Galois lattices and toric varieties

V.E.Voskresenskii[1]

Various questions lead to consideration of algebraic varieties defined over a non-closed field k or over a ring. Let X be such variety, k_s a separable closure of the field k, $\mathcal{G} = \mathrm{Gal}\,(k_s/k)$ the Galois group of the k_s/k. Then we have the object which contains very rich information — the variety $\bar{X} = X \otimes_k k_s$ defined over the field k_s with the action of the group $\mathcal{G}$ on $\bar{X}$ through the second factor. So we get a large collection of associated $\mathcal{G}$-sets and $\mathcal{G}$-Galois modules: points $X(k_s)$, differential forms, divisors, $\mathrm{Pic}\,\bar{X}$, $\mathrm{Br}\,\bar{X}$, etc. So the investigation of the variety X can be divided into two steps: the geometric one — the investigation $\bar{X}$ over the field k_s, and the algebraic one — the investigation of Galois modules associated to the scheme $\bar{X}$ which is considered over k. This survey contains a detailed account of the second — algebraic — aspect of the investigation of the variety X. We suppose that the geometrical part is known.

The main part of the text is devoted to the theory of algebraic tori which are considered from the point of view of birational geometry.

During the past thirty years a new branch of mathematics was created — the theory of toric varieties which allows one to reduce a number of nonlinear problems to problems on integer points in some polyhedra. We can note such important problems as resolution of singularities, estimating the number of solutions of systems of equations, birational geometry of linear algebraic groups, the theory of invariants of transformation groups. Retrospectively, we see that the arithmetic of algebraic groups was missing more profound information about birational nature of group varieties at that time.

In the present text we give a comprehensive survey of results on birational geometry of algebraic tori. The author tried to expose some interesting results of Russian mathematicians published in hardly accessible journals. We also present here some new results on the rationality problem and on the arithmetic of integer models of tori defined over a p-adic field.

1. Diagonalizable groups and algebraic tori. First recall some facts and definitions. Let G be a linear algebraic group over a field k, $G = \mathrm{Spec}\,A$, where A is a Hopf algebra over k, that is A is a commutative associative k-algebra endowed with additional homomorphisms:

$$\begin{array}{rlll} m^*: & A \to & A \otimes_k A & (\textit{comultiplication}), \\ i^*: & A \to & A & (\textit{coinversion}), \\ m^*: & A \to & k & (\textit{counit}), \end{array}$$

which are subject to standard conditions of co-associativity, co-inversion, and co-unit.

It is well known that group structures on the affine scheme $\mathrm{Spec}\,A$ are in one-to-one correspondence with Hopf algebra structures on the algebra A. We note that this definition of group structure can be used not only for an algebra A over a field k but also for an arbitrary commutative algebra A over a commutative ring k with unity. If necessary, we shall use such a possibility. The group $G = \mathrm{Spec}\,A$ defined over a field k is a linear algebraic group in the case when A is of finite type over k and has no nilpotents.

Let us consider the structure of algebraic k-tori. Let $D_k(n)$ be a diagonal k-group, $D_k(n) = \mathrm{Spec}\,A$, $A = k[x_1, .., x_n, x_1^{-1}, .., x_n^{-1}]$, x_i are independent variables. Using the diagonal multiplication we can easily see that

$$m^*(x_i) = x_i \otimes x_i,\ i^*(x_i) = x_i^{-1},\ e^*(x_i) = 1.$$

[1]Partially supported by a grant of RFFI Grant 02-01-00017

Let A^* be the group of invertible elements of the ring A. In our case the group A^* is the direct product $A^* = k^* \times < x_1, .., x_n >$ where $< x_1, .., x_n >$ is the free Abelian group multiplicatively generated by elements x_i, the function x_i determines the regular map: $x_i : D_k(n) \to D_k(1) = G_{m,k}$ which is a group homomorphism. We shall call the function x_i a rational character of the group $D_k(n)$.

We shall denote the group $< x_1, .., x_n >$ by $\widehat{D(n)}$ and call it the group of rational characters of the diagonal group $D(n)$. Every character is of the form $x^a = x_1^{a_1} x_2^{a_2} ... x_n^{a_n}$, where $a_i \in Z$. The correspondence

$$x^a \to (a_1, a_2, .., a_n)$$

defines an isomorphism between the multiplicative group $\widehat{D(n)}$ and the additive group Z^n. Working with characters we shall freely go over from the multiplicative writing to the additive one and vice versa. We have $A^* = k^* \times \widehat{D(n)}$, and the ring A is the group ring $k[\widehat{D(n)}]$ of the multiplicative group $\widehat{D(n)}$.

Definition. A group T defined over a field k is called an algebraic torus if we have the following group isomorphism over the algebraic closure

$$T \otimes_k \bar{k} \cong D_{\bar{k}}(n). \tag{1}$$

In other words, T is a k-form of the group $D_k(n)$.

It is easy to show that in relation (1) we can replace the field $\bar{k}$ by k_s. We have an isomorphism of Hopf algebras $k_s[T]$ and $k_s[\widehat{D(n)}]$ which shows that $k_s[T]^*$ is the direct product of the groups ${k_s}^* \times \hat{T}$, where $\hat{T}$ is the group of rational characters of the torus $T \otimes k_s$. The Galois group $\mathcal{G}$ takes invertible elements to invertible ones, and since the unit of the group T is defined over the field k, the group $\mathcal{G}$ maps the group $\hat{T}$ into itself. So the group $\hat{T}$ is a $\mathcal{G}$-module. Let $x_1, .., x_n$ be a basis of the group $\hat{T}$, $\sigma \in \mathcal{G}$, then

$$\sigma(x_j) = \prod_{i=1}^{n} x_i^{a_{ij}}.$$

The matrix (a_{ij}) lies in the group $GL(n, \mathbf{Z})$. We have a representation $\varphi : G \to GL(n, \mathbf{Z})$ with finite image. Let $L = {k_s}^{\ker \varphi}$, $(L : k) = m$. Then L/k is the minimal splitting field of the torus $T : T \otimes_k L \cong D_L(n)$, the group $\Pi = \mathrm{Gal}\,(L/k)$ is isomorphic to the group $\varphi(G)$. The torus T can be explicitly described if the Π-module $\hat{T}$ and the extension L/k are known, where $\Pi = \mathrm{Gal}\,(L/k)$. Let us consider the group ring $L[\hat{T}]$, let $A = (L[\hat{T}])^{\Pi}$ be the ring of invariants. Then $\mathrm{Spec}\, A = T$. Let B be an arbitrary commutative k-algebra. It is easy to describe the group of points $T(B)$. In fact,

$$T(B) = \mathrm{Hom}_{\,k-ring}(k[T], B) = \mathrm{Hom}_{\,L-ring}(L[T], B \otimes_k L)^{\Pi} =$$

$$\mathrm{Hom}_{\,gr}(\hat{T}, (B \otimes_k L)^*)^{\Pi} = \mathrm{Hom}_{\,\Pi}(\hat{T}, (B \otimes_k L)^*).$$

In particular, $T(k) = \mathrm{Hom}_{\,\Pi}(\hat{T}, L^*)$. So the torus T represents the functor

$$B \to \mathrm{Hom}_{\,\Pi}(\hat{T}, (B \otimes_k L)^*).$$

Examples. 1). The group $\mathbf{Z}$ has one generator $\mathbf{Z} =< e >$, either Galois group $\mathcal{G}$ acts trivially: $\sigma(e) = e, \;\; \forall \sigma \in \mathcal{G}$ or there is an element $\sigma \in \mathcal{G}$ such that $\sigma(e) = -e$. In the first case $T = D(1)$, in the second case the splitting field of a one dimensional torus T is a quadratic extension L, $(L : k) = 2$, $\Pi = \mathrm{Gal}\,(L/k) =< \sigma >$, $\sigma^2 = 1$, and

$$T(k) = \mathrm{Hom}_{\,\Pi}(\hat{T}, L^*) = \{\alpha \in L \mid \sigma(\alpha) = \alpha^{-1}\} = \{\alpha \in L \mid N_{L/k}(\alpha) = 1\}.$$

If $L = k(\sqrt{D})$ then the torus T is defined by the equation $x^2 - Dy^2 = 1$.

2). It is necessary to find all finite subgroups in $GL(2, \mathbf{Z})$ up to conjugacy. There are two maximal non-conjugate groups: W_1 and W_2. The group W_1 is the group of all integer automorphisms of the quadratic form $x_1^2 + x_2^2$, the group W_2 is group of all integer automorphisms of the form $x_1^2 + x_1x_2 + x_2^2$. The group $W_1 = D_4$ is a dihedral group, $|W_1| = 8$. The group $W_2 = D_6$ is a dihedral group, $|W_2| = 12$.

Explicit geometric constructions describing the groups W_1 and W_2 allow one to find affine and projective realizations of the corresponding algebraic tori. We shall return to this question later. It should be noted that the tori corresponding to the subgroups of the group W_1 are realized as open subsets of two-dimensional quadrics; the tori corresponding to the subgroups of W_2 are realized either as open subsets of the projective plane $\mathbf{P}_k^2$ or as open subsets of a Del Pezzo surface of degree six. Here is an example. Suppose $U \subset W_2$, $|U| = 6$, $F = \mathbf{Q}(\sqrt[3]{D})$, $(F\colon \mathbf{Q}) = 3$, then the norm torus is determined by the following equation

$$T\colon x^3 + Dy^3 + D^2z^3 - 3Dxyz = 1.$$

Tori of the form $R_{F/k}(G_m)$, which are elementary examples after trivial tori $D_k(n) = G_{m,k}^n$, play the most important role in problems of affine realization of algebraic tori.

The group $R_{F/k}(G_m)$. We know that the coordinate ring of the diagonal torus $D_k(n)$ is the ring of Laurent polynomials.

$$k[D(n)] = k[x_1, .., x_n, x_1^{-1}, .., x_n^{-1}]$$

The embedding of the ring of polynomials of $k[A^n] = k[x_1, .., x_n]$ in $k[D_n]$ and the diagonal map : $k[A^n] \to k[A^n] \otimes_k k[D(n)]$ determine both the embedding of corresponding spectra $D(n) \to A^n$ and the action of the group $D(n)$ on A^n. Let a $\mathcal{G}$-module $\hat{T}$ of finite $\mathbf{Z}$-rank (torsion-free) be given by generators $x_1, .., x_n$ on which the group $\mathcal{G}$ acts transitively by permutations. Then we have a $\mathcal{G}$-invariant embedding

$$k_s[x_1, .., x_n] \to k_s[x_1, .., x_n, x_1^{-1}, .., x_n^{-1}] = k_s[\hat{T}]$$

Going over to $\mathcal{G}$-invariants and the corresponding spectra we get an open k-embedding of the torus T into A_k^n with a natural action of the torus T on A_k^n. Let $\mathcal{G}_1$ be a subgroup in $\mathcal{G}$ consisting of all elements which leave elements of module $\hat{T}$ fixed. Then $\hat{T}$ is a Π-module where $\Pi = \mathcal{G}/\mathcal{G}_1$. Let $L = k_s^{\mathcal{G}_1}$ is the minimal splitting field of T, $\Pi = \mathrm{Gal}\,(L/k)$, π is the stabilizer of the element x_1 in $\hat{T}$, $F = L^{\Pi}$, $(F : k) = n$. Then the Π-module $\hat{T}$ is isomorphic to the Π-module $\mathbf{Z}[\Pi/\pi] = \mathbf{Z}\Pi \otimes_\pi \mathbf{Z}$ spanned by the left cosets of Π with respect to the subgroup π. The torus T with the module $\hat{T} = \mathbf{Z}[\Pi/\pi]$ is denoted $R_{F/k}(G_m)$. The group of k-points $T(k)$ is of the form

$$T(k) = R_{F/k}(G_m)(k) = \mathrm{Hom}_{\,\Pi}(\mathbf{Z}\Pi \otimes_\pi \mathbf{Z}, L^*) = \mathrm{Hom}_{\,\pi}(\mathbf{Z}, L^*) = F^*.$$

The last relation allows one to describe the torus $T(k) = R_{F/k}(G_m)$ in the most simple and natural way. Let $w_1, ..., w_n$ be a basis of the extension F/k. We have the regular faithful representation of the elements of the field F by square matrices of order n with entries from the field k.

$$(\alpha w_1, ..., \alpha w_n) = (w_1, ..., w_n)T_\alpha, \quad \alpha \to T_\alpha,\ T_\alpha \in GL(n, k),\ \alpha \neq 0.$$

The matrices T_α, $\alpha \in F^*$, generate a maximal k-torus in $GL_k(n)$ which is $R_{F/k}(G_m)$.

