An introduction to arithmetic groups

(via group schemes)

Steffen Kionke

FernUniversität in Hagen

25.06.2020

Content

- First definition of arithmetic groups
- Group schemes
- Definition of arithmetic groups via group schemes

Examples of arithmetic groups

a. $\mathrm{SL}_n(\mathbb{Z})$

b. $\mathrm{SL}_n(\mathbb{Z}[\sqrt{-5}])$

c. $H_3(\mathbb{Z}) = \{ \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} \mid x, y, z \in \mathbb{Z}\}$

d. $U(p,q)(\mathbb{Z}) = \{g \in \mathrm{GL}_n(\mathbb{Z}[i]) \mid \overline{g}^T I_{p,q} g = I_{p,q}\}$

e. The unit group $\Lambda^\times$

where Λ is the ring

$$\Lambda = \mathbb{Z} \oplus i\mathbb{Z} \oplus j\mathbb{Z} \oplus ij\mathbb{Z} \quad \text{with} \quad i^2 = 2,\ j^2 = 5,\ ij = -ji.$$

Examples of arithmetic groups

- a $\mathrm{SL}_n(\mathbb{Z}) \quad \subseteq \mathrm{SL}_n(\mathbb{R})$
- b $\mathrm{SL}_n(\mathbb{Z}[\sqrt{-5}]) \quad \subseteq \mathrm{SL}_n(\mathbb{C})$
- c $H_3(\mathbb{Z}) = \{ \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} \mid x, y, z \in \mathbb{Z}\} \quad \subseteq H_3(\mathbb{R})$
- d $U(p,q)(\mathbb{Z}) = \{g \in \mathrm{GL}_n(\mathbb{Z}[i]) \mid \overline{g}^T I_{p,q} g = I_{p,q}\} \quad \subseteq U(p,q)$
- e The unit group $\Lambda^\times \quad \subseteq \mathrm{GL}_2(\mathbb{R})$

  where Λ is the ring

  $$\Lambda = \mathbb{Z} \oplus i\mathbb{Z} \oplus j\mathbb{Z} \oplus ij\mathbb{Z} \quad \text{with} \quad i^2 = 2,\ j^2 = 5,\ ij = -ji.$$

A first definition

Definition:

Let $G \subseteq \mathrm{GL}_n(\mathbb{C})$ be a Zariski closed subgroup defined over $\mathbb{Q}$. vanishing set of polynomial with $\mathbb{Q}$ coeff.

An arithmetic subgroup of G is a subgroup

$$\Gamma \subseteq G \cap \mathrm{GL}_n(\mathbb{Q})$$

which is *commensurable* to $G \cap \mathrm{GL}_n(\mathbb{Z})$.

$A = \Gamma$

$B = G \cap GL(\mathbb{Z})$

commensurable: $A, B \leq H$ commensurable

if $A \cap B$ has finite index in A, B

Group schemes

R: commutative unital ring

$\underline{\mathrm{Alg}}_R$: Category of commutative R-algebras

Definition: An affine group scheme (of finite type over R) is a covariant functor

$$G\colon \underline{\mathrm{Alg}}_R \to \underline{\mathrm{Grp}} \qquad A \mapsto G(A)$$

Group schemes

R: commutative unital ring

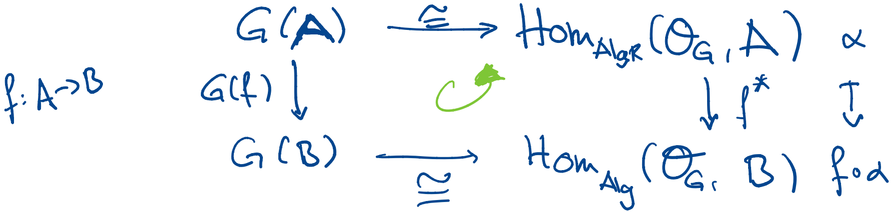
$\underline{\mathrm{Alg}}_R$: Category of commutative R-algebras

Definition: An affine group scheme (of finite type over R) is a covariant functor

$$G \colon \underline{\mathrm{Alg}}_R \to \underline{\mathrm{Grp}}$$

which is *representable* by a finitely generated R-algebra $\mathcal{O}_G$,

i.e., there is a natural equivalence $G \to \mathrm{Hom}_{\underline{\mathrm{Alg}}_R}(\mathcal{O}_G, \cdot)$.* as functors sets



