Bad primes and Cyclotomic Root Systems

Michel Broué

Université Paris-Diderot Paris 7

July 4th, 2016

A joint work with Ruth Corran and Jean Michel

Bad primes

Let V be an r-dimensional $\mathbb{Q}$-vector space, let W be an irreducible finite subgroup of $\mathrm{GL}(V)$ generated by reflections – thus $\mathbb{G} := (V, W)$ is a rational "reflection datum" (and W is a Weyl group !).

$*$ We denote by $\mathfrak{R}$ a root system for W in V, by $Q(\mathfrak{R})$ the corresponding *root lattice* and by $P(\mathfrak{R})$ the corresponding *weight lattice*. The *connection index* is $c_{\mathfrak{R}} := |P(\mathfrak{R})/Q(\mathfrak{R})|$.

$*$ We recall that there exists a finite set $\mathrm{UnCh}(\mathbb{G})$ (*"unipotent characters for* $\mathbb{G}$*"*) and a family of polynomials $(\mathrm{Deg}_\rho(X))_{\rho\in\mathrm{UnCh}(\mathbb{G})})$ (*"generic degrees for* $\mathbb{G}$*"*) such that

- $\mathrm{Deg}_\rho(X) \in \mathbb{Q}[X]$,
- If we set $S_\rho(X) := |\mathbb{G}|(X)/\mathrm{Deg}_\rho(X)$ (the *Schur element of* ρ), then $S_\rho(X) \in \mathbb{Z}[X]$,

which satisfy the following property (and a lot of other properties as well!)

[Genericity of unipotent characters]

- Whenever q is a prime power, $\mathbb{F}_q$ is a field with q elements, $\overline{\mathbb{F}}_q$ is an algebraic closure of $\mathbb{F}_q$,
- and $\mathbf{G}$ is a connected algebraic group over $\overline{\mathbb{F}}_q$ with Weyl group W endowed with a Frobenius endomorphism F inducing a split $\mathbb{F}_q$-rational structure on $\mathbf{G}$,

the set $\mathrm{UnCh}(\mathbb{G})$ parametrizes the set of unipotent characters of the finite reductive group $\mathbf{G}^F$, *via* a bijection

$$\rho \mapsto \rho_q \text{ such that } \mathrm{Deg}_\rho(q) = \rho_q(1)\,.$$

Let ℓ be a prime. The following are equivalent.

[BAD PRIMES FROM ROOT SYSTEMS]

(i) If $(v_1, \dots, v_r)$ is a set of simple roots for $\mathfrak{R}$ and $n_1 v_1 + \cdots + n_r v_r$ is the corresponding highest root, then ℓ divides $n_1 \cdots n_r$.

(ii) The prime ℓ divides $|W|/(r! c_{\mathfrak{R}})$.

(iii) There is a reflection subgroup W_1 of W of rank r, a root system $\mathfrak{R}$ for W, and a root system $\mathfrak{R}_1$ for W_1 with $Q(\mathfrak{R}_1) \subset Q(\mathfrak{R})$ such that ℓ divides $|Q(\mathfrak{R})/Q(\mathfrak{R}_1)|$.

[BAD PRIMES FROM GENERIC DEGREES]

(iv) There exists $\rho \in \mathrm{UnCh}(\mathbb{G})$ such that ℓ divides $S_\rho(X)$.

(v) There exists $\rho \in \mathrm{UnCh}(\mathbb{G})$ and an integer n such that $\Phi_{n\ell}(X)$ divides $S_\rho(x)$ while $\Phi_n(X)$ does not divide $S_\rho(X)$.

Spetses

1993 : Gunter Malle, Jean Michel, Michel B.,

from 2010 $+ \epsilon$: Olivier Dudas, Cédric Bonnafé.

AIM: Do whatever was done for Weyl groups replacing them by a *spetsial* complex reflection group, *i.e.*, choose

* an abelian number field k, and a finite dimensional k vector space V,
* a (pseudo-)reflection "spetsial" finite subgroup W of $\mathrm{GL}(V)$,
* and set $\mathbb{G} := (V, W)$.

It turned out it is possible to construct $\mathrm{UnCh}(\mathbb{G})$ and the family $\mathrm{Deg}_\rho(X) \in k[X]$, such that $S_\rho(X) := |\mathbb{G}|(X)/\mathrm{Deg}_\rho(X) \in \mathbb{Z}_k[X]$, and satisfying many (many) features of what was known in the case of Weyl groups.

$\mathfrak{R}$, $c_{\mathfrak{R}}$, etc. remained to be done...

