5 Arithmetic Groups

Arithmetic groups are subgroups of linear algebraic groups. So we have to start with some remarks on these.

Definition 5.1. A linear algebraic group defined over a field k is a set of polynomials that cut out a subgroup of $\mathrm{SL}_n(K)$ for any superfield $K \supseteq k$. We also call these things k-groups.

Remark 5.2. You might wonder why definition (5.1) requires the set of polynomials to define a subgroup for every superfield of k. The reason is that for finite fields a certain set of polynomials might happen accidentally to define a subgroup of $\mathrm{SL}_n(k)$. What we really want, however, is that the polynomials are kind of a group like object: It should be provable by algebraic manipulations alone that the set of solutions to the equations is closed with respect to taking quotients. In fact, it suffices to require that the subgroup in $\mathrm{SL}_n(\overline{k})$ is a group.

Exercise 5.3. Show that the polynomial $(a_{21}+1)^3 = 1$ defines a subgroup of $\mathrm{SL}_2(\mathbb{F}_2)$, but it does not define a subgroup of $\mathrm{SL}_2(\mathbb{F}_4)$.

Remark 5.4. You also might wonder why we require the determinant to be 1 and do not leave the freedom to have this equation, which is a polynomial equation anyway, among our defining equations or not. Here, the reason is that we want the coefficients of the inverse of an element g to be polynomials in the coefficients of that matrix g.

Again, it turns out that this does not result in a loss of generality because $\mathrm{GL}_n(k)$ embeds into $\mathrm{SL}_{n+1}(k)$.

Remark 5.5. This is the more down to earth definition of linear algebraic groups. In a more scary way, we could define them as group objects in the category of affine k-varieties without referring to a particular representation in SL. It turns out that we do not really loose generality that way since affine algebraic groups always have faithful linear representations and thus are isomorphic to linear algebraic groups.

Example 5.6. Let $\mathfrak{G}$ be a nilpotent $\mathbb{Q}$-Lie algebra. Then the Campbell-Baker-Hausdorff formula

$$\mathfrak{g} \bullet \mathfrak{h} := \mathfrak{g} + \mathfrak{h} + \frac{1}{2}[\mathfrak{g}, \mathfrak{h}] + \frac{1}{12}([\mathfrak{g}, [\mathfrak{g}, \mathfrak{h}]] + [\mathfrak{h}, [\mathfrak{h}, \mathfrak{g}]]) + \cdots$$

defines a group law on the set $\mathfrak{G}$. Recall that the Campbell-Baker-Hausdorff series is made to satisfy

$$\mathrm{e}^{\mathfrak{g} \bullet \mathfrak{h}} = \mathrm{e}^{\mathfrak{g}} \, \mathrm{e}^{\mathfrak{h}}$$

for non-commuting $\mathfrak{g}$ and $\mathfrak{h}$.

Since $\mathfrak{G}$ is nilpotent, this is a polynomial group law. Observe that $-\mathfrak{g}$ is the inverse of $\mathfrak{g}$ with respect to this weird multiplication. Thus, $\mathfrak{G}$ is an affine algebraic group with multiplication $\bullet$ whose underlying variety is just an affine space: the vector space underlying $\mathfrak{G}$.

We turn the class of linear algebraic groups into a category by saying what morphisms ought to be.

Definition 5.7. Let G and H be two linear algebraic groups defined over k. A <u>k-homomorphism</u> from G to H is a polynomial map with coefficients taken from k that defines a group homomorphism $G(K) \to H(K)$ for any superfield K.

Example 5.8. The group SL_2 defined over $\mathbb{Q}$ is isomorphic to the subgroup of SL_3 defined by

$$\begin{pmatrix} \star & \star & 0 \\ \star & \star & 0 \\ 0 & 0 & 1 \end{pmatrix} = MXM^{-1}$$

where $M \in \mathrm{GL}_3(\mathbb{Q})$ is fixed. The isomorphism is given by

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \mapsto M^{-1} \begin{pmatrix} a_{11} & a_{12} & 0 \\ a_{21} & a_{22} & 0 \\ 0 & 0 & 1 \end{pmatrix} M.$$

Let us consider $k = \mathbb{Q}$ and $K = \mathbb{R}$. In this case, a linear algebraic group defines a subset of $\mathrm{SL}_n(\mathbb{R})$ by polynomial equations. Hence the set of solutions is a differentiable manifolds, at least at the non-critical points, which form a dense subset. However, since the group acts transitively on its set of points, actually all points look alike and are non-critical. Hence a linear algebraic group defined over $\mathbb{Q}$ is always a Lie group.

