, -\beta_j\}, \quad \text{for } 0 \leq j \leq r.$$

Given $k \geq 0$, we let $j(k) \in \{1, \ldots, r\}$ be the unique integer with $k \equiv j(k) \pmod r$. Let

$$\varepsilon_k := \begin{cases} 1, & \text{if } k \equiv j(k) \pmod{2r}, \\ -1, & \text{otherwise.} \end{cases}$$

Put $\beta_k := \varepsilon_k \beta_{j(k)}$ and $\Delta^{(k)} := \varepsilon_k \Delta^{(j(k))}$, and then

$$\Sigma^{(k)} := \varepsilon_k \Sigma^{(j(k))} = \Sigma^+_{\Delta^{(k)}} = \{\beta_{k+1}, \beta_{k+2}, \ldots, \beta_{k+r}\}.$$

Then $\Sigma^{(0)} = \Sigma$ and the sequence $(\Sigma^{(k)})_{k \in \mathbb{Z}_{\geq 0}}$ is $2r$-periodic. See also Figure 4.1 below.

(b) Let $\alpha \in \Sigma$ and write $\alpha = \epsilon_\beta \beta$ for the unique $\beta \in \Phi_{\mathrm{red}}$. Define

$$\varphi_\alpha := \epsilon_\beta \varphi_\beta \colon U^*_\alpha \to \mathbb{Z}.$$

(c) For each $\alpha \in \Sigma$ we fix a lift $n_\alpha \in N \cap K$ of $s_\alpha \in W_0$.

(d) Given a basis Δ' of Σ, we denote by $U_{\Delta'}$ the group generated by $\bigcup_{\alpha \in \Sigma^+_{\Delta'}} U_\alpha$.

Recall from Section 2.4 that $K \cap U_\alpha = U_{(\alpha,0)}$, for all $\alpha \in \Sigma$.

Algorithm 4.2. Let $z, z' \in Z$ and $u \in U$ such that $uz' \in KzK$. We define sequences $(u^{(k)})_{k \geq 0}$ and $(z^{(k)})_{k \geq 0}$ with the following properties:

- $u^{(0)} = u$ and $z^{(0)} = z'$;
- $u^{(k)} \in U_{\Delta^{(k)}} \cap U_{\Delta^{(k-1)}}$ and $z^{(k)} \in Z$, for all $k \geq 1$;
- $u^{(k)} z^{(k)} \in KzK$, for all $k \geq 0$.

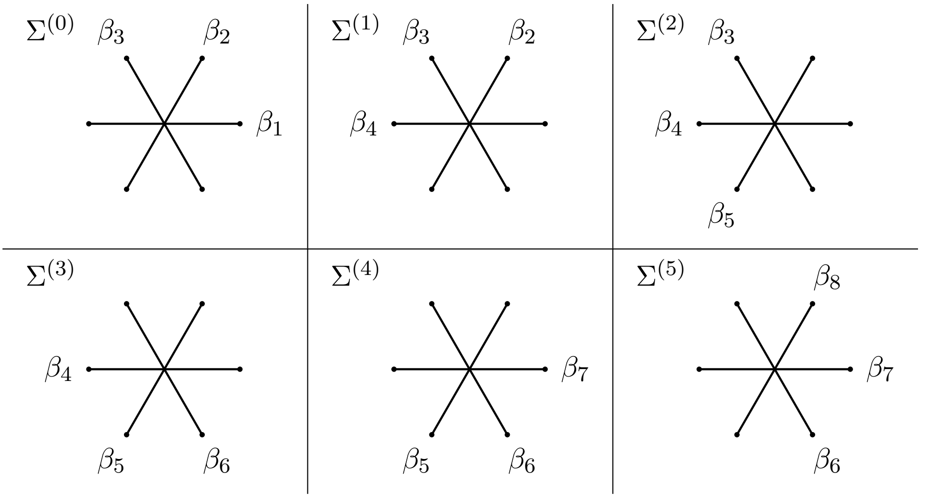


Figure 4.1. A visual aid for the sets $\Sigma^{(k)}$ relative to the reduced decomposition $w_0 = s_1 s_2 s_1$, where $\alpha_1 = \beta_1$ and $\alpha_2 = \beta_3$.

Suppose we have constructed $u^{(k)}$ and $z^{(k)}$ for some $k \geq 0$. Write

$$u^{(k)} = u^{(k)}_{\beta_{k+r}} \cdot u^{(k)}_{\beta_{k+r-1}} \cdots u^{(k)}_{\beta_{k+1}} \in \begin{cases} U_\Delta, & \text{if } k = 0,\\ U_{\Delta^{(k)}} \cap U_{\Delta^{(k-1)}}, & \text{if } k \geq 1,\end{cases}$$

for uniquely determined $u^{(k)}_{\beta_i} \in U_{\beta_i}$.[1] Depending on $\varphi_{\beta_{k+1}}(u^{(k)}_{\beta_{k+1}})$ we distinguish three cases:

(**Alg-1**)*: Case* $\varphi_{\beta_{k+1}}(u^{(k)}_{\beta_{k+1}}) + \langle \beta_{k+1}, \nu(z^{(k)})\rangle \geq 0$. By (2.2) this is equivalent to

$$x := \big(z^{(k)}\big)^{-1} \cdot u^{(k)}_{\beta_{k+1}} \cdot z^{(k)} \in U_{(\beta_{k+1},0)} = U_{\beta_{k+1}} \cap K.$$

We then define

$$z^{(k+1)} := z^{(k)},$$
$$u^{(k+1)} := u^{(k)} \cdot \big(u^{(k)}_{\beta_{k+1}}\big)^{-1} \in U_{\Delta^{(k+1)}} \cap U_{\Delta^{(k)}}.$$

Then $u^{(k+1)} z^{(k+1)} = u^{(k)} z^{(k)} x^{-1} \in KzK$.

(**Alg-2**)*: Case* $\varphi_{\beta_{k+1}}(u^{(k)}_{\beta_{k+1}}) \geq 0$ *and not* (**Alg-1**). Then $u^{(k)}_{\beta_{k+1}} \in K$ and we define

$$z^{(k+1)} := z^{(k)},$$
$$u^{(k+1)} := \big(u^{(k)}_{\beta_{k+1}}\big)^{-1} \cdot u^{(k)} \in U_{\Delta^{(k+1)}} \cap U_{\Delta^{(k)}}.$$

[1] Note that $u^{(k)}_{\beta_{k+r}} = 1$ unless $k = 0$.

The fact that $u^{(k+1)} \in U_{\Delta^{(k+1)}}$ follows from (DR2) and $\Sigma^{(k)} \smallsetminus \{\beta_{k+1}\} = \Sigma^{(k+1)} \cap \Sigma^{(k)}$.

(**Alg-3**)*: Case* $f_k := \varphi_{\beta_{k+1}}(u^{(k)}_{\beta_{k+1}}) < \min\{0, -\langle \beta_{k+1}, \nu(z^{(k)})\rangle\}$. Note that $u^{(k)}_{\beta_{k+1}} \neq 1$. By Lemma 2.1 there exist unique $u', u'' \in U_{-\beta_{k+1}}$ such that

$$m^{(k)} := u' u^{(k)}_{\beta_{k+1}} u'' \in N.$$

By [5, Prop. (6.2.10)(ii)] the element $m^{(k)}$ acts on $\mathscr{A}$ as the orthogonal reflection s_{β_{k+1},f_k} in the hyperplane H_{β_{k+1},f_k}. Observe that the element

$$z^{(k+1)} := m^{(k)} z^{(k)} n_{\beta_{k+1}}$$

lies in Z, because its image in $W_0 = N/Z$ is trivial. Considering how $z^{(k+1)}$ acts on $\varphi \in \mathscr{A}$, we deduce

$$\nu(z^{(k+1)}) = s_{\beta_{k+1},f_k}(\nu(z^{(k)})) = \nu(z^{(k)}) - (\langle \beta_{k+1}, \nu(z^{(k)})\rangle + f_k) \cdot \beta^\vee_{k+1}. \tag{4.1}$$

Applying $\langle \beta_{k+1}, - \rangle$ to this equation, and rearranging, we obtain

$$\varphi_{\beta_{k+1}}(u^{(k)}_{\beta_{k+1}}) = f_k = -\frac{1}{2} \cdot \Big(\langle \beta_{k+1}, \nu(z^{(k)})\rangle + \langle \beta_{k+1}, \nu(z^{(k+1)})\rangle\Big). \tag{4.2}$$

By (V5) and (2.2) we have

$$\begin{aligned} &\varphi_{-\beta_{k+1}}(u') = -f_k > 0 \\ \text{and} \quad &\varphi_{-\beta_{k+1}}\big((z^{(k)})^{-1} u'' z^{(k)}\big) = -f_k - \langle \beta_{k+1}, \nu(z^{(k)})\rangle > 0. \end{aligned}$$

This entails that u' and $\big(z^{(k)}\big)^{-1} u'' z^{(k)}$ lie in K. We now define

$$u^{(k+1)} := u' \cdot u^{(k)} \cdot (u^{(k)}_{\beta_{k+1}})^{-1} \cdot (u')^{-1} \in U_{\Delta^{(k+1)}} \cap U_{\Delta^{(k)}}.$$

We remark that $u^{(k+1)}_{\beta_{k+2}} = u^{(k)}_{\beta_{k+2}}$ as can be seen from (V3) and the fact that β_{k+2} is extremal in $\Sigma^{(k+1)}$. Finally, we compute

$$\begin{aligned} u^{(k+1)} z^{(k+1)} &= u' \cdot u^{(k)} \cdot (u^{(k)}_{\beta_{k+1}})^{-1} \cdot (u')^{-1} \cdot m^{(k)} \cdot z^{(k)} \cdot n_{\beta_{k+1}} \\ &= u' \cdot u^{(k)} z^{(k)} \cdot \big(z^{(k)}\big)^{-1} u'' z^{(k)} \cdot n_{\beta_{k+1}} \in KzK. \end{aligned}$$

Note that, as a byproduct, at each step the algorithm provides a lower bound for $\varphi_{\beta_{k+1}}(u^{(k)}_{\beta_{k+1}})$. It is because of this property that Algorithm 4.2 will be useful for us later.

The next result will not be used in the sequel.

Proposition 4.3. *Algorithm 4.2 terminates, that is, there exists* $l \geq 0$ *such that* $u^{(l)} = 1$*. Moreover,* $\nu(z^{(l)})$ *lies in the* W_0*-orbit of* $\nu(z)$*.*

Proof. Let $u \in U$, $z', z \in Z$ with $uz' \in KzK$. Suppose we are in case (**Alg-3**) at the k-th step. Then $\nu(z^{(k+1)})$ is obtained by reflecting $\nu(z^{(k)})$ along the hyperplane H_{β_{k+1},f_k}. But since we have $\langle \beta_{k+1}, 0\rangle + f_k = f_k < 0$ and $\langle \beta_{k+1}, \nu(z^{(k)})\rangle + f_k < 0$, it follows that 0 and $\nu(z^{(k)})$ are on the same side of H_{β_{k+1},f_k}, whereas $\nu(z^{(k+1)})$ lies on the other. An elementary argument in Euclidean geometry now shows $\|\nu(z^{(k)})\| < \|\nu(z^{(k+1)})\|$.

As $\nu(Z)$ is a lattice in V, its intersection with the convex polytope C spanned by the W_0-orbit of $\nu(z)$ is finite. Since $u^{(k)}z^{(k)} \in KzK$, we have $\nu(z^{(k)}) \in C$, for all $k \geq 0$, see Section 2.6. As the $z^{(k)}$ remain unchanged in the cases (**Alg-1**) and (**Alg-2**), the above discussion shows that there are only finitely many instances of case (**Alg-3**).

Let $k \geq 0$ such that $\|\nu(z^{(k)})\|$ is maximal. As only the cases (**Alg-1**) and (**Alg-2**) occur, it follows that for all $j \geq 0$ we have $z^{(k+j)} = z^{(k)}$ and $u^{(k+j)} \in U_{\Delta^{(k+j)}} \cap U_{\Delta^{(k)}}$. In particular, we have $u^{(k+r)} \in U_{\Delta^{(k+r)}} \cap U_{\Delta^{(k)}} = U_{-\Delta^{(k)}} \cap U_{\Delta^{(k)}} = \{1\}$. Hence, Algorithm 4.2 terminates with $l = k + r$. Moreover, we have $Kz^{(k+r)}K = KzK$ by the construction in Algorithm 4.2 and the fact that $u^{(k+r)} = 1$, and hence the last assertion follows from the Cartan decomposition 2.3. □

We are now ready to prove our main technical result, which may be of independent interest.

Theorem 4.4. *Let* $\mathbf{P} = \mathbf{U_P M}$ *be a non-obtuse parabolic. Let* $a \in Z$ *be strictly* M*-positive. Let* $u \in U_P$, $z \in Z^-$, *and* $z' \in Z$ *such that* $\nu(z) \leq \nu(a^{-1})$ *and* $uz' \in KzK$. *Then the following assertions hold:*

(i) $az' \in M^+$;
(ii) $aua^{-1} \in K_P = K \cap P$.

Proof. Note that $uz' \in KzK$ implies $w.\nu(z') \leq \nu(z)$ for all $w \in W_0$, see Remark 2.6.c. Let λ (resp. μ) be the image of a (resp. z') in Λ. Then (i) is equivalent to

$$\langle \alpha, \nu(\lambda + \mu)\rangle \leq 0, \qquad \text{for all } \alpha \in \Sigma^+ \smallsetminus \Sigma_M \tag{4.3}$$

(cf. (2.5)). But this follows from Lemma 3.3, since by assumption λ is strictly M-positive and $\nu(w(\mu)) \leq \nu(z) \leq \nu(-\lambda)$ for all $w \in W_0$.

We now prove (ii). As $\mathbf{P}$ is maximal parabolic, the roots appearing in $\mathbf{U_P}$ are contained in a single irreducible component Φ_1 of Φ. Since all computations will be done in the subgroup of G generated by Z and U_α, for $\alpha \in \Phi_1$, we may assume for notational convenience that Φ (and hence Σ) is irreducible. As in Section 3 we write $\alpha_1, \ldots, \alpha_n$ for the simple roots in Σ and put $\Sigma_{U_P} = \Sigma^+ \smallsetminus \Sigma_M$. Let w_0 (resp. $w_{0,M}$) be the longest element in W_0 (resp. $W_{0,M}$). Denote α_0 the highest root of Σ and write $\alpha_0 = \sum_{i=1}^n c_i(\alpha_0)\alpha_i$.

