1. Week 3: Algebraic groups

Aim of this week. The aim of this week is to introduce the notion of an algebraic group and its fundamental properties. The main references of this week are [Spr09] and [Bor91].

1.1. **Comments on scheme theory.** Let $\overline{k}$ be an algebraically closed field. Let $\mathbb{A}^n_{\overline{k}}$ be the n-dimensional affine space over k (here, let us simply understand that $\mathbb{A}^n_{\overline{k}}$ is the set of n-tuples of elements of $\overline{k}$). Roughly speaking, an *affine algebraic variety* is a subset of $\mathbb{A}^n_{\overline{k}}$ consisting of simultaneous solutions to a tuple of polynomials in $k[x_1, \ldots, x_n]$. We can equip an affine variety with a topology called *Zariski topology.* A *algebraic variety* is a space obtained by patching affine algebraic varieties.

From the modern viewpoint, the classical theory of algebraic varieties can be far more generalized by the theory of schemes. For any commutative ring R, the *affine scheme* $\operatorname{Spec} R$ is defined to be the set of prime ideals of R. We can equip $\operatorname{Spec} R$ with the Zariski topology in a similar manner to the classical case. In addition, we can also introduce a further structure on $\operatorname{Spec} R$, that is, a sheaf of rings on $\operatorname{Spec} R$; this makes $\operatorname{Spec} R$ so-called a locally ringed space. A *scheme* is a locally ringed space obtained by patching affine schemes.

When a scheme X equipped with a morphism to $\operatorname{Spec} \overline{k}$ (this amounts to that the rings R defining X are $\overline{k}$-algebras) satisfies certain conditions ("separated, reduced, of finite type"), we can associate an algebraic variety to X. This algebraic variety is given to be the set of all "$\overline{k}$-valued points" of X. We'll give a bit more explanation on the notion of "valued points" later. Conversely, any algebraic variety can be realized in this way from a scheme. Roughly speaking, an *algebraic group* is an algebraic variety equipped with a group structure. Thus we have two choices of languages to study algebraic groups; the classical theory of algebraic varieties and the modern theory of schemes.[1]

When an algebraic variety X has defining polynomials whose coefficients are in a subfield k of $\overline{k}$, we say that X *is defined over* k. In the language of scheme theory, this amounts to that there exists a scheme X_0 equipped with a morphism to $\operatorname{Spec} k$ such that its *base change to* $\overline{k}$ (i.e., the fibered product of $X_0 \to \operatorname{Spec} k$ and $\operatorname{Spec} \overline{k} \to \operatorname{Spec} k$) is isomorphic to X. One advantage of using scheme theory is that it makes it theoretically easier to treat algebraic varieties over a field k which is not necessarily algebraically closed. This is particularly important for us because eventually we want to discuss algebraic groups defined over a finite field. On the other hand, we can understand algebraic groups in a more intuitive way by appealing to the classical theory of algebraic varieties.

In any case, it is unavoidable to rely on these languages of algebraic geometry, but we do not go into the details of algebraic geometry in this course.[2] Rather, our aim is to get familiar with algebraic groups through several concrete examples.

1.2. **Definition and examples of algebraic groups.** Let k be a field. In the following, let us furthermore assume that k is perfect. (In this course, eventually,

[1] Indeed, [Spr09] is written via the theory of algebraic varieties while [Bor91] is written via scheme theory.

[2] For example, see [Spr09, Chapter 1] or [Bor91, Chapter AG] for a summary on algebraic geometry.

k will be taken to be a finite field $\mathbb{F}_q$.) We write Γ_k for the absolute Galois group $\mathrm{Gal}(\overline{k}/k)$ of k.

By "an algebraic variety over k", we mean a scheme X equipped with a morphism to $\mathrm{Spec}\, k$ such that its base change $X_{\overline{k}}$ to $\mathrm{Spec}\, \overline{k}$ is an algebraic variety.