Examples

(1) The additive group $\mathbb{G}_a$ (over R):

$$\mathbb{G}_a \colon A \mapsto (A, +)$$

Representable?

$$\mathcal{O}_{\mathbb{G}_a} = R[T]$$

$$\begin{aligned} \mathrm{Hom}_{\mathrm{Alg}_R}(R[T], A) &\xrightarrow{\cong} A \\ \alpha &\mapsto \alpha(T) \end{aligned}$$

Examples

(2) The multiplicative group $\mathbb{G}_m$ (over R):

$$\mathbb{G}_m \colon A \mapsto (A^\times, \cdot)$$

Representable?

$$\mathcal{O}_{\mathbb{G}_m} = R[T, T^{-1}]$$

$$\mathrm{Hom}_{\mathrm{Alg}_R}(R[T, T^{-1}], A) \longrightarrow A^\times$$

$$\alpha \mapsto \alpha(T)$$

Examples

(3) The special linear group SL_n (over R):

$$\mathrm{SL}_n \colon A \mapsto \mathrm{SL}_n(A)$$

Representable?

$$\mathcal{O}_{SL_n} = R[T_{ij} \mid i,j \in \{1,\dots,n\}] \big/ (\det((T_{ij})) - 1)$$

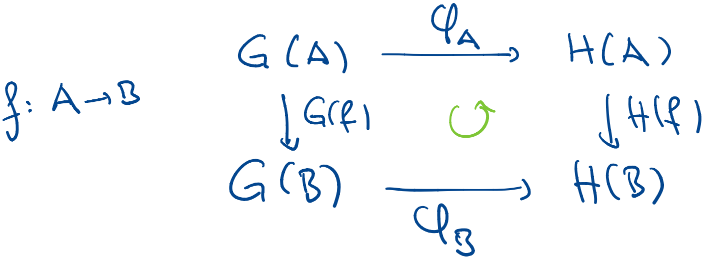
$$\mathrm{Hom}_{\mathrm{Alg}_R}(\mathcal{O}_{SL_n}, A) \longrightarrow SL_n(A)$$

$$\alpha \longmapsto (\alpha(T_{ij}))_{ij}$$

Homomorphisms of group schemes

G, H affine group schemes over R.

Definition: A homomorphism $\varphi\colon G \to H$ is a natural transformation of functors.



Fact: [Yoneda's lemma] $\varphi^* : \mathcal{O}_H \longrightarrow \mathcal{O}_G$

$$\varphi_A : G(A) \cong \mathrm{Hom}(\mathcal{O}_G, A) \longrightarrow \mathrm{Hom}(\mathcal{O}_H, A) \cong H(A)$$

$$\alpha \mapsto \alpha \circ \varphi^*$$

Example

$$\varphi\colon \mathbb{G}_m \to \mathrm{SL}_2$$

$$\varphi_A\colon A^\times \to \mathrm{SL}_2(A) \quad \text{with} \quad a \mapsto \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$$

On coordinate rings?

$$R[T_{11}, T_{22}, T_{12}, T_{21}] / (T_{11}T_{22} - T_{12}T_{21} - 1) \longrightarrow R[T, T^{-1}]$$

$$T_{11} \longmapsto T$$

$$T_{22} \longmapsto T^{-1}$$

$$T_{12}, T_{21} \longmapsto 0$$

Coordinates

G an affine group scheme.