Let L/k be a Galois extension, $\Pi = \mathrm{Gal}\,(L/k)$. We denote the category of algebraic tori defined over k and split over L by $C(L/k)$, let $C(\Pi)$ be the category of torsion-free

Π-modules of finite $\mathbf{Z}$-rank. The correspondence $T \to \hat{T}$ defines a duality between the categories $C(L/k)$ and $C(\Pi)$. Let $\hat{S}$ be a permutation Π-module of the category $C(\Pi)$, i.e. $\hat{S}$ has a basis on which the group Π acts by permutations. Dividing the permutation basis into orbits of the group Π we get a representation of the Π-module $\hat{S}$ as a direct sum of indecomposable permutation modules $\hat{S}_i$

$$\hat{S} = \hat{S}_1 \oplus ... \oplus \hat{S}_t$$

. This construction gives a representation of the torus S as a direct product

$$S = R_{F_1/k}(G_m) \times ... \times R_{F_t/k}(G_m)$$

. Tori of such form are called quasi-split. The torus S is a maximal torus in the general linear group $GL_k(n)$, $n = \dim S$, and

$$S(k) = F_1^* \times ... \times F_t^*$$

Let T be an arbitrary torus of the category $C(L/k)$, $\hat{T}$ the corresponding Π-module of rational characters. The module $\hat{T}$ is the quotient $\hat{S}/\hat{R}$, where $\hat{S}$ is some permutation Π-module (for example, a free Π-module). An epimorphism $\hat{S} \to \hat{T}$ defines the embedding $T \to S$, and since S can be realized as a maximal torus of the general linear group $GL_k(n)$, $n = \dim S$, we get a faithful linear representation of our torus T. It is clear how to get a linear representation of minimal degree. Let us consider one more application of quasi-split tori. Let $\hat{T}^0 = \mathrm{Hom}\,(\hat{T}, Z)$ be the module dual to the module $\hat{T}$. For $\sigma \in \Pi$ and $f \in \hat{T}^0$ let $(\sigma f)(m) = \sigma[f(\sigma^{-1}m]$, $m \in \hat{T}$. Let us write an exact sequence of Π-modules

$$0 \to \hat{R} \to \hat{S} \to \hat{T}^0 \to 0,$$

where $\hat{S}$ is a permutation module. Going over to dual modules we get the exact sequence

$$0 \to \hat{T} \to \hat{S}^0 \to \hat{R}^0 \to 0,$$

We note that $\hat{S^0} \cong \hat{S}$, therefore we have an epimorphism of tori $S \to T$ and see that the function field $k(T)$ is a subfield of the $k(S)$ which is a purely transcendental extension of k. So every k-torus T is a unirational variety.

2. Picard group and Brauer group of a linear algebraic group. Let k be a field of characteristic 0, X an algebraic variety defined over k, $\bar{X} = X \otimes_k \bar{k}$, $\mathcal{G} = \mathrm{Gal}\,(\bar{k}/k)$. There is the Hochschild–Serre spectral sequence

$$H^p(\mathcal{G}, H^q(\bar{X}, G_m)) \Rightarrow H^n(X, G_m)$$

in étale cohomology which yields the eight-term exact sequence of abelian groups

$$0 \to H^1(k, \bar{k}[X]^*) \to \mathrm{Pic}\, X \to (\mathrm{Pic}\, \bar{X})^{\mathcal{G}} \to H^2(k, k[X]^*) \to$$

$$\to \ker(\mathrm{Br}\, X \to \mathrm{Br}\, \bar{X}) \to H^1(k, \mathrm{Pic}\, \bar{X}) \to H^3(k, \bar{k}[X]^*),$$

$$\mathrm{Pic}\, X = H^1(X, G_m),\ \mathrm{Br}\, X = H^2(X, G_m).$$

If the set of rational points $X(k)$ is not empty, we have a retraction $\mathrm{Spec}\, k \to X \to \mathrm{Spec}\, k$, and get a decomposition into direct sum

$$H^q(k, \bar{k}[X]^*) = H^q(k, k^*) \oplus H^q(k, U(\bar{X})) \quad where\ U(X) = k[X]^*/k^*$$

In this case the image of the homomorphism $H^1(k, \operatorname{Pic}\bar{X}) \to H^3(k, \bar{k}[X]^*)$ lies in $H^3(k, U(\bar{X})$. These facts can be applied in the case when X is the underlying variety of a connected linear algebraic k-group G. In this case $k[G]^* = \bar{k}^* \times \hat{G}$, and sequence (1) is of the form

$$0 \to H^1(k, \hat{G}) \to \operatorname{Pic} G \to (\operatorname{Pic}\bar{G})^{\mathcal{G}} \to H^2(k, \hat{G}) \to$$

$$\to \operatorname{Br} G/\operatorname{Br} k \to H^1(k, \operatorname{Pic}\bar{G}) \to H^3(k, \hat{G})$$

In particular, if $G = T$ is an algebraic torus then $\operatorname{Pic}\bar{T} = 0$, and we have

$$\operatorname{Pic} T = H^1(k, \hat{T}), \ \operatorname{Br} T = \operatorname{Br} k \oplus H^2(k, \hat{T})$$

If G is a connected semisimple group, then $\hat{G} = 0$ and this sequence is divided into two sequences:

$$\operatorname{Pic} G = (\operatorname{Pic} G)^{\mathcal{G}}, \ \operatorname{Br} G = \operatorname{Br} k \oplus H^1(k, \operatorname{Pic}\bar{G})$$

The group $\bar{G}$ contains a Borel subgroup B which is a semidirect product of a unipotent group N and a maximal torus T. The group G contains an open subset U which is isomorphic to the direct product $N \times T \times N$, and the complement $\bar{G} - \bar{U}$ is a union $\bigcup_{i=1}^{r} F_i$, where F_i is a prime divisor of the variety $\bar{G}$, r is the rank of the group $\bar{G}$ i.e. $r = \dim T$. Since all varieties are considered over the field $\bar{k}$, we have $\operatorname{Pic} U = 0$ and $\operatorname{Pic}\bar{G}$ is a finite group. Since $\operatorname{Pic} G = (\operatorname{Pic}\bar{G})^{\mathcal{G}}$, $\operatorname{Pic} G$ is a finite group for any connected semisimple group, taking into account an analogous result for tori we can see that $\operatorname{Pic} G$ is a finite group for any connected algebraic group. If $\tilde{G}$ is a connected simply connected semisimple group then, comparing étale and analytic cohomology, we get $\operatorname{Pic}\tilde{G} = 0$ and, more generally, $\operatorname{Pic} G = \widehat{\pi(\bar{k})}^{\mathcal{G}}$, where π is the fundamental group of a connected semisimple k- group G, $\widehat{\pi(\bar{k})} = \operatorname{Hom}(\pi(\bar{k}), \bar{k}^*)$. The articles [Po, Sa, V1] are dedicated to the calculation of the group $\operatorname{Pic} G$.

3. Birational invariants of algebraic varieties. Let G be a connected linear algebraic group defined over a field k, and let $k(G)$ be the field of rational functions of G. If k is a perfect field, G is a group variety unirational over k. This was proved by Chevalley for groups defined over a field of characteristic zero [Che], and then generalized by Rosenlicht to the case of an arbitrary perfect field of definition [Ro]. If k is algebraically closed, then $k(G)$ is purely transcendental over k, but for non algebraically closed fields Chevalley and Rosenlicht gave examples of groups G which are not rational over k. Further success has been reached using projective embeddings of a linear group. Methods using on this way are based, on the one hand, on the fundamental result of Hironaka about possibility of a resolution of singularities of rational maps of algebraic varieties, and on the other hand, on the theory of birational invariants developed in works of Yu.I. Manin and I.R. Shafarevich [Ma]. Since Hironaka's theorems are proved in general only in characteristic zero, we shall assume that k is of characteristic 0.

Thus, let X and Y be nonsingular projective irreducible varieties defined over a field k of characteristic 0, and assume that there is a birational morphism $\varphi : X \to Y$. We have the direct image

$$\varphi_* : \operatorname{Pic} X \to \operatorname{Pic} Y$$

which is an epimorphism and $\operatorname{Ker}\varphi_* = S$ is a free abelian group generated by finite number of prime divisors of variety X with supports in a closed subset $F \subset X$, where $F = \varphi^{-1}(W)$, W is a closed subset in Y consisting of all points in which the rational map φ^{-1} is not defined. Since we have the inverse image

$$\varphi^* : \operatorname{Pic} Y \to \operatorname{Pic} X$$

where $\varphi_*\varphi^* = Id$, the group $\mathrm{Pic}\, X$ is isomorphic to the direct sum:

$$\mathrm{Pic}\, X \cong \mathrm{Pic}\, Y \oplus S$$

If L is a normal extension of k, $\Pi = \mathrm{Gal}\,(L/k)$, then the morphism φ defines a birational L-morphism

$$\varphi \otimes 1 : X_L = X \otimes_k L \to Y \otimes_k L = Y_L$$

, and we get a Π-isomorphism

$$\mathrm{Pic}\, X_L \cong \mathrm{Pic}\, Y_L \oplus M, \tag{1}$$

where M is a torsion-free permutation Π-module of finite type. Let X and Y be birationally equivalent over k. Hironaka showed that there exist a nonsingular projective variety Z over the field k and birational morphisms $Z \to X$ and $Z \to Y$. Then from (1) it follows that there are permutation Π- modules S_1 and S_2 such that the direct sums $\mathrm{Pic}\, X_L \bigoplus S_1$ and $\mathrm{Pic}\, Y_L \bigoplus S_2$ are Π-isomorphic.

Definition. Let Π be a group, A and B arbitrary Π-modules. We call modules A and B similar if they differ only by permutation direct summands. The similarity class of a Π-module A is denoted by [A].

Theorem. (*Necessary condition of birational equivalence.*)

Let X and Y be nonsingular projective algebraic varieties over a field k of characteristic 0, L/k a normal extension with Galois group Π. If X and Y are birationally equivalent over k, then Π-modules $\mathrm{Pic}\, X_L$ and $\mathrm{Pic}\, Y_L$ are similar.

Corollary 1. Under the hypotheses of the theorem let F be an intermediate field, $k \subset F \subset L$, $\pi = \mathrm{Gal}\,(L/F)$. Then $H^1(L/F, \mathrm{Pic}\, X_L) = H^1(L/F, \mathrm{Pic}\, Y_L)$, the groups $H^1(L/F, \mathrm{Pic}\, X_L)$ are birational invariants of the variety X. For a finite extension L/k the groups $H^{-1}(L/F, \mathrm{Pic}\, X_L)$ are also birational invariants.

Let now a variety X be rational over $\bar{k}$. Then $\bar{X} = X \otimes_k \bar{k}$ is birationally equivalent to the projective space $\mathbf{P}^n \otimes_k \bar{k}$. Since $\mathrm{Pic}\, \mathbf{P}^n = \mathbf{Z}$, we have $\mathrm{Pic}\,(\bar{X}) \oplus S \cong \mathbf{Z} \oplus S_1$.

Corollary 2. Let X be a smooth projective variety defined over a field k of characteristic 0. If X is rational over $\bar{k}$ then the Π-module $\mathrm{Pic}\, X_L$ is torsion-free of finite $\mathbf{Z}$-rank. If the variety X is rational over the base field k, then $[\mathrm{Pic}\, X_L] = [0]$ and $H^{\pm 1}(L/F, \mathrm{Pic}\, X_L) = 0$ for any normal extension L/k, $k \subset F \subset L$.