Definition 1.1 (algebraic group)**.** Let G be an algebraic variety over k. We say that G is an *algebraic group over* k if G is equipped with a group structure, i.e., morphisms of schemes over k

- $m\colon G \times_k G \to G$ ("multiplication morphism"),
- $i\colon G \to G$ ("inversion morphism"), and
- $e\colon \mathrm{Spec}\, k \to G$ ("unit element")

satisfying the axioms of groups. More precisely, the following diagrams are commutative:

$$\begin{tikzcd}
G \times_k G \times_k G \arrow[r, "m \times \mathrm{id}"] \arrow[d, "\mathrm{id} \times m"'] \arrow[dr, phantom, "\circlearrowright"] & G \times_k G \arrow[d, "m"] \\
G \times_k G \arrow[r, "m"] & G
\end{tikzcd}
\qquad
\begin{tikzcd}
G \arrow[r, "\mathrm{id} \times e"] \arrow[d, "e \times \mathrm{id}"'] \arrow[dr, "\mathrm{id}" description, "\circlearrowright", "\circlearrowright"'] & G \times_k G \arrow[d, "m"] \\
G \times_k G \arrow[r, "m"] & G
\end{tikzcd}$$

$$\begin{tikzcd}
G \times_k G \arrow[d, "\mathrm{id} \times i"'] \arrow[dr, phantom, "\circlearrowright"] & G \arrow[l, "\Delta"'] \arrow[r, "\Delta"] \arrow[d, "\epsilon"'] \arrow[dr, phantom, "\circlearrowright"] & G \times_k G \arrow[d, "i \times \mathrm{id}"] \\
G \times_k G \arrow[r, "m"] & G & G \times_k G \arrow[l, "m"']
\end{tikzcd}$$

Here, ϵ denotes the composition of the structure morphism $G \to \mathrm{Spec}\, k$ and $e\colon \mathrm{Spec}\, k \to G$.

Remark 1.2. Suppose that G is an affine algebraic variety with coordinate ring $k[G]$ (i.e., $G = \mathrm{Spec}\, k[G]$). Recall that the category of affine schemes is (anti-) equivalent to the category of commutative rings. Thus giving G an algebraic group structure is equivalent to defining ring homomorphisms corresponding to m, i, e and satisfying analogous axioms. For example, the ring homomorphism corresponding to m must be a k-algebra homomorphism $R \to R \otimes_k R$. In general, a commutative ring equipped with such an additional structure is called a *Hopf algebra*.

Various notions in the usual group theory can be formulated also for algebraic groups. For example, for an algebraic group G over k, we can define its center $Z(G)$, its derived subgroup (commutator subgroup) $G_{\mathrm{der}} = [G, G]$, and so on, as algebraic groups over k. The notion of a homomorphism between algebraic groups is also defined in a natural way. For an algebraic group G over k, its Zariski-connected component containing (the image of) the unit element e is closed under the multiplication, i.e., G° is an algebraic subgroup of G over k. We refer *the identity component of* G to it.

Example 1.3. (1) We put $\mathbb{G}_{\mathrm{a}} := \mathrm{Spec}\, k[x]$ and define m, i, and e at the level of rings as follows:

- $m\colon k[x] \to k[x] \otimes_k k[x]; \quad x \mapsto x \otimes 1 + 1 \otimes x,$
- $i\colon k[x] \to k[x]; \quad x \mapsto -x,$
- $e\colon k[x] \to k; \quad x \mapsto 0.$

Then $\mathbb{G}_{\mathrm{a}}$ is an algebraic group over k with respect to these operations. We call $\mathbb{G}_{\mathrm{a}}$ the *additive group* over k.

(2) We put $\mathbb{G}_{\mathrm{m}} := \operatorname{Spec} k[x, x^{-1}]$ and define m, i, and e at the level of rings as follows:
- $m\colon k[x] \to k[x, x^{-1}] \otimes_k k[x, x^{-1}]; \quad x \mapsto x \otimes x$,
- $i\colon k[x] \to k[x]; \quad x \mapsto x^{-1}$,
- $e\colon k[x] \to k; \quad x \mapsto 1$.