Definition:

A set of coordinates is an ordered tuple $c = (t_1, \ldots, t_n)$ of elements of $\mathcal{O}_G$ such that $t_1, \ldots, t_n$ generate $\mathcal{O}_G$.

$$R[T_1, \ldots, T_n]/I_c \xrightarrow{\cong} \mathcal{O}_G$$

$$T_i \longmapsto t_i$$

Coordinate map:

$$\psi_{c,A} \colon G(A) \xrightarrow{\cong} \mathrm{Hom}_{\underline{\mathrm{Alg}}_R}(\mathcal{O}_G, A) \xrightarrow{\cong} V_A(I_c) \subseteq A^n$$

$$\alpha \qquad (\alpha(t_1), \ldots, \alpha(t_n))$$

$$V_A(I_c) = \{(a_1, \ldots, a_n) \in A^n \mid f(a_1 \ldots a_n) = 0 \text{ for all } f \in I_c\}$$

$\mathcal{O}_G$ is a Hopf algebra

Comultiplication:

$$\Delta\colon \mathcal{O}_G \to \mathcal{O}_G \otimes_R \mathcal{O}_G$$

Coinversion:

$$I\colon \mathcal{O}_G \to \mathcal{O}_G$$

Counit:

$$\varepsilon\colon \mathcal{O} \to R$$

Satisfy axioms dual to the group axioms, e.g.,

left inverse

$$\begin{array}{ccc} G(A) & \xrightarrow{(\text{inv}, \text{id})} & G(A) \times G(A) \\ \downarrow & & \downarrow \text{mult} \\ \{1\} & \longrightarrow & G(A) \end{array} \qquad \begin{array}{ccc} \mathcal{O}_G & \xleftarrow{(I, \text{id})} & \mathcal{O}_G \otimes_R \mathcal{O}_G \\ \uparrow & & \uparrow \Delta \\ R & \xleftarrow[\varepsilon]{} & \mathcal{O}_G \end{array}$$

The counit of a group scheme

The counit of G is the homomorphism $\varepsilon\colon \mathcal{O}_G \to R$ corresponding to the unit $1 \in G(R)$ via

$$G(R) \xrightarrow{\cong} \mathrm{Hom}_{\underline{\mathrm{Alg}}_R}(\mathcal{O}_G, R).$$

$$1 \longmapsto \varepsilon$$

Every R-algebra A is equipped with the *structure morphism*

$$\iota\colon R \to A$$

Usually $\iota \circ \varepsilon$ is also called *counit* and denoted by ε.

$$\begin{array}{ccccc} 1 & G(R) & \xrightarrow{G(\iota)} & G(A) & 1 \\ & \cong\uparrow & & \uparrow\cong & \\ & \mathrm{Hom}(\mathcal{O}_G, R) & \longrightarrow & \mathrm{Hom}(\mathcal{O}_G, A) & \\ & \varepsilon & & \iota\circ\varepsilon & = \varepsilon \end{array}$$

Extension of scalars

affine

G a group scheme over R.

$\mathbb{Z} \subseteq \mathbb{Q}$

$R \subseteq S$ a ring extension.

Observation:

The functor

$$E_{S/R}(G)\colon \underline{\mathrm{Alg}}_S \to \underline{\mathrm{Grp}}$$
$$E_{S/R}(G)(A) = G(A|_R)$$

consider A as R-algebra

is an affine group scheme over S.

$$\mathcal{O}_{E_{S/R}(G)} = S \otimes_R \mathcal{O}_G$$

Linear algebraic groups

K a field.

Definition:

A linear algebraic group over K is an affine group scheme over K such that $\mathcal{O}_G$ has no nilpotent elements.

„$\mathcal{O}_G$ is reduced"

Remark: $\mathrm{char}(K) = 0 \implies$ the ring $\mathcal{O}_G$ is reduced.

Integral forms & arithmetic groups

Let G be a linear algebraic group over $\mathbb{Q}$.

Definition:

An integral form of G is a group scheme G_0 over $\mathbb{Z}$ with an isomorphism

$$E_{\mathbb{Q}/\mathbb{Z}}(G_0) \cong G.$$

Definition:

A subgroup $\Gamma \subseteq G(\mathbb{Q})$ is arithmetic if it is commensurable to $G_0(\mathbb{Z})$ for some integral form G_0 of G.

An example

Quaternion algebra:

$$D = (2, 5 \mid \mathbb{Q}) = \mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}ij$$

with $i^2 = 2$, $j^2 = 5$, $ij = -ji$.

Linear algebraic group over $\mathbb{Q}$:

$$G(A) = (A \otimes_{\mathbb{Q}} D)^{\times}$$

Exercise: check that this is a group scheme.

An example

Quaternion algebra:

$$D = (2, 5 |\ \mathbb{Q}) = \mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}ij$$

with $i^2 = 2$, $j^2 = 5$, $ij = -ji$.