Root systems and Weyl groups: Bourbaki's definition

Let V and $V^\vee$ be finite dimensional $\mathbb{Q}$-vector spaces endowed with a duality $V \times V^\vee \to \mathbb{Q}\,,\ ,\ (v, v^\vee) \mapsto \langle v, v^\vee \rangle\,.$

Let $\mathfrak{R} := \{(\alpha, \alpha^\vee)\} \subset V \times V^\vee$ be a family of nonzero vectors. We say that $\mathfrak{R}$ is a *root system* if

(RS1) $\mathfrak{R}$ is finite and its projection on V generates V,

(RS2) if $(\alpha, \alpha^\vee) \in \mathfrak{R}$, then $\langle \alpha, \alpha^\vee \rangle = 2$ and the reflection $s_{\alpha,\alpha^\vee} : v \mapsto v - \langle v, \alpha^\vee \rangle \alpha$ stabilizes $\mathfrak{R}$,

(RS3) if $(\alpha, \alpha^\vee)$ and $(\beta, \beta^\vee) \in \mathfrak{R}$, then $\langle \alpha, \beta^\vee \rangle \in \mathbb{Z}$.

The group generated by all reflections $s_{\alpha,\alpha^\vee}$ is the *Weyl group* $W(\mathfrak{R})$.

On can classify first the root systems $\mathfrak{R}$, and then classify the Weyl groups $W(\mathfrak{R})$ (the usual approach). Or proceed the opposite way: it's what we did for cyclotomic root systems and their (cyclotomic) Weyl groups.

Complex (or, rather, cyclotomic) reflection groups

Let k be a subfield of $\mathbb{C}$ which is stable under complex conjugation.

Let V and $V^\vee$ be finite dimensional k-vector spaces endowed with a hermitian duality $V \times V^\vee \to k$.

A reflection s on V is defined by a triple (L_s, M_s, ζ_s) where

- $\zeta_s \in \boldsymbol{\mu}(k)$,
- L_s is a line in V and M_s is a line in $V^\vee$ such that $\langle L_s, M_s \rangle \neq 0$

and s is the automorphism of V defined by

$$s(v) = v - \langle v, \alpha^\vee \rangle \alpha$$

whenever $\alpha \in L_s$ and $\alpha^\vee \in M_s$ are such that $\langle \alpha, \alpha^\vee \rangle = 1 - \zeta_s$.

Shephard–Todd groups and their fields

IRREDUCIBLE CYCLOTOMIC REFLECTION GROUPS ARE CLASSIFIED.

- An infinite series $G(de, e, r)$ for $d, e, r \in \mathbb{N} - \{0\}$,

  $$G(de, e, r) \subset \mathrm{GL}_r(\mathbb{Q}(\zeta_{de})) \text{ is irreducible}$$

  $\to$ except for $d = e = r = 1$ or 2.

  $$\text{Its field of definition is } \mathbb{Q}(\zeta_{de}),$$

  $\to$ except for $d = 1$ and $r = 2$ where it is the real field $\mathbb{Q}(\zeta_e + \zeta_e^{-1})$.

  $$\text{The ring of integers of } \mathbb{Q}(\zeta_n) \text{ is } \mathbb{Z}[\zeta_n].$$

  In general (for example if $n > 90$, but also for other values of n between 22 and 90) it is *not* a principal ideal domain.

- 34 exceptional irreducible groups in dimension 2 to 8.

  Their field of definition (which are all subfields of "small" cyclotomic fields) have the remarkable property that all their rings of integers are principal ideal domains.

Ordinary (Weyl) Root systems

Let us repeat Bourbaki's definition of root systems.

Let V and $V^\vee$ be finite dimensional $\mathbb{Q}$-vector spaces endowed with a duality $V \times V^\vee \to \mathbb{Q}$.

Let $\mathfrak{R} := \{(\alpha, \alpha^\vee)\} \subset V \times V^\vee$ be a family of nonzero vectors.

We say that $\mathfrak{R}$ is a root system if

(RS1) $\mathfrak{R}$ is finite and its projection on V generates V,

(RS2) for all $(\alpha, \alpha^\vee) \in \mathfrak{R}$, $\langle \alpha, \alpha^\vee \rangle = 2$ and the reflection $s_{\alpha,\alpha^\vee} : v \mapsto v - \langle v, \alpha^\vee \rangle \alpha$ stabilizes $\mathfrak{R}$,

(RS3) for all $(\alpha, \alpha^\vee), (\beta, \beta^\vee) \in \mathfrak{R}$, $\langle \alpha, \beta^\vee \rangle \in \mathbb{Z}$.

