LECTURE 6. THE AX-SCHANUEL THEOREM

6.1. **Commutative algebraic groups.** Let k be algebraically closed field and let G be a *commutative connected* algebraic group. This means that G is an algebraic variety (over k) equipped with a regular map

$$m : G \times G \to G$$

such that (G, m) is a commutative group (in the usual sense). The assumption that G is connected means that G is irreducible as an algebraic variety. Equivalently:

Exercise 6.1. *Let G be a (commutative) algebraic group. Show that G is irreducible as an algebraic variety if and only if G does not have nontrivial finite quotients.*

Proof. If G is an algebraic group then G acts transitively on the (finite) set of its irreducible components. Hence, producing a nontrivial finite quotient of G whenever G is not irreducible. Conversely, if G has a nontrivial finite quotient, the Zariski-closures of the cosets of the subgroup defining this quotient define a partition of X into (irredundant) Zariski-closed subsets of G which has to be trivial by irreducibility. □

Examples of connected algebraic groups includes

- the additive group G_a which as an algebraic variety is the affine line k and with multiplication given by the polynomial
$$(x_1, x_2) \mapsto x_1 + x_2$$
with ring of regular functions $k[x]$ the ring of polynomials
- the multiplicative group G_m which as an algebraic variety is the open subset k^* of k given by $y \neq 0$ and with multiplication and with multiplication given by
$$(y_1, y_2) \mapsto y_1 \cdot y_2$$
with ring of regular functions $k[y, y^{-1}]$.
- any elliptic curve E and any product of such groups
$$G = \mathrm{G}_a^k \times \mathrm{G}_m^l \times E^m \text{ where } k, l, m \in \mathbb{N}.$$

For the purpose of this course, we will focus on the case of the additive and the multiplicative group and hence on the groups of the form

$$G = \mathrm{G}_a^k \times \mathrm{G}_m^l, k, l \in \mathbb{N}$$

but the proof of the Ax-Schanuel theorem goes through for the exponential maps of elliptic curves as well. We write the ring of regular functions on G as:

$$k[G] = k[x_1, \dots, x_k, y_1, \dots, y_l, y_1^{-1}, \dots, y_l^{-1}]$$

where $k[x_1, \dots, x_k]$ is the ring of regular functions on G_a^k and $k[y_1, \dots, y_l, y_1^{-1}, \dots, y_l^{-1}]$ is the ring of regular functions on G_m^l.

Lemma 6.2 (Goursat's lemma)**.** *Any algebraic subgroup H of $G = \mathrm{G}_a^k \times \mathrm{G}_m^l, k, l \in \mathbb{N}$ is of the form*

$$H = H_1 \times H_2$$

where $H_1 \subset \mathrm{G}_a^k$ and $H_2 \subset \mathrm{G}_m^l$ are subgroups. Moreover, any subgroup H_1 of G_a^n is a k-subvector space and any subgroup H_2 of G_m^l can be written as

$$H_2 = \bigcap_{(n_1, \dots, n_l) \in S} \mathrm{Ker}(\chi_{n_1, \dots, n_l})$$

where $\chi_{n_1, \dots, n_l}(y_1, \dots, y_n) = y_1^{n_1} \cdots y_l^{n_l}$ and S is a finite set of l-tuples of integers.

Proof. We first prove the second part of the statement. First note that if H_1 is a subgroup of G_a^k then

$$C(H_2) = \{x \in k^* \mid x \cdot H_1 = H_1\}$$

is a definable subset of k which contains $\mathbb{Z}$. By elimination of quantifiers in the theory ACF_0; it follows that $C(H_1)$ is a cofinite subgroup of k^* and hence equal to k^*. It follows that H_1 is a k-vector subspace of G_a^k. Now consider H_2 a subgroup of G_m^l and set

$$\pi : \mathrm{G}_m^l \to \mathrm{G}_m^l / H_2.$$

The group $N = \mathrm{G}_m^l/H_2$ is commutative connected and linear as these properties are preserved under quotient. Consider now the subgroup

$$\mathrm{Tor}(N) = \{x \in N \mid \exists n \in \mathbb{N}, n \cdot x = e_N\}.$$