Linear algebraic group over $\mathbb{Q}$:

$$G(A) = (A \otimes_{\mathbb{Q}} D)^{\times}$$

Integral form:

$\mathbb{Q} \otimes_{\mathbb{Z}} \Lambda \cong D$

$$\Lambda = \mathbb{Z} \oplus i\mathbb{Z} \oplus j\mathbb{Z} \oplus ij\mathbb{Z}$$

$$G_0(A) = (A \otimes_{\mathbb{Z}} \Lambda)^{\times}$$

$G_0(\mathbb{Z}) = \Lambda^{\times}$ is an arithetic subgroup of $D^{\times}$

Relation to first definition?

Fact:

Let G be a linear algebraic group over K. There is a "closed embedding" $G \hookrightarrow \mathrm{GL}_n$.

$\varphi : G \to \mathrm{GL}_n$ closed embedding

$\varphi^* : \mathcal{O}_{\mathrm{GL}_n} \twoheadrightarrow \mathcal{O}_G$ onto

Proposition:

Let G be a linear algebraic group over $\mathbb{Q}$ and $\varphi\colon G \hookrightarrow \mathrm{GL}_n$ a closed embedding. Then there is an integral form G_0 of G such that

$$\varphi^{-1}(\mathrm{GL}_n(\mathbb{Z})) = G_0(\mathbb{Z}).$$

$G \cap \mathrm{GL}_n(\mathbb{Z})$

Two results

Let G be a linear algebraic group over $\mathbb{Q}$.

Theorem 1:

If G_0, G_1 are integral forms of G, then $G_0(\mathbb{Z})$ and $G_1(\mathbb{Z})$ are commensurable as subgroups of $G(\mathbb{Q})$.

Two results

Let G be a linear algebraic group over $\mathbb{Q}$.

Theorem 1:

If G_0, G_1 are integral forms of G, then $G_0(\mathbb{Z})$ and $G_1(\mathbb{Z})$ are commensurable as subgroups of $G(\mathbb{Q})$.

Lemma 2:

Arithmetic groups are residually finite.

Γ is residually finite

$\forall \gamma \in \Gamma \setminus \{1\} \; \exists \beta : \Gamma \to F$ (finite)

$$\beta(\gamma) \neq 1_F$$

Observe: Sufficient to prove that $G(\mathbb{Z})$ is residually finite

Principal congruence subgroups

G a group scheme over $\mathbb{Z}$, $m \in \mathbb{N}$

$$\begin{aligned} \pi_m : \quad \mathbb{Z} &\to \mathbb{Z}/m\mathbb{Z} \\ G(\pi_m)\colon G(\mathbb{Z}) &\to G(\mathbb{Z}/m\mathbb{Z}) \end{aligned}$$

finite

Observation: $G(\mathbb{Z}/m\mathbb{Z})$ is finite.

pick coordinates

$$G(\mathbb{Z}/m\mathbb{Z}) \xrightarrow{\cong} V_{\mathbb{Z}/m\mathbb{Z}}(I_c) \subseteq (\mathbb{Z}/m\mathbb{Z})^n$$

Principal congruence subgroup:

$$G(\mathbb{Z}, m) = \ker(G(\pi_m)) \leq_{f.i.} G(\mathbb{Z}).$$

Proof of Lemma 2

Lemma 2: Arithmetic groups are residually finite.

$\gamma \in G(\mathbb{Z}) \qquad \gamma \neq 1$

Consider: $\gamma : \mathcal{O}_G \longrightarrow \mathbb{Z}$, $\gamma \neq \varepsilon$

$\gamma(x) \neq \varepsilon(x)$ for some $x \in \mathcal{O}_G$

$\Rightarrow \quad \gamma(x) \not\equiv \varepsilon(x) \bmod m \quad (\text{for } m \gg 1)$

$G(\pi_m)(\gamma) = \pi_m \circ \gamma \neq \pi_m \circ \varepsilon = 1 \in G(\mathbb{Z}/m\mathbb{Z})$

Proof of Theorem 1

Theorem 1: If G_0, G_1 are integral forms of G, then $G_0(\mathbb{Z})$ and $G_1(\mathbb{Z})$ are commensurable as subgroups of $G(\mathbb{Q})$.