$\mathbb{Z}_k$–Root Systems

[A plain generalization of Bourbaki's definition]

It is a set of triples $\mathfrak{R} = \{\mathfrak{r} = (I_\mathfrak{r}, J_\mathfrak{r}, \zeta_\mathfrak{r})\}$ where

- $\zeta_\mathfrak{r} \in \boldsymbol{\mu}(k)$,
- $I_\mathfrak{r}$ is a rank one $\mathbb{Z}_k$-submodule of V, and $J_\mathfrak{r}$ is a rank one $\mathbb{Z}_k$-submodule of $V^\vee$,

such that

(RS1) the family $(I_\mathfrak{r})$ generates V,

(RS2) $\langle I_\mathfrak{r}, J_\mathfrak{r} \rangle = (1 - \zeta_\mathfrak{r})\mathbb{Z}_k$, and if $\sum_i \langle \alpha_i, \beta_i \rangle = 1 - \zeta_\mathfrak{r}$, then the reflection

$$s_\mathfrak{r} : v \mapsto v - \sum_i \langle v, \beta_i \rangle \alpha_i$$

stabilizes $\mathfrak{R}$,

(RS3) whenever $\mathfrak{r}, \mathfrak{r}' \in \mathfrak{R}$, $\langle I_\mathfrak{r}, J_{\mathfrak{r}'} \rangle \subset \mathbb{Z}_k$.

$\mathbb{Z}_k$-Root Systems (continued)

$\mathrm{GL}(V)$ acts on root systems : $g \cdot (I, J, \zeta) := (g(I), g^\vee(J), \zeta)$.

If $\mathfrak{a}$ is a fractional ideal in k, we set $\mathfrak{a} \cdot (I, J, \zeta) := (\mathfrak{a}I, \mathfrak{a}^{-*}J, \zeta)$.

Theorem

(1) Given a $\mathbb{Z}_k$-root system $\mathfrak{R}$, the group $W(\mathfrak{R}) := \langle s_\mathfrak{r} \rangle_{\mathfrak{r} \in \mathfrak{R}}$ is finite and $V^{W(\mathfrak{R})} = 0$.

(2) Conversely, whenever W is a finite subgroup of $\mathrm{GL}(V)$ generated by reflections such that $V^W = 0$, there exists a $\mathbb{Z}_k$-root system $\mathfrak{R}$ such that $W = W(\mathfrak{R})$.

From now on

We only consider *restricted* $\mathbb{Z}_k$-root systems $\mathfrak{R}$, *i.e.*, such that the map $\mathfrak{r} \mapsto s_\mathfrak{r}$ is a bijection between $\mathfrak{R}$ and the set of *distinguished* reflections of $W(\mathfrak{R})$.

Cartan matrices

- For $\mathfrak{r}, \mathfrak{t} \in \mathfrak{R}$, we set $\mathfrak{n}(\mathfrak{r}, \mathfrak{t}) := \langle I_\mathfrak{r}, J_\mathfrak{t} \rangle$.
- For a subset $\mathcal{S}$ of $\mathfrak{R}$, its *Cartan matrix* is the $\mathcal{S} \times \mathcal{S}$-matrix whose entries are the ideals $\mathfrak{n}(\mathfrak{r}, \mathfrak{t})$.

Proposition

Assume that the family $(s_\mathfrak{r})_{\mathfrak{r} \in \mathcal{S}}$ generates $W(\mathfrak{R})$, and contains an element of each conjugacy class of reflections of $W(\mathfrak{R})$. Then the Cartan matrix of $\mathcal{S}$ determines $\mathfrak{R}$ up to genera.

Classification

For each irreducible reflection group W, we provide a classification (up to genera),

over its ring of definition $\mathbb{Z}_k$,

of restricted root systems for all irreducible complex reflection groups.

Genera, Root and Weight Lattices

Root lattices, weight lattices:

$$Q(\mathfrak{R}) := \sum_{\mathfrak{r}\in\mathfrak{R}} I_{\mathfrak{r}} \quad \text{and} \quad Q(\mathfrak{R}^\vee) := \sum_{\mathfrak{r}\in\mathfrak{R}} J_{\mathfrak{r}}$$

$$P(\mathfrak{R}) := \{x \in V \mid \forall y \in Q(\mathfrak{R}^\vee)\,,\ \langle x, y\rangle \in \mathbb{Z}_k\} \quad \text{and} \quad P(\mathfrak{R}^\vee) := \ldots$$

There is a $\mathrm{Aut}(\mathfrak{R})/W(\mathfrak{R})$-invariant natural pairing

$$(P(\mathfrak{R})/Q(\mathfrak{R})) \times (P(\mathfrak{R}^\vee)/Q(\mathfrak{R}^\vee)) \to k/\mathbb{Z}_k\,.$$

