Modelling algebraic and finite reductive groups on a computer

Frank Lübeck
Lehrstuhl D für Mathematik, RWTH Aachen

ICTS Bangalore, Oct 14-23, 2019

Prototype examples of connected reductive groups: $G = \mathrm{SL}_n(K)$ or $G = \mathrm{GL}_n(K)$

K: algebraically closed field (here usually $K = \bar{\mathbb{F}}_p$)

T: diagonal matrices in G (a maximal torus $\cong (K^\times)^n$)

B: upper triangular matrices in G (a Borel subgroup, solvable)

U_{ij}, $1 \le i, j \le n$, $i \ne j$: subgroup $\{u_{ij}(a) = 1 + aE_{ij} \mid a \in K\} \cong K^+$ (a root subgroup, for $t = \mathrm{diag}(t_1, \dots, t_n) \in T$ we have $u_{ij}(a)^t = u_{ij}(t_j t_i^{-1} a)$)

$U := \langle U_{ij} \mid i < j \rangle \lhd B$ (unipotent radical of B)

N: the normalizer $N_G(T)$ = subgroup of monomial matrices

$W = N/T$: this is $\cong S_n$, the symmetric group (the Weyl group of G)

We have

- $G = \langle T, U_{i,j} \mid i, j \rangle$, ($G = \langle U_{i,j} \rangle$ in case SL),
- $B = T \ltimes U$ and $T = B \cap N$,
- $\mathrm{SL}_2(K) \twoheadrightarrow \langle U_{ij}, U_{ji} \rangle$ for $i \ne j$,
- $G = \bigcup_{w \in W} B\dot{w}B$ (Bruhat decomposition).

Roots, coroots and Weyl group

$T \cong (K^\times)^r$: a maximal torus of G

$X = \mathrm{Hom}(T, K^\times) = \{x : T \to K^\times, (t_1, \ldots, t_r) \mapsto t_1^{a_1} \cdots t_r^{a_r} \mid a_i \in \mathbb{Z}\}$

(character group of T)

$Y = \mathrm{Hom}(K^\times, T) = \{y : K^\times \to T, t \mapsto (t^{a_1}, \ldots, t^{a_r}) \mid a_i \in \mathbb{Z}\}$

(cocharacter group of T)

$X \cong \mathbb{Z}^r$, $Y \cong \mathbb{Z}^r$, dual via $\langle \cdot, \cdot \rangle : X \times Y \to \mathbb{Z}$ $\quad (\langle x, y \rangle = k$ if $x \circ y : t \mapsto t^k)$

For root subgroup write $U_\alpha = \{u_\alpha(a) \mid a \in K\}$ if $\alpha \in X$ with

$t^{-1} u_\alpha(a) t = u_\alpha(\alpha(t) a)$ for all $t \in T$

For U_α restrict $\mathrm{SL}_2(K) \twoheadrightarrow \langle U_\alpha, U_{-\alpha} \rangle$ to $\mathrm{diag}(t^{-1}, t)$ to find $\alpha^\vee \in Y$

Yields set of roots $\Phi \subset X$ and corresponding coroots $\Phi^\vee \subset Y$ of G

$\Delta \subset \Phi$ set of simple roots if linearly independent and $\Phi \subset \pm \mathbb{Z}_{\geq 0} \Delta$

For $\alpha \in \Phi$ set $s_\alpha : X \to X, x \mapsto x - \langle x, \alpha^\vee \rangle \alpha$ (reflection on X)

Weyl group $W \cong \langle s_\alpha \mid \alpha \in \Delta \rangle$ as Coxeter group