Remark 5.9. Although it might not be obvious, the same holds true in general: A linear algebraic group defined over any field is always a smooth variety whose irreducible components and connected components coincide and are finite in number. In fact, this not only true but it is true for the same reason as in the case $k = \mathbb{Q}$ provided the reason is formulated carefully.

Definition 5.10. Let G be a linear algebraic group over k. A Borel-subgroup $B \leq G$ is a maximal connected solvable subgroup.

The radical $\mathrm{Rad}(G)$ of G is defined to be the connected component of the identity of the intersection of all Borel-subgroups of G:

$$\mathrm{Rad}(G) := \left(\bigcap_{B \in \mathcal{B}} B \right)^0 .$$

The group G is called semi-simple if $\mathrm{Rad}(G) = 1$.

Remark 5.11. The radical of G is a connected solvable normal subgroup of G. The quotient $G / \mathrm{Rad}(G)$ is semi-simple. Hence the study of linear algebraic groups naturally centers around the study of connected solvable groups on the one hand and semi-simple groups on the other hand.

Example 5.12. Groups of upper triangular matrices are solvable. The group SL_n is semi-simple.

Definition 5.13. Let G be a linear algebraic group defined over $\mathbb{Q}$. We denote by $G(\mathbb{Z})$ the subgroup of $G(\mathbb{Q})$ that consists of matrices with integer coefficients only.

Definition 5.14. Two subgroups of a common supergroup are called <u>commensurable</u> if their intersection has finite index in both of them.

Exercise 5.15. Let $\varphi : G \to H$ be a $\mathbb{Q}$-isomorphism of $\mathbb{Q}$-groups. Show that $\varphi(G(\mathbb{Z}))$ and $H(\mathbb{Z})$ are commensurable.

Exercise 5.16. Let $\varphi : G \to H$ be a $\mathbb{Q}$-epimorphism of $\mathbb{Q}$-groups. Show that $\varphi(G(\mathbb{Z})) \cap H(\mathbb{Z})$ has finite index in $\varphi(G(\mathbb{Z}))$.

Exercise 5.17. Let $\varphi : G \to H$ be a $\mathbb{Q}$-morphism of $\mathbb{Q}$-groups. Show that $\varphi^{-1}(H(\mathbb{Z})) \cap G(\mathbb{Z})$ has finite index in $G(\mathbb{Z})$.

Definition 5.18. Let G be a linear algebraic groups over $\mathbb{Q}$. An arithmetic subgroup of G is a subgroup of $G(\mathbb{Q})$ commensurable with $G(\mathbb{Z})$.

An abstract group is called arithmetic if it is isomorphic to an arithmetic subgroup of some $\mathbb{Q}$-group.

Exercise 5.19. Let k be a finite extension of $\mathbb{Q}$, let $\mathcal{O} \subseteq k$ be the subring of algebraic integers in k, and let G be a k-group. Prove that $G(\mathcal{O})$ is an arithmetic group. Hint: Represent k as a matrix algebra over $\mathbb{Q}$ and use this to find a rational representation of $G(\mathcal{O})$.

Example 5.20. The group of diagonal 2×2-matrices with determinant 1

$$\left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \middle| \; ab = 1 \right\}$$

is isomorphic to the multiplicative group. Hence its arithmetic subgroup is $\{\pm 1\}$ which is the group with two elements. In particular, the trivial group is arithmetic.

Exercise 5.21. Show that any finite group is arithmetic.

Example 5.22. The infinite cyclic group is arithmetic. In fact, it is the arithmetic subgroup of the $\mathbb{Q}$-group

$$\begin{pmatrix} 1 & \star \\ 0 & 1 \end{pmatrix}.$$

Fact 5.23 (Mal'cev). *Any torsion free finitely generated nilpotent group is arithmetic.*

Fact 5.24 (from rational homotopy theory). *The mapping class group of any simply connected finite CW-complex is arithmetic. Conversely, any torsion free arithmetic group arises this way.*