Write $u = \prod_{\alpha\in\Sigma_{U_P}} u_\alpha$ for some ordering of the factors (to be specified later). Since we have $K_P \cap U_P = \prod_{\alpha\in\Sigma_{U_P}} U_{(\alpha,0)}$, and because $U_{\beta,0} \cap U_{2\beta} = U_{2\beta,0}$ whenever $\beta, 2\beta \in \Phi$ (by (V4)), it suffices to prove $\varphi_\alpha(au_\alpha a^{-1}) = \varphi_\alpha(u_\alpha) - \langle\alpha, \nu(a)\rangle \geq 0$, that is,

$$\varphi_\alpha(u_\alpha) \geq \langle\alpha, \nu(a)\rangle, \qquad \text{for all } \alpha \in \Sigma_{U_P}. \tag{4.4}$$

The general procedure is as follows: We fix an ordering o of Σ_{U_P} with respect to which we write $u = \prod_{\alpha\in\Sigma_{U_P}} u_\alpha$. For each $\alpha \in \Sigma_{U_P}$ we apply Algorithm 4.2 in order to estimate $\varphi_\alpha(u_\alpha)$. This necessitates to temporarily consider a different ordering, and we need to ensure that in the notation of Algorithm 4.2 we have $\varphi_\alpha(u_\alpha) = \varphi_\alpha(u^{(k)}_{\beta_{k+1}})$, for the minimal $k \geq 0$ for which $\beta_{k+1} = \alpha$. (In many cases we will even have $u_\alpha = u^{(k)}_{\beta_{k+1}}$.) The next step in the algorithm then provides the desired estimate for $\varphi_\alpha(u_\alpha)$. Finally, we go back to the initial ordering o and repeat this procedure with another root of Σ_{U_P}.

(a). Let $w_0 = s_{i_1}\cdots s_{i_r}$ be a reduced decomposition and apply Algorithm 4.2. At the k-th step we have

$$u^{(k)} = u^{(k)}_{\beta_{k+r}} u^{(k)}_{\beta_{k+r-1}} \cdots u^{(k)}_{\beta_{k+1}}.$$

Note that, by (i), we have $az^{(k)} \in M^+$, for all $k \geq 0$. Assume $\beta_{k+1} \in \Sigma_{U_P}$, so that $\langle\beta_{k+1}, \nu(az^{(k)})\rangle \leq 0$. In case (**Alg-1**) this implies

$$\varphi_{\beta_{k+1}}(u^{(k)}_{\beta_{k+1}}) \geq -\langle\beta_{k+1}, \nu(z^{(k)})\rangle \geq \langle\beta_{k+1}, \nu(a)\rangle.$$

In case (**Alg-2**) we estimate $\varphi_{\beta_{k+1}}(u^{(k)}_{\beta_{k+1}}) \geq 0 \geq \langle\beta_{k+1}, \nu(a)\rangle$. If, however, we are in case (**Alg-3**), then (4.2) implies

$$\varphi_{\beta_{k+1}}(u^{(k)}_{\beta_{k+1}}) = -\frac{1}{2} \cdot \Big(\langle\beta_{k+1}, \nu(z^{(k)})\rangle + \langle\beta_{k+1}, \nu(z^{(k+1)})\rangle\Big) \geq \langle\beta_{k+1}, \nu(a)\rangle.$$

Thus, whenever $\beta_{k+1} \in \Sigma_{U_P}$, we have

$$\varphi_{\beta_{k+1}}(u^{(k)}_{\beta_{k+1}}) \geq \langle\beta_{k+1}, \nu(a)\rangle. \tag{4.5}$$

(b). Let α_{i_0} be the unique simple root in Σ_{U_P}. Let $\alpha \in \Sigma_{U_P}$ with the same length as α_{i_0}. By Corollary 3.8 we find a reduced decomposition $w_0 = s_{i_1}\cdots s_{i_r}$ such that for some $0 \leq l < r$ we have $\beta_1, \dots, \beta_l \in \Sigma_M$ and $\beta_{l+1} = \alpha$. We apply Algorithm 4.2 to this reduced decomposition. Note that $u^{(0)}_{\beta_1} = \cdots = u^{(0)}_{\beta_l} = 1$. As $\alpha = \beta_{l+1}$ is a simple root in $\Sigma^+_{s_{i_1}\cdots s_{i_l}(\Delta)}$ (which contains Σ_{U_P}) it follows that α cannot be expressed as the sum of two or more roots in Σ_{U_P}. Hence, (DR2) implies $u_\alpha = u^{(0)}_{\beta_{l+1}}$. Now, case (**Alg-1**) applies for the first l steps. Consequently, we have $u^{(l)}_{\beta_{l+1}} = u_\alpha$. Hence, (4.5) shows $\varphi_\alpha(u_\alpha) \geq \langle\alpha, \nu(a)\rangle$.

This proves (4.4) in the case where α and α_{i_0} have the same length. When Σ is simply-laced, that is, of type ADE, then all roots have the same length. This proves (ii) in this case.

It remains to study the cases where Σ is of type B_n or C_n, and where $\alpha \in \Sigma_{U_P}$ and α_{i_0} have different lengths.

(c). Suppose that Σ of type B_n and that $\mathbf{P}$ corresponds to $\alpha_n = e_n$ in the notation of (B_n) in the proof of Proposition 3.5. (Note that Φ is not necessarily reduced.)

We have

$$\Sigma_{U_P} = \{e_i \,|\, 1 \leq i \leq n\} \cup \{e_i + e_j \,|\, 1 \leq i < j \leq n\}\,.$$

We choose a specific ordering of the factors as follows: Let $o\colon \Sigma_{U_P} \xrightarrow{\cong} \{1, 2, \ldots, |\Sigma_{U_P}|\}$ be a bijection such that, writing $u = \prod_{i=1}^{|\Sigma_{U_P}|} u_{o^{-1}(i)}$ with $u_{o^{-1}(i)} \in U_{o^{-1}(i)}$, we have: $\varphi_{e_i}(u_{e_i}) < \varphi_{e_j}(u_{e_j})$ implies $o(e_i) > o(e_j)$. With this choice of ordering we will prove (4.4). For each $\alpha \in \Sigma_{U_P}$ we will apply Algorithm 4.2 to estimate $\varphi_\alpha(u_\alpha)$. As the algorithm changes the ordering, we have to ensure that $\varphi_\alpha(u_\alpha) = \varphi_\alpha(u_\alpha^{(0)})$.

Note that e_i cannot be written as the sum of two or more roots in Σ_{U_P}. An application of (DR2) shows that for any ordering the e_i-component of u coincides with u_{e_i}. Therefore, the estimate for $\varphi_{e_i}(u_{e_i})$ is provided by (b).

Observe that, given $\gamma_1, \gamma_2 \in \Sigma_{U_P}$, we have $e_i + e_j = \gamma_1 + \gamma_2$ only if $\{e_i, e_j\} = \{\gamma_1, \gamma_2\}$. An application of (DR2) shows that the $(e_i + e_j)$-component of u in a reordering depends only on the relative position of u_{e_i} and u_{e_j}. In order to estimate $\varphi_{e_i+e_j}(u_{e_i+e_j})$, we thus have to ensure that the reordering needed for applying Algorithm 4.2 does not change the relative position of u_{e_i} and u_{e_j}.

Note that every reduced decomposition of $w_{0,M}w_0$ necessarily starts with $s_n s_{n-1} \cdots$. Indeed, this follows, since $s_1, \ldots, s_{n-1} \in W_{0,M}$ and $\ell(ww_{0,M}w_0) = \ell(w) + \ell(w_{0,M}w_0)$, for all $w \in W_{0,M}$, and $s_n s_i = s_i s_n$, for all $1 \leq i \leq n-2$. Fix $1 \leq i, j \leq n$ with $o(e_i) > o(e_j)$ and choose $w \in W_{0,M} \cong \mathfrak{S}_n$ such that $w(e_n) = e_i$ and $w(e_{n-1}) = e_j$. As in the proof of Corollary 3.8 we find a reduced decomposition $w_0 = s_{i_1} \cdots s_{i_r}$ such that $s_{i_1} \cdots s_{i_l}$ is a reduced decomposition of w (for some $0 \leq l \leq r-2$) and $s_{i_{l+1}} = s_n$ and $s_{i_{l+2}} = s_{n-1}$. In particular, we have $\beta_1, \ldots, \beta_l \in \Sigma_M$ and $\beta_{l+1} = e_i$. Since $s_n(e_{n-1} - e_n) = e_{n-1} + e_n$, we also deduce $\beta_{l+2} = e_i + e_j$. Note that $e_j = \beta_{l'}$ for some $l' > l + 2$.

We apply Algorithm 4.2 to this reduced decomposition and observe that, by construction, the relative position of u_{e_i}, u_{e_j} and $u_{e_i}^{(0)}$, $u_{e_j}^{(0)}$ is the same; therefore, we have $u_{e_i+e_j} = u_{e_i+e_j}^{(0)}$. Note that $u^{(l)} = u^{(0)}$ in U_P, and hence

$u^{(l)}_{\beta_{l+1}} = u^{(0)}_{e_i} = u_{e_i}$ and $u^{(l)}_{\beta_{l+2}} = u^{(0)}_{\beta_{l+2}} = u_{e_i+e_j}$. We now prove

$$\varphi_{e_i+e_j}(u_{e_i+e_j}) \geq \langle e_i + e_j, \nu(a)\rangle. \tag{4.6}$$

In cases (**Alg-1**) and (**Alg-3**) we have $u^{(l+1)}_{\beta_{l+2}} = u^{(l)}_{\beta_{l+2}} = u_{e_i+e_j}$. Therefore, (4.6) follows from (4.5). Assume that we are in case (**Alg-2**), so that $\varphi_{e_j}(u_{e_j}) \geq \varphi_{e_i}(u_{e_i}) \geq 0$. Then

$$u^{-1}_{e_i} u_{e_j} = u_{e_j} u^{-1}_{e_i} \cdot [u_{e_i}, u^{-1}_{e_j}]$$

with $[u_{e_i}, u^{-1}_{e_j}] \in U_{(e_i+e_j,0)}$, by (V3). This means $u^{(l+1)}_{\beta_{l+2}} = [u_{e_i}, u^{-1}_{e_j}] \cdot u_{e_i+e_j}$. Thus, we have either $\varphi_{e_i+e_j}(u_{e_i+e_j}) \geq 0 \geq \langle e_i + e_j, \nu(a)\rangle$ or we have $\varphi_{\beta_{l+2}}(u^{(l+1)}_{\beta_{l+2}}) = \varphi_{e_i+e_j}(u_{e_i+e_j})$. In the latter case, (4.6) follows, again, from (4.5). This proves (ii) in case Σ is of type B_n and $\mathbf{P}$ corresponds to α_n.

(d). If Σ is of type C_n and $\mathbf{P}$ corresponds to $\alpha_n = 2e_n$, then a similar argument as in (c) applies. The argument becomes easier, though, since U_P is commutative (use (DR2) and the fact that $c_n(\alpha_0) = 1$).

(e). Assume that Φ is of type BC_n and $\mathbf{P}$ corresponds to $\alpha_1 = e_1 - e_2$ in the notation of (B_n) in the proof of Proposition 3.5. The other cases, where Φ is of type B_n or C_n (and where $\mathbf{P}$ corresponds to α_1) are proved in essentially the same way.

Note that Σ is of type B_n and we have

$$\Sigma_{U_P} = \{e_1\} \cup \{e_1 \pm e_i \,|\, 2 \leq i \leq n\}\,.$$

We remark that, again by (DR2), the $u_{e_1 \pm e_i}$ do not depend on the ordering of the factors. By (b) we have $\varphi_{e_1 \pm e_i}(u_{e_1 \pm e_i}) \geq \langle e_1 \pm e_i, \nu(a)\rangle$. It remains to prove

$$\varphi_{e_1}(u_{e_1}) \geq \langle e_1, \nu(a)\rangle. \tag{4.7}$$

Note that if $2\varphi_{e_1}(u_{e_1}) \geq \varphi_{e_1-e_i}(u_{e_1-e_i}) + \varphi_{e_1+e_i}(u_{e_1+e_i})$, for some $2 \leq i \leq n$ and some ordering of the factors, then we easily obtain (4.7). Therefore, we assume from now on

$$2\varphi_{e_1}(u_{e_1}) < \varphi_{e_1-e_i}(u_{e_1-e_i}) + \varphi_{e_1+e_i}(u_{e_1+e_i}) \tag{4.8}$$

for all $2 \leq i \leq n$ and all orderings of the factors.

Given $v \in V$, we denote s_v the orthogonal reflection in the hyperplane orthogonal to v.

Claim 4.4.1. The decomposition

$$s_{e_1} = (s_1 s_2 \cdots s_{n-1}) s_n (s_{n-1} s_{n-2} \cdots s_1)$$

is reduced.

Proof. We write this decomposition as $s_{i_1} \cdots s_{i_{2n-1}}$ and put $\beta_j := s_{i_1} \cdots s_{i_{j-1}}(\alpha_{i_j})$, for all $1 \leq j \leq 2n-1$. Then we have

$$\beta_j = \begin{cases} s_1 \cdots s_{j-1}(e_j - e_{j+1}) = e_1 - e_{j+1}, & \text{for } 1 \leq j \leq n-1; \\ s_1 \cdots s_{n-1}(e_n) = e_1, & \text{for } j = n. \end{cases}$$

For $1 \leq j \leq n-1$ we compute

$$\begin{aligned} \beta_{2n-j} &= s_1 s_2 \cdots s_j s_{j+1} \cdots s_n s_{n-1} \cdots s_{j+1}(e_j - e_{j+1}) \\ &= s_1 \cdots s_j s_{e_{j+1}}(e_j - e_{j+1}) \\ &= s_1 \cdots s_j (e_j + e_{j+1}) \\ &= e_1 + e_{j+1}. \end{aligned}$$

Therefore, the elements $\beta_1, \ldots, \beta_{2n-1}$ are pairwise distinct and [4, Ch. IV, §1, no. 4, Lem. 2] shows that $\ell(s_{e_1}) = 2n-1$. $\square$

We fix a reduced decomposition $s_{i_1} \cdots s_{i_r}$ of w_0 whose initial piece is $s_1 s_2 \cdots s_n s_{n-1} \cdots s_1$. Since the u_γ, for $\gamma \in \Sigma_{U_P} \smallsetminus \{e_1\}$, are independent of the chosen ordering, we are free to choose a convenient ordering in order to estimate $\varphi_{e_1}(u_{e_1})$. We take the ordering given by the fixed reduced decomposition of w_0, so that $u_{e_1} = u_{e_1}^{(0)}$, and apply Algorithm 4.2. We need to study the *support* of $u^{(k)}$, that is, the set $\{\gamma \in \Sigma \mid u_\gamma^{(k)} \neq 1\}$. We define recursively $\Psi^{(0)} := \Sigma_{U_P}$ and then $\Psi^{(k)}$ as the closed[2] subset of $\Sigma^{(k)}$ generated by $\Psi^{(k-1)} \smallsetminus \{e_1 - e_{k+1}\}$ and $e_{k+1} - e_1$, for $1 \leq k \leq n-1$. Concretely, we have for all $0 \leq k \leq n-1$:

$$\begin{aligned} \Psi^{(k)} = \{e_1 \pm e_i \,|\, k+2 \leq i \leq n\} &\cup \{e_i \pm e_1 \,|\, 2 \leq i \leq k+1\} \\ &\cup \{e_i \pm e_j \,|\, 2 \leq i \leq k+1,\ i < j \leq n\} \cup \{e_i \,|\, 1 \leq i \leq k+1\}. \end{aligned}$$

By construction, the support of $u^{(k)}$ is contained in $\Psi^{(k)}$.