Then $\mathbb{G}_{\mathrm{m}}$ is an algebraic group over k with respect to these operations. We call $\mathbb{G}_{\mathrm{m}}$ the *multiplicative group* over k.

(3) We put $\mathrm{GL}_n := \operatorname{Spec} k[x_{ij}, D^{-1} \mid 1 \leq i, j \leq n]$, where $D := \det(x_{ij})_{1 \leq i,j \leq n}$. We define m, i, and e at the level of rings as follows:
- $m(x_{ij}) := \sum_{k=1}^{n} x_{ik} \otimes x_{kj}$,
- $i(x_{ij}) :=$ the (i, j)-entry of the inverse of the matrix $(x_{ij})_{1 \leq i,j \leq n}$,
- $e(x_{ij}) := \delta_{ij}$ (Kronecker's delta).

Then GL_n is an algebraic group over k with respect to these operations. We call GL_n the *general linear group (of rank n)* over k. (Note that $\mathrm{GL}_1 \cong \mathbb{G}_{\mathrm{m}}$.)

In fact, it is not always practical to know the structure ring of an algebraic group and the ring homomorphisms defining the algebraic group structure. Instead, by relying on the philosophy of "the functor of points", we may understand algebraic groups over k intuitively as follows. Recall that any affine scheme $X = \operatorname{Spec} k[X]$ over k defines the following functor (*functor of points*) from the category of k-algebras to the category of sets:

$$(k\text{-algebras}) \to (\text{sets})\colon R \mapsto X(R) := \operatorname{Hom}_k(\operatorname{Spec} R, X)\ (\cong \operatorname{Hom}_k(k[X], R)).$$

(The set $X(R)$ is called the *set of R-valued points of X.*) By Yoneda's lemma, regarding X as a functor in this way does not lose any information of X essentially. Moreover, if X is an affine algebraic group over k, then the morphisms m, i, and e induce a group structure on the set $X(R)$ of R-valued points of X. Hence the above functor takes values in the category of groups. In other words, we may regard an affine algebraic group over k as a "machine" which associates a group to each k-algebra. One practical way of treating (affine) algebraic groups over k is to care only about the groups associated to (all) k-algebras. Recall that, in our convention, an algebraic variety X over k is a scheme whose base change to $\overline{k}$ can be regarded as an algebraic variety in the classical sense; as a set, this algebraic variety is nothing but $X(\overline{k})$.

Let us present several basic examples:

Example 1.4. (1) For a k-algebra R, we have $\mathbb{G}_{\mathrm{a}}(R) \cong R$, where the group structure on R is given by the additive structure of R. Indeed, we have

$$\mathbb{G}_{\mathrm{a}}(R) = \operatorname{Hom}_k(\operatorname{Spec} R, \mathbb{G}_{\mathrm{a}}) \cong \operatorname{Hom}_k(k[x], R) \cong R,$$

where the last map is given by $f \mapsto f(x)$. This is why $\mathbb{G}_{\mathrm{a}}$ is called the "additive group".

(2) For a k-algebra R, we have $\mathbb{G}_{\mathrm{m}}(R) \cong R^{\times}$, where $R^{\times}$ denotes the unit group of R with respect to the multiplicative structure of R. Indeed, we have

$$\mathbb{G}_{\mathrm{m}}(R) = \operatorname{Hom}_k(\operatorname{Spec} R, \mathbb{G}_{\mathrm{m}}) \cong \operatorname{Hom}_k(k[x, x^{-1}], R) \cong R^{\times},$$

where the last map is given by $f \mapsto f(x)$. This is why $\mathbb{G}_{\mathrm{m}}$ is called the "multiplicative group".