Theorem

Assume that $\Pi \in \mathfrak{R}$ is such that $|\Pi| = r$ and $\{s_{\mathfrak{r}} \mid \mathfrak{r} \in \Pi\}$ generates $W(\mathfrak{R})$. Then

$$Q(\mathfrak{R}) = \bigoplus_{\mathfrak{r}\in\Pi} I_{\mathfrak{r}} \quad \text{and} \quad Q(\mathfrak{R}^\vee) = \bigoplus_{\mathfrak{r}\in\Pi} J_{\mathfrak{r}}\,.$$

Connection index

For W a Weyl group and $\mathfrak{R}$ an associated root system, the connection index is the integer $c_{\mathfrak{R}}$ defined as

$$c_{\mathfrak{R}} := |P(\mathfrak{R})/Q(\mathfrak{R})| .$$

For W any reflection group, the connection index of an associated root system $\mathfrak{R}$ is defined to be the ideal $\mathfrak{c}_{\mathfrak{R}}$ of $\mathbb{Z}_k$ defined by the equality

$$\Lambda^r Q(\mathfrak{R}) = \mathfrak{c}_{\mathfrak{R}} \Lambda^r P(\mathfrak{R}) .$$

Theorem

Let (V, W) be an irreducible reflection group of rank r.

1. The ideal $c_{\mathfrak{R}}$ does not depend on the choice of the root system $\mathfrak{R}$.
2. The ideal $(r!)c_{\mathfrak{R}}$ divides $|W|$ (in $\mathbb{Z}_k$).

Spetsial groups

Spetsial groups in red.

$G(e,1,r), G(e,e,r)$, and

Group G_n	4	5	6	7	8	9	10	11	12	13	14	15	16
Rank	2	2	2	2	2	2	2	2	2	2	2	2	2

Group G_n	17	18	19	20	21	22	23	24	25	26	27
Rank	2	2	2	2	2	2	3	3	3	3	3
Remark							H_3				

Group G_n	28	29	30	31	32	33	34	35	36	37
Rank	4	4	4	4	4	5	6	6	7	8
Remark	F_4		H_4					E_6	E_7	E_8

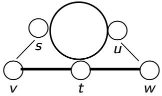
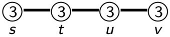
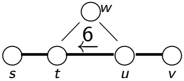
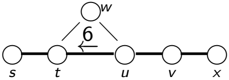
Bad primes for spetsial groups

Theorem (or should it be called "fact" ?)

Let $\mathbb{G} := (V, W)$ where W is a spetsial group of rank r.
Let ℓ be a prime ideal in $\mathbb{Z}_k$.
The following assertions are equivalent.

(i) The ideal ℓ divides $|W|/((r!)c_{\mathfrak{R}})$ (in $\mathbb{Z}_k$).

(ii) There exists $\rho \in \mathrm{UnCh}(\mathbb{G})$ such that the ideal ℓ divides $S_\rho(X)$ (in $\mathbb{Z}_k[X]$).

Name	Diagram	Cartan matrix	Orbits	$\mathbb{Z}_k$	connection index
G_{31}		$\begin{pmatrix} 2 & i+1 & 1-i & -i & 0 \\ 1-i & 2 & 1-i & -1 & -1 \\ i+1 & i+1 & 2 & 0 & -1 \\ i & -1 & 0 & 2 & 0 \\ 0 & -1 & -1 & 0 & 2 \end{pmatrix}$	s	$\mathbb{Z}[i]$	1
G_{32}		$\begin{pmatrix} 1-\zeta_3 & \zeta_3^2 & 0 & 0 \\ -\zeta_3^2 & 1-\zeta_3 & \zeta_3^2 & 0 \\ 0 & -\zeta_3^2 & 1-\zeta_3 & \zeta_3^2 \\ 0 & 0 & -\zeta_3^2 & 1-\zeta_3 \end{pmatrix}$	s	$\mathbb{Z}[\zeta_3]$	1
G_{33}		$\begin{pmatrix} 2 & -1 & 0 & 0 & 0 \\ -1 & 2 & -1 & -\zeta_3^2 & 0 \\ 0 & -1 & 2 & -1 & 0 \\ 0 & -\zeta_3 & -1 & 2 & -1 \\ 0 & 0 & 0 & -1 & 2 \end{pmatrix}$	s	$\mathbb{Z}[\zeta_3]$	2
G_{34}		$\begin{pmatrix} 2 & -1 & 0 & 0 & 0 & 0 \\ -1 & 2 & -1 & -\zeta_3^2 & 0 & 0 \\ 0 & -1 & 2 & -1 & 0 & 0 \\ 0 & -\zeta_3 & -1 & 2 & -1 & 0 \\ 0 & 0 & 0 & -1 & 2 & -1 \\ 0 & 0 & 0 & 0 & -1 & 2 \end{pmatrix}$	s	$\mathbb{Z}[\zeta_3]$	1