4. Projective models of linear algebraic groups. Let G be a connected linear algebraic group defined over a field k of characteristic zero. Consider a nonsingular projective variety X over k which contains G as an open subset. The variety X is called a projective model of the group G. The variety $\bar{G} = G \otimes_k \bar{k}$ and, hence, $\bar{X}$ are rational over $\bar{k}$. So, $\mathcal{G}$- module $\mathrm{Pic}\, \bar{X}$ is torsion-free of finite $\mathbf{Z}$-rank. Although the model X is not uniquely determined if $\dim G > 1$, the similarity class of the $\mathcal{G}$-module $\mathrm{Pic}\, \bar{X}$ is determined uniquely. We shall denote it by $p_k(G)$ or simply $p(G)$ and call it the Picard class of the group G. It is easy to show that $p(G_1 \times G_2) = p(G_1) \bigoplus p(G_2)$, where the addition in the right-hand side is defined by direct sum. From the embedding $G \to X$ we get an exact sequence of modules

$$0 \to \hat{G} \to \hat{S} \to \mathrm{Pic}\, \bar{X} \to \mathrm{Pic}\, \bar{G} \to 0$$

where $\hat{S}$ is a permutation $\mathcal{G}$-module generated by the components of the closed subset $\bar{F} = \bar{X} \backslash \bar{G}$. Since the variety G is normal, $\bar{F}$ is an unmixed variety of codimension one. Let us consider two extreme cases:

a) $G = T$ is an algebraic torus. Then $\mathrm{Pic}\,\bar{T} = 0$ and we have an exact sequence of torsion-free modules

$$0 \to \hat{T} \to \hat{S} \to \mathrm{Pic}\,\bar{X} \to 0; \tag{1}$$

b) G is semisimple. Then $\hat{G} = 0$, we have

$$0 \to \hat{S} \to \mathrm{Pic}\,\bar{X} \to \mathrm{Pic}\,\bar{G} \to 0.$$

If $\bar{G}$ is simply connected, then $\mathrm{Pic}\,\bar{G} = 0$, in this case $\mathrm{Pic}\,\bar{X}$ is a permutation G-module. Let us consider the case a) in detail at finite level. Let L/k be a finite Galois extension with group Π, $T \in C(L/k)$. Similarly to (1) we can write the exact sequence (1) at finite level

$$0 \to \hat{T} \to \hat{S} \to \mathrm{Pic}\,\bar{X}_L \to 0 \tag{2}$$

Sequence (2) is a sequence of Π-modules, $\hat{S}$ is a permutation module. Let T_0 be the maximal subtorus in T split over k, $T_1 = T/T_0$ is anisotropic, i.e. $(\hat{T}_1)^\Pi = (0)$. The variety T is birationally equivalent to the product $T_0 \times T_1$ whence

$$p(T) = p(T_0 \times T_1) = p(T_1) \ and\ H^{-1}(L/k, p(T)) = H^{-1}(L/k, p((T_1)). \tag{3}$$

From sequence (2) we get an exact sequence

$$0 \to H^{-1}(L/k, \mathrm{Pic}\,X_L) \to \hat{H}^0(L/k, \hat{T}).$$

If the torus T is anisotropic, then $H^{-1}(L/k, \mathrm{Pic}\,X_L) = 0$. Formula (3) shows that for any torus $T \in G(L/k)$ the birational invariant $H^{-1}(L/k, p(T))$ equals 0. But then this is true for every intermediate field F, $k \subset F \subset L$.

Theorem 1. Let $T \in C(L/k)$, $k \subset F \subset L$. Then

$$H^{-1}(L/F, p_k(T)) = H^{-1}(L/F, p_F(T \otimes_k F)) = 0.$$

This is an unexpected result which is one of the most important in birational classification of algebraic tori. Now we can give a purely algebraic description of the birational invariant $[\mathrm{Pic}\,X_L] = p_{L/k}(T)$. Let $\hat{N}$ be a Π-module of the category $C(\Pi)$ with properties: $H^{-1}(\pi, \hat{N}) = 0$ for all subgroups π of Π. Following Colliot-Thélène and Sansuc we shall call such modules flasque modules. We shall call the exact sequence of Π-modules of the category $C(\Pi)$

$$0 \to \hat{T} \to \hat{S} \to \hat{N} \to 0, \tag{4}$$

where $\hat{S}$ is a permutation module, $\hat{N}$ is a flasque one, a flasque resolution of the module $\hat{T}$. One of flasque resolutions is sequence (2) obtained by geometric arguments. We have an important statement

Theorem 2. The similarity class $[\hat{N}]$ of the module $\hat{N}$ in the sequence (4) does not depend on the choice of a flasque resolution of the module $\hat{T}$. Therefore,

$$p_{L/k}(T) = [\mathrm{Pic}\,X_L] = [\hat{N}].$$

Since the algebraic definition of the birational invariant $p(T)$ is absolutely independent on the characteristic of the ground field, we want to extend these concepts to the case of characteristic $p > 0$. It can be done in the following way.

Let X be a smooth variety (not necessary projective) over a field k of arbitrary characteristic, and let L be a finite Galois extension of k with group Π. We assume that $\mathrm{Pic}\,X_L$ is of finite type. Then there is a nonempty open subset U in X such that $\mathrm{Pic}\,(U_L) = 0$.

The module $L[U]^*/L^*$ is torsion-free of finite type. Let $p(L[U]^*/L^*)$ be its Picard class in $C(\Pi)$. This class does not depend on the choice of a neighbourhood $U \subset X$ and is a birational invariant of the k-variety X. If X is a smooth projective variety, then $p(L[U]^*/L^*) = [\operatorname{Pic} X_L]$. Since a k-torus T always has a smooth projective model X in arbitrary characteristic (it will be mentioned later), the class $p(T)$ is a birational invariant in arbitrary characteristic.

5. The semigroup of stable equivalence. We shall call two k-varieties X_1 and X_2 *stably equivalent* if there is a birational isomorphism

$$X_1 \times_k A^m \cong X_2 \times_k A^n$$

for some m and n.

In the case if $X \times_k A^m \cong A^p$ we shall call X *stably rational.*

Clearly, if algebraic tori T_1 and T_2 are stably equivalent then $p(T_1) = p(T_2)$; if a torus T is stably rational then $p(T) = [0]$.

Let $\{T\}$ be class of stable equivalence of the torus T in the category $C(L/k)$. On the set of classes $\{T\}$ we shall define a structure of commutative semigroup setting

$$\{T_1\} \circ \{T_2\} = \{T_1 \times_k T_2\}.$$

The class of the tori which are stably rational over the field k plays the role of unity. We shall denote this semigroup by the symbol $Z(L/k)$. Let us introduce some notation. Let $S(\Pi)$ be the class of all permutation Π-modules of finite type,

$$H^q(\Pi) = \{M \in C(\Pi) \mid H^q(\pi, M) = 0 \ \forall \pi \subset \Pi\},$$

where H^q is the Tate cohomology. Clearly,

$$S(\Pi) \subset H^{-1}(\Pi) \cap H^1(\Pi) = \tilde{H}(\Pi)$$

Let

$$D(\Pi) = \{M \in C(\Pi) \mid M \oplus M' \in S(\Pi)\}$$

We have the following filtration:

$$S(\Pi) \subset D(\Pi) \subset \tilde{H}(\Pi) \subset H^{\pm 1}(\Pi) \subset C(\Pi)$$

The operation of direct sum of modules defines the structure of commutative semigroup on the set of similarity classes $C(\Pi)/S(\Pi)$, and the zero element is the class $S(\Pi)$. The classes $D(\Pi)/S(\Pi)$ form the maximal subgroup in the semigroup $C(\Pi)/S(\Pi)$. From the results of Jacobinski in the theory of lattices [Ja] it follows that this group is finitely generated. The assumption that $\tilde{H}(\Pi) = D(\Pi)$ is not true, we shall give an example later. The map $p_{L/k} : Z(L/k) \to H^{-1}(\Pi)/S(\Pi)$ was studied in the work of the author [V3].

Theorem 1. The map $p_{L/k}$ is an isomorphism of semigroups.

We are especially interested in tori from the kernel of the map p.

Theorem 2. The following conditions are equivalent:

a) a torus T is stably rational over the field k;

b) the Picard class $p(T)$ is equal to zero;

c) the module of rational characters $\hat{T}$ of the torus T can be embedded into an exact sequence of the form

$$0 \to \hat{T} \to \hat{S} \to \hat{S}_1 \to 0,$$

where $\hat{S}$ and $\hat{S}_1 \in S(\Pi)$.

6. Chevalley modules. Let us give now some important examples illustrating efficeince of the criteria mentioned in the previous paragraphs. Let Π be a finite group, π its subgroup, $\mathbf{Z}(\Pi)$ the group ring, $\mathbf{Z}[\Pi/\pi]$ the module spanned by cosets $e_1, ..., e_n$ on which the group Π acts by permutations. Let us consider the map $\varepsilon : \mathbf{Z}[\Pi/\pi] \to \mathbf{Z}$, defined by the equality

$$\varepsilon(\sum_{i=1}^{n} a_i e_i) = \sum_{i=1}^{n} a_i.$$

Clearly ε is a Π-homomorphism. Let $I_{\Pi/\pi} = \mathrm{Ker}\,\varepsilon$. We have

$$0 \ \to \ I_{\Pi/\pi} \ \to \ \mathbf{Z}[\Pi/\pi] \xrightarrow{\varepsilon} \ Z \ \to \ 0. \tag{1}$$

Going over to dual modules we get the dual sequence

$$0 \to Z \xrightarrow{\varepsilon_0} Z[\Pi/\pi] \to J_{\Pi/\pi} \to 0, \tag{2}$$

where $J_{\Pi/\pi} = I^0_{\Pi/\pi}$, $\varepsilon_0(1) = e_1 + ... + e_n$. Let L/k be a Galois extension with group Π, F an intermediate field such that $\mathrm{Gal}\,(L/F) = \pi$. Sequences (1) and (2) define exact sequences of k-tori

$$1 \to G_{m,k} \to R_{F/k}(G_m) \to T_1 \to 1,$$

$$1 \to T_2 \to R_{F/k}(G_m) \to G_{m,k} \to 1.$$

Since $R_{F/k}(G_m)$ can be identified with an open subset in $R_{F/k}(A^1) = A^n_k$, the torus T_1 admits an open embedding into the projective space P^{n-1}_k, hence, T_1 is rational over k, $p(T_1) = [0]$. From this point of view the torus T_2 is more interesting. The variety T_2 can be represented as a norm hypersurface $N(x_1, ..., x_n) = 1$ in the space A^n_k, where $x_1, ..., x_n$ are the coordinates of an element of the field F in some basis. The torus T_2 has a standard notation $R^{(1)}_{F/k}(G_m)$, its module of rational characters $J_{\Pi/\pi}$ is called Chevalley module. Chevalley was the first mathematician who discovered nonrationality of tori of the form $R^{(1)}_{F/k}(G_m)$ for some extensions F/k [Che]. We consider a special case. When $\pi = (1)$, the sequence (2) takes the form

$$0 \to I_\Pi \to Z[\Pi] \xrightarrow{\varepsilon} Z \to 0 \tag{3}$$

An arbitrary module is a quotient of a free module, hence we have an exact sequence

$$0 \to \hat{N}^0 \to \hat{P}^0 \to I_\Pi \to 0, \tag{4}$$

where P is a free Π-module. From (3) and (4) it follows that

$$H^1(\pi, \hat{N}^0) = \hat{H}^0(\pi, I_\Pi) = H^{-1}(\pi, Z) = 0$$

for any subgroup π of Π. So

$$\hat{N} = \mathrm{Hom}\,(\hat{N}^0, Z) \in H^{-1}(\Pi).$$

Going over in (4) to dual modules, we get a flasque resolution of the Chevalley module

$$0 \ \to \ J_\Pi \ \to \ \hat{P} \ \to \ \hat{N} \ \to \ 0$$

From (3) and (4) we conclude that $H^1(\pi, \hat{N}) = H^3(\pi, Z)$ is a birational invariant of the torus $R^{(1)}_{L/k}(G_m) = T$. This fact allos one to find non-rational tori. For example, if Π contains a subgroup π of the form $Z/pZ \times Z/pZ$, where p is prime, then the torus $R^{(1)}_{L/k}(G_m)$ is not rational over the field L^{Π} and moreover, over the field k, because

$$H^3(Z/pZ \times Z/pZ, Z) = Z/pZ \neq 0.$$

For a cyclic group Π the modules I_{Π} and J_{Π} are isomorphic, therefore for a cyclic extension L/k the torus $R^{(1)}_{L/k}(G_m)$ is rational over k.