(3) For a k-algebra R, we have

$$\mathrm{GL}_n(R) \cong \{g = (g_{ij})_{i,j} \in M_n(R) \mid \det(g) \in R^{\times}\}.$$

Indeed, by definition, we have

$$\mathrm{GL}_n(R) = \mathrm{Hom}_k(\mathrm{Spec}\, R, \mathrm{GL}_n) \cong \mathrm{Hom}_k(k[x_{ij}, D^{-1} \mid 1 \leq i, j \leq n], R).$$

The right-hand side is isomorphic to (at least as sets) $\{g = (g_{ij})_{i,j} \in M_n(R) \mid \det(g) \in R^\times\}$ by the map $f \mapsto (f(x_{ij}))_{i,j}$. It is a routine work to check that this bijection is indeed a group isomorphism.

(4) The *symplectic group* Sp_{2n} is an affine algebraic group such that the group of its R-valued points is given as follows:

$$\mathrm{Sp}_{2n}(R) \cong \{g = (g_{ij})_{i,j} \in \mathrm{GL}_{2n}(R) \mid {}^t g J_{2n} g = J_{2n}\},$$

where J_{2n} denotes the antidiagonal matrix whose antidiagonal entries are given by 1 and -1 alternatively:

$$J_{2n} := \begin{pmatrix} & & & 1 \\ & & -1 & \\ & 1 & & \\ \iddots & & & \end{pmatrix}.$$

(5) Here let's assume that the characteristic of k is not 2. Let J be an element of $\mathrm{GL}_n(k)$ which is symmetric, i.e., its transpose ${}^t J$ equals J. Then the *orthogonal group (associated to J)* $\mathrm{O}(J)$ is an affine algebraic group such that the group of its R-valued points is given as follows:

$$\mathrm{O}(J)(R) \cong \{g = (g_{ij})_{i,j} \in \mathrm{GL}_n(R) \mid {}^t g J g = J\}.$$

This group is disconnected and has 2 connected components. The identity component of $\mathrm{O}(J)$ is denoted by $\mathrm{SO}(J)$ and called the *special orthogonal group (associated to J)*.[3] When J is taken to be the anti-diagonal matrix whose anti-diagonal entries are all given by 1, we simply write O_n and SO_n.

Here, we don't explain how to define the structure rings of $\mathrm{SO}(J)$ or Sp_{2n} and also how to introduce the group structure at the level of their structure rings. Only the important viewpoint here is what kind of groups are associated as the groups of R-valued points! (When we are only interested in the algebro-geometric nature of a given algebraic group, we even look at only its $\overline{k}$-valued points.) So, in this course, let us just believe that the "functors" $\mathrm{SO}(J)$ or Sp_{2n} are indeed *representable*, i.e., realized as the functors of points of some affine algebraic groups. This remark is always applied to any affine algebraic group which we will encounter in the future.

1.3. **Jordan decomposition.**

We first begin with the following proposition, which is a consequence of the theory of Jordan normal form in linear algebra.

Proposition 1.5. *Let g be an element of $\mathrm{GL}_n(k)$. Then there exists a unique decomposition $g = g_s + g_n$ such that*

- $g_s g_n = g_n g_s$,
- $g_s \in \mathrm{GL}_n(k)$ *is semisimple, i.e., diagonalizable in* $\mathrm{GL}_n(\overline{k})$, *and*
- $g_n \in \mathrm{GL}_n(k)$ *is nilpotent, i.e., all the eigenvalues are* 0 *(equivalently, some power of g_n is zero).*

[3] Note that J_{2n} is symmetric if the characteristic of k is 2 since -1 equals 1! When the characteristic is 2, we have to define orthogonal groups in terms of quadratic forms; so the point is that the notion of a quadratic form is not equivalent to the notion of a symmetric bilinear form when the characteristic is 2.

Proof. Let us briefly the sketch of the proof. We first work over the algebraic closure $\overline{k}$ (this is the same as the separable closure of k since we assume that k is perfect).