Under the addition map $\Psi^{(k)} \times \Psi^{(k)} \to \mathbb{R}^n$ the preimage of $\{e_1, 2e_1\}$ is the set of pairs $(e_1 \pm e_i, e_1 \mp e_i)$, for $k+2 \leq i \leq n$. The preimage of $e_1 \pm e_i$ is empty for $k+2 \leq i \leq n$. Together with our assumption (4.8) we show that this implies the following claim:

Claim 4.4.2. For all $0 \leq k \leq n-1$ one has:

(1) $\varphi_{e_1}(u_{e_1}^{(k)}) = \varphi_{e_1}(u_{e_1}^{(k-1)})$;

(2) $u_{e_1 \pm e_i}^{(k)} = u_{e_1 \pm e_i}^{(k-1)}$, for all $k+2 \leq i \leq n$.

(We put $u_\gamma^{(-1)} := u_\gamma$, for $\gamma \in \Sigma$.)

Proof. We prove the claim by induction on k, the case $k = 0$ being trivial. Assume the claim holds for some $0 \leq k \leq n-2$ and all $0 \leq j \leq k$. Recall that $\beta_{k+1} = e_1 - e_{k+2}$.

[2] A subset $X \subseteq \Sigma^{(k)}$ is called *closed* if $\gamma, \delta \in X$ with $\gamma + \delta \in \Sigma^{(k)}$ implies $\gamma + \delta \in X$.

Assume we are in case (**Alg-1**), so that

$$\varphi_{e_1-e_{k+2}}\big(u^{(k)}_{e_1-e_{k+2}}\big) \geq -\big\langle \beta_{k+1}, \nu\big(z^{(k)}\big)\big\rangle.$$

In this case, we have $u^{(k+1)}_\gamma = u^{(k)}_\gamma$, for all $\gamma \in \Psi^{(k)} \smallsetminus \{e_1 - e_{k+2}\}$, which proves the induction step in this case.

Suppose we are in case (**Alg-3**). Then $u^{(k+1)}_{e_1 \pm e_i} = u^{(k)}_{e_1 \pm e_i}$, for all $k + 3 \leq i \leq n$, and $u^{(k+1)}_{e_1} = u^{(k)}_{e_1}$. This shows the induction step in this case.

Finally, assume we are in case (**Alg-2**) so that $\varphi_{e_1-e_{k+2}}\big(u^{(k)}_{e_1-e_{k+2}}\big) \geq 0$. We then have $u^{(k+1)}_{e_1 \pm e_i} = u^{(k)}_{e_1 \pm e_i}$, for all $k + 3 \leq i \leq n$. Moreover, we have

$$u^{(k+1)}_{e_1} = u^{(k)}_{e_1} \cdot \big[u^{(k)}_{e_1-e_{k+2}}, \big(u^{(k)}_{e_1+e_{k+2}}\big)^{-1}\big] \in U_{e_1}.$$

The induction hypothesis implies $\varphi_{e_1}\big(u^{(k)}_{e_1}\big) = \varphi_{e_1}(u_{e_1})$ and $u^{(k)}_{e_1 \pm e_{k+2}} = u_{e_1 \pm e_{k+2}}$. Using (V4), (V3), and (4.8), we compute

$$\begin{aligned} 2\varphi_{e_1}\big(\big[u^{(k)}_{e_1-e_{k+2}}, \big(u^{(k)}_{e_1+e_{k+2}}\big)^{-1}\big]\big) &= \varphi_{2e_1}\big(\big[u^{(k)}_{e_1-e_{k+2}}, \big(u^{(k)}_{e_1+e_{k+2}}\big)^{-1}\big]\big) \\ &\geq \varphi_{e_1-e_{k+2}}\big(u^{(k)}_{e_1-e_{k+2}}\big) + \varphi_{e_1+e_{k+2}}\big(u^{(k)}_{e_1+e_{k+2}}\big) \\ &> 2\varphi_{e_1}\big(u^{(k)}_{e_1}\big). \end{aligned}$$

Therefore, we conclude $\varphi_{e_1}\big(u^{(k+1)}_{e_1}\big) = \varphi_{e_1}\big(u^{(k)}_{e_1}\big)$. This proves the induction step in this case and finishes the proof. □

Now, Claim 4.4.2 and (4.5) show $\varphi_{e_1}(u_{e_1}) = \varphi_{\beta_n}\big(u^{(n-1)}_{\beta_n}\big) \geq \langle e_1, \nu(a)\rangle$. This shows (4.7) and finishes the proof. □

5. Decomposition of Hecke polynomials

We fix a commutative ring R with 1. In Sections 5.2 and 5.6 we will assume that p be invertible in R.

5.1. Parabolic Hecke algebras. Parabolic Hecke algebras for the general linear and the symplectic group were introduced and studied by Andrianov, see [1], [2], and the book [3].

Definition 5.1. Let $\mathbf{P}$ be a parabolic subgroup of $\mathbf{G}$. Then

$$\mathcal{H}_R(K_P, P)$$

is called a *parabolic Hecke algebra.*

Lemma 5.2. *Let* $\mathbf{P}$ *and* $\mathbf{Q}$ *be (not necessarily proper) parabolic subgroups of* $\mathbf{G}$ *with* $\mathbf{P} \subseteq \mathbf{Q}$. *Then the map*

$$\begin{aligned} \varepsilon_{P,Q} \colon \mathcal{H}_R(K_Q, Q) &\longhookrightarrow \mathcal{H}_R(K_P, P), \\ \sum_i r_i \cdot (K_Q g_i) &\longmapsto \sum_i r_i \cdot (K_P g_i), \end{aligned}$$

where one may choose $g_i \in P$, is a well-defined injective R-algebra homomorphism. Moreover, the following diagram is commutative:

$$\begin{array}{ccc} \mathcal{H}_R(K,G) & \xhookrightarrow{\varepsilon_{Q,G}} & \mathcal{H}_R(K_Q,Q) \\ & \searrow^{\varepsilon_{P,G}} & \big\downarrow \varepsilon_{P,Q} \\ & & \mathcal{H}_R(K_P,P). \end{array}$$

Proof. Clearly, we have $K_P \subseteq K_Q$ and $K_Q \cap P = K_P$. The Iwasawa decomposition 2.5 implies $Q = K_Q P$. Therefore, the conditions (2.7) for $(\Gamma, S) = (K_Q, Q)$ and $(\Gamma_0, S_0) = (K_P, P)$ are satisfied and the first statement follows from Proposition 2.7. The commutativity of the diagram is obvious. □

Let $\mathbf{P} = \mathbf{U_P M}$ be a parabolic subgroup of $\mathbf{G}$. Let $\mathrm{pr}_{\mathbf{M}} \colon \mathbf{P} \to \mathbf{M}$ be the canonical projection. Note that $K_M = K \cap M$ is a special parahoric subgroup of M (see Section 2.4). The map

$$\begin{aligned} \Theta_M^P \colon \mathcal{H}_R(K_P,P) &\longrightarrow \mathcal{H}_R(K_M,M), \\ \sum_i r_i \cdot (K_P g_i) &\longmapsto \sum_i r_i \cdot \big(K_M \,\mathrm{pr}_{\mathbf{M}}(g_i)\big) \end{aligned}$$

is a homomorphism of R-algebras.

Definition 5.3. The composition

$$\mathcal{S}_M^G \colon \mathcal{H}_R(K,G) \xrightarrow{\varepsilon_{P,G}} \mathcal{H}_R(K_P,P) \xrightarrow{\Theta_M^P} \mathcal{H}_R(K_M,M)$$

is called the *(partial) Satake homomorphism.*

If $\mathbf{P} = \mathbf{B}$ and $\mathbf{M} = \mathbf{Z}$, then the subgroup K_Z is normal in Z and hence $\mathcal{H}_R(K_Z,Z)$ identifies with the commutative group algebra $R[K_Z \backslash Z] = R[\Lambda]$. In this case, the Satake homomorphism takes the form

$$\mathcal{S}^G \coloneqq \mathcal{S}_Z^G \colon \mathcal{H}_R(K,G) \longrightarrow R[\Lambda].$$

Lemma 5.4. *Let $\mathbf{Q} = \mathbf{U_Q L}$ and $\mathbf{P} = \mathbf{U_P M}$ be parabolic subgroups of $\mathbf{G}$ and assume that $\mathbf{Q} \subseteq \mathbf{P}$. The diagram*

$$\begin{array}{ccc} \mathcal{H}_R(K_P,P) & \xrightarrow{\Theta_M^P} & \mathcal{H}_R(K_M,M) \\ \varepsilon_{Q,P} \big\downarrow & & \big\downarrow \mathcal{S}_L^M \\ \mathcal{H}_R(K_Q,Q) & \xrightarrow[\Theta_L^Q]{} & \mathcal{H}_R(K_L,L) \end{array}$$

is commutative. In particular, one has $\mathcal{S}_L^G = \mathcal{S}_L^M \circ \mathcal{S}_M^G$.

Proof. Note that $\mathbf{Q} \cap \mathbf{M}$ is a parabolic subgroup of $\mathbf{M}$ with Levi $\mathbf{L}$. Given $b \in Q$, we have $\mathrm{pr}_{\mathbf{M}}(b) \in Q \cap M$ and $\mathrm{pr}_{\mathbf{L}}(\mathrm{pr}_{\mathbf{M}}(b)) = \mathrm{pr}_{\mathbf{L}}(b)$. Hence, for all $\sum_i r_i \cdot (K_P b_i) \in \mathcal{H}_R(K_P, P)$, where, by the Iwasawa decomposition 2.5, we may choose $b_i \in Q$, we compute

$$\begin{aligned}
\mathcal{S}_L^M\left(\Theta_M^P\left(\sum_i r_i \cdot (K_P b_i)\right)\right) &= \mathcal{S}_L^M\left(\sum_i r_i \cdot (K_M \,\mathrm{pr}_{\mathbf{M}}(b_i))\right) \\
&= \sum_i r_i \cdot (K_L \,\mathrm{pr}_{\mathbf{L}}(\mathrm{pr}_{\mathbf{M}}(b_i))) \\
&= \sum_i r_i \cdot (K_L \,\mathrm{pr}_{\mathbf{L}}(b_i)) \\
&= \Theta_L^Q\left(\sum_i r_i \cdot (K_Q b_i)\right) \\
&= \Theta_L^Q\left(\varepsilon_{Q,P}\left(\sum_i r_i \cdot (K_P b_i)\right)\right).
\end{aligned}$$

In particular, in view of Lemma 5.2, we have

$$\mathcal{S}_L^M \circ \mathcal{S}_M^G = \mathcal{S}_L^M \circ \Theta_M^P \circ \varepsilon_{P,G} = \Theta_L^Q \circ \varepsilon_{Q,P} \circ \varepsilon_{P,G} = \Theta_L^Q \circ \varepsilon_{Q,G} = \mathcal{S}_L^G. \quad \square$$

5.2. The twisted action. Assume that R is a $\mathbb{Z}[1/p]$-algebra. The twisted action of W_0 on $R[\Lambda]$ was defined by Henniart–Vignéras, [14, 7.11, 7.12], in order to describe the image of the integral Satake homomorphism. We give a slightly different presentation.

Given $b \in B$, we consider the integers (see (2.4) in Section 2.5)

$$\mu_U(b) \coloneqq [K_U : K_U \cap b^{-1} K_U b].$$

Observe that μ_U is constant on K_Z-cosets, since K_Z normalizes K_U. Therefore, we obtain an induced map

$$\mu_U \colon \Lambda \longrightarrow q^{\mathbb{Z}_{\geq 0}}.$$

Note that $\mu_U(\lambda) = 1$ if and only if $\lambda \in \Lambda^+$.

We employ the exponential notation e^λ when we view $\lambda \in \Lambda$ as an element of $R[\Lambda]$.

Definition 5.5. The *twisted action* of W_0 on $R[\Lambda]$ is defined by

$$w \star e^\lambda \coloneqq \frac{\mu_U(w(\lambda))}{\mu_U(\lambda)} \cdot e^{w(\lambda)}, \qquad \text{for } \lambda \in \Lambda,\ w \in W_0.$$

In order to describe the relation with the twisted action in [14, 7.11], we recall the modulus character

$$\delta \colon B \longrightarrow q^{\mathbb{Z}}, \qquad \delta(b) \coloneqq [b K_U b^{-1} : K_U] = \mu_U(b)/\mu_U(b^{-1}),$$

where $[bK_Ub^{-1} : K_U] \coloneqq \frac{[bK_Ub^{-1} : bK_Ub^{-1} \cap K_U]}{[K_U : bK_Ub^{-1} \cap K_U]}$ denotes the generalized index. Similar to the above, δ induces a character

$$\delta \colon \Lambda \longrightarrow q^{\mathbb{Z}}.$$

Lemma 5.6. *For all $w \in W_0$ and $\lambda \in \Lambda$, one has*

$$\frac{\delta(w(\lambda))}{\delta(\lambda)} = \left(\frac{\mu_U(w(\lambda))}{\mu_U(\lambda)}\right)^2 = \left(\frac{\mu_U(-\lambda)}{\mu_U(-w(\lambda))}\right)^2.$$

Proof. Note that $\frac{\delta(w(\lambda))}{\delta(\lambda)} = \frac{\mu_U(w(\lambda)) \cdot \mu_U(-\lambda)}{\mu_U(\lambda) \cdot \mu_U(-w(\lambda))}$. Therefore, for both equalities it suffices to show

$$\mu_U(\lambda) \cdot \mu_U(-\lambda) = \mu_U\big(w(\lambda)\big) \cdot \mu_U\big(-w(\lambda)\big).$$

But this follows from $\mu_U(\lambda)\mu_U(-\lambda) = q_\lambda$ (cf. [18, Prop. 3.14.(a)]) and $q_\lambda = q_{w(\lambda)}$ (cf. [28, Prop. 5.13]). □

5.3. The Satake isomorphism. Given $\lambda \in \Lambda$, we denote $W_{0,\lambda}$ the stabilizer of λ under the (usual) W_0-action on Λ. Then $W_{0,\lambda}$ is also the stabilizer of e^λ under the twisted action of W_0 on $R[\Lambda]$.