As it has been shown in investigations of, mainly, S. Endo and T. Miyata [E-M1,E-M2], the condition of invertibility of the element $p(J_{\Pi})$ imposes very serious restrictions on the structure of Π. Let us state the results in the order of strengthening of requirements.

Theorem 1. The following conditions are equivalent:
1) every Sylow subgroup of Π is either cyclic or a generalized quaternion group;
2) all abelian subgroups of Π are cyclic;
3) $H^3(\pi, Z) = 0$ for all subgroups $\pi \in \Pi$;
4) $p(J_{\Pi}) \in H^1(\Pi)/S(\Pi)$.

We shall call a finite group *metacyclic* if all its Sylow subgroups are cyclic.

Theorem 2. The following conditions are equivalent:
1) the group Π is metacyclic;
2) the class $p(J_{\Pi})$ is invertible;
3) $H^1(\Pi) = H^{-1}(\Pi) = D(\Pi)$.

Example. Let Π be the quaternion group of the order 8. Then by Theorem 1, $p(J_{\Pi}) \in H^1(\Pi)/S(\Pi)$, but $p(J_{\Pi})$ is not invertible by Theorem 2. Hence,$\tilde{H}(\Pi) \neq D(\Pi)$.

The following subtle theorem [E-M1, E-M2] completely describes stably rational tori of the form $R^1_{L/k}(G_m)$ in the case when L/k is a Galois extension.

Theorem 3. Let Π be a finite group. The following conditions are equivalent:
1) $\Pi =< s, t >$, $t^m = s^{2^n} = 1$, $sts^{-1} = t^2$, m – odd, $r^2 \equiv 1 (mod\ m)$;
2) $p(J_{\Pi}) = 0$;
3) $p(J_{\Pi})$ has a finite order.

The rank of the group $D(\Pi)/S(\Pi)$ was calculated by A. Dress [Dr], the torsion in some cases was studied by Endo and Miyata [E-M1, E-M2]. For example, if Π is a finite p-group, then the group $D(\Pi)/S(\Pi)$ is a factor of the projective class group of the ring $Z(\Pi)$ and hence is finite.

Let us consider one more important example, which was obtained recently by Colliot-Thélène and Kunyavskii (independently). Let F/k be a separable extension of prime degree p, $T = R^{(1)}_{F/k}(G_m)$. If the extension F/k is normal then the torus T is rational over k; since F/k is cyclic, $J_{\Pi} = I_{\Pi}$. Let the extension F/k be not normal, let L be the normal closure of the field F in k_s, $\Pi = \mathrm{Gal}\,(L/k)$, $\pi = \mathrm{Gal}\,(L/F)$, $(F : k) = p$, $(L : F) = m$, $(m, p) = 1$. Let us choose a Π-module $\hat{N}$ from the class $p_{L/k}(T)$. For an arbitrary Sylow subgroup Π_q of Π, the Π_q-module $\hat{N}$ lies in $D(\Pi_q)$. But then $\hat{N} \in D(\Pi)$. Thus there is $\hat{N}' \in C(\Pi_q)$ such that $\hat{N} \bigoplus \hat{N}' \in S(\Pi)$. It has been shown that the product of the tori $T \times_k N$ is k-rational variety. The simplest nontrivial example is given by a non-normal extension F of degree five over k such that $(L : k) = 20$. In this case $p(R^{(1)}_{F/k}(G_m))$ is invertible but has infinite order in the group $D(\Pi)/S(\Pi)$.

7. Tori of small dimension. All one-dimensional tori are k-rational. As it was mentioned at the beginning, two-dimensional tori are determined by subgroups of maximal finite subgroups W_1 and W_2 in the group $GL(2, \mathbf{Z})$. The group W_1 of order 8 is the group of motions of a square, it acts biregularly on $\mathbf{G}_m \times \mathbf{G}_m$, and using the embedding

$\mathbf{G}_m \times \mathbf{G}_m \to \mathbf{P}^1 \times \mathbf{P}^1$ its action can be extended to a biregular action on $\mathbf{P}^1 \times \mathbf{P}^1$. Therefore the tori of type W_1 can be embedded into projective models which are k-forms of the variety $\mathbf{P}^1 \times \mathbf{P}^1$. All such k-forms are rational over k if they have a rational k-point. Thus the tori of this type are k-rational.

The group W_2 is the group of motions of a regular hexagon. It acts regularly on $\mathbf{G}_m \times \mathbf{G}_m$ and birationally on $\mathbf{A}^2$ or $\mathbf{P}^2$. In the homogeneous coordinates $(x:y:z)$ of the plane $\mathbf{P}^2$ the action of the group $W_2 =< \sigma, \tau, \omega >$ can be given as follows: σ cyclically permutes the coordinates $(x:y:z)$; $\tau(a,b) = (a^{-1}, b^{-1})$, where $a = x/z, b = y/z$; ω is a the transposition $(x:y:z) \to (x:z:y)$. Let us choose the following rational functions on $\mathbf{P}^2$

$$u = \frac{y-z}{x-y}, \quad v = au = \frac{x(y-z)}{z(x-y)}$$

The fields $k(u,v)$ and $k(a,b)$ are isomorphic, and explicit calculations show that in the basis (u,v) the group W_2 acts by the rule

$$\sigma(u,v) = \left(-\frac{u+1}{u}, -\frac{v+1}{v}\right), \qquad \tau(u,v) = (v,u), \qquad \omega(u,v) = \left(-\frac{u}{u+1}, -\frac{v}{v+1}\right).$$

So the group W_2 is conjugate in the group of birational k-transformations of the plane to a subgroup of the group $Aut_k(\mathbf{P}^1 \times \mathbf{P}^1)$. Therefore, as in the previous case, the corresponding torus is birationally equivalent over k to a form of the variety $\mathbf{P}^1 \times \mathbf{P}^1$ and, hence, is rational over k. Thus all tori of dimension 2 are rational over the ground field.

The classification of 3-dimensional tori over a ground field was studied by B. Kunyavskii [Ku1, Ku2]. Most tori are no longer rational over k but every stably rational k-torus of dimension 3 is in fact k-rational. He also studied tori with biquadratic splitting field [Ku1]. It has been shown that an arbitrary torus $T \in C(L/k)$, $\Pi = \mathrm{Gal}\,(L/k) = Z/2Z \times Z/2Z$ has a permutation resolution:

$$0 \to \hat{T} \to \hat{S} \to \hat{S}_1 \to \hat{S}_2 \to 0,$$

where $\hat{S}, \hat{S}_1, \hat{S}_2 \in S(\Pi)$. It turned out that the semigroup $Z(L/k)$ has one generator and is isomorphic to the additivr semigroup $\mathbf{Z}_+$ of natural numbers (with zero). The generator is the class of the 3-dimensional torus $R^{(1)}_{L/k}(G_m)$. Moreover B. Kunyavskii obtained a full classification of the tori of the category $C(L/k)$ up to birational equivalence. It turned out that any torus $T \in C(L/k)$ is birationally equivalent to a direct product

$$T \cong (R^{(1)}_{L/k}(G_m)^n \times G^d_{m,k}$$

The tori $R^{(1)}_{L/k}(G_m)^n \times G^d_{m,k}$ and $R^{(1)}_{L/k}(G_m)^m \times G^r_{m,k}$ are birationally equivalent iff $n = m$, $d = r$. Thus every stably rational torus $T \in C(L/k)$ is rational.

The question about the number of generators of the semigroup $Z(L/k)$ was studied in the work of A.L. Chistov [Ch2]. He has shown that as a rule the semigroup $Z(L/k)$ has infinite number of generators. Thus, if $\Pi = \mathrm{Gal}\,(L/k)$ is a p-group and $p > 2$ then $Z(L/k)$ has a finite number of generators only in the case of a cyclic group. For a 2-group Π it has been shown that $Z(L/k)$ is not finitely generated if the minimal number of generators of the group Π is more than two. Then, if the order of Π is equal to 2^n and Π is not isomorphic to a cyclic group, a dihedral group D_{2^n}, a generalized quaternion group H_{2^n} or the group Q_n with generators σ, τ and relations

$$\sigma^{2^{n-1}} = \tau^2 = 1,\ \tau\sigma = \sigma^m\tau, \quad m = 2^{n-2} - 1,$$

then the semigroup $Z(L/k)$ in not finitely generated. The cases D_{2^n} H_{2^n} Q_n, $n \geq 4$, remain open. If $\Pi = D_8$ then $Z(L/k) \cong \mathbf{Z}_+^{11}$; if $\Pi = H_8$ then $Z(L/k) = \mathbf{Z}_+^6$, if $\Pi = Q_3 = \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$, then $Z(L/k)$ is not a finitely generated.

8. Tori with a cyclic splitting field. Let Π be the cyclic group of order n with generator $\sigma, \Pi = \mathrm{Gal}\,(L/k)$. The group ring $\Lambda = \mathbf{Z}[\Pi] = \mathbf{Z}[\sigma]$ is isomorphic to the ring $Z[x]/(x^n - 1)$. Let ζ_n be a primitive root of the polynomial $x^n - 1$, $\Phi_n(x)$ a cyclotomic polynomial, i.e. the minimal polynomial of the ring $\mathbf{Z}[x]$ for which ζ_n is a root. We have a decomposition

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

The ring $\mathbf{Z}[x]/(\Phi_n(x))$ is isomorphic to the ring of integers $Z[\zeta_d]$ of the cyclotomic field $\mathbf{Q}(\zeta_d)$. For any monic polynomial $f \in \mathbf{Z}[x]$ dividing $x^n - 1$, let $R(f)$ be the torus from $C(L/k)$ with Π-module of rational characters $\mathbf{Z}[\sigma]/(f(\sigma))$. Clearly $R(x^n-1) = R_{L/k}(G_m)$. Let $h_d(x) = x^d-1$, $d \mid n$, and $f \in \mathbf{Z}[x]$ such that $fh_d \mid h_n$. Then we have an exact sequence of k-tori

$$1 \to R(h_d) \overset{\alpha}{\to} R(fh_d) \overset{\beta}{\to} R(f) \to 1$$

and the morphism B has a rational k-section. So we have a birational isomorphism

$$R(fh_d) \cong R(h_d) \times_k R(h_d), \tag{1}$$

which allows us to carry out inductive arguments. Using such "dévissage" we get the following representation.

Theorem 1. For a cyclic extension L/k we have a birational isomorphism of varieties

$$R_{L/k}(G_m) \cong \prod_{d|n} R(\Phi_d).$$

The torus $R(\Phi_d)$ has as the module of rational characters the ring of integers $\mathbf{Z}[\zeta_d]$.

Corollary. The torus $R(\Phi_n)$ is stably rational over k for any n.

Thus, over a number field we have infinitely many stably rational tori of rather simple construction. The question about rationality of these tori as we shall see later is very basic but unfortunately the answer has been obtained only in very particular cases. We can simplify the problem. Let $n = p_1^{d_1}, ...p_s^{d_s}$ be the canonical decomposition of the number n, $d_i \geq 1$, $n_0 = p_1...p_s$ the square-free kernel of the number n, Π_0 - a subgroup of order n_0 of the group Π, L_0 the field of Π_0-invariants of the field L. The formula $\Phi_n(x) = \Phi_{n_0}(y)$, $y = x^{n/n_0}$ shows that

$$R(\Phi_n) = R_{L_0/k}(R(\Phi_{n_0})).$$

It follows that the rationality of the form $R(\Phi_n)$ will be proved if it will be done for square-free numbers n.