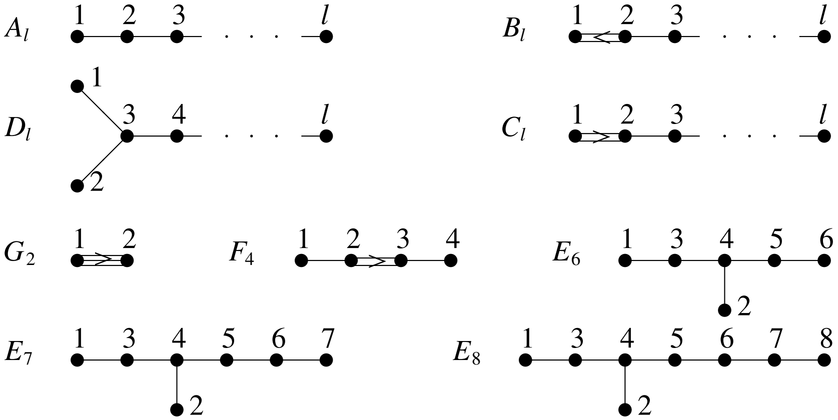
Root data

Let $X \cong \mathbb{Z}^r \cong Y$ in duality via $\langle \cdot, \cdot \rangle : X \times Y \to \mathbb{Z}$.

Let $\Delta = \{\alpha_1, \ldots \alpha_l\} \subset X$ and $\Delta^\vee = \{\alpha_1^\vee, \ldots, \alpha_l^\vee\} \subset Y$.

Definition. $(\Delta, \Delta^\vee)$ is called a root datum, if and only if $C = (\langle \alpha_j, \alpha_i^\vee \rangle)_{1 \leq i, j \leq l}$ is the Cartan matrix of a finite root system.

That is, after possible reordering, C is block diagonal with blocks described by diagrams



Diagonal entries of C are 2 and if nodes i, j are connected by k bonds the $C_{i,j}$ and $C_{j,i}$ are -1 and $-k$.

Root data

Let $X \cong \mathbb{Z}^r \cong Y$ in duality via $\langle \cdot, \cdot \rangle : X \times Y \to \mathbb{Z}$.

Let $\Delta = \{\alpha_1, \ldots \alpha_l\} \subset X$ and $\Delta^\vee = \{\alpha_1^\vee, \ldots, \alpha_l^\vee\} \subset Y$.

Definition. $(\Delta, \Delta^\vee)$ is called a root datum, if and only if $C = (\langle \alpha_j, \alpha_i^\vee \rangle)_{1 \leq i, j \leq l}$ is the Cartan matrix of a finite root system.

From root datum compute generating matrices of $W = \{s_\alpha \mid \alpha \in \Delta\}$. Compute all roots Φ and coroots $\Phi^\vee$ as W-orbits of simple roots and coroots. This yields $(X, \Phi, Y, \Phi^\vee)$ which often occurs as "root datum" in the literature.

Existence- and Isomorphism Theorem [Chevalley, Steinberg]: Each root datum comes from a connected reductive group G over any $K = \bar{K}$.

The root datum determines a presentation of G over any K.

Examples of root data

We write elements of Δ and $\Delta^\vee$ in rows of matrices with respect to dual bases of X and Y.

$G = \mathrm{GL}_n(K)$ yields root datum

$$\Delta = \begin{pmatrix} -1 & 1 & & & & \\ & -1 & 1 & & & \\ & & \dots & \dots & & \\ & & & & -1 & 1 \end{pmatrix} = \Delta^\vee$$

and $G = \mathrm{SL}_n(K)$ yields root datum

$$\Delta = \begin{pmatrix} -1 & 1 & & & \\ & -1 & 1 & & \\ & & \dots & \dots & \\ & & & -1 & 1 \\ -1 & -1 & -1 & -1 & -2 \end{pmatrix}, \quad \Delta^\vee = \begin{pmatrix} -1 & 1 & & & \\ & -1 & 1 & & \\ & & \dots & \dots & \\ & & & -1 & 1 \\ & & & & -1 \end{pmatrix}$$

Both yield the same Cartan matrix of type A_l:

$$C = \Delta^\vee \Delta^{tr} = \left(\begin{array}{rrrrr} 2 & -1 & 0 & 0 & 0 \\ -1 & 2 & -1 & 0 & 0 \\ & \dots & \dots & & \\ 0 & 0 & 0 & -1 & 2 \end{array} \right)$$

Frobenius morphisms

From now p is a prime and $K = \bar{\mathbb{F}}_p$, G is a linear algebraic group over K.

For any power q of p define $F_q : \mathrm{GL}_n(K) \to \mathrm{GL}_n(K)$, $(a_{ij}) \mapsto (a_{ij}^q)$.