We regard $g \in \mathrm{GL}_n(\overline{k})$ as an endomorphism of $V := \overline{k}^{\otimes n}$. We let $\{\alpha_1, \ldots, \alpha_r\}$ be the set of eigenvalues of g. Recall that the generalized eigenspace of g with respect to its eigenvalue α_i is defined by

$$V_i := \mathrm{Ker}(g - \alpha_i \cdot I_n)^{n_i},$$

where n_i is any sufficiently large integer (then V_i is equal to the subspace $\{v \in V \mid (g - \alpha_i \cdot I_n)^m(v) = 0 \text{ for some } m > 0\}$). Then the theorem of Cayley–Hamilton implies that we have $V = \bigoplus_{i=1}^r V_i$.

We put $g_i := g|_{V_i} \in \mathrm{End}_k(V_i)$. If we put $g_{i,s} := \alpha_i \cdot I_{\dim V_i}$ and $g_{i,n} := g_i - g_{i,s}$, then we have

- $g_{i,s}$ is semisimple,
- $g_{i,n}$ is nilpotent, and
- $g_{i,s}g_{i,n} = g_{i,n}g_{i,s}$.

Thus, by putting $g_s := \bigoplus_{i=1}^r g_{i,s}$ and $g_n := \bigoplus_{i=1}^r g_{i,n}$, we get a decomposition $g = g_s + g_n$ satisfying the desired conditions. To check the uniqueness of such a decomposition, suppose that we also have another such decomposition $g = g'_s + g'_n$. Then, since g'_s commutes with g, g'_s preserves each V_i. By noting that $g_i - (g'_s)|_{V_i} = (g'_n)|_{V_i}$, which is nilpotent, we see that g and g'_s have the same eigenvalues on V_i. As g'_s is semisimple, this implies that g'_s must be equal to $\alpha_i \cdot I_{\dim V_i}$. Hence we also get $g_n = g'_n$.

Next suppose that $g \in \mathrm{GL}_n(k)$. Then, by what we proved so far, we can find a decomposition $g = g_s + g_n$ satisfying the desired conditions in $\mathrm{GL}_n(\overline{k})$. For any $\sigma \in \mathrm{Gal}(\overline{k}/k)$, we have $\sigma(g) = \sigma(g_s) + \sigma(g_n)$. However, as we have $\sigma(g) = g$ and this decomposition also satisfies the desired conditions, the uniqueness property implies that $\sigma(g_s) = g_s$ and $\sigma(g_n) = g_n$. In other words, g_s and g_n belong to $\mathrm{GL}_n(k)$. □

The decomposition $g = g_s + g_n$ here is called the *additive Jordan decomposition* of g.

Corollary 1.6. *Let g be an element of $\mathrm{GL}_n(k)$. Then there exists a unique decomposition $g = g_s g_u$ such that*

- $g_s g_u = g_u g_s$,
- *g_s is semisimple, and*
- *g_u is unipotent, i.e., all the eigenvalues are 1 (equivalently, $g_u - 1$ is nilpotent).*

Proof. Let $g = g_s + g_n$ be the additive Jordan decomposition of g. Then we have $g = g_s(1 + g_s^{-1}g_n)$. Since $g_s^{-1}g_n$ is nilpotent (use that g_s and g_n commute), $1 + g_s^{-1}g_n$ is unipotent. Let us put $g_u := 1 + g_s^{-1}g_n$. As g_s commutes with g_u, $g = g_s g_u$ is a desired decomposition.

To check the uniqueness, let us assume that $g = g'_s g'_u$ is another such decomposition. Then, by putting $g'_n := g'_s(g'_u - 1)$, we get the additive Jordan decomposition $g = g'_s + g'_n$. By the uniqueness of the additive Jordan decomposition, we have $g'_s = g_s$ and $g'_u = g_u$. □

The decomposition $g = g_s g_u$ is called the *Jordan decomposition* of g.

In fact, the notion of the Jordan decomposition can be extended to much more general class of algebraic groups. The idea is to reduce the problem to the case of GL_n.