Let now T be an arbitrary torus of the category $C(L/k)$ where L/k is a cyclic extension with group Π. Consider a flasque resolution of the Π-module of rational characters $\hat{T}$

$$0 \longrightarrow \hat{T} \longrightarrow \hat{S} \longrightarrow \hat{N} \longrightarrow 0 \tag{2}$$

All properties of the Picard class considered above used the invertibility of the class $p(T)$ for the tori with a cyclic splitting field. This is a really basic fact, and it implies excellent algebraic-arithmetic properties of cyclic extensions. To prove invertibility of the class $[\hat{N}]$, consider a flasque resolution of the module $\hat{N}$

$$0 \longrightarrow \hat{N} \longrightarrow \hat{S}_1 \longrightarrow \hat{M} \longrightarrow 0 \tag{3}$$

We have $Ext_{\Pi}(\hat{M},\hat{N}) = H^1(\Pi, \mathrm{Hom}\,(\hat{M},\hat{N}))$. Furthermore,

$$\hat{M}, \hat{N} \in H^{-1}(\Pi) = H^1(\Pi),$$

because Π is a cyclic group. Let Π_p be the p-Sylow subgroup of Π. By induction we can check that the Π_p-modules $\hat{M}$ and $\hat{N}$ lie in $D(\Pi_p)$. But then $H^1(\Pi_p, \mathrm{Hom}\,(\hat{M},\hat{N})) = 0$ for all Sylow subgroups Π_p of Π, whence $Ext_{\Pi}(\hat{M},\hat{N}) = 0$. Hence $\hat{N} \bigoplus \hat{M} \cong \hat{S}_1$ and $H^1(\Pi) = D(\Pi)$.

Using invertibility of the classes $[\hat{N}]$ of a flasque module $\hat{N}$ in the cyclic case, A. Chistov introduced new multiplication on the category $C(\Pi)$ as follows. First, since the group Π is commutative, any left Π-module A can be also viewed as a right Π-module. Then the tensor product $A \otimes_{\Pi} B$ is also equipped with the structure of Π-module. If one of the modules $\hat{T}_1$, $\hat{T}_2$ lies in $D(\Pi)$, set

$$\hat{T}_1 \circ \hat{T}_2 = (\hat{T}_1 \otimes_{\Pi} \hat{T}_2)/t(\hat{T}_1 \otimes_{\Pi} \hat{T}_2)$$

where $t(A)$ is the torsion submodule of the module A. If $\hat{T}_1$ and $\hat{T}_2$ are arbitrary modules from $C(\Pi)$ and

$$0 \longrightarrow \hat{T}_1 \longrightarrow \hat{S}_1 \xrightarrow{p_1} \hat{N}_1 \longrightarrow 0$$
$$0 \longrightarrow \hat{T}_2 \longrightarrow \hat{S}_2 \xrightarrow{p_2} \hat{N}_2 \longrightarrow 0$$

are their flasque resolutions, we have an epimorphism

$$\tilde{p}_2(\hat{T}_1) : \hat{T}_1 \circ \hat{S}_2 \to \hat{T}_1 \circ \hat{N}_2,$$

induced by the projection p_2. We set

$$\hat{T}_1 \circ \hat{T}_2 = \ker \tilde{p}_2(\hat{T}_1)$$

One can check that the product $\hat{T}_1 \circ \hat{T}_2$ does not depend on the choice of flasque resolutions and there are canonical isomorphisms:

$$\hat{T}_1 \circ \hat{T}_2 = \hat{T}_2 \circ \hat{T}_1, \qquad \hat{T}_1 \circ (\hat{T}_2 \circ \hat{T}_3) = (\hat{T}_1 \circ \hat{T}_2) \circ \hat{T}_3$$

. Note that $\hat{T} \circ Z\Pi = \hat{T}$. Let T_1 and T_2 be algebraic tori of the category $C(L/k)$. Define $T_1 \circ T_2 \in C(L/k)$ as the torus dual to the Π-module $\hat{T}_1 \circ \hat{T}_2$. For an arbitrary torus $T \in C(L/k)$ and a monic polynomial $f \in \mathbf{Z}[X]$, $f \mid (x^n - 1)$, we set $T(f) = T \circ R(f)$. Note that the Π-module $\widehat{T}(\Phi_d)$ can be regarded as a $\mathbf{Z}[\zeta_d]$-module, and since it is torsion-free, $\widehat{T}(\Phi_d)$ is a projective $\mathbf{Z}[\zeta_d]$-module, $d \mid n$. The following important lemma is a generalization of the relation (1).

Lemma. Let f be a monic polynomial from $\mathbf{Z}[X]$ such that $fh_d \mid h_n$. Then for any torus $T \in C(L/k)$ we have a birational isomorphism of varieties

$$T(fh_d) \cong T(f) \times_k T(h_d).$$

Now we can make the “dévissage” of an arbitrary torus $T \in C(L/k)$ by similar arguments. We get the following remarkable theorem of Chistov [Chi1].

Theorem 2. Let L/k be a cyclic extension of degree n. Any torus $T \in C(L/k)$ is birationally equivalent over k to the product

$$\prod_{d|n} T(\Phi_d).$$

For any $d \mid n$ the character module $\widehat{T}(\Phi_d)$ is a projective $\mathbf{Z}[\zeta_d]$-module. A torus T is stably rational over k iff for any d, $d \mid n$, the module $\widehat{T}(\Phi_d)$ is $\mathbf{Z}[\zeta_d]$-free.

Corollary 1. In the case when Π is a cyclic p-group, every stably rational k-torus T is rational over k, $T \in C(L/k)$, $\Pi = \mathrm{Gal}\,(L/k)$.

In this case the theorem reduces to checking the tori $T(\Phi_d)$ for which $T(\Phi_d) = \mathbf{Z}[\zeta_d]$, $d = p^\alpha$. Further reduction reduces the problem to the module $\mathbf{Z}[\zeta_p]$ for which the torus $R(\Phi_p)$ is rational.

Corollary 2. Let L/k be a cyclic extension. Then the group $Z(L/k)$ is a finite group isomorphic to the direct product over all $d \mid n$ of the class groups of the rings $\mathbf{Z}[\zeta_d]$.

Corollary 3. Under the hypotheses of the theorem, let $\hat{T}$ be a projective Π-module. Then the following conditions are equivalent:

1) $p(T) = 0$,
2) $\widehat{T}(\Phi_d)$ is a free $\mathbf{Z}[\zeta_d]$-module for $d \mid n$,
3) the torus T is rational over k.

Why from projectivity of $\hat{T}$ and stable rationality of T does k-rationality follow? The answer is as follows. Every projective Π -module is a direct sum of a free Π-module $\hat{T}_1$ and a projective ideal $\hat{T}_2 \in \mathbf{Z}[\Pi]$. The torus T_1 is k-rational and the $\mathbf{Z}$-rank of the module $\hat{T}_2$ is equal to n. Hence,

$$T_2 \cong \prod_{d \mid n} T_2(\Phi_d) \cong \prod_{d \mid n} R(\Phi_d) \cong R_{L/k}(G_m).$$

9. Projective invariant Demazure models. As we have seen problems of birational classification of varieties of linear algebraic groups necessarily lead to consideration of smooth projective varieties containing a given group as an open set. The existence of such projective models follows (in characteristic zero) from Hironaka's theorem on the resolution of singularities. In many cases we manage to get valuable information from the very fact of the existence of such smooth models but more delicate questions require an explicit construction of the model, or least information about its Picard group. For algebraic tori we have a rather simple (we can say, canonical) construction of complete models suggested by Demazure. Since we are mainly interested in models defined over non-closed fields, our ficus is on toric varieties with maximal symmetry groups.

Let T be an algebraic k-torus, $\hat{T}$ its group of rational characters. First consider the case of an algebraically closed field k. The group $\hat{T}$ is a free abelian group of rank $n = \dim T$, let $T_{\mathbf{Q}} = \mathbf{Q} \otimes \hat{T}$ be the corresponding linear space over $\mathbf{Q}$ with natural embedding $\hat{T} \subset \hat{T}_{\mathbf{Q}}$. We call a cone σ in $\hat{T}_{\mathbf{Q}}$ a polyhedral cone generated by a finite system of elements $m_1, ...m_N$ from $\hat{T}$:

$$\sigma = \left\{ \sum_{i=1}^{N} \lambda_i m_i \mid \lambda_i \geq 0 \right\}.$$

If the cone σ contains no subspaces from $\hat{T}_{\mathbf{Q}}$ besides (0), then we say that the cone has a vertex.

It is necessary for us to have two different realizations of the group $\hat{T}$: additive and multiplicative. The multiplicative writing is necessary for construction of subrings of the group ring $k[\hat{T}]$, the additive one is suitable in geometric constructions. The group $\hat{T}$ with additive structure will be often called a lattice. Let $m_1, ..., m_n$ be a basis of the lattice $\hat{T}$, and let $x_i = e^{m_i}$ be symbols generating the multiplicative group $\hat{T}$. Let us denote by A_σ the semigroup k-algebra $k[\sigma \bigcap \hat{T}]$ which consists of the Laurent polynomials $\sum s_m x^m$ where $a_m \in k$, $m \in \sigma \bigcap \hat{T}$ and almost all coefficients a_m are equal to zero. We call the scheme X_σ an affine toric variety. The diagonal embedding $A_\sigma \to A_\sigma \otimes_k k[\hat{T}]$ defines an action of the torus T on the scheme X_σ. It is convenient to use dual objects. Let $\hat{T}^0 = \mathrm{Hom}\,(\hat{T}, \mathbf{Z})$ be the dual lattice and

$$\sigma^0 = \left\{ r \in \hat{T}^0_{\mathbf{Q}} \mid r(m) \geq 0 \quad \forall m \in \sigma \right\}$$

be the dual cone in the space $\hat{T}^0_{\mathbf{Q}}$. The scheme X_σ is smooth iff the dual cone σ^0 is generated by a part of a basis of the lattice $\hat{T}^0$ [Da, De, Ke].

A complete toric variety is constricted by gluing affine toric varieties, and the scheme of gluing is determined by some set of cones called a fan. It is convenient to work with fans in the space $\hat{T}^0_{\mathbf{Q}}$.

Definition. We call a fan in the space $\hat{T}^0_{\mathbf{Q}}$ a finite set $\sum$ of cones satisfying the conditions

a) all cones from $\sum$ have vertices;

b) if τ is a face of a cone $\sigma \in \sum$, then $\tau \in \sum$;

c) for σ and $\sigma' \in \sum$ the intersection is a face both in σ and in σ'

Let $\sigma \in \sum$, and let σ^0 be the dual cone in $\hat{T}_Q$. The symbol X_σ now stands for $\mathrm{Spec}\, k[\sigma^0 \bigcap \hat{T}]$. Note that every X_σ contains an open set on which the torus T acts regularly $\dim X_\sigma = n$. If τ is a face of a cone $\sigma \in \sum$, then we have a canonical morphism $X_\tau \to X_\sigma$ which is an open embedding. Gluing together the affine parts X_σ with respect to the open embeddings

$$X_{\sigma \bigcap \sigma'} \to X_\sigma, \quad X_{\sigma \bigcap \sigma'} \to X_{\sigma'}$$

we get a normal algebraic variety X_Σ defined over k with an action of the torus T on X_Σ. A fan is called complete if $\bigcup_{\sigma \in \Sigma} \sigma = \hat{T}^0_{\mathbf{Q}}$ It is a necessary and sufficient condition of for X_Σ to be a complete variety. Smoothness of the variety X_Σ means that all cones $\sigma \in \sum$ are simplicial and spanned by parts of a basis of the lattice $\hat{T}^0$. In dimensions greater than 2 complete toric varieties may be non-projective. A criterion of projectivity says that the fan consists of cones generated by faces of a convex polyhedron $D \subset \hat{T}^0_{\mathbf{Q}}$ containing 0 as an inner point. The fan $\sum$ admits another interpretation in the language of orbits of the torus T acting on X_Σ. For an open affine T-invariant subset $U \subset X_\Sigma$ we denote by $\hat{T}(U)$ the set of characters which can be continued to regular functions on U. Let

$$\sigma(U) = \left\{ r \in \hat{T}^0_{\mathbf{Q}} \mid r(m) \geq 0 \;\; \forall m \in \hat{T}(U) \right\}$$