Definition. A morphism $F : G \to G$ is a Frobenius morphism if there is a q and $\phi : G \hookrightarrow \mathrm{GL}_n(K)$ such that for some power e and all $g \in G$ we have $\phi(F^e(g)) = F_{q^e}(\phi(g))$.

If $q = p^f$ is an integer we say that G is defined over $\mathbb{F}_q$ via F.

The group of fixed points $G^F = G(q) = \{g \in G \mid F(g) = g\}$ is finite.

Definition. If G is a connected reductive group with Frobenius morphism F, then G^F is called a finite group of Lie type.

Examples. $G = \mathrm{GL}_n(\bar{\mathbb{F}}_q)$, $F = F_q$, then $G^F = \mathrm{GL}_n(q)$.
$G = \mathrm{SL}_n(\bar{\mathbb{F}}_q)$, $F(A) := F_q(A^{-tr})$, then $G^F = \mathrm{SU}_n(q)$. $G = F_4(\bar{\mathbb{F}}_2)$, $m \in \mathbb{N}$, there is F with $F^2 = F_{2^{2m+1}}$ and $G^F = {}^2F_4(2^{2m+1})$ are the large Ree groups.

Root datum with F-action

G: connected reductive with Frobenius morphism F
T: maximal torus with $F(T) = T$.

F induces a map on X (via $F(x)(t) = x(F(t))$ for $t \in T$) of form qF_0 with an automorphism F_0 of finite order. When $q \in \mathbb{Z}$ then $F_0(\Phi) = \Phi$, and for the dual map on Y we have $F_0^{tr}(\Phi^\vee) = \Phi^\vee$.

Vice versa, given such F_0 and a p-power q there is a corresponding Frobenius morphism of G fixing T (unique up to inner automorphism, isogeny theorem).

$F_0(\Delta)$ is also a set of simple roots, there is unique $w \in W$ with $F_0(\Delta w) = \Delta$. So wF_0 induces a permutation of Δ (a graph automorphism of the Dynkin diagram).

Definition. A triple $(\Delta, \Delta^\vee, F_0)$ with $F_0 \in \mathbb{Z}^{r\times r}$ of finite order is a root datum with Frobenius action if $(\Delta, \Delta^\vee)$ represents a root datum, and $\Phi F_0 = \Phi$, $\Phi^\vee F_0^{tr} = \Phi^\vee$.

Theorem. A root datum with Frobenius action defines for every prime power q a finite group of Lie type $G(q)$ (unique up to isomorphism).

Definition. Fix a root datum with Frobenius action. Then the set of corresponding groups $\{G(q) \mid q \text{ a prime power}\}$ is called a series of groups of Lie type. (These are infinitely many groups for each prime p.)

Example $G = GL_n(K)$: $F = F_q$ yields $F_0 = \mathrm{id}$, then $G(q) = \mathrm{GL}_n(q)$.
$F : G \to G$, $g \mapsto F_q(g^{-tr})$ yields $F_0 = -\mathrm{id}$, then $G(q) = \mathrm{GU}_n(q)$.

Computing with torus elements

$\bar{\mathbb{F}}_p^\times \cong (\mathbb{Q}/\mathbb{Z})_{p'}^+ \cong \mu_{p'}$ (roots of unity of p'-order in $\mathbb{C}$)

$\zeta_{q-1} \mapsto \frac{1}{q-1}(\pmod{\mathbb{Z}}) \mapsto \exp(2\pi i/(q-1)$ for certain primitive roots ζ_{q-1}

Then $T \cong Y \otimes_{\mathbb{Z}} \bar{\mathbb{F}}_p^\times \cong Y \otimes_{\mathbb{Z}} (\mathbb{Q}/\mathbb{Z})_{p'} \cong (\mathbb{Q}/\mathbb{Z})_{p'})^r$

On $t \in T = (\mathbb{Q}/\mathbb{Z})_{p'})^r$ (row "vector") the actions of $x \in X$, F and $w \in W$ on t can be written as matrix multiplication:

$x(t) = t x^{tr}$, $F(t) = t(q F_0)$, $t^w = t w_X$ where w_X is the action matrix of w on X.