All the elements of $\mathrm{Tor}(N)$ are diagonalizable and hence codiagonalisable since this is a commutative group. Since N is the Zariski-closure of $\mathrm{Tor}(N)$, it follows that $N \subset G_m^p$ for some p and therefore that

$$H_2 = \bigcap_{\chi \in S} \mathrm{Ker}(\chi)$$

where $\chi : \mathrm{G}_m^l \to \mathrm{G}_m$ are group morphism and S is a finite set of such morphisms. It remains to show that any such morphism has the form

$$(y_1, \ldots, y_l) \mapsto y_1^{e_1} \cdots y_l^{e_l}$$

To see this consider

$$\begin{cases} k[y, y^{-1}] & \to k[y_1, \ldots, y_l, y_1^{-1}, \ldots, y_l^{-1}] \\ f \mapsto & f \circ \chi \end{cases}$$

and note that y must be sent to an invertible element of $k[y_1, \ldots, y_l, y_1^{-1}, \ldots, y_l^{-1}]$ and therefore $y = y_1^{e_1} \cdot y_s^{e_l}$ as required.

Now to prove the first part of the statement, denote by N_1 the intersection of H with $\mathrm{G}_a^k \times \{e\}$, H_1 the image of H in G_a^k and correspondingly N_2 the intersection of H with $\{e\} \times \mathrm{G}_m^l$ and H_2 the image of H in G_m^l. Following Goursat, we claim that H defines an algebraic group morphism

$$\phi_H : H_2/N_2 \to H_1/N_1.$$

given by

$$\phi_H([y]) = [x] \text{ iff } (x, y) \in H$$

By the first part of the statement, H_2/N_2 has dense torsion points and H_1/N_1 has no torsion points. It follows that ϕ_H is the trivial morphism. Rewinding the definition of ϕ_H, we obtain that $H = H_1 \times H_2$ as required. □

Definition 6.3. Let G be a commutative connected algebraic group. Denote by $R_g : x \mapsto x \cdot g$ the right multiplication by g. We say that a one-form $\omega \in \Omega^1(k(G)/k)$ is G-invariant if

$$R_g^* \omega = \omega \text{ for all } g \in G. \tag{1}$$

Lemma 6.4. *Let G be a commutative (affine) algebraic group and $\omega \neq 0$ an invariant one-form on G. Then the one-form ω is regular on G, closed and does not vanish at any point $p \in G$.*

Proof. Take U an open set of X such that ω is a regular one-form on U and consider the associated function

$$\hat{\omega} : TU \to k$$

For every $g \in G$, $\hat{\omega} \circ TR_g : T(R_g(U)) \to k$ is the function corresponding to $R_g^*\omega$ and the equality (1) means that the functions $\hat{\omega}$ and $TR_g \circ \hat{\omega}$ agree on $TR_g(U) \cap TU = T(U \cap R_g(U))$. Since $\{TR_g(U) \mid g \in G\}$ is an open cover of X, this function can be glued together to produce a global function $\hat{\overline{\omega}} : TG \to k$ which defines a regular one-form $\overline{\omega}$ on the whole of G. Hence, any G-invariant form extends to a regular form on G. Note moreover that if

$$\hat{\omega}(e) : T_eG \to k$$

is the linear form defined by ω on T_eG then

$$\hat{\omega}(g) = \hat{\omega}(e) \circ dR_{g^{-1}} : T_gG \to T_eG \to k$$

is the one-form defined by ω on G. It follows that ω does not vanish at any point $p \in G$ and that the space of G-invariant forms is a complex vector space of finite dimension. Finally to see that ω is closed, we assume for simplicity that $G = G_m^k \times G_a^l$. Note that

$$\omega = \lambda_1 dx_1 + \cdots + \lambda_k dx_k \text{ and } \eta = \mu_1 dy_1/y_1 + \ldots + \mu_k dy_l/y_l$$

form the k-vector space of invariant forms on G_a^k and G_m^l respectively. It follows that a closed invariant one-form on $G_a^l \times G_m^k$ is of the form $\lambda_1 dx_1 + \cdots + \lambda_k dx_k + \mu_1 dy_1/y_1 + \ldots + \mu_k dy_l/y_l$ which is closed by a direction inspection. □