. Then $\sigma(U) \in \sum$. On the other hand, every such U contains a unique closed in U orbit (the orbit of minimal dimension). This gives a one-to-one correspondence $\sigma \to O_\sigma$ between cones from $\sum$ and orbits O_σ of the torus T in X_Σ. In this case $\sigma \subset \tau \Leftrightarrow O_\tau \subset O_\sigma$ and $\dim \sigma = \mathrm{codim}\, O_\sigma$. For example, orbits of codimension 1 are in one-to-one correspondence to one-dimensional cones (rays) from $\sum$. Every such ray $\sigma \in \sum$ is generated by a unique primitive vector $r \in \hat{T}^0$, let $|\sum|$ be the collection of these primitive vectors, and let O_r, $r \in |\sum|$ be the corresponding orbit of codimension 1. The closure $O_r = D_r$ of an orbit O_r in X_Σ is a divisor of the variety X_Σ. Let X_Σ be a smooth complete toric variety. The embedding $T \subset X_\Sigma$ defines an exact sequence of lattices

$$0 \to \hat{T} \xrightarrow{\alpha} \hat{S} \to \mathrm{Pic}\, X_\Sigma \to 0, \tag{1}$$

where $\hat{S}$ is a free $\mathbf{Z}$-module generated by the prime divisors from the complement $X \setminus T$. We see that the divisors D_r, $r \in |\sum|$ form a basis of the group $\hat{S}$ so that the rank of $\hat{S}$ is equal to the cardinality of the set $|\sum|$. The map α is defined by the rule:

$$\alpha(m) = \sum_r r(m) D_r, \quad r \in |\Sigma|, \quad m \in \hat{T}$$

The anticanonical divisor of a complete smooth variety X_Σ is of the form

$$-K = \sum D_r, \quad r \in |\Sigma|.$$

Let now k be a non-closed field, $\mathcal{G} = \mathrm{Gal}\,(k_s/k)$, T an algebraic n-dimensional torus defined over k. We have an integral representation $h : \mathcal{G} \to GL(n, \mathbf{Z})$ defined by the action of the group $\mathcal{G}$ on the characters $\hat{T}$ of the torus T. The splitting group $h(\mathcal{G})$ is a finite subgroup in $GL(n, \mathbf{Z})$. The torus T can be reconstructed using h as follows. The group $G_m^n \otimes_k k_s$ carries two representations of the group $\mathcal{G}$: the geometric one $g \to h(g) \otimes 1$ and the arithmetic one $g \to 1 \otimes g$, $g \in \mathcal{G}$. They commute. Consider the representation $u(g) = h(g) \otimes g$ of $\mathcal{G}$ in $Aut_k(G_m^n \otimes k_s)$. Then T is isomorphic to the factor $(G_m^n \otimes_k k_s)/u(\mathcal{G})$. Let us choose in the lattice $\hat{T}^0$ a smooth projective fan $\sum$ invariant under the finite group $h(\mathcal{G})$. We can always do it by a suitable partition starting with any complete fan [Br]. Then the group $h(\mathcal{G})$ acts naturally by automorphisms of X_Σ, and we have an equivariant embedding $G_m^n \subset X_\Sigma$. The factor $X = (X_\Sigma \otimes_k k_s)/u(\mathcal{G})$ is a k-form of the variety $X_\Sigma \otimes k$ containing the torus T as an open subset. This proves the existence of a smooth projective model of the torus T over an arbitrary field. The scheme X will be called a Demazure model of the torus T. It is very convenient for the calculation of the $\mathcal{G}$-module $\mathrm{Pic}\,(X \otimes_k k_s)$ because the $\mathcal{G}$-module $\mathrm{Pic}\,(X \otimes_k k_s)$ is isomorphic to the $\mathcal{G}$-module $\mathrm{Pic}\, X_\Sigma$ on which the group $\mathcal{G}$ acts geometrically. The sequence (1) allows one to calculate the action of the group $\mathcal{G}$ on $\mathrm{Pic}\, X_\Sigma$ if we know the action of the group $\mathcal{G}$ on $\hat{T}$ and on the edges of the fan $\sum$. Now let us go over to the question of practical construction of invariant projective fans and Demazure varieties of dimension n. Jordan's theorem says that there is a finite number of non-conjugate finite subgroups in the group $GL(n, \mathbf{Z})$. For every such group W we can construct a projective invariant fan in the lattice $M^0 = \mathbf{Z}^n$ and the model X_Σ. Certainly, here the question about the most economic construction with minimal number of simplices arises. Of course, for distinct groups $W_1 \subset W_2 \subset GL(n, \mathbf{Z})$ their minimal fan can be the same. If we shall not take care about minimality of the model, it will be sufficient to construct projective invariant fans for maximal finite subgroups of the group $GL(n, \mathbf{Z})$. The number of maximal subgroups is less than the number of all subgroups. For example, for $n = 2$ there are 17 subgroups and 2 maximal subgroups; for $n = 3$ there are 73 subgroups and 4 maximal ones; for $n = 4$ there are 710 groups and 9 maximal ones.

Example. 1) There is only one smooth projective one-dimensional toric model, the projective line $\mathbf{P}^1$.

2) For $n = 2$ there are two maximal subgroups W_1 and W_2. The group W_1 is of order 8, it is the group of automorphisms of the root system of type B_2. The root lattice B_2 is a usual square lattice. The fan consists of 4 basic quadrants and all its parts. We have $X_\Sigma = \mathbf{P}^1 \times \mathbf{P}^1$.

The group W_2 is of order 12, it is the group of automorphisms of the root system A_2. The fan contains 6 basic cones. The scheme $X_\Sigma \otimes k$ is a Del Pezzo surface of degree 6 obtained from P^2 by blowing up three points.

3) In dimension 3 we have 4 maximal finite subgroups in the group $GL(3, \mathbf{Z})$. They are, respectively, the groups of automorphisms of the cubic lattice L_0, the cubic lattice with the centers of cubes added L_1, the cubic lattice the centers of faces added L_2, and the group of automorphisms of the lattice which is a direct sum of the one-dimensional lattice and the two-dimensional hexagonal lattice.

Using these explicit geometric constructions, B. Kunyavskii obtained a complete birational classification of three-dimensional tori [Ku2]. From 73 three-dimensional lattices he selected 15 lattices for which the corresponding tori are not rational and are not pairwise stably equivalent. All tori of dimension 3 except these 15 tori are k-rational. In particular, all stably rational three-dimensional tori are in fact rational.

Let us consider the birational invariant $H^1(k, p(T)) = H^1(\mathcal{G}, \operatorname{Pic} X_\Sigma)$ more carefully. The sequence (1) shows that for its calculation we only need information on the action of the finite group $\Pi = h(\mathcal{G})$ on the lattice $\mathbf{Z}^n$. The flasque resolution (1) defines a commutative diagram with exact rows

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^1(\Pi, \hat{N}) & \longrightarrow & H^2(\Pi, \hat{T}) & \longrightarrow & H^2(\Pi, \hat{S}) \\ & & \downarrow res & & \downarrow res & & \downarrow res \\ 0 & \longrightarrow & H^1(< g >, \hat{N}) & \longrightarrow & H^2(< g >, \hat{T}) & \longrightarrow & H^2(< g >, \hat{S}) \end{array}$$

where $\hat{N} = \operatorname{Pic} X_\Sigma$, $g \in \Pi$. This diagram gives a natural monomorphism

$$0 \ \to \ H^1(\Pi, \hat{N}) \ \to \ \ker[H^2(\Pi, \hat{T}) \ \stackrel{res}{\to} \ \bigoplus_{g \in \Pi} H^2(< g >, \hat{T})].$$

From the injectivity of the map

$$H^2(\Pi, \hat{S}) \ \to \ \bigoplus_{g \in \Pi} H^2(< g >, \hat{S})$$

it follows that

$$H^1(\Pi, p(T)) = \ker[H^2(\Pi, \hat{T}) \ \to \ \bigoplus_{g \in \Pi} H^2(< g >, \hat{T})].$$

This formula can be found in [Sa]. An important class of tori is that of maximal tori in semisimple groups. B. Kunyavskii studying three-dimensional tori found the following phenomenon [Ku2]. Although there are finite subgroups $\Pi \subset GL(3, \mathbf{Z})$ for which $H^1(\Pi, \operatorname{Pic} X_\Sigma) \neq 0$ but for all maximal finite subgroups $\Pi \subset GL(3, \mathbf{Z})$ and the corresponding invariant fans $\sum$ we have the equality $H^1(\Pi, \operatorname{Pic} X_\Sigma) = 0$. The lattices L_0, L_1, L_2 are lattices of roots or weights of semisimple groups of rank 3. Further investigations of Kunyavskii in collaboration with the author [V-Ku] show that for a maximal k-torus T without affect in a connected adjoint semisimple group of classical type we have $H^1(k, p(T)) = 0$. We say that a maximal k-torus T in a semisimple group G has no affect if the splitting group of the torus T is isomorphic to the splitting group of the generic maximal torus of the group G [V5]. The situation with maximal tori was clarified by the following result of A. Klyachko [Kl].

Theorem. Let $W(R)$ and $A(R)$ be the Weyl group and the group of automorphisms of the root system R of a semisimple k-group G, $Q(R)$ and $P(R)$ be the root lattices and the weight lattice, respectively. Then

1) $H^1(W, p(T)) = 0$ for any W-lattice $\hat{T}$, $Q(R) \subseteq \hat{T} \subseteq P(R)$;
2) $H^1(\Pi, p(P(R)) = H^1(\Pi, p(Q(R)) = 0$, $W(R) \subseteq \Pi \subseteq A(R)$;
3) if the system R is irreducible then

$$H^1(\Pi, p(T)) = 0 \quad W(R) \subseteq \Pi \subseteq A(R), \quad Q(R) \subseteq \hat{T} \subseteq P(R).$$

This theorem has interesting applications to the arithmetic of linear algebraic groups. Let us consider maximal tori in adjoint groups of type A_n in more detail. The cases $n = 1, 2$ will be omitted because in these cases all tori are rational. The root lattice $Q(R)$ is constructed as follows: we choose the sublattice I_{n+1} in $\mathbf{Z}^{n+1}$ consisting of the points with zero sum of coordinates, then $Q(R) = I_{n+1}$. The symmetric group $S_{n+1} = W(R)$

acts naturally on $Q(R)$. The group of automorphisms $A(R)$ is a direct product $W(R)\times S_2$ where the second factor acts on $Q(R)$ by multiplication on (-1). Let us consider the $A(R)$-module $\hat{T} = I_{n+1} \otimes I_2$. T is a maximal k-torus without affect in the adjoint group G of type A_n, and the Galois group acts on $\hat{T}$ via the group $A(R)$. Consider two cases:
1) G is an inner form of type A_n. In this case the Galois group acts via $W(R)$, the factor I_2 is not needed, we have an open embedding of the torus T in $\mathbf{P}^n$ over k, all maximal tori and the group G are k-rational.
2) G is an outer form of type A_n, $\hat{T} = I_{n+1} \otimes I_2$. In this case one can prove that for even n the torus T_n and the group G are k-rational [V-Kl]. The torus T_3 is not rational for the splitting group $S_4 \times S_2$.