Note that, if $R = \mathbb{Z}[1/p]$ and $\lambda \in \Lambda^+$, one has

$$S_\lambda \coloneqq \sum_{w \in W_0/W_{0,\lambda}} w \star e^\lambda \in \mathbb{Z}[\Lambda]. \tag{5.1}$$

With our notations, the main result of [14] is the following:

Theorem 5.7. *Let R be a commutative ring with 1 and consider the Satake homomorphism $\mathcal{S}^G \colon \mathcal{H}_R(K, G) \to R[\Lambda]$.*

(i) *$\mathcal{S}^G$ is injective.*

(ii) *The image of $\mathcal{S}^G$ is a free R-module with basis $\{1 \otimes S_\lambda \mid \lambda \in \Lambda^+\}$.*
If $p \in R^\times$, then the image coincides with $R[\Lambda]^{W_0,\star}$, the algebra of W_0-invariants under the twisted action.

(iii) *Both $R[\Lambda]$ and $\mathcal{H}_R(K, G)$ are commutative algebras of finite type over R.*

Proof. We briefly explain how our notations relate to the notations in [14]. Consider the space $C_c^\infty(K\backslash G/K, R)$ of compactly supported K-biinvariant functions $G \to R$ with product given by convolution:

$$(f_1 * f_2)(g) = \sum_{h \in G/K} f_1(h) \cdot f_2(h^{-1}g),$$

for $f_1, f_2 \in C_c^\infty(K\backslash G/K, R)$ and $g \in G$, and where "$h \in G/K$" means that h runs through a set of representatives for the left cosets in G/K. The map

$$\rho_G \colon C_c^\infty(K\backslash G/K, R) \longrightarrow \mathcal{H}_R(K, G), \quad f \longmapsto \sum_{g \in K\backslash G} f(g^{-1}) \cdot (Kg)$$

is an anti-isomorphism of R-algebras.[3] Following [15], the Satake homomorphism in [14] is defined as

$$\mathcal{S}'\colon C_c^\infty(K\backslash G/K,R) \longrightarrow C_c^\infty(Z/K_Z,R) \cong R[\Lambda],$$
$$f \longmapsto \Bigg[z \mapsto \sum_{u\in U/K_U} f(zu)\Bigg],$$

where $K_U = K\cap U$. Now, the diagram

$$\begin{array}{ccc} C_c^\infty(K\backslash G/K,R) & \xrightarrow{\mathcal{S}'} & C_c^\infty(Z/K_Z,R) \\ \Big\downarrow{\scriptstyle \rho_G} & & \Big\downarrow{\scriptstyle \rho_Z} \\ \mathcal{H}_R(K,G) & \xrightarrow[\mathcal{S}^G]{} & \mathcal{H}_R(K_Z,Z) \end{array}$$

commutes: Fix a representing system $\Gamma \subseteq Z$ for the coset space $K_Z\backslash Z$, so that $K_U\backslash U \times \Gamma \cong K\backslash G$ via $(K_U u, z) \mapsto Kuz$. Then for each $f \in C_c^\infty(K\backslash G/K,R)$ we compute

$$\begin{aligned}\rho_Z\big(\mathcal{S}'(f)\big) &= \sum_{z\in\Gamma} \mathcal{S}'(f)(z^{-1})\cdot(K_Z z) = \sum_{z\in\Gamma}\sum_{u\in U/K_U} f(z^{-1}u)\cdot(K_Z z)\\ &= \sum_{z\in\Gamma}\sum_{u\in K_U\backslash U} f\big((uz)^{-1}\big)\cdot(K_Z z) = \sum_{uz\in K\backslash G} f\big((uz)^{-1}\big)\cdot(K_Z z)\\ &= \mathcal{S}^G\Bigg(\sum_{uz\in K\backslash G} f\big((uz)^{-1}\big)\cdot(Kuz)\Bigg) = \mathcal{S}^G\big(\rho_G(f)\big).\end{aligned}$$

If $p\in R^\times$, then the twisted action of W_0 on $C_c^\infty(Z/K_Z,R)$ is defined by

$$w\circ e^\lambda := \delta^{1/2}(\lambda - w(\lambda))\cdot e^{w(\lambda)},$$

where $\delta^{1/2}$ is a square root of δ. This is indeed defined over R, since Lemma 5.6 shows that $\delta^{1/2}(\lambda-w(\lambda))$ actually lies in $q^{\mathbb{Z}}$. The same lemma also shows that $\rho_Z(w\circ e^\lambda) = w\star e^{-\lambda}$.

Therefore, we have $\rho_Z\big(\sum_{w\in W_0/W_{0,\lambda}} w\circ e^\lambda\big) = S_{-\lambda}$ in $R[\Lambda]$, for all $\lambda\in\Lambda^-$.

Now, (i) and (ii) are [14, 7.15 Thm. and 7.13 Cor.], and (iii) is [14, 7.16]. □

Remark 5.8. Let $z\in Z^-$ and put $\lambda = zK_Z \in \Lambda$. It follows from Remark 2.6 (a) and (b) that

$$\mathcal{S}^G\big((z)_K\big) = e^\lambda + \sum_{\substack{\mu\in\Lambda \text{ s.t.}\\ \nu(\mu)<\nu(\lambda)}} a_\mu\cdot e^\mu \in \mathbb{Z}[1/p][\Lambda]. \tag{5.2}$$

By Theorem 5.7, $\mathcal{S}^G\big((z)_K\big)$ is invariant under the twisted action of W_0. Therefore, $\frac{a_\mu}{\mu_U(\mu)} = \frac{a_{w(\mu)}}{\mu_U(w(\mu))}$, for all $w\in W_0$ and all $\mu\in\Lambda$. In particular,

[3] As $C_c^\infty(K\backslash G/K,R)$ turns out to be commutative, ρ_G is in fact a homomorphism.

$a_\mu \neq 0$ if and only if $a_{w(\mu)} \neq 0$ for all $w \in W_0$. Now, (5.2) shows $w(\mu) \leq \lambda$, for all $w \in W_0$ and all $\mu \in \Lambda$ with $\mu \leq \lambda$. This explains Remark 2.6.c.

5.4. Centralizers in parabolic Hecke algebras. Let $\mathbf{P} = \mathbf{U_P M}$ be a parabolic subgroup of $\mathbf{G}$. We choose a strictly M-positive element $a_P \in Z$, see Section 2.5. This means that a_P lies in the center of M and satisfies

$$\langle \alpha, \nu(a_P) \rangle < 0, \qquad \text{for all } \alpha \in \Sigma^+ \smallsetminus \Sigma_M.$$

Note that $K_P a_P K_P = K_P a_P$ and hence $(a_P)_{K_P} = (K_P a_P)$ in $\mathcal{H}_R(K_P, P)$. We consider the centralizer algebra

$$C_P^+ := \{ X \in \mathcal{H}_R(K_P, P) \mid X \cdot (a_P)_{K_P} = (a_P)_{K_P} \cdot X \}.$$

The algebra C_P^+ was originally studied by Andrianov when $\mathbf{P}$ is the "Siegel parabolic" of a symplectic group, see [1, 2].

Lemma 5.9. *The following statements hold true:*

(i) $C_P^+ = \left\{ X \in \mathcal{H}_R(K_P, P) \,\middle|\, \begin{array}{l} X = \sum_i r_i \cdot (K_P m_i) \\ \textit{with } m_i \in M \textit{ and } r_i \in R \end{array} \right\}.$

(ii) *For all $X \in \mathcal{H}_R(K_P, P)$, there exists $n > 0$ such that $(a_P)_{K_P}^n X \in C_P^+$.*

(iii) *The map Θ_M^P restricts to an isomorphism $C_P^+ \cong \mathcal{H}_R(K_M, M^+)$. In particular, C_P^+ is commutative.*

Proof. See [17, Lem. 4 and Cor.y 5]. The last assertion in (iii) follows from the fact that $\mathcal{H}_R(K_M, M)$ is commutative by Theorem 5.7 applied to M. ☐

Note that Lemma 5.9 (i) shows that C_P^+ is independent of the choice of a_P.

Recall the anti-involution ζ_P on $\mathcal{H}_R(K_P, P)$, cf. (2.8), which is given by $\zeta_P((g)_{K_P}) = (g^{-1})_{K_P}$.

Remark 5.10. Let $a_P \in Z$ be a strictly M-positive element. Then a_P^{-1} is strictly M-negative and

$$\zeta_P(C_P^+) = C_P^- := \left\{ X \in \mathcal{H}_R(K_P, P) \,\middle|\, X \cdot (a_P^{-1})_{K_P} = (a_P^{-1})_{K_P} \cdot X \right\}.$$

The analog of Lemma 5.9 for C_P^- also holds.[4]

Lemma 5.11. *One has*

$$\zeta_P(\operatorname{Ker} \Theta_M^P) = \operatorname{Ker} \Theta_M^P.$$

[4] However, note that it is not Θ_M^P which induces an isomorphism $C_P^- \cong \mathcal{H}_R(K_M, M^-)$, but rather $\zeta_M \circ \Theta_M^P \circ \zeta_P$.

Proof. Note that, for each $g \in P$, the index $\mu(g) := [K_P : K_P \cap g^{-1}K_P g]$ counts the number of right K_P-cosets in $K_P g K_P$, by (2.6). Similarly, $\mu_M(m) := [K_M : K_M \cap m^{-1}K_M m]$ counts the number of right K_M-cosets in $K_M m K_M$. Moreover,

$$\delta\colon P \to q^{\mathbb{Z}}, \qquad \delta(g) := [gK_P g^{-1} : K_P] = \frac{\mu(g)}{\mu(g^{-1})}$$

is the modulus character of P. As every element in U_P is contained in a compact group, we have $\delta\big|_{U_P} = 1$, by [27, Ch. I, 2.7]. Therefore,

$$\delta(g) = \delta\big(\mathrm{pr}_{\mathbf{M}}(g)\big), \qquad \text{for all } g \in P. \tag{5.3}$$

Note that $\Theta_M^P((g)_{K_P}) = \frac{\mu(g)}{\mu_M(\mathrm{pr}_{\mathbf{M}}(g))} \cdot \big(\mathrm{pr}_{\mathbf{M}}(g)\big)_{K_M}$ by [18, Prop. 4.3], and hence $\operatorname{Ker}\Theta_M^P$ is generated by elements of the form $(g)_{K_P} - \frac{\mu(g)}{\mu(\mathrm{pr}_{\mathbf{M}}(g))} \cdot (\mathrm{pr}_{\mathbf{M}}(g))_{K_P}$. We compute

$$\begin{aligned}
\Theta_M^P\bigg(\zeta_P\Big((g)_{K_P} &- \frac{\mu(g)}{\mu(\mathrm{pr}_{\mathbf{M}}(g))} \cdot \big(\mathrm{pr}_{\mathbf{M}}(g)\big)_{K_P}\Big)\bigg) \\
&= \frac{\mu(g^{-1})}{\mu_M(\mathrm{pr}_{\mathbf{M}}(g^{-1}))} \cdot \big(\mathrm{pr}_{\mathbf{M}}(g^{-1})\big)_{K_M} \\
&\qquad - \frac{\mu(g)\cdot\mu(\mathrm{pr}_{\mathbf{M}}(g^{-1}))}{\mu(\mathrm{pr}_{\mathbf{M}}(g))\cdot\mu_M(\mathrm{pr}_{\mathbf{M}}(g^{-1}))} \cdot \big(\mathrm{pr}_{\mathbf{M}}(g^{-1})\big)_{K_M} \\
&= 0, \qquad \text{(by (5.3))}.
\end{aligned}$$

This shows $\zeta_P(\operatorname{Ker}\Theta_M^P) \subseteq \operatorname{Ker}\Theta_M^P$. The assertion follows from $\zeta_P^2 = \mathrm{id}$. □

Remark 5.12. One has $\Theta_M^P \circ \zeta_P \neq \zeta_M \circ \Theta_M^P$ (apply both maps to $(a_P)_{K_P}$ for a strictly M-positive a_P).

5.5. Example of a parabolic Hecke algebra. The purpose of this section is to work out an example of the setup so far.

Let $\mathcal{O}_{\mathfrak{F}}$ be the valuation ring of $\mathfrak{F}$ and fix a uniformizer $\pi \in \mathcal{O}_{\mathfrak{F}}$. Consider the group $G = \mathrm{GL}_2(\mathfrak{F})$ and the maximal compact subgroup $K = \mathrm{GL}_2(\mathcal{O}_{\mathfrak{F}})$. Let $B \subseteq G$ be the subgroup of upper triangular matrices and $Z \subseteq B$ the subgroup of diagonal matrices. Fix a coefficient ring R. A variant of the parabolic Hecke algebra $\mathcal{H}_R(K_B, B)$ is briefly discussed in Vienney's thesis [26, p. 102]. We prove the following structure result of $\mathcal{H}_R(K_B, B)$ in Appendix A.

Theorem 5.13. *The R-algebra $\mathcal{H}_R(K_B, B)$ is generated by the elements*

$$X_+ := \left(\begin{pmatrix} \pi & 0 \\ 0 & 1 \end{pmatrix}\right)_{K_B}, \qquad X_- := \left(\begin{pmatrix} \pi^{-1} & 0 \\ 0 & 1 \end{pmatrix}\right)_{K_B}, \tag{5.4}$$

$$Y := (\pi E_2)_{K_B}, \qquad Y^{-1} := (\pi^{-1}E_2)_{K_B}, \tag{5.5}$$

where E_2 is the 2×2 identity matrix, subject only to the following relations:

$$
(5.6)\qquad
\begin{aligned}
YY^{-1} &= Y^{-1}Y = 1,\\
YX_+ &= X_+Y,\\
YX_- &= X_-Y,\\
X_+X_- &= q\cdot 1.
\end{aligned}
$$

In particular, $\mathcal{H}_R(K_B, B)$ is non-commutative.