Proposition 6.5. *Let G be a commutative (affine) algebraic group and ω an invariant one-form on G. There exists a subgroup H of G such that the partition of G into ω-leaves given by Frobenius integrability Theorem is the partition of G into H-cosets.*

Proof. Since the one-form ω is invariant so is the partition $X = \bigsqcup_{a \in A} \mathcal{L}_a$ into ω-leaves. It follows that any ω-leaf is of the form $\mathcal{L}_e \cdot g$ for some $g \in G$ and hence it is enough to see that $\mathcal{L}_e$ is a subgroup of G. To see this, note that if $g \in \mathcal{L}_e$ then

$$\mathcal{L}_e \cdot g = \mathcal{L}_e$$

as they are two equivalence classes containing a common element. It follows that the inverse of g lies in $\mathcal{L}_e$ and that if $g, h \in \mathcal{L}_e$ then

$$g \cdot h \in \mathcal{L}_e \cdot (g \cdot h) = \mathcal{L}_e \cdot h = \mathcal{L}_e$$

□

6.2. **An exact sequence.** Let K/k be a field extension of characteristic zero and consider L an intermediate subfield. We construct two morphisms of K-vector spaces.

(1) Viewing $\Omega^1(K/k)$ as an L-vector space, we obtain a morphism of L-vector spaces

$$i_L : \Omega^1(L/k) \to \Omega^1(K/k)$$

obtained by applying Lemma **??** to $d_{|L} : L \to \Omega^1(K/k)$.

The usual properties of the tensor product gives an identification

$$\mathrm{Hom}_{L-vect}(\Omega^1(L/k), \Omega^1(K/k)) \simeq \mathrm{Hom}_{K-vect}(\Omega^1(L/k) \otimes_L K, \Omega^1(K/k))$$

which is the (functorial) adjunction between extension and restriction of scalars in commutative algebra. So that the morphism i_l corresponds to a morphism of K-vector spaces:

$$j_L : \Omega^1(L/k) \otimes_L K \to \Omega^1(K/k)$$

(2) Applying Lemma **??** to the extension K/k and the morphism $d = d_{K/L} : K \to \Omega^1(K/L)$, we obtain a morphism of K-vector spaces

$$s_L : \Omega^1(K/k) \to \Omega^1(K/L).$$

Corollary 6.6. *With the notation above, the sequence*

$$0 \to \Omega^1(L/k) \otimes_L K \xrightarrow{j_L} \Omega^1(K/k) \xrightarrow{s_L} \Omega^1(L/K) \to 0$$

is a short exact sequence of K-vector spaces

Proof. To see that j_L is injective, it is enough to see that i_L is injective. This follows from Theorem **??** and the fact that a transcendence basis of L/k can be completed into a transcendence basis of K/k. Similarly any transcendence basis of K/L can be completed into a transcendence basis of K/k so that s_L is surjective by Theorem **??**. Finally, the property that $s_L \circ j_L = 0$ follows from the fact

$$s_L(d_{K/k} f) = d_{L/k} f = 0 \text{ for any } f \in L$$

and that $\Omega^1(L/k) \otimes_L K$ is generated as a K-vector space by one-forms of this form. □

6.3. **Liouville-Rosenlicht Theorem.**

Theorem 6.7 (Liouville-Rosenlicht Theorem)**.** *Let K/k be an extension of fields of characteristic zero with k algebraically closed. Assume that $f_1, \ldots, f_n \in K^*$ and $g \in K$ are elements of K chosen such that*

$$\sum_{i=1}^{n} c_i \cdot \frac{df_i}{f_i} + dg = 0 \in \Omega^1(K/k)$$

where the c_i are $\mathbb{Q}$-linearly independent elements from k. Then $f_1, \ldots, f_n, g \in k$.