Definition 1.7. When an algebraic group G is isomorphic to a closed subgroup of GL_n for some n, we say that G is a *linear algebraic group.*

Definition 1.8 (Jordan decomposition)**.** Let G be a linear algebraic group over k. Let $\rho\colon G \hookrightarrow \mathrm{GL}_n$ be a closed embedding of algebraic group.

(1) We say that an element s of $G(k)$ is *semisimple* if $\rho(s) \in \mathrm{GL}_n(k)$ is semisimple.
(2) We say that an element u of $G(k)$ is *unipotent* if $\rho(u) \in \mathrm{GL}_n(k)$ is unipotent.
(3) For $g \in G(k)$, we say that g has a *Jordan decomposition* if there exist a semisimple $g_s \in G(k)$ and a unipotent $g_u \in G(k)$ satisfying $g = g_s g_u = g_u g_s$.

Proposition 1.9. *Being semisimple/unipotent is independent of the choice of* ρ*. Moreover, every element of* $G(k)$ *has a Jordan decomposition uniquely.*

Then, when can an algebraic group be linear? In fact, we have the following:

Proposition 1.10. *Let* G *be an algebraic group. Then* G *is affine if and only if* G *is linear.*

We don't give proofs of Propositions 1.9 and 1.10. See, for example, [Spr09, Section 2.4]. (In both propositions, the point of the proofs is to consider the action of G on its coordinate ring $k[G]$, which gives rise to a faithful representation of G.)

Remark 1.11. The Jordan decomposition can be explained in a quite simple way when the base field k is a finite field. Let us suppose that $k = \mathbb{F}_q$, whose characteristic is $p > 0$. Note that then, for any linear algebraic group G, the group $G(k)$ of its k-valued points is a finite group. In particular, any element $g \in G(k)$ is of finite order. In fact, we can show that $g \in G(k)$ is semisimple (resp. unipotent) if and only if the order of g is prime to p (resp. p-power). Furthermore, appealing to these characterizations, we can show the unique existence of the Jordan decomposition by an elementary arithmetic argument.

Exercise 1.12. Give a proof to the statement given in the above remark. To be more precise, prove that, for any element $g \in G(k)$,

(1) $g \in G(k)$ is semisimple if and only if the order of g is prime to p,
(2) $g \in G(k)$ is unipotent if and only if the order of g is p-power,
(3) there exists a unique decomposition $g = g_s g_u$ such that $g_s g_u = g_u g_s$, g_s is of prime-to-p order, and g_u is of p-power order.

1.4. **Tori.**

We investigate linear algebraic groups consisting only of semisimple elements:

Definition 1.13 (tori/diagonalizable groups)**.**

(1) We say that an algebraic group T over k is a *(k-rational) torus* if it is isomorphic to $\mathbb{G}_{\mathrm{m}}^r$ for some r (called the *rank* of T) over $\overline{k}$.
(2) We say that an algebraic group D over k is *diagonalizable* if it is isomorphic to a closed subgroup of a k-rational torus.

Proposition 1.14. *A connected linear algebraic group* G *over* k *is a torus if and only if* $G(\overline{k})$ *consists only of semisimple elements.*

Proof. See, for example, [Spr09, Corollary 6.3.6]. □

For an algebraic group G over k, we put

$$X^*(G) := \mathrm{Hom}_{\overline{k}}(G_{\overline{k}}, \mathbb{G}_{\mathrm{m}}),$$

i.e., the set of homomorphisms (as algebraic groups) from $G_{\overline{k}}$ to $\mathbb{G}_{\mathrm{m}}$ over $\overline{k}$. Such a homomorphism is called a *(absolute) character* of G. As $X^*(G)$ has a natural group structure, $X^*(G)$ is called the *(absolute) character group* of G. We also define the (absolute) cocharacter group of G by

$$X_*(G) := \mathrm{Hom}_{\overline{k}}(\mathbb{G}_{\mathrm{m}}, G_{\overline{k}})$$

(any homomorphism from $\mathbb{G}_{\mathrm{m}}$ to $G_{\overline{k}}$ is called a (absolute) cocharacter).