Remark 5.14. It follows from Theorem 5.13 that X_+ is a left zero-divisor (resp. X_- is a right zero-divisor), because

$$X_+\cdot(X_-X_+ - q\cdot 1) = (X_-X_+ - q\cdot 1)\cdot X_- = 0.$$

If q is invertible in R, then X_+ is right invertible (resp. X_- is left invertible), since

$$X_+\cdot q^{-1}X_- = q^{-1}X_+\cdot X_- = 1.$$

Since $\Lambda\cong\mathbb{Z}^2$, the Hecke algebra $\mathcal{H}_R(K_Z, Z)$ identifies with $R[x^{\pm 1}, y^{\pm}]$ via $((\begin{smallmatrix}\pi & 0\\ 0 & 1\end{smallmatrix}))_{K_Z}\mapsto x$ and $((\begin{smallmatrix}1 & 0\\ 0 & \pi\end{smallmatrix}))_{K_Z}\mapsto y$. Then the map Θ_Z^B is given by

$$
\begin{aligned}
\Theta_Z^B\colon \mathcal{H}_R(K_B, B) &\longrightarrow \mathcal{H}_R(K_Z, Z),\\
X_+ &\longmapsto x,\\
X_- &\longmapsto qx^{-1},\\
Y &\longmapsto xy.
\end{aligned}
$$

The kernel of Θ_Z^B is the two-sided ideal generated by $X_-X_+ - q\cdot 1$.

Assume $q\in R^\times$. The twisted action of $W_0 = \{1, w_0 = (\begin{smallmatrix}0 & 1\\ 1 & 0\end{smallmatrix})\}$ on $R[x^{\pm 1}, y^{\pm 1}]$ is given by

$$w_0\star x = qy \qquad\text{and}\qquad w_0\star y = q^{-1}x.$$

For all $a, b, c\in\mathbb{Z}$ with $a > b$, the elements

$$(5.7)\qquad S_{a,b} := x^a y^b + q^{a-b}x^b y^a, \qquad\qquad S_{c,c} := (xy)^c$$

are W_0-invariant with respect to the twisted action; in fact they constitute an R-basis of $R[\Lambda]^{W_0,\star}$. Moreover, the relations

$$
\begin{aligned}
&(5.8) & S_{c,c} &= S_{1,1}^c, && \text{for } c\in\mathbb{Z},\\
&(5.9) & S_{a,b} &= S_{b,b}\cdot S_{a-b,0} = S_{a-b,0}\cdot S_{b,b}, && \text{for } a, b\in\mathbb{Z} \text{ with } a > b,\\
&(5.10) & S_{n,0}\cdot S_{1,0} &= S_{n+1,0} + q\cdot S_{1,1}\cdot S_{n-1,0}, && \text{for } n\in\mathbb{Z}_{\geq 1}
\end{aligned}
$$

are immediate. Thus, $R[\Lambda]^{W_0,\star} = R[S_{1,0}, S_{1,1}^{\pm 1}] = R[x + qy, (xy)^{\pm 1}]$.

We identify Λ^+ with $\{(a, b)\in\mathbb{Z}^2 \mid a\geq b\}$. By the Cartan decomposition 2.3, every double coset in G is uniquely of the form $K\left(\begin{smallmatrix}\pi^a & 0\\ 0 & \pi^b\end{smallmatrix}\right)K$ with $(a, b)\in\Lambda^+$. Let us compute the Satake homomorphism $\mathcal{S}^G\colon \mathcal{H}_R(K, G)\to$

$R[\Lambda]$. Let $A \subseteq \mathcal{O}_{\mathfrak{F}}$ be a complete system of representatives for the residue field of $\mathfrak{F}$ such that $0 \in A$. Note that $|A| = q$. For each $(a,b) \in \Lambda^+$ we have

$$
\begin{aligned}
K\begin{pmatrix}\pi^a & 0\\ 0 & \pi^b\end{pmatrix}K = K\begin{pmatrix}\pi^a & 0\\ 0 & \pi^b\end{pmatrix}
&\sqcup \coprod_{c=1}^{a-b-1} \coprod_{\substack{\beta_b,\dots,\beta_{b+c-1}\in A\\ \beta_b\neq 0}} K\begin{pmatrix}\pi^{a-c} & \sum_{i=b}^{b+c-1}\beta_i\pi^i\\ 0 & \pi^{b+c}\end{pmatrix}\\
&\sqcup \coprod_{\beta_b,\dots,\beta_{a-1}\in A} K\begin{pmatrix}\pi^b & \sum_{i=b}^{a-1}\beta_i\pi^i\\ 0 & \pi^a\end{pmatrix}.
\end{aligned}
$$

Let $\gamma \coloneqq \lfloor \frac{a-b}{2} \rfloor$ be the largest integer $\leq \frac{a-b}{2}$. We deduce

$$
\begin{aligned}
\mathcal{S}^G\left(\left(\begin{pmatrix}\pi^a & 0\\ 0 & \pi^b\end{pmatrix}\right)_K\right) &= x^a y^b + \sum_{c=1}^{a-b-1}(q-1)q^{c-1}x^{a-c}y^{b+c} + q^{a-b}x^b y^a\\
&= S_{a,b} + (q-1)\cdot\sum_{c=1}^{\gamma} q^{c-1}S_{a-c,b+c} + \epsilon\cdot(q-1)q^{\gamma-1}S_{\gamma,\gamma},
\end{aligned}
$$

and where $\epsilon = 1$ if $a-b$ is even and non-zero, and $\epsilon = 0$ otherwise. Consider on Λ the partial ordering defined by $(c,d) \leq (a,b)$ if $c \leq a$ and $c+d = a+b$. As usual we write $(c,d) < (a,b)$ if $(c,d) \leq (a,b)$ and $(c,d) \neq (a,b)$. Note that for each $(a,b) \in \Lambda^+$ there are only finitely many elements (c,d) in Λ^+ satisfying $(c,d) < (a,b)$. Then we have shown

$$
\mathcal{S}^G\left(\left(\begin{pmatrix}\pi^a & 0\\ 0 & \pi^b\end{pmatrix}\right)_K\right) \in S_{a,b} + \sum_{\substack{(c,d)\in\Lambda^+,\\ (c,d)<(a,b)}} \mathbb{Z}.S_{c,d}.
$$

By a "triangular argument" it follows that $\mathcal{S}^G$ is an injective map with image $R[\Lambda]^{W_0,\star}$. In particular, $\mathcal{H}_R(K,G)$ is commutative. Moreover,

$$
\begin{aligned}
\mathcal{S}^G\left(\left(\begin{pmatrix}\pi & 0\\ 0 & 1\end{pmatrix}\right)_K\right) &= S_{1,0} = x + qy,\\
\mathcal{S}^G\big((\pi E_2)_K\big) &= S_{1,1} = xy,
\end{aligned}
$$

which shows that $\mathcal{H}_R(K,G)$ identifies with the polynomial ring generated by $((\begin{smallmatrix}\pi & 0\\ 0 & 1\end{smallmatrix}))_K$ and $(\pi E_2)_K$, with $(\pi E_2)_K$ invertible. We have verified Theorem 5.7 in this specific example.

We can also view $\mathcal{H}_R(K,G)$ as a subalgebra of $\mathcal{H}_R(K_B,B)$ via the embedding

$$\begin{aligned}\varepsilon_{B,G}\colon \mathcal{H}_R(K,G) &\longhookrightarrow \mathcal{H}_R(K_B,B),\\ \left(\begin{pmatrix}\pi & 0\\ 0 & 1\end{pmatrix}\right)_K &\longmapsto X_+ + X_-Y,\\ (\pi E_2)_K &\longmapsto Y.\end{aligned}$$

Note that C_B^+ is the centralizer of X_+. Explicitly, C_B^+ is the polynomial algebra

$$C_B^+ = R[X_+, Y^{\pm 1}] \subseteq \mathcal{H}_R(K_B,B).$$

The anti-involution ζ_B on $\mathcal{H}_R(K_B,B)$ is determined by $\zeta_B(X_+) = X_-$ and $\zeta_B(Y) = Y^{-1}$.

Consider the polynomial

$$Q(t) = 1 - \left(\begin{pmatrix}\pi & 0\\ 0 & 1\end{pmatrix}\right)_K \cdot t + q\cdot(\pi\cdot E_2)_K\cdot t^2 \in \mathcal{H}_R(K,G)[t].$$

Applying $\mathcal{S}^G$ to the coefficients of Q, the resulting polynomial $Q^{\mathcal{S}^G}(t)$ decomposes as follows:

$$Q^{\mathcal{S}^G}(t) = 1-(x+qy)\cdot t + qxy\cdot t^2 = (1-xt)\cdot(1-qyt) \in R[x^{\pm 1}, y^{\pm 1}][t].$$

One may ask whether this decomposition can be lifted to a decomposition of $Q(t)$ in $\mathcal{H}_R(K,G)[t]$. Unfortunately, this is false. But it turns out that one can find a decomposition of $Q(t)$ over the parabolic Hecke algebra $\mathcal{H}_R(K_B,B)$: Applying $\varepsilon_{B,G}$ to the coefficients of $Q(t)$, we obtain

$$\begin{aligned}Q^{\varepsilon_{B,G}}(t) &= 1-(X_+ + X_-Y)\cdot t + qYt^2\\ &= (1-X_+t)\cdot(1-X_-Yt) \in \mathcal{H}_R(K_B,B)[t].\end{aligned}$$

Here, the free variable t in $\mathcal{H}_R(K_B,B)[t]$ commutes with the elements in $\mathcal{H}_R(K_B,B)$. Note that the order of the factors is important, because $\mathcal{H}_R(K_B,B)$ is non-commutative.

In the next subsection we prove a general decomposition theorem following the ideas of Andrianov [1, 3].

5.6. The decomposition theorem. From now on we assume that R is a $\mathbb{Z}[1/p]$-algebra. Let $\mathbf{P} = \mathbf{U_P M}$ be a parabolic subgroup of $\mathbf{G}$. We view the embeddings $\varepsilon_{P,G}\colon \mathcal{H}_R(K,G) \hookrightarrow \mathcal{H}_R(K_P,P)$ and $\varepsilon_{B,P}\colon \mathcal{H}_R(K_P,P) \hookrightarrow \mathcal{H}_R(K_B,B)$ as inclusions.

Let $a_P \in Z$ be a strictly M-positive element and denote its image in Λ by λ_P. Choose a representing system W_0^M of $W_0/W_{0,M}$ in W_0. Consider the polynomial

$$\widetilde{\chi}_{a_P}(t) \coloneqq \prod_{w\in W_0^M}(1 - w\star e^{-\lambda_P}\cdot t) \in 1 + tR[\Lambda][t].$$

This definition does not depend on the choice of W_0^M, because $W_{0,M}$ fixes $e^{-\lambda_P} \in R[\Lambda]$ with respect to the twisted action. Note that, by construction, we have $\widetilde{\chi}_{a_P}(e^{\lambda_P}) = 0$, and the coefficients of $\widetilde{\chi}_{a_P}(t)$ are W_0-invariant for the twisted action. By Theorem 5.7 (ii) the coefficients of $\widetilde{\chi}_{a_P}(t)$ lie in the image of the Satake map $\mathcal{S}^G$. Since, by Theorem 5.7 (i), $\mathcal{S}^G$ is injective, there exists a unique polynomial

$$\chi_{a_P}(t) = \sum_{i=0}^{|W_0^M|} X_i \cdot t^i \in 1 + t\mathcal{H}_R(K,G)[t] \tag{5.11}$$

with $\sum_i \mathcal{S}^G(X_i) \cdot t^i = \widetilde{\chi}_{a_P}(t)$. (Note that $X_0 = 1$.) Explicitly, we have, for all $0 \le i \le |W_0^M|$,

$$\mathcal{S}^G(X_i) = (-1)^i \mu_U(-\lambda_P)^{-i} \cdot \sum_{\substack{J \subseteq W_0^M \\ |J|=i}} \prod_{w \in J} \mu_U\big(w(-\lambda_P)\big) \cdot e^{\sum_{w\in J} w(-\lambda_P)} \in R[\Lambda]. \tag{5.12}$$

Lemma 5.15. *One has*

$$\chi_{a_P}\big((a_P)_{K_P}\big) \coloneqq \sum_{i=0}^{|W_0^M|} (a_P)_{K_P}^i \cdot X_i \in \operatorname{Ker} \Theta_M^P.$$

Proof. By Lemma 5.4 we have $\mathcal{S}^M\big(\Theta_M^P((a_P)_{K_P})\big) = \Theta_Z^B\big((a_P)_{K_B}\big) = e^{\lambda_P}$, and the restriction of $\mathcal{S}^M \circ \Theta_M^P$ to $\mathcal{H}_R(K,G)$ coincides with $\mathcal{S}^G$. We compute

$$(\mathcal{S}^M \circ \Theta_M^P)\big(\chi_{a_P}((a_P)_{K_P})\big) = \sum_i e^{i\lambda_P} \cdot \mathcal{S}^G(X_i) = \widetilde{\chi}_{a_P}(e^{\lambda_P}) = 0.$$

Since by Theorem 5.7 (i) the map $\mathcal{S}^M$ is injective, the assertion follows. □

In order for the theory to work, one needs to assume the following strengthening of Lemma 5.15:

Hypothesis 5.16. *The element $(a_P)_{K_P}$ is a left root of $\chi_{a_P}(t)$, meaning that*

$$\chi_{a_P}\big((a_P)_{K_P}\big) = 0 \qquad \text{in } \mathcal{H}_R(K_P, P).$$

This hypothesis has been verified in many cases: Andrianov [1] essentially proved it for $G = \mathrm{Sp}_{2n}(\mathfrak{F})$ with P being the “Siegel parabolic”, i.e., the subgroup of matrices whose lower left quadrant is zero. Gritsenko then adapted the methods of Andrianov to prove it for $G = \mathrm{GL}_n(\mathfrak{F})$ and all parabolics [10, 12]. Finally, Gritsenko verified Hypothesis 5.16 for the classical groups $\mathrm{Sp}_{2n}(\mathfrak{F})$, $\mathrm{SU}_n(\mathfrak{F})$, and $\mathrm{SO}_n(\mathfrak{F})$, for the parabolics fixing a line in the standard representation, see [11].