We assume that $k = \mathbb{C}$ in the proof which will be sufficient for our purposes. The interested reader can check that the general case actually follows from this particular case (exercise).

Proof. Set $L = k(f_1, \ldots, f_n, g)$. Since the canonical morphism

$$\Omega^1(L/k) \to \Omega^1(K/k)$$

is injective, we may assume that $K = L$. This implies that:

(i) K is finitely generated over k and hence write $K = k(X)$ as the function field of an irreducible algebraic variety X over k.

(ii) $f_1, \ldots, f_n, g$ can be identified as rational functions on X and

$$(f_1, \ldots, f_n, g) : X \dashrightarrow \mathrm{G}_m^n \times \mathrm{G}_a$$

defines a birational equivalence between X and the Zariski-closure of its image in $\mathrm{G}_m^n \times \mathrm{G}_a$.

So we may assume that $K = k(X)$ where X is an irreducible Zariski-closed subset of $G = \mathrm{G}_m^n \times \mathrm{G}_a$. The hypothesis then says that the invariant one-form on G given by

$$\omega = \sum_{i=1}^{n} c_i \cdot \frac{dy_i}{y_i} + dx$$

vanishes identically along X that is $i^*\omega = 0$ where $i : X \to \mathrm{G}_m^n \times \mathrm{G}_a$. It follows from Frobenius integrability theorem that (the image of) X is contained in a ω-leaf of ω in $\mathrm{G}_m^n \times \mathrm{G}_a$. Up to a replacing X by a translate, we may assume that X is contains the identity element of $\mathrm{G}_m^n \times \mathrm{G}_a$ and is therefore contained in the leaf $\mathcal{L}_e$ through the identity element e. We now set

$$H = \langle X \rangle \subset \mathcal{L}_e \subsetneq G$$

and use:

Theorem 6.8 (Chevalley-Zilber)**.** *Let X be an irreducible subvariety of an algebraic group G containing the identity element of G. Then the group $\langle X \rangle$ generated by X is a connected algebraic subgroup of G.*

which implies that:

$$H \subsetneq G = \mathrm{G}_a \times \mathrm{G}_m$$

is an algebraic subgroup. The first part of Goursat's lemma then implies that

$$H = H_1 \times H_2 \subset \mathrm{G}_a \times \mathrm{G}_m^n$$

Note that H_2 is a proper algebraic subgroup of G_m^n since the projection of $\mathcal{L}_e$ in G_m^n is the η-leaf of

$$\eta = \sum_{i=1}^{n} \lambda_i \frac{dy_i}{y_i}$$

which is a proper subgroup of G_m^n. It follows from the second part of Goursat's lemma that

$$H_2 = \bigcap_{(n_1, \ldots, n_l) \in S} \mathrm{Ker}(\chi_{n_1, \ldots, n_l}).$$

so that $T_e H_2$ contains a nontrivial vector □

6.4. **The Ax Schanuel Theorem.**

Theorem 6.9 (Ax-Schanuel). *Let K be a differential field (for a derivation ∂) with an algebraically closed field of constants C. Consider $x_1, \ldots, x_n \in K$ and write $y_1, \ldots, y_n \in K$ for exponentials of $x_1, \ldots, x_n \in K$. Then*

$$\mathrm{td}(x_1, \ldots, x_n, y_1, \ldots, y_n/C) > n$$

provided $x_1, \ldots, x_n$ are $\mathbb{Q}$-linearly independent modulo C.