Suppose that T is a k-rational torus of rank r. Then $X^*(T)$ is a free abelian group of rank r equipped with an action of Γ_k defined by

$$\sigma(\chi) := \sigma_T \circ \chi \circ \sigma_T^{-1}$$

for any $\sigma \in \Gamma_k$ and $\chi \in X^*(T)$. Here, the symbol "σ_T" on the right-hand side denotes the isomorphism of $T_{\overline{k}}$ obtained by the pull-back of $\sigma\colon \operatorname{Spec}\overline{k} \to \operatorname{Spec}\overline{k}$ along the structure morphism (say $f\colon T_{\overline{k}} \to \operatorname{Spec}\overline{k}$):

$$\begin{tikzcd}
T_{\overline{k}} \arrow[r, "\sigma_T"] \arrow[d] & T_{\overline{k}} \arrow[d, "f"] \\
\operatorname{Spec}\overline{k} \arrow[r, "\sigma"] & \operatorname{Spec}\overline{k}
\end{tikzcd}$$

In fact, we have the following:

Proposition 1.15. *The association $T \mapsto X^*(T)$ defines an equivalence of categories between*

- *the category of tori over k and*
- *the category of free abelian groups of finite rank equipped with a Γ_k-action.*

Although any k-rational torus T is isomorphic to $\mathbb{G}_{\mathrm{m}}^r$ over $\overline{k}$ by definition, it might happen (quite often!) that T is not isomorphic to $\mathbb{G}_{\mathrm{m}}^r$ over k. In the above equivalence, $\mathbb{G}_{\mathrm{m}}^r$ corresponds to the free abelian group $\mathbb{Z}^{\oplus r}$ with trivial Galois action. We call the k-rational torus $\mathbb{G}_{\mathrm{m}}^r$ the *split torus (of rank r)*. In some sense, the nontriviality of the action of Γ_k on $X^*(T)$ exactly measures how T is far from being split.

Note that, for any k-rational torus T of rank r, its cocharacter group is also a free abelian group of rank r equipped with a Galois action. If we define a pairing $\langle -, - \rangle$ between $X^*(T)$ and $X_*(T)$ by

$$\mathrm{Hom}_{\overline{k}}(G_{\overline{k}}, \mathbb{G}_{\mathrm{m}}) \times \mathrm{Hom}_{\overline{k}}(\mathbb{G}_{\mathrm{m}}, G_{\overline{k}}) \to \mathrm{Hom}_{\overline{k}}(\mathbb{G}_{\mathrm{m}}, \mathbb{G}_{\mathrm{m}}) \cong \mathbb{Z}\colon (\chi, \chi^\vee) \mapsto \chi \circ \chi^\vee,$$

then $\langle -, - \rangle$ is perfect and equivariant with respect to the Galois actions. Here, the identification $\mathrm{Hom}_{\overline{k}}(\mathbb{G}_{\mathrm{m}}, \mathbb{G}_{\mathrm{m}}) \cong \mathbb{Z}$ is given by $[x \mapsto x^n] \leftrightarrow n$.

Example 1.16. Let k'/k be a finite extension. In general, for any linear algebraic group G' over k', there exists a linear algebraic group over k denoted by $\mathrm{Res}_{k'/k} G'$ and called *the Weil restriction (along k'/k) of G'*. As a functor of points, this linear algebraic group associates $G'(R \otimes_k k')$ to any k-algebra R. By applying this construction to the multiplicative group $\mathbb{G}_{\mathrm{m}}$ over k', we obtain a linear algebraic group $\mathrm{Res}_{k'/k} \mathbb{G}_{\mathrm{m}}$ such that $(\mathrm{Res}_{k'/k} \mathbb{G}_{\mathrm{m}})(R) = \mathbb{G}_{\mathrm{m}}(R \otimes_k k') = (R \otimes_k k')^\times$. (Note that, in particular, we have $(\mathrm{Res}_{k'/k}\mathbb{G}_{\mathrm{m}})(k) = k'^{\times}$.) In fact, $\mathrm{Res}_{k'/k}\mathbb{G}_{\mathrm{m}}$ is a k-rational torus whose character group is given by $\mathrm{Ind}_{\Gamma_{k'}}^{\Gamma_k}\mathbb{Z}$ as a free abelian group equipped with a Γ_k-action. We call a torus which is isomorphic to a product of tori of this form an *induced torus.*