The main contribution of this article is the verification of Hypothesis 5.16 for general connected reductive groups and *non-obtuse* parabolics, cf. Section 3. This covers, in particular, all the cases mentioned above.

Theorem 5.17. *Assume that* $\mathbf{P}$ *is non-obtuse. Then Hypothesis 5.16 holds true.*

Proof. Lemma 5.9 (iii) shows $C_P^+ \cap \operatorname{Ker} \Theta_M^P = \{0\}$. Hence, in view of Lemma 5.15, it suffices to prove $(a_P)_{K_P}^i X_i \in C_P^+$, for all $0 \leq i \leq |W_0^M|$.

Let i be arbitrary but fixed. Recall the explicit description (5.12). Note that $\sum_{w \in J} \nu(w(-\lambda_P)) \leq \nu(-i\lambda_P)$, where $J \subseteq W_0^M$ is such that $|J| = i$, see [4, Ch. VI, §1, no. 6, Prop. 18]. If we write

$$X_i = \sum_{j=1}^{n} c_j \cdot (z_j)_K \qquad \text{in } \mathcal{H}_R(K, G),$$

then this and (5.2) imply $\nu(z_j) \leq \nu(a_P^{-i})$, for all $1 \leq j \leq n$. In view of the Cartan decomposition 2.3 we may choose $z_j \in Z^-$.

By the Iwasawa decomposition 2.5 for G and the Cartan decomposition 2.3 for M, we have

$$G = KP = KU_P M = KU_P K_M Z^{+,M} K_M = KU_P Z^{+,M} K_M,$$

because K_M normalizes U_P. Therefore, we can write, for every j,

$$(z_j)_K = \sum_{l=1}^{n_j} c_{jl} \cdot (K u_{jl} z'_{jl} k_{jl}),$$

with $u_{jl} \in U_P$, $z'_{jl} \in Z^{+,M}$, and $k_{jl} \in K_M$. Note that $u_{jl} z'_{jl} \in K z_j K$, for all j, l.

Since $\mathbf{P}$ is non-obtuse, Theorem 4.4 implies $a_P^i u_{jl} a_P^{-i} \in K_P$, for all j, l. Now, since $a_P^i z'_{jl} k_{jl} \in M$, Lemma 5.9 (i) implies

$$(a_P)_{K_P}^i \cdot X_i = \sum_{j=1}^{n} \sum_{l=1}^{n_j} c_j c_{jl} \cdot (K_P a_P^i z'_{jl} k_{jl}) \in C_P^+. \qquad \square$$

Consider the submodules

$$\mathscr{O}_P^+ := C_P^+ . \mathcal{H}_R(K, G) := \left\{ \sum_i Y_i Z_i \,\middle|\, Y_i \in C_P^+,\ Z_i \in \mathcal{H}_R(K, G) \right\},$$
$$\mathscr{O}_P^- := \zeta_P(\mathscr{O}_P^+) = \mathcal{H}_R(K, G).C_P^-$$

of $\mathcal{H}_R(K_P, P)$. (Note that ζ_P preserves $\mathcal{H}_R(K, G)$ by Lemma 2.9.)

Definition 5.18. Assume that Hypothesis 5.16 is satisfied. For every $n \in \mathbb{Z}_{\geq 1}$ we define recursively the "negative powers" of $(a_P)_{K_P}$ as

$$(a_P)_{K_P}^{-n} := -\sum_{i=1}^{|W_0^M|} (a_P)_{K_P}^{i-n} \cdot X_i \in \mathscr{O}_P^+.$$

It should be noted that $(a_P)_{K_P}$ is not invertible in $\mathcal{H}_R(K_P, P)$. In fact, for $n > 1$, one even has $\big((a_P)_{K_P}^{-1}\big)^n \neq (a_P)_{K_P}^{-n}$. However, by a simple induction on d we have

$$(a_P)_{K_P}^n \cdot (a_P)_{K_P}^d = (a_P)_{K_P}^{n+d}, \qquad \text{for all } n \in \mathbb{Z}_{\geq 0} \text{ and } d \in \mathbb{Z}.$$

Example 5.19. Let us compute "negative powers" for $G = \mathrm{GL}_2(\mathfrak{F})$. The notations are the same as in Section 5.5. Choose the strictly positive element $a_B = \left(\begin{smallmatrix} \pi & 0 \\ 0 & 1 \end{smallmatrix}\right)$, so that $(a_B)_{K_B} = X_+$ in $\mathcal{H}_R(K_B, B)$. The polynomial

$$\begin{aligned} \widetilde{\chi}_{a_B}(t) &= (1 - x^{-1}t) \cdot (1 - (qy)^{-1}t) \\ &= 1 - \big(x^{-1} + (qy)^{-1}\big) \cdot t + (qxy)^{-1} \cdot t^2 \in R[x^{\pm 1}, y^{\pm 1}][t] \end{aligned}$$

annihilates $\Theta_Z^B\big((a_B)_{K_B}\big) = x$. We compute

$$\begin{aligned} \mathcal{S}^G\left(q^{-1}(\pi E_2)_K^{-1} \cdot \left(\begin{pmatrix} \pi & 0 \\ 0 & 1 \end{pmatrix}\right)_K\right) &= q^{-1} \cdot (xy)^{-1} \cdot (x + qy) \\ &= x^{-1} + (qy)^{-1} \\ \mathcal{S}^G\big(q^{-1}(\pi E_2)_K^{-1}\big) &= (qxy)^{-1}, \end{aligned}$$

and

$$\begin{aligned} \varepsilon_{B,G}\left(q^{-1} \cdot (\pi E_2)_K^{-1} \cdot \left(\begin{pmatrix} \pi & 0 \\ 0 & 1 \end{pmatrix}\right)_K\right) &= q^{-1}Y^{-1} \cdot (X_+ + X_- Y) \\ &= q^{-1} \cdot (X_+ Y^{-1} + X_-), \\ \varepsilon_{B,G}\big(q^{-1} \cdot (\pi E_2)_K^{-1}\big) &= q^{-1}Y^{-1}. \end{aligned}$$

Therefore,

$$\chi_{a_B}(t) = 1 - q^{-1} \cdot (X_+ Y^{-1} + X_-) \cdot t + q^{-1} Y^{-1} \cdot t^2.$$

It is clear that X_+ is a left root of $\chi_{a_B}(t)$. We compute

$$\begin{aligned}
X_+^{-1} &= q^{-1}\cdot(X_+Y^{-1}+X_-) - q^{-1}X_+Y^{-1}\\
&= q^{-1}X_-,\\
X_+^{-2} &= q^{-1}X_+^{-1}\cdot(X_+Y^{-1}+X_-) - q^{-1}Y^{-1}\\
&= q^{-2}X_-^2 + q^{-2}Y^{-1}(X_-X_+ - q\cdot 1)\\
X_+^{-3} &= q^{-1}X_+^{-2}(X_+Y^{-1}+X_-) - q^{-1}X_+^{-1}Y^{-1}\\
&= q^{-3}X_-^3 + q^{-3}(X_-X_+ - q\cdot 1)X_+Y^{-2} + q^{-3}X_-(X_-X_+ - q\cdot 1)Y^{-1}.
\end{aligned}$$

Recall from Lemma 5.9 (ii) that for every $X \in \mathscr{O}_P^+$ there exists $n > 0$ such that $(a_P)^n_{K_P}X \in C_P^+$. Using "negative powers" it is possible to reconstruct X from $(a_P)^n_{K_P}X$.

Lemma 5.20. *Assume that Hypothesis 5.16 is satisfied (for* $\mathbf{P}$*).*

(i) *For every* $X \in \mathcal{H}_R(K,G)$ *and every* $n \geq 0$ *with* $(a_P)^n_{K_P}X \in C_P^+$ *we have*

$$(a_P)^n_{K_P}\cdot X\cdot (a_P)^d_{K_P} = (a_P)^{n+d}_{K_P}\cdot X, \qquad \text{for all } d \in \mathbb{Z}.$$

(ii) *Let* $\mathbf{Q}$ *be a parabolic contained in* $\mathbf{P}$*. For every* $X \in \mathscr{O}_Q^+$ *we have, inside* $\mathcal{H}_R(K_Q,Q)$*,*

$$(a_P)^n_{K_P}\cdot X\cdot (a_P)^{-n}_{K_P} = X, \qquad \text{for all } n \gg 0.$$

Proof. (i). Let $X \in \mathcal{H}_R(K,G)$ and let $n \geq 0$ such that $(a_P)^n_{K_P}X \in C_P^+$. We prove the assertion by descending induction on d. If $d \geq 0$, this follows from the assumption that $(a_P)^n_{K_P}X$ centralizes $(a_P)_{K_P}$. Now assume $d < 0$. Since $\mathcal{H}_R(K,G)$ is commutative by Theorem 5.7, we compute

$$\begin{aligned}
(a_P)^n_{K_P}\cdot X\cdot (a_P)^d_{K_P} &= -\sum_{i=1}^{|W_0^M|}(a_P)^n_{K_P}\cdot X\cdot (a_P)^{i+d}_{K_P}\cdot X_i\\
&= -\sum_{i=1}^{|W_0^M|}(a_P)^{n+i+d}_{K_P}\cdot XX_i\\
&= \left(-\sum_{i=1}^{|W_0^M|}(a_P)^{n+i+d}_{K_P}X_i\right)\cdot X\\
&= (a_P)^{n+d}_{K_P}\cdot X,
\end{aligned}$$

where the second equality uses the induction hypothesis and the third that $\mathcal{H}_R(K,G)$ is commutative. This finishes the induction step.

(ii). Write $X = \sum_j Y_j Z_j$ with $Y_j \in C_Q^+$ and $Z_j \in \mathcal{H}_R(K,G)$. Choose $n \in \mathbb{Z}_{>0}$ such that $(a_P)_{K_P}^n Z_j \in C_P^+$ for all j. From Lemma 5.9 (i) applied to $\mathbf{Q}$, it follows easily that $(a_P)_{K_P}$ centralizes C_Q^+. Using (i), we compute

$$(a_P)_{K_P}^n \cdot X \cdot (a_P)_{K_P}^{-n} = \sum_j Y_j \cdot (a_P)_{K_P}^n Z_j (a_P)_{K_P}^{-n} = \sum_j Y_j Z_j = X. \qquad \square$$

We are now able to prove the following characterization of Hypothesis 5.16:

Proposition 5.21. *The following assertions are equivalent:*

(i) *Hypothesis 5.16 is satisfied.*
(ii) *If $X \in \mathscr{O}_P^+$ and $n \geq 0$ are such that $(a_P)_{K_P}^n X = 0$, then $X = 0$.*
(iii) $\mathscr{O}_P^+ \cap \operatorname{Ker} \Theta_M^P = \{0\}$.
(iv) *If $X \in \mathscr{O}_P^-$ and $n \geq 0$ are such that $X \cdot (a_P^{-1})_{K_P}^n = 0$, then $X = 0$.*
(v) $\mathscr{O}_P^- \cap \operatorname{Ker} \Theta_M^P = \{0\}$.

Proof. The equivalence (ii) $\iff$ (iv) follows from $\zeta_P(\mathscr{O}_P^+) = \mathscr{O}_P^-$, and (iii) $\iff$ (v) follows from $\zeta_P(\mathscr{O}_P^+) = \mathscr{O}_P^-$ and Lemma 5.11.

Since $\chi_{a_P}\big((a_P)_{K_P}\big) \in \mathscr{O}_P^+ \cap \operatorname{Ker} \Theta_M^P$ by Lemma 5.15, it follows that (iii) implies (i).

Assume that (i) holds. Let $X \in \mathscr{O}_P^+$ and $n \geq 0$ such that $(a_P)_{K_P}^n X = 0$. After possibly enlarging n, it follows from Lemma 5.20.(ii) that $X = (a_P)_{K_P}^n X (a_P)_{K_P}^{-n} = 0$, whence (ii).

Assume that (ii) holds. Let $X \in \mathscr{O}_P^+$ such that $\Theta_M^P(X) = 0$. By Lemma 5.9 (ii) there exists $n \geq 0$ such that $(a_P)_{K_P}^n X \in C_P^+$. But we also have $(a_P)_{K_P}^n X \in \operatorname{Ker} \Theta_M^P$, hence Lemma 5.9 (iii) implies $(a_P)_{K_P}^n X = 0$. By the assumption we deduce $X = 0$. This proves (iii). $\square$

Corollary 5.22. *Assume that Hypothesis 5.16 is satisfied. Then*

$$\mathcal{H}_R(K_P, P) = \mathscr{O}_P^+ \oplus \operatorname{Ker} \Theta_M^P = \mathscr{O}_P^- \oplus \operatorname{Ker} \Theta_M^P.$$

Proof. In view of Lemma 5.11 it suffices to prove the first equality. By Proposition 5.21 it remains to prove $\mathcal{H}_R(K_P, P) \subseteq \mathscr{O}_P^+ + \operatorname{Ker} \Theta_M^P$. So let $X \in \mathcal{H}_R(K_P, P)$ and choose $n \in \mathbb{Z}_{>0}$ such that $(a_P)_{K_P}^n X \in C_P^+$. Then $(a_P)_{K_P}^n X (a_P)_{K_P}^{-n} \in \mathscr{O}_P^+$ and $X - (a_P)_{K_P}^n X (a_P)_{K_P}^{-n} \in \operatorname{Ker} \Theta_M^P$. $\square$

The next result implies that it suffices to verify Hypothesis 5.16 for *maximal* parabolics only.

Proposition 5.23. *Let $\mathbf{Q}$ be another parabolic subgroup of $\mathbf{G}$ with Levi $\mathbf{L}$. Assume that Hypothesis 5.16 is satisfied for $\mathbf{P}$ and $\mathbf{Q}$. Then Hypothesis 5.16 is satisfied for $\mathbf{P} \cap \mathbf{Q}$.*

Proof. Let $a_Q \in Z$ be a strictly L-positive element. Then $a_{P\cap Q} \coloneqq a_P a_Q$ is strictly $L\cap M$-positive. The elements $(a_P)_{K_P}$ and $(a_Q)_{K_Q}$ commute inside $\mathcal{H}_R(K_{P\cap Q}, P\cap Q)$ and we have $(a_{P\cap Q})_{K_{P\cap Q}} = (a_P)_{K_P}(a_Q)_{K_Q}$ in $\mathcal{H}_R(K_{P\cap Q}, P\cap Q)$. Let $X \in \mathscr{O}^+_{P\cap Q}$ and $n \geq 0$ such that $(a_{P\cap Q})^n_{K_{P\cap Q}} X = 0$.