$G_0(\mathbb{Z}) \subseteq G_0(\mathbb{Q}) \cong G(\mathbb{Q}) \cong G_1(\mathbb{Q}) \supseteq G_1(\mathbb{Z})$

Aim:

$$G_0(\mathbb{Z}) \cap G_1(\mathbb{Z}) \supseteq G_0(\mathbb{Z}, b) \quad \text{for some } b \in \mathbb{N}$$

Similarly " $\supseteq G_1(\mathbb{Z}, b')$"

Proof of Theorem 1

Theorem 1: If G_0, G_1 are integral forms of G, then $G_0(\mathbb{Z})$ and $G_1(\mathbb{Z})$ are commensurable as subgroups of $G(\mathbb{Q})$.

Aim:

$$G_0(\mathbb{Z}) \cap G_1(\mathbb{Z}) \supseteq G_0(\mathbb{Z}, b) \quad \text{for some } b \in \mathbb{N}$$

We know $\quad \mathbb{Q} \otimes_{\mathbb{Z}} \mathcal{O}_{G_0} \cong \mathcal{O}_G \cong \mathbb{Q} \otimes_{\mathbb{Z}} \mathcal{O}_{G_1}.$

For simplicity we assume $\quad \mathcal{O}_{G_0}, \mathcal{O}_{G_1} \subseteq \mathcal{O}_G.$

They generate $\mathcal{O}_G$ as $\mathbb{Q}$-algebra

Observation: $\quad 1 \in G_0(\mathbb{Z}), G_1(\mathbb{Z}) \subseteq G(\mathbb{Q})$

$$\varepsilon : \mathcal{O}_G \longrightarrow \mathbb{Q}$$

$$\varepsilon(\mathcal{O}_{G_0}) \subseteq \mathbb{Z}$$

$$\varepsilon(\mathcal{O}_{G_1}) \subseteq \mathbb{Z}$$

Proof of Theorem 1

if we replace f_i by $f_i - \varepsilon(f_i)$

Choose coordinates

$$f_1, \ldots, f_k \in \mathcal{O}_{G_0} \quad \text{with } \varepsilon(f_i) = 0$$
$$g_1, \ldots, g_\ell \in \mathcal{O}_{G_1} \quad \text{with } \varepsilon(g_j) = 0$$

Since $f_1, \ldots, f_k$ generate $\mathcal{O}_G$ as $\mathbb{Q}$-algebra, there are polynomials $p_1, \ldots, p_\ell \in \mathbb{Q}[X_1, \ldots, X_k]$ s.t.

$$p_j(f_1, \ldots, f_k) = g_j \qquad \text{for all } j \in \{1, \ldots, \ell\}$$

Observe: p_j has constant term 0

$$0 = \varepsilon(g_j) = \varepsilon(p_j(f_1, \ldots, f_k)) = p_j(\varepsilon(f_1), \ldots, \varepsilon(f_k))$$
$$= p_j(0, \ldots, 0)$$

Proof of Theorem 1

$b \in \mathbb{N}$: a common denominator of all coefficients of $p_1, \ldots, p_\ell$.

Claim:

$$G_0(\mathbb{Z}, b) \subseteq G_0(\mathbb{Z}) \cap G_1(\mathbb{Z})$$

$\gamma \in G_0(\mathbb{Z}, b)$ $\quad \gamma : \mathcal{O}_G \to \mathbb{Q}$ $\quad \gamma(\mathcal{O}_{G_0}) \subseteq \mathbb{Z}$

$\gamma(x) \equiv \varepsilon(x) \bmod b$ for all $x \in \mathcal{O}_{G_0}$

To show: $\gamma(\mathcal{O}_{G_1}) \subseteq \mathbb{Z}$ $\quad (\gamma \in G_1(\mathbb{Z}))$

i.e. $\gamma(g_j) \in \mathbb{Z}$ for all j

$$\gamma(g_j) = \gamma(p_j(f_1 \ldots f_n)) = p_j(\gamma(f_1) \ldots \gamma(f_n)) \in \mathbb{Z}$$

$\equiv 0 \bmod b$