Definition 1.17. Let G be a linear algebraic group over k. We say that a k-rational subtori T of G is a *(k-rational) maximal torus of* G if it is maximal among all k-rational subtori of G.

Example 1.18. Let $G := \mathrm{GL}_n$. Let T be the subgroup of G consisting of diagonal matrices. Then it is obvious that T is defined over k and isomorphic to $\mathbb{G}_{\mathrm{m}}^r$; especially, T is a k-rational subtorus of G. Let us check that T is a maximal torus. To do this, we suppose that T is contained in another k-rational subtorus T' of G. By taking the centralizers of T and T' in G, we get an inclusion $Z_G(T) \supset Z_G(T')$. (Recall that $Z_G(T) = \{g \in G \mid gtg^{-1} = t \text{ for any } t \in T\}$.) By an elementary computation, we can directly check that $Z_G(T)$ is equal to T itself. On the other hand, since T' is commutative, $Z_G(T')$ must include T'. Thus we get $T \supset T'$, which implies that $T = T'$.

Exercise 1.19. Prove the fact $Z_{\mathrm{GL}_n}(T) = T$, which is used in the above example.

Proposition 1.20. *Let G be a linear algebraic group over k. Then there exists a k-rational maximal torus of G. Moreover, all k-rational maximal tori of G are conjugate over $\overline{k}$. More precisely, if T_1 and T_2 are k-rational maximal tori of G, then there exists an element $g \in G(\overline{k})$ satisfying $T_2 = gT_1g^{-1}$.*

Proof. See, for example, [Spr09, 13.3.6. and 6.4.1.]. □

Note that this proposition does **not** say that all k-rational maximal tori are conjugate over k.

Example 1.21. Suppose that k'/k is a finite extension of degree n. If we choose a k-basis of k', then we can embed k' into $M_n(k)$ by sending $x \in k'$ to the matrix representation of the x-multiplication endomorphism of $k' \cong k^{\oplus n}$. This embedding induces an injective group homomorphism $(k' \otimes_k R)^{\times} \hookrightarrow \mathrm{GL}_n(R)$ for any k-algebra R functorially. In other words, we get an embedding of a torus $\mathrm{Res}_{k'/k}\mathbb{G}_{\mathrm{m}}$ into GL_n. The image of this embedding gives a k-rational maximal torus of GL_n which is not conjugate to the diagonal maximal torus over k. Indeed, it has the same rank as the split diagonal maximal torus, it must be maximal. But the Galois action on its character group is not trivial as explained in Example 1.16. Thus it cannot be conjugate to the split diagonal maximal torus over k.

In general, classifying all $G(k)$-conjugacy classes of k-rational maximal tori of a linear algebraic group over k could be a very deep problem. However, when $k = \mathbb{F}_q$ and G is "reductive", we can classify them in a simple and beautiful way. Because this classification is an important step for understanding Deligne–Lusztig theory, we will investigate it in detail later (2 or 3 weeks later?).

References

[Bor91] A. Borel, *Linear algebraic groups*, second ed., Graduate Texts in Mathematics, vol. 126, Springer-Verlag, New York, 1991.

[Spr09] T. A. Springer, *Linear algebraic groups*, second ed., Modern Birkhäuser Classics, Birkhäuser Boston, Inc., Boston, MA, 2009.

7:33pm, September 22, 2024