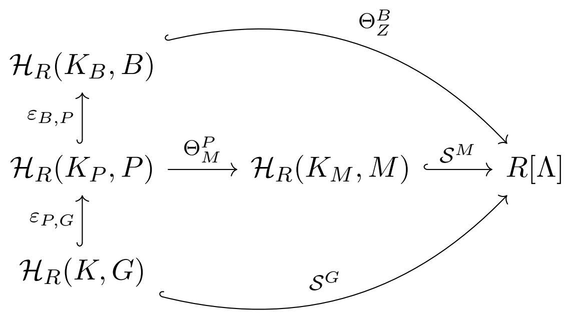
After enlarging n if necessary, Lemma 5.20.(ii) shows

$$\begin{aligned} 0 &= (a_{P\cap Q})^n_{K_{P\cap Q}} X \cdot (a_Q)^{-n}_{K_Q}(a_P)^{-n}_{K_P} \\ &= (a_P)^n_{K_P}(a_Q)^n_{K_Q} X \cdot (a_Q)^{-n}_{K_Q}(a_P)^{-n}_{K_P} \\ &= (a_P)^n_{K_P} X \cdot (a_P)^{-n}_{K_P} \\ &= X. \end{aligned}$$

The assertion now follows from "(ii) $\Longrightarrow$ (i)" in Proposition 5.21. ☐

Notation. If $\psi\colon A \to B$ is a homomorphism of R-algebras and $f(t) = \sum_i a_i t^i \in A[t]$ is a polynomial, we denote $f^\psi(t) \coloneqq \sum_i \psi(a_i)t^i \in B[t]$ the polynomial obtained by applying ψ to the coefficients of $f(t)$.

We now prove the decomposition theorem for Hecke polynomials. Recall the following commutative diagram:



Theorem 5.24 (Decomposition Theorem)**.** *Assume that Hypothesis 5.16 holds true. Let $d(t) \in \mathcal{H}_R(K,G)[t]$ be a polynomial and assume that there is a decomposition*

$$d^{\mathcal{S}^G}(t) = \widetilde{f}(t)\cdot\widetilde{g}(t) \qquad \textit{in } R[\Lambda][t],$$

such that one of the following properties is satisfied:

(a) *$\widetilde{f}(t)$ has coefficients in $(\mathcal{S}^M \circ \Theta^P_M)(C^+_P)$ with constant term 1, or*
(b) *$\widetilde{g}(t)$ has coefficients in $(\mathcal{S}^M \circ \Theta^P_M)(C^-_P)$ with constant term 1.*

Then there exist polynomials $f(t), g(t) \in \mathcal{H}_R(K_P, P)[t]$ such that

$$\begin{aligned} \deg f(t) &= \deg \widetilde{f}(t), & f^{\mathcal{S}^M\circ\Theta^P_M}(t) &= \widetilde{f}(t), \\ \deg g(t) &= \deg \widetilde{g}(t), & g^{\mathcal{S}^M\circ\Theta^P_M}(t) &= \widetilde{g}(t), \end{aligned}$$

and

$$d(t) = f(t)\cdot g(t) \quad \textit{in } \mathcal{H}_R(K_P, P)[t].$$

Proof. Note that $\Theta_Z^B|_{\mathcal{H}_R(K_P,P)} = \mathcal{S}^M \circ \Theta_M^P$ and $\Theta_Z^B|_{\mathcal{H}_R(K,G)} = \mathcal{S}^G$.

Assume that (a) is satisfied. The case (b) is completely analogous. By Proposition 5.21 the restriction of Θ_M^P to $\mathscr{O}_P^+$ is injective. As $\mathcal{S}^M$ is injective by Theorem 5.7, it follows that the restriction of Θ_Z^B to $\mathscr{O}_P^+$ is injective. By the assumption there exists a unique polynomial $f(t) \in C_P^+[t]$ satisfying $f^{\Theta_Z^B}(t) = \widetilde{f}(t)$. Its constant term is necessarily 1, and hence there exists a power series $h(t) = \sum_{i=0}^{\infty} h_i t^i \in C_P^+[\![t]\!]$ with $h(t) \cdot f(t) = f(t) \cdot h(t) = 1$. Now, set

$$g(t) \coloneqq h(t) \cdot d(t) \in \mathscr{O}_P^+[\![t]\!].$$

Then $g^{\Theta_Z^B}(t) = h^{\Theta_Z^B}(t) \cdot d^{\Theta_Z^B}(t) = h^{\Theta_Z^B}(t) \cdot \widetilde{f}(t) \cdot \widetilde{g}(t) = \widetilde{g}(t)$. As the restriction of Θ_Z^B to $\mathscr{O}_P^+$ is injective, it follows that $g(t)$ is a polynomial of degree $\deg \widetilde{g}(t)$. Moreover, we have $f(t) \cdot g(t) = f(t) \cdot h(t) \cdot d(t) = d(t)$ in $\mathcal{H}_R(K_P, P)[t]$. □

Remark 5.25. Suppose we are in the situation of Theorem 5.24.

- (i) The polynomial $d^{\mathcal{S}_M^G}(t)$ decomposes in $\mathcal{H}_R(K_M, M)[t]$.
- (ii) In case (a) the proof shows that one can choose $f(t) \in C_P^+[t]$ and $g(t) \in \mathscr{O}_P^+[t]$. Since, by Proposition 5.21, the restriction of Θ_M^P to $\mathscr{O}_P^+$ is injective, it follows that $f(t)$ and $g(t)$ are unique with these properties.
- (iii) Similarly, in case (b) one can choose $f(t) \in \mathscr{O}_P^-[t]$ and $g(t) \in C_P^-[t]$, and both polynomials are unique with these properties.

We draw some consequences of Theorem 5.24, cf. also [1, Thm. 6.2 and Cor.].

Corollary 5.26. *Assume that Hypothesis 5.16 holds true.*

- (i) *Let $f(t) \in C_P^+[t]$ be a polynomial with constant term* 1*. Then there exists a polynomial $g(t) \in \mathcal{H}_R(K_P, P)[t]$ with constant term* 1 *and $\deg g(t) \leq \deg f(t) \cdot \big(|W_0^M| - 1\big)$ such that*

$$f(t) \cdot g(t) \in \mathcal{H}_R(K, G)[t].$$

- (ii) *Let $X \in C_P^+$. Then there exists a monic polynomial $d(t) = \sum_i d_i t^i \in \mathcal{H}_R(K, G)[t]$ such that $\deg d(t) \leq |W_0^M|$ and*

$$\sum_i X^i d_i = 0.$$

- (i′) *Let $g(t) \in C_P^-[t]$ be a polynomial with constant term* 1*. Then there exists a polynomial $f(t) \in \mathcal{H}_R(K_P, P)[t]$ with constant term* 1 *and $\deg f(t) \leq \deg g(t) \cdot \big(|W_0^M| - 1\big)$ such that*

$$f(t) \cdot g(t) \in \mathcal{H}_R(K, G)[t].$$

(ii′) *Let* $X \in C_P^-$. *Then there exists a monic polynomial* $d(t) = \sum_i d_i t^i \in \mathcal{H}_R(K,G)[t]$ *such that* $\deg d(t) \leq |W_0^M|$ *and*

$$\sum_i d_i X^i = 0.$$

Proof. Note that, using the anti-automorphism ζ_P on $\mathcal{H}_R(K_P,P)$, which on $\mathcal{H}_R(K,G)$ restricts to ζ_G by Lemma 2.9, one can easily deduce (i′) and (ii′) from (i) and (ii), respectively.

Let us prove (i). So let $f(t)$ be a polynomial with coefficients in C_P^+ and constant term 1. Write $f^{\Theta_Z^B}(t) =: \widetilde{f}(t) = \sum_i f_i t^i \in R[\Lambda][t]$. Since we have $\mathcal{S}^M \circ \Theta_M^P = \Theta_Z^B \circ \varepsilon_{B,P}$ by Lemma 5.4, the coefficients of $\widetilde{f}(t)$ lie in $\mathcal{S}^M(\mathcal{H}_R(K_M,M))$. Hence, the coefficients of $\widetilde{f}(t)$ are invariant under the twisted action of $W_{0,M}$. Given $w \in W_0$, write $\widetilde{f}^w(t) = \sum_i (w \star f_i) \cdot t^i$. The polynomial $\widetilde{d}(t) := \prod_{w \in W_0^M} \widetilde{f}^w(t)$ is then W_0-invariant with respect to the twisted action and hence has coefficients in $\mathcal{S}^G(\mathcal{H}_R(K,G))$. Moreover, it factors as $\widetilde{d}(t) = \widetilde{f}(t) \cdot \widetilde{g}(t)$ for some $\widetilde{g}(t) \in R[\Lambda][t]$ with constant term 1 and $\widetilde{g}(t) \leq \deg f(t) \cdot (|W_0^M| - 1)$. The existence of the polynomial $g(t)$ with the desired properties now follows from Theorem 5.24.

We now prove (ii). Let $X \in C_P^+$. Applying (i) to the polynomial $f(t) := 1 - Xt$, we find a polynomial $g(t) = \sum_{i=0}^{r-1} g_i t^i \in \mathcal{H}_R(K_P,P)[t]$ with $g_0 = 1$ and $r \leq |W_0^M|$ and such that

$$f(t) \cdot g(t) =: \sum_{i=0}^{r} d_{r-i} t^i \in \mathcal{H}_R(K,G)[t].$$

Since $f(t) \cdot g(t) = 1 + \sum_{i=1}^{r-1} (g_i - X g_{i-1}) t^i - X g_{r-1} t^r$, a comparison of coefficients shows that $d_0 = -X g_{r-1}$, $d_i = g_{r-i} - X g_{r-(i+1)}$ for $1 \leq i \leq r-1$, and $d_r = g_0 = 1$. Therefore, the polynomial $\sum_{i=0}^{r} d_i t^i \in \mathcal{H}_R(K,G)[t]$ is monic, of degree $r \leq |W_0^M|$, and satisfies

$$\sum_{i=0}^{r} X^i d_i = -X g_{r-1} + \sum_{i=1}^{r-1} \big(X^i g_{r-i} - X^{i+1} g_{r-(i+1)}\big) + X^r = 0. \qquad \square$$

Example 5.27. We continue Example 5.19 and apply Theorem 5.24 to the polynomial

$$\chi_{a_B}(t) = 1 - q^{-1} \cdot (X_+ Y^{-1} + X_-) \cdot t + q^{-1} Y^{-1} t^2 \in \mathcal{H}_R(K,G)[t].$$

Then $\chi_{a_B}^{\mathcal{S}^G}(t) = 1 - \big((qy)^{-1} + x^{-1}\big) \cdot t + (qxy)^{-1} t^2$ decomposes in $R[x^{\pm 1}, y^{\pm 1}][t]$ as $\widetilde{f}(t) \cdot \widetilde{g}(t)$ with $\widetilde{f}(t) = 1 - (qy)^{-1} t$ and $\widetilde{g}(t) = 1 - x^{-1} t$. Then $f(t) := 1 - q^{-1} X_+ Y^{-1} t \in C_P^+[t]$ is the unique polynomial with $f^{\Theta_Z^B}(t) = \widetilde{f}(t)$. Let

$h(t) := \sum_{i=0}^{\infty}(q^{-1}X_+Y^{-1})^i t^i \in C_B^+[\![t]\!]$ be the inverse power series. Then

$$\begin{aligned} g(t) &:= h(t)\cdot\chi_{a_B}(t) \\ &= \underbrace{h(t) - h(t)\cdot q^{-1}X_+Y^{-1}t}_{=1} - h(t)q^{-1}X_-t + h(t)\cdot q^{-1}Y^{-1}t^2 \\ &= 1 - q^{-1}X_-t - \sum_{i=1}^{\infty}(q^{-1}X_+Y^{-1})^{i-1}\cdot q^{-1}Y^{-1}t^{i+1} \\ &\quad + \sum_{i=0}^{\infty}(q^{-1}X_+Y^{-1})^{i}\cdot q^{-1}Y^{-1}t^{i+2} \\ &= 1 - q^{-1}X_-t. \end{aligned}$$

Hence, $\chi_{a_B}(t)$ decomposes in $\mathcal{H}_R(K_B,B)[t]$ as

$$\chi_{a_B}(t) = (1 - q^{-1}X_+Y^{-1}t)\cdot(1 - q^{-1}X_-t).$$

Appendix A. Proof of Theorem 5.13

Let $B \subseteq \mathrm{GL}_2(\mathfrak{F})$ be the subgroup of upper triangular matrices and let K_B be the subgroup of B with entries in $\mathcal{O}_{\mathfrak{F}}$. Fix a uniformizer $\pi \in \mathcal{O}_{\mathfrak{F}}$ and recall that q denotes the cardinality of the residue field of $\mathfrak{F}$. Let R be a coefficient ring.

We describe the R-algebra $\mathcal{H}_R(K_B,B) = R\otimes_{\mathbb{Z}}\mathcal{H}(K_B,B)$ in terms of generators and relations. As $R\otimes_{\mathbb{Z}} -$ is right exact, we may reduce to the case $R=\mathbb{Z}$.

First, we need to understand the double cosets of B with respect to K_B. Let A be a complete system of representatives for $\mathcal{O}_{\mathfrak{F}}/(\pi)$ with $0\in A$. Then $A_B := \{\sum_{i=1}^{n} a_i\pi^{-i} \mid n\in\mathbb{Z}_{>0}, a_i\in A\}$ is a complete system of representatives for $\mathfrak{F}/\mathcal{O}_{\mathfrak{F}}$.