Proof. Set $L = C(x_1, \ldots, x_n, y_1, \ldots, y_n)$ and consider for $i = 1, \ldots, n$

$$\omega_i = \frac{dy_i}{y_i} - dx_i \in \Omega^1(L/C) \subset \Omega^1(K/C)$$

where the inclusion is given by the canonical identification of $\Omega^1(L/C)$ with a L-vector subspace of $\Omega^1(K/C)$

Claim. *As elements of $\Omega^1(K/C)$, we have for $i = 1, \ldots, n$, $\mathcal{L}_\partial(\omega_i) = 0$.*

Proof. This is a direct consequence of the definition of the Lie-derivative using additivity, the chain rule and the Leibniz rule. Indeed, we have

$$\mathcal{L}_\partial(\frac{dy_i}{y_i}) = -\frac{\partial(y_i)}{y_i^2}dy_i + \frac{d(\partial(y_i))}{y_i} = d(\frac{\partial(y_i)}{y_i})$$

so that

$$\mathcal{L}_\partial(\omega_i) = \mathcal{L}_\partial(\frac{dy_i}{y_i} - dx_i) = d(\frac{\partial(y_i)}{y_i} - \partial(x_i)) = 0.$$

□

Claim. *$\omega_1, \ldots \omega_n$ are K-linearly independent in $\Omega^1(K/C)$.*

Proof. Otherwise, $\omega_1, \ldots \omega_n$ are K-linearly dependent. We first show that $\omega_1, \ldots, \omega_n$ are C-linearly dependent. Take

$$\sum_{i=1}^{e} \lambda_i \cdot \omega_i = 0$$

by a linear combination with a minimal number of nonzero coefficients. Without loss of generality, we may assume that $\lambda_1 = 1$. Applying the Lie-derivative, we obtain

$$\mathcal{L}_\partial(\sum_{i=1}^{e} \lambda_i \cdot \omega_i) = \sum_{i=2}^{e} \partial(\lambda_i) \cdot \omega_i$$

from which it follows by minimality of the nontrivial linear combination that all $\lambda_i \in C$. It follows that $\omega_1, \ldots, \omega_n$ are C-linearly dependent so that we have a one-form

$$\omega = \sum_{i=1}^{n} \lambda_i \omega_i = 0 = \sum_{i=1}^{n} \lambda_i \cdot \frac{dy_i}{y_i} - d(\sum_{i=1}^{n} \lambda_i \cdot x_i)$$

where $\lambda_i \in \mathbb{C}$. Up to replacing (x_i, y_i) for $i = 1, \ldots, n$ by

$$z_j = \prod_{i=1}^{n} y_i^{e_{i,j}} \text{ and } \xi_j = \sum_{i=1}^{n} e_{i,j} \cdot x_i$$

for $j = 1, \ldots, s$, we obtain a relation of the form

$$d(\sum_{j=1}^{s} \gamma_j \cdot \xi_j) = \sum_{j=1}^{s} \gamma_j \cdot \frac{dz_j}{z_j}$$

where the γ_j are $\mathbb{Q}$-linearly independent complex numbers which by Liouville-Rosenlicht's theorem implies that $\xi_1, \ldots, \xi_s$ and therefore $x_1, \ldots, x_n$ are $\mathbb{Q}$-linearly dependent modulo $\mathbb{C}$. □

To finish the proof of the theorem, note that we have obtained that

$$\mathrm{Span}_L(\omega_1, \ldots, \omega_n) \subset \Omega^1(L/C)$$

so that $\mathrm{td}(L/C) = \mathrm{ldim}_L(\Omega^1(L/C)) \geq n$. To obtain the strict inequality, it is enough to show that

$$\mathrm{Span}_L(\omega_1, \ldots, \omega_n) \neq \Omega^1(L/C).$$

To see this, consider the restriction of the derivation

$$\partial_{|L} : L \to K$$

as a K-valued derivation on L which is nontrivial since $\partial(x_i) \neq 0$ for example. Using the universal properties of $\Omega^1(L/k)$, we do obtain a morphism of L-vector spaces

$$\phi : \Omega^1(L/C) \to K$$

such that $\phi(df) = \partial(f)$ for any $f \in L$. It follows that

$$\phi(\omega_i) = \phi(\frac{dy_i}{y_i} - dx_i) = \frac{\partial(y_i)}{y_i} - \partial(x_i) = 0$$

and therefore

$$\mathrm{Span}_L(\omega_1, \ldots, \omega_n) \subset \mathrm{Ker}(\phi) \subsetneq \Omega^1(L/C)$$

as required. This concludes the proof of the Ax-Schanuel Theorem. □