10. Arithmetic of linear algebraic groups. Let k be a number field, i.e. a finite extension of the field of rational numbers $\mathbf{Q}$, let $n = [k : \mathbf{Q}]$ be the degree of this extension. For any valuation v of the field k we denote by k_v the completion of k with respect to v. It is known that there are finitely many $r_1 + r_2$ archimedian normalized valuations and a countable set of non-archimedian ones for every prime ideal $\wp$ of the field k, and $r_1 + 2r_2 = n$. In the case of a non-archimedian valuation we shall often write $k_\wp$ instead of k_v. There is an important product formula for normalized valuations

$$\prod_v v(a) = 1, \quad a \neq 0, \quad a \in k$$

Instead $v(a)$ we often write $|a|_v$. The symbol $\mathcal{O}$ will denote the ring of integers of the field k, $\mathcal{O}_\wp$ is the ring of integers of the field $k_\wp$. Let now W be a vector space over the field k of finite dimension m, M a lattice in W, i.e. a finitely generated $\mathcal{O}$-module in W containing a basis of W. In this case $k \otimes_{\mathcal{O}} M \cong kM = W$. For every valuation v of k we set $W_v = k_v \otimes_k W$ and identify W with the k-space in W_v consisting of the elements $1 \otimes x$, $x \in W$. Let G be a linear algebraic group defined over k. We call an integer form of the group G a group $\mathcal{O}$-scheme X such that there is a group isomorphism of k-groups $X \otimes_v k \cong G$. The existence of an integer form X for a group G is checked very easily. One of the methods of its construction is the following one [V-F]. We have a faithful linear representation of the group G in the general linear group $\varphi : G \to GL_k(n)$ that gives an epimorphism $\varphi^* : k[GL(n) \to k[G]$ of Hopf algebras. The ring $k[GL(n)]$ is of the form $k[x_{11}, ...x_{nn}, y^{-1}]$, $y = \det(x_{ij})$, the O-algebra $O[x_{11}, ...x_{nn}, y^{-1}]$ defines in $GL_k(n)$ the integer group structure $GL_{\mathcal{O}}(n)$ and $\varphi^*(O[x_{11}, ...x_{nn}, y^{-1}]) = A$ is an O-Hopf algebra in $k[G]$. Note that the choice of coordinates x_{ij} in $GL_k(n)$ is the group of automorphisms of V. Let $M =< e_1, ..., e_n >$ be a free O-lattice in V. Thus, every faithful linear representation φ of G defines a group O-form $G_{\varphi,M} = \operatorname{Spec} A$ of G. Although the structure of Hopf algebra $k[G]$ does not depend on the choice of a faithful representation φ, but a priori this cannot be said about the groups $G_{\varphi,M}$. Note that all O-forms X of the form $G_{\varphi,M}$ are of finite type over $\mathcal{O}$, they are reduced and faithfully flat over $\mathcal{O}$. The ring A is a subring in $k[G]$ with the conditions :

1) A is an O-Hopf algebra of finite type over $\mathcal{O}$;

2) $A \bigcap k = \mathcal{O}$, $kA = k[G]$;

3) the structure of Hopf algebra in the ring A is induced by the structure of Hopf algebra $k[G]$.

Definition. A subring A of the ring $k[G]$ satisfying conditions 1) - 3) is called an *O-Hopf order* in $k[G]$, $X = \operatorname{Spec} A$ is a group O-form of finite type of the group G.

Having an O-form X we can consider the scheme $X \otimes_{\mathcal{O}} \mathcal{O}/\wp$, which is a group scheme over the finite field $\mathcal{F}_\wp = \mathcal{O}/\wp$, and it is natural to call it the reduction of the scheme X modulo prime $\wp$. Certainly, this reduction depends on the choice of an integer model X, but in the case of algebraic tori we can choose a canonical model.

Let now A be the adele ring of k,

$$A^\infty = \prod_{v|\infty} k_v \prod_p \mathcal{O}_p$$

the subring of integer adeles of the ring A. We shall call the class number $h(X)$ of the group X the number of double cosets

$$G(k) \setminus G(A)/X(A^\infty) = H(X)$$

Problem. For a given k-group G, to decribe $\mathcal{O}$-forms X with minimal class number $h(X)$.

If G is commutative, the set $H(X)$ is a finite abelian group, it will be called the class group of the scheme X.

Let us remind two important arithmetic characteristics of linear algebraic groups G defined over a number field k. The monomorphism $G(k) \to G(k_v)$ defines the diagonal embedding $G(k) \to \prod_v G(k_v)$. The closure $\overline{G(k)}$ of the group $G(k)$ in the topology of direct product is a normal subgroup and the factor

$$A(G) = (\prod_v G(k_v))/\overline{G(k)}$$

is a finite commutative group. If $A(G) = 0$ then we shall say that the group G has weak approximation property. The group $A(G)$ is a birational invariant in the category of connected linear algebraic groups over k, $A(G) = 0$ for a stably rational group G. The second invariant appears when studying the set $H^1(k, G)$ of principal homogeneous spaces of the group G. We have a natural map

$$\varphi : H^1(k, G) \to \prod_v H^1(k_v, G).$$

The kernel of the map φ is denoted by $Sh(G)$, it is finite and consists of all principal homogeneous space of G having rational points in all fields k_v. As it was shown by Sansuc [Sa] the set $Sh(G)$ has a natural structure of an abelian group, it is called the Shafarevich-Tate group and is also a birational invariant of the group G. In the work [V2, V4] the author shows that these two arithmetic invariants $A(G)$ and $Sh(G)$ are closely related to the birational invariant $H^1(k, \operatorname{Pic} \bar{X})$ in the case when $G = T$ is a k-torus. Namely, there is an exact sequence of abelian groups

$$0 \to A(T) \to H^1(k, \operatorname{Pic} \bar{X})^\vee \to Sh(T) \to 0, \tag{1}$$

where $B^\vee = \operatorname{Hom}(B, \mathbf{Q}/\mathbf{Z})$. Hence, $A(T) = Sh(T) = 0$ if T has a metacyclic splitting field. We were sure that formula (1) is valid for every connected linear algebraic group G but realization of this idea required some efforts. First, formula (1) was not proved for semisimple connected simply connected groups, and it was an important problem. The point is that the module $\operatorname{Pic} \bar{X}$ is a permutation module for a simply connected group G, hence $H^1(k, \operatorname{Pic} \bar{X}) = 0$ and, having (1), we would easily get the relation $A(G) = Sh(G) = 0$ for simply connected groups. In fact, all terms of sequence (1) for simply connected groups are zero, but we have to calculate them independently from each other. Verification of the equality $Sh(G) = 0$ for simply connected groups required exhaustive work. The complete calculation can be found in the book [P-R]. Having equality (1) for tori and using triviality of $A(G)$, $Sh(G)$, $H^1(k, \operatorname{Pic} \bar{X})$ for simply connected groups, Sansuc established the formula

$$0 \to A(G) \to H^1(k, \operatorname{Pic} \bar{X})^\vee \to Sh(G) \to 0,$$

which is true for all connected linear algebraic groups [Sa]. Recently B. Kunyavskii and A. Skorobogatov gave an elegant proof of weak approximation property which includes the results of Kneser–Harder–Platonov–Sansuc [Ku-S]. They proved the following fact.

Theorem. Let G be a connected semisimple linear algebraic group defined over a number field k, let Y be the variety of maximal tori of the group G, $F = k(Y)$, and let H be a generic torus of the group G over F. If $H^1(F, p(H)) = 0$ then $A(G) = 0$.

The proof is based on the existence of dense set of points in $Y(k)$ over which the corresponding tori have no affect and on rationality of the variety Y.

Using the results of A. Klyachko from Section 9 we get $A(G) = 0$ for the following connected semisimple groups G:

1) G is simply connected,

2) G is adjoint,

3) G is absolutely simple.

We want to have something similar for calculation of the group $Sh(G)$ for semisimple simply connected group G.

Let us come back to algebraic tori. Let k be the field of $\wp$-adic numbers, and let T be a torus over k. The group $T(k)$ is locally compact. Let U be the maximal compact subgroup of $T(k)$. Consider the $\mathcal{O}$-algebra

$$B = \{f \in k[T] \mid f(u) \in \mathcal{O} \quad \forall u \in U\}$$

Since the group U is Zariski dense in $T(k)$, the restriction of Hopf operators of the algebra $k[T]$ to B defines the structure of Hopf O-algebra on B. Then $Y = \operatorname{Spec} B$ is a group scheme over O and $Y \otimes_O k \;\cong\; T$. We shall call the scheme $Y = \operatorname{Spec} B$ the *minimal integer model* of the torus T. The definition of Y is very easy but in general the model Y is not of finite type. (This fact was pointed out by B. Moroz.) Now we study another integral model of T which is also determined only by the parameters of T, see [P-V] and [VKM]. Let L/k be the minimal splitting field of T, $\Pi = \operatorname{Gal}(L/k)$. Let $\hat{T}$ be the Π-module of rational characters of T. The ring $k[T]$ is the ring of invariants of the group Π. This group acts on the field L and on the group $\hat{T}$. The Hopf algebra $k[T]$ of the torus T is of the form $(L[\hat{T}])^{\Pi}$ where $L[\hat{T}]$ is the group ring of the multiplicative group $\hat{T}$. The torus T is an L/k-form of the trivial torus $G^d_{m,k}$, $d = \dim T$, i.e. the embedding $k[T] \to L[\hat{T}]$ can be extended to an isomorphism $L \otimes_k C \;\cong\; LC = L[\hat{T}]$, here $C = k[T]$. Let us choose a basis $\omega_1, ..., \omega_n$ of L/k, then we have the decomposition into a direct sum

$$L[\hat{T}] = C\omega_1 \oplus \cdots \oplus C\omega_n. \tag{2}$$

Let $\chi \in \hat{T}$, then (2) implies the equality

$$\chi = f_1^{(\chi)}\omega_1 + \cdots + f_n^{(\chi)}\omega_n, \tag{3}$$

where $f_i^{(\chi)} \in C$. Clearly, the algebra $C = k[T]$ is generated by the coordinate functions $f_i^{(\chi)}$. A finite system of generators of the algebra C can be obtained by decomposing basic characters $\chi_1, .., \chi_d$ and inverse elements $\chi_1^{-1}, .., \chi_d^{-1}$, $d = \dim T$.

Choose an integral basis $\omega_1, ..., \omega_n$ of L/k and consider the ring A generated by the functions $f_i^{(\chi)}$ with integral coefficients. The algebra A does not depend on the choice of an integral basis L/k, it is of finite type over O, $A \cap k = O$, $kA = k[T]$. We claim that A is a Hopf algebra compatible with the operators of $k[T]$. The Hopf operators act on the basic characters by

$$m^*(\chi_i) = \chi_i \otimes \chi_i, \; i^*(\chi_i) = \chi_i^{-1}, \; e^*(\chi_i) = 1, \tag{4}$$

where $\chi_1, .., \chi_d$ is a basis of the group $\hat{T}$. Let

$$\chi_m = \sum_{k=1}^{n} x_k^{(m)} \omega_k$$

be the decomposition of a basic character according to (3), and let $y_m \in k[T]$ be the product of all distinct characters conjugate to χ_m,,

$$\omega_i \omega_j = \sum_{k=1}^{n} c_{ij}^k \omega_k, \tag{5}$$

where $c_{ij}^k \in O$ are the structure constants of the extension L/k. Easy calculations show that (4) can be written in the form

$$m^*(x_k^{(m)}) = \sum c_{ij}^k x_i^{(m)} \otimes x_j^{(m)};$$

$$i^*(x_k^{(m)}) = \frac{F_k^{(m)}}{y_m}, \quad \chi_m^{-1} = \frac{F_1^{(m)}}{y_m} \omega_1 + ... + \frac{F_n^{(m)}}{y_m} \omega_n; \tag{6}$$

$$e^*(x_k^{(m)}) = c_k, \; 1 = \sum_{j=1}^{n} c_j \omega_j.$$

The ring A is of the form $A = O[x_j^{(i)}, y_i^{-1}], \; 1 \leq i \leq d, \; 1 \leq j \leq n$. From (5), (6) it follows that the Hopf operators act on the ring and define the structure of O-Hopf algebra on A. The group scheme $X = \operatorname{Spec} A$ is of finite type over O, it is reduced and faithfully flat over O. This form does not depend on the choice of an integral basis of L/k, nor on the choice of a basis of the group $\hat{T}$. We call this model the *canonical minimal model* of T. The scheme Y constructed at the beginning of this section will be called the *maximal integral model* of T.