Lemma A.1. *As a set B decomposes as*

$$B = \bigsqcup_{\substack{a,b,c\in\mathbb{Z},\\ b\le\min\{a,c\}}} K_B\begin{pmatrix}\pi^a & \pi^b\\ 0 & \pi^c\end{pmatrix}K_B,$$

and for all $a,b,c\in\mathbb{Z}$ with $b\le\min\{a,c\}$ one has the decomposition

$$K_B\begin{pmatrix}\pi^a & \pi^b\\ 0 & \pi^c\end{pmatrix}K_B = \begin{cases}\bigsqcup_{\substack{\beta\in A_B\pi^c,\\ \mathrm{val}_{\mathfrak{F}}(\beta)=b}} K_B\begin{pmatrix}\pi^a & \beta\\ 0 & \pi^c\end{pmatrix}, & \text{if } b<\min\{a,c\};\\ \bigsqcup_{\substack{\beta\in A_B\pi^c,\\ \mathrm{val}_{\mathfrak{F}}(\beta)\ge a}} K_B\begin{pmatrix}\pi^a & \beta\\ 0 & \pi^c\end{pmatrix}, & \text{if } b=\min\{a,c\}.\end{cases}$$

Proof. Let $\left(\begin{smallmatrix}\alpha & \beta\\ 0 & \gamma\end{smallmatrix}\right)\in B$. Write $\alpha=\alpha_0\pi^a$ and $\gamma=\gamma_0\pi^c$, where $\alpha_0,\gamma_0\in\mathcal{O}_{\mathfrak{F}}^{\times}$, $a,c\in\mathbb{Z}$, and write $\frac{\beta}{\alpha_0\pi^c}=\beta'+x$, with $\beta'\in A_B$ and $x\in\mathcal{O}_{\mathfrak{F}}$. Then $\beta'=0$

or $\mathrm{val}_{\mathfrak{F}}(\beta) = \mathrm{val}_{\mathfrak{F}}(\beta'\pi^c)$. Moreover,

$$\begin{pmatrix} \alpha & \beta \\ 0 & \gamma \end{pmatrix} = \begin{pmatrix} \alpha_0 & \alpha_0 x \\ 0 & \gamma_0 \end{pmatrix} \cdot \begin{pmatrix} \pi^a & \beta'\pi^c \\ 0 & \pi^c \end{pmatrix} \in K_B \begin{pmatrix} \pi^a & \beta'\pi^c \\ 0 & \pi^c \end{pmatrix}.$$

Let now $a, a', c, c' \in \mathbb{Z}$ and $\beta, \beta' \in A_B$ with

$$\begin{pmatrix} \pi^a & \beta\pi^c \\ 0 & \pi^c \end{pmatrix} \cdot \begin{pmatrix} \pi^{a'} & \beta'\pi^{c'} \\ 0 & \pi^{c'} \end{pmatrix}^{-1} = \begin{pmatrix} \pi^{a-a'} & \beta\pi^{c-c'} - \beta'\pi^{a-a'} \\ 0 & \pi^{c-c'} \end{pmatrix} \in K_B.$$

Then $a = a'$ and $c = c'$, and then $\beta - \beta' \in \mathcal{O}_{\mathfrak{F}}$, that is, $\beta = \beta'$. This shows that B is the disjoint union of the right cosets $K_B\left(\begin{smallmatrix} \pi^a & \beta\pi^c \\ 0 & \pi^c \end{smallmatrix}\right)$, where $a, c \in \mathbb{Z}$ and $\beta \in A_B$.

Let now $a, c \in \mathbb{Z}$. Take any $0 \neq \beta = \beta_0 \pi^{\mathrm{val}_{\mathfrak{F}}(\beta)} \in A_B \pi^c$ with $\beta_0 \in \mathcal{O}_{\mathfrak{F}}^{\times}$. If $\mathrm{val}_{\mathfrak{F}}(\beta) < \min\{a, c\}$, then

$$\begin{pmatrix} \pi^a & \beta \\ 0 & \pi^c \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & \beta_0^{-1} \end{pmatrix} \cdot \begin{pmatrix} \pi^a & \pi^{\mathrm{val}_{\mathfrak{F}}(\beta)} \\ 0 & \pi^c \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & \beta_0 \end{pmatrix} \in K_B \begin{pmatrix} \pi^a & \pi^{\mathrm{val}_{\mathfrak{F}}(\beta)} \\ 0 & \pi^c \end{pmatrix} K_B.$$

If $\mathrm{val}_{\mathfrak{F}}(\beta) \geq \min\{a, c\}$, then $\mathrm{val}_{\mathfrak{F}}(\beta) \geq a$, because $\mathrm{val}_{\mathfrak{F}}(\beta) < c$ always holds true. Hence,

$$\begin{pmatrix} \pi^a & \beta \\ 0 & \pi^c \end{pmatrix} = \begin{pmatrix} \pi^a & 0 \\ 0 & \pi^c \end{pmatrix} \cdot \begin{pmatrix} 1 & \beta\pi^{-a} \\ 0 & 1 \end{pmatrix} \in K_B \begin{pmatrix} \pi^a & 0 \\ 0 & \pi^c \end{pmatrix} K_B.$$

The lemma follows. $\square$

We now prove Theorem 5.13. Let $\mathcal{H}$ be the $\mathbb{Z}$-algebra generated by the variables X_+, X_-, Y, and Y^{-1}, subject to the relations (5.6). This means that Y is central and invertible and we have $X_+ X_- = q \cdot 1$ in $\mathcal{H}$. We show that

$$\begin{aligned} \rho\colon \mathcal{H} &\longrightarrow \mathcal{H}(K_B, B), \\ X_+ &\longmapsto \left(\begin{pmatrix} \pi & 0 \\ 0 & 1 \end{pmatrix}\right)_{K_B}, \\ X_- &\longmapsto \left(\begin{pmatrix} \pi^{-1} & 0 \\ 0 & 1 \end{pmatrix}\right)_{K_B}, \\ Y &\longmapsto (\pi E_2)_{K_B} \end{aligned}$$

gives a well-defined isomorphism of algebras.

It is clear that (K_B) is the unit in $\mathcal{H}(K_B, B)$, and that $(\pi E_2)_{K_B}$ is central and invertible with inverse $(\pi^{-1} E_2)_{K_B}$. In addition, using Lemma A.1, we compute

$$\left(\begin{pmatrix}\pi & 0\\ 0 & 1\end{pmatrix}\right)_{K_B} \cdot \left(\begin{pmatrix}\pi^{-1} & 0\\ 0 & 1\end{pmatrix}\right)_{K_B} = \left(K_B\begin{pmatrix}\pi & 0\\ 0 & 1\end{pmatrix}\right) \cdot \sum_{\beta\in A}\left(K_B\begin{pmatrix}\pi^{-1} & \beta\pi^{-1}\\ 0 & 1\end{pmatrix}\right)$$
$$= \sum_{\beta\in A}\left(K_B\begin{pmatrix}1 & \beta\\ 0 & 1\end{pmatrix}\right) = q\cdot(K_B).$$

Therefore, ρ is a well-defined algebra homomorphism.

Observe that $\rho(X_+^m) = ((\begin{smallmatrix}\pi^m & 0\\ 0 & 1\end{smallmatrix}))_{K_B}$ and $\rho(Y^k) = (\pi^k E_2)_{K_B}$, for all $m \in \mathbb{Z}_{\geq 0}$ and $k \in \mathbb{Z}$. For each $n \in \mathbb{Z}_{\geq 0}$ we compute

$$\rho(X_-^n) = \rho(X_-)^n = \left(\sum_{\beta\in A}\left(K_B\begin{pmatrix}\pi^{-1} & \beta\pi^{-1}\\ 0 & 1\end{pmatrix}\right)\right)^n$$
$$= \sum_{\beta_1,\dots,\beta_n\in A}\left(K_B\begin{pmatrix}\pi^{-n} & \sum_{i=1}^n\beta_i\pi^{-i}\\ 0 & 1\end{pmatrix}\right) = \left(\begin{pmatrix}\pi^{-n} & 0\\ 0 & 1\end{pmatrix}\right)_{K_B}.$$

Given $m, n \in \mathbb{Z}_{\geq 0}$ and $k \in \mathbb{Z}$, this shows

$$\rho(X_-^n X_+^m Y^k) = \left(\begin{pmatrix}\pi^{-n} & 0\\ 0 & 1\end{pmatrix}\right)_{K_B} \cdot \left(\begin{pmatrix}\pi^{m} & 0\\ 0 & 1\end{pmatrix}\right)_{K_B} \cdot (\pi^k E_2)_{K_B}$$
$$= \sum_{\beta_1,\dots,\beta_n\in A}\left(K_B\begin{pmatrix}\pi^{m+k-n} & \pi^k\sum_{i=1}^n\beta_i\pi^{-i}\\ 0 & \pi^k\end{pmatrix}\right)$$
$$= \sum_{b=k-n}^{\min\{k,m+k-n\}}\left(\begin{pmatrix}\pi^{m+k-n} & \pi^b\\ 0 & \pi^k\end{pmatrix}\right)_{K_B}.$$

For $m, n \in \mathbb{Z}_{\geq 1}$ and $k \in \mathbb{Z}$ this implies

$$\rho\big(X_-^n X_+^m Y^k - X_-^{n-1}X_+^{m-1}Y^k\big) = \left(\begin{pmatrix}\pi^{m+k-n} & \pi^{k-n}\\ 0 & \pi^k\end{pmatrix}\right)_{K_B}.$$

Now notice that

$$\text{(A.1)}\quad \left\{X_+^m Y^k \,\middle|\, m\in\mathbb{Z}_{\geq 0}, k\in\mathbb{Z}\right\} \cup \left\{X_-^n Y^k \,\middle|\, n\in\mathbb{Z}_{\geq 1}, k\in\mathbb{Z}\right\}$$
$$\cup \left\{X_-^n X_+^m Y^k - X_-^{n-1}X_+^{m-1}Y^k \,\middle|\, m,n\in\mathbb{Z}_{\geq 1}, k\in\mathbb{Z}\right\}$$

generates $\mathcal{H}$ as a $\mathbb{Z}$-module and identifies via ρ with the double coset basis of $\mathcal{H}(K_B, B)$. It follows that (A.1) is in fact $\mathbb{Z}$-linearly independent, hence a $\mathbb{Z}$-basis of $\mathcal{H}$. Consequently, ρ is an isomorphism.

References

[1] A. N. Andrianov, "On factorization of Hecke polynomials for the symplectic groups of genus n", *Math. USSR, Sb.* **33** (1977), no. 3, p. 343-373.

[2] ———, "The multiplicative arithmetic or Siegel modular forms", *Russ. Math. Surv.* **34** (1979), no. 1, p. 75-148.

[3] A. N. ANDRIANOV & V. G. ZHURAVLEV, *Modular Forms and Hecke Operators*, Translations of Mathematical Monographs, vol. 145, American Mathematical Society, 1995.

[4] N. BOURBAKI, *Groupes et algèbres de lie: Chapitres 4, 5 et 6*, Éléments de Mathématiques, Masson, 1981.

[5] F. BRUHAT & J. TITS, "Groupes réductifs sur un corps local. I: Données radicielles valuées", *Publ. Math., Inst. Hautes Étud. Sci.* **41** (1972), p. 5-251.

[6] ———, "Groupes réductifs sur un corps local. II: Schémas en groupes. Existence d'une donnée radicielle valuée", *Publ. Math., Inst. Hautes Étud. Sci.* **60** (1984), p. 5-184.

[7] C. J. BUSHNELL & P. C. KUTZKO, "Smooth representations of reductive p-adic groups: structure theory via types", *Proc. Lond. Math. Soc.* **77** (1998), no. 3, p. 582-634.

[8] R. DĄBROWSKI, "Comparison of the Bruhat and the Iwahori decompositions of a p-Adic Chevalley group", *J. Algebra* **167** (1994), no. 3, p. 704-723.

[9] V. A. GRITSENKO, "The action of modular operators on the Fourier–Jacobi coefficients of modular forms", *Math. USSR, Sb.* **47** (1984), no. 1, p. 237-268.

[10] ———, "Parabolic extensions of a Hecke ring of the general linear group", *J. Sov. Math.* **43** (1988), no. 4, p. 2533-2540.

[11] ———, "Expansion of Hecke polynomials of classical groups", *Math. USSR, Sb.* **65** (1990), no. 2, p. 333-356.

[12] ———, "Parabolic extensions of the Hecke ring of the general linear group. II", *J. Sov. Math.* **62** (1992), no. 4, p. 2869-2882.

[13] T. J. HAINES & S. ROSTAMI, "The Satake isomorphism for special maximal parahoric Hecke algebras", *Represent. Theory* **14** (2010), p. 264-284.

[14] G. HENNIART & M.-F. VIGNÉRAS, "A Satake isomorphism for representations modulo p of reductive groups over local fields", *J. Reine Angew. Math.* **701** (2015), p. 33-75.

[15] F. HERZIG, "A Satake isomorphism in characteristic p", *Compos. Math.* **147** (2011), no. 1, p. 263-283.

[16] C. HEYER, "Applications of parabolic Hecke algebras: parabolic induction and Hecke polynomials", PhD Thesis, Humboldt-Universität zu Berlin, 2019.

[17] ———, "Localization of the Parabolic Hecke Algebra at a Strictly Positive Element", `https://arxiv.org/abs/2103.16949`, 2021.

[18] ———, "Parabolic induction via the parabolic pro-p Iwahori–Hecke algebra", *Represent. Theory* **25** (2021), p. 807-843.

[19] J. E. HUMPHREYS, *Reflection groups and coxeter groups*, Cambridge Studies in Advanced Mathematics, vol. 29, Cambridge University Press, 1990.

[20] F. JANUSZEWSKI, "On p-adic L-functions for $\mathrm{GL}(n)\times\mathrm{GL}(n-1)$ over totally real fields", *Int. Math. Res. Not.* **2015** (2015), no. 17, p. 7884-7949.

[21] J. M. LANSKY, "Decomposition of double cosets in p-adic groups", *Pac. J. Math.* **197** (2001), no. 1, p. 97-117.

[22] I. G. MACDONALD, *Spherical functions on a group of p-adic type*, Publ. Ramanujan Inst., vol. 2, 1971.

[23] ———, *Affine Hecke algebras and orthogonal polynomials*, Cambridge Tracts in Mathematics, vol. 157, Cambridge University Press, 2003.

[24] M. RAPOPORT, "A positivity property of the Satake isomorphism", *Manuscr. Math.* **101** (2000), no. 2, p. 153-166.

[25] P. SCHNEIDER & U. STUHLER, "Representation theory and sheaves on the Bruhat-Tits building", *Publ. Math., Inst. Hautes Étud. Sci.* **85** (1997), no. 1, p. 97-191.

[26] M. VIENNEY, "Construction de (φ,γ)-modules en caractéristique p", PhD Thesis, École normale supérieure de Lyon – ENS LYON, 2012.

[27] M.-F. VIGNÉRAS, *Représentations l-modulaires d'un groupe réductif p-adique avec* $l\neq p$, Progress in Mathematics, vol. 137, Birkhäuser, 1996.

[28] M.-F. VIGNERAS, "The pro-p Iwahori Hecke algebra of a reductive p-adic group I", *Compos. Math.* **152** (2016), no. 4, p. 693-753.

Claudius Heyer
Einsteinstraße 62, 48149 Münster, Germany
E-mail: cheyer@uni-muenster.de
URL: https://claudius-heyer.github.io