We have the embedding $O_L[\hat{T}] \;\subset\; A \otimes_O O_L$, where O_L is the ring of integers of the field L. An element $\chi \in \hat{T}$ defines a homomorphism $\chi : X(L) = T(L) \to L^*$. Consider the restriction of the map χ to the maximal compact subgroup U of $T(k) \subset T(L)$. The group $\chi(U)$ is a compact subgroup of L^*, i.e. χ maps the group U into O_L^*. Formulas (3) show that the values of any function $f(u), u \in U$, are from O. In other words, we have an inclusion of Hopf algebras $A \subset B$ and a homomorphism of group schemes $Y \to X$. Hence, we can formulate the following statements.

Theorem 1. Let k be a field of $\wp$-adic numbers with ring of integers O, T an algebraic k-torus. Then there exist two Hopf O-algebras A and B in $k[T]$ which are uniquely determined by the Π-module $\hat{T}$ according to the rules mentioned above. The schemes $X = \operatorname{Spec} A$ and $Y = \operatorname{Spec} B$ are O-forms of k-torus T. They have the following properties:

1. $B = \{f \in k[T] \mid f(u) \in O \;\; \forall u \in U\}$;

2. $A \subset B \subset k[T], \; A \cap k = B \cap k = O, \; k \otimes_O A = k \otimes_O B \cong kA = kB = k[T]$;

3. the algebra A is of finite type over O;

4. $X(O) = U = \operatorname{Hom}_{\Pi}(\hat{T}, O_L^*)$;

5. $O_L[\hat{T}] \subset O_L A$;

Proof. Clearly we only have to prove property 4). Let V be a vector space over k of dimension m and $T \subset GL(V)$. Choose a lattice M in V which is invariant under the action of the group U and $kM = V$. The elements of U can be represented by matrices from $GL(m, O)$ in a basis of M. Thus

$$X(O) = X(k) \cap GL(m, O) = U,$$

and

$$T(k) = \mathrm{Hom}_{\Pi}(\hat{T}, L^*) \subset \mathrm{Hom}\,(\hat{T}, L^*) = T(L) \simeq (L^*)^d, \ d = \dim T.$$

The group $\mathrm{Hom}\,(\hat{T}, O_L^*) \cong (O_L^*)^d$ is the maximal compact subgroup U_L of the group $T(L)$. The equality $T(k) = (T(L))^{\Pi}$ implies

$$X(O) \ = \ U \ = \ U_L \cap T(k) \ = \ U_L^{\Pi} \ = \ \mathrm{Hom}_{\Pi}(\hat{T}, O_L^*).$$

It should be mentioned that the isomorphism $U_L \cong (O_L^*)^d$ is not a Π-isomorphism.

Definition 1. We call the *reduction* $T_\wp$ of the torus T modulo $\wp$ the reduction

$$T_\wp = X \otimes_O O/\wp = \mathrm{Spec}\,(O/\wp \otimes_O A).$$

of its canonical integral model X.

The reduction is always a group scheme over the finite field $r_k = O/\wp$. We call the reduction *very nice* if $T_\wp$ is a torus over r_k; *nice* if $T_\wp$ is an algebraic group over r_k (reduced); *bad* if the group scheme $T_\wp$ is not reduced.

Theorem 2. If L/k is unramified then the minimal integral model of a k-torus T split over L is of the form $X = \mathrm{Spec}\, A$, where $A = (O_L[\hat{T}])^{\Pi}$. The scheme X is a torus over the ring O, the reduction $T_\wp$ is very nice.

Proof. We have an embedding $O_L[\hat{T}] \subset O_L A$ and the decomposition $\chi = f_1\omega_1 + ... + f_n\omega_n, \ f_i \in A, \ \chi \in \hat{T}$, where $\omega_1, .., \omega_n$ is an integral basis of L/k. For all $\sigma \in \Pi$ we have

$$\sigma\chi = f_1\sigma(\omega_1) + ... + f_n\sigma(\omega_n).$$

Since L/k is unramified, the determinant of the matrix $(\sigma_i(\omega_j))$ is invertible in the ring O_L, so $f_i \in O_L[\hat{T}]$ and $A = (O_L[\hat{T}])^{\Pi}$.

The reduction of a quasi-split torus. One of important objects in the theory of algebraic tori is a so-called quasi-split torus which can be represented as a product of tori of the form $R_{F/k}(\mathbf{G}_m)$. Recall the structure of the minimal model of the quasi-split torus described in [V-F]. Let $\omega_1, .., \omega_n$ be an integral basis of F/k, L the normal closure of F in k_s, $\Pi = \mathrm{Gal}\,(L/k)$, $\Pi_1 = \mathrm{Gal}\,(L/F)$, $S = R_{F/k}(\mathbf{G}_m)$, $\hat{S} = \mathbf{Z}[\Pi/\Pi_1] = \mathbf{Z}[\Pi] \otimes_{\Pi_1} \mathbf{Z}$. Choose a basis $\chi_1, .., \chi_n$ of the group $\hat{S}$ such that the group Π acts on it by permutations, Π_1 is the stabilizer of the element χ_1. We have decompositions

$$\chi_1 = x_1\omega_1 + ... + x_n\omega_n,$$
$$\chi_i = \sigma_i\chi_1 = x_1\sigma_i(\omega_1) + ... + x_n\sigma_i(\omega_n).$$

The Hopf algebra A of the minimal integral model of the torus S is of the form: $A = O[x_1, .., x_n, y^{-1}]$, here $y = \chi_1..\chi_n$ is a norm form of degree n in n variables $x_1, .., x_n$. The scheme $X = \mathrm{Spec}\, A$ is an O-form of the torus S. Since $O[x_1, .., x_n, y^{-1}]$ is a localization of the polynomial ring $O[x_1, .., x_n]$, the scheme X is smooth and connected. Consequently, $X_\wp$ is a connected algebraic group over r_k. Let us study the reduction in detail.

Let E be the maximal unramified extension of k in F. Then F/E is a totally ramified extension, $k \subset E \subset F$, $(E : k) = f$, $(F : E) = e$, $ef = n$, O_E and O_F are the rings of integers of the fields E and F, respectively. We can choose an integral basis in O_F in the following way. Let $\omega_1, ..., \omega_f$ be a basis of the unramified extension O_E/O and $1, \pi, ..., \pi^{e-1}$ an integral basis of O_F/O_E. Then $\omega_i \pi^j$ is an integral basis of the extension F/k. Note that

$$S = R_{F/k}(\mathbf{G}_m) = R_{E/k}(R_{F/E}(\mathbf{G}_m)).$$

Let $Y = \operatorname{Spec} C$ be the canonical integral model of E-torus $R_{F/E}(\mathbf{G}_m)$. The algebra C is of the form

$$C = O_E[z_0, ..., z_{e-1},\ u^{-1}],$$

where z_i are the coefficients of the decomposition

$$\chi_1 = z_0 + z_1\pi + ... + z_{e-1}\pi^{e-1},\ z_i \in E[R_{F/E}(\mathbf{G}_m)],$$

and u is the product of e distinct characters conjugated to χ_1 with respect to E. Since E/k is unramified, the discriminant of the basis $\omega_1, ..., \omega_f$ is a unit of O, so we can introduce new coordinates $x_k^{(i)}$ by the rule $z_i = \sum_{k=1}^{f} x_k^{(i)} \omega_k$. In other words, $X = R_{O_E/O_k}(Y)$. Let us study the structure of the reduction $Y_{\wp_E}$ of the scheme Y. It is well known that the residue fields r_F and r_E are equal and $u \equiv z_0^e \ (mod\ \wp_E)$. So

$$r_E \otimes_{O_E} C = r_E[z_0, z_1, ..., z_{e-1}, z_0^{-1}] = r_E[z_0, z_0^{-1}] \otimes r_E[z_1, ..., z_{e-1}],$$

i.e. the group r_E-scheme Y is a direct product of the torus $\mathbf{G}_{m,r_E}$ and the commutative r_E-group U_E. The group U_E is isomorphic to the affine r_E-group $\mathbf{A}_{r_E}^{e-1}$. Consider the regular representation of the group Y in the basis $1, \pi, ..., \pi^{e-1}$. One can see that the group $Y(r_E)$ can be represented by triangular matrices of the form

$$\begin{pmatrix} z_0 & 0 & \dots & 0 & 0 \\ z_1 & z_0 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ z_{e-2} & z_{e-3} & \dots & z_0 & 0 \\ z_{e-1} & z_{e-2} & \dots & z_1 & z_0 \end{pmatrix}.$$

Hence, the group U_E is triangular and the eigenvalues of U_E are equal to 1, i.e. U_E is unipotent. The reader can find a detailed description of connected unipotent groups over r_k, $char\ r_k = p > 0$ in [Se]. In particular, it is well known that any commutative unipotent r_k-group of period p is isomorphic to the product of groups $\mathbf{G}_{a,r_k}$. Our group U_E is of period p if $e \leq p$. Thus we have proved

Theorem. The reduction $X_\wp = R_{r_E/r_k}(Y_{\wp_E})$ of the torus $R_{F/k}(\mathbf{G}_m)$ can be represented as a direct product of the maximal torus $T_\wp = R_{r_E/r_k}(\mathbf{G}_m)$ of dimension f and a connected unipotent group $U_\wp = R_{r_E/r_k}(U_E)$ of dimension $(e-1)f$. If $e \leq p$ (where $p = char\ r_k$) then $U_\wp \ \cong\ \mathbf{G}_{a,k}^{(e-1)f}$.

If S is a quasi-split k-torus, i.e. S is a direct product of tori $R_{F/k}(\mathbf{G}_m)$, then the canonical integral model X of S is a product of canonical integral models of the tori $R_{F/k}(\mathbf{G}_m)$. Hence, the reduction $X_\wp$ is the product of the reductions of factors.

REFERENCES

[Br] Brylinski, J.-L., Decomposition simpliciale d'un réseau invariante par un groupe fini d'automorphismes, C.R.Acad.Sci.Paris, Ser. A-B **288** (1979), A137-A139.

[Che] Chevalley, C., On algebraic group varieties, J. Math. Soc. Japan **6** (1954), 303-324.

[Chi1] Chistov, A., On birational equivalence of tori with cyclic splitting field, Sem. LOMI Akad. Nauk SSSR **64** (1976), 153-158.

[Chi2] Chistov, A., On the semigroup of classes of stable equivalence of algebraic tori, Dokl. Akad. Nauk SSSR **242** (1978), No. 5, 1027-1029.

[C-S] Colliot-Thélène, J.-L. and Sansuc, J.-J., La R-équivalence sur les tores, Ann. Sci. Ecole Norm. Sup. **10** (1977), 175-230.

[Da] Danilov, V., The geometry of toric varieties, Uspekhi Math.Nauk **33** (1978), No. 2, 85-134.

[De] Demazure, M., Sous-groupes algébriques de rang maximum du groupe de Cremona, Ann. Sci. Ecole Norm. Sup. **4** (1970), No. 3, 507-588.

[Dr] Dress, A., The permutation class group of finite groups, J. Pure Appl. Algebra **6** (1975), 1-12.

[E-M1] Endo, S. and Miyta, T., Quasi-permutation modules over finite groups I, II, J. Math. Soc. Japan **25** (1973), 397-421 and **26** (1974), 698-713.

[E-M2] Endo, S. and Miyata, T., On a classification of the function fields of algebraic tori, Nagoya Math. J. **56** (1974), 85-104.

[Ja] Jacobinski, H., Genera and decompositions of lattices over orders, Acta Math. **121** (1968), 1-29.

[Ke] Kempf, G. et al., Toroidal embeddings I, Lecture Notes in Math. **339** (1973), Springer-Verlag.

[Kl] Klyachko, A., Tori without affect in semisimple groups, Arithmetic and Geometry of varieties, Kuibychev Univ., (1989), 67-78.

[Ku1] Kunyavskii, B., On tori with a biquadratic splitting field, Izv.Akad.Nauk SSSR, Ser.Math. **42** (1978), No 3, 580-587.

[Ku2] Kunyavskii, B., Arithmetic of three-dimensional algebraic tori, Sem. LOMI Akad. Nauk SSSR **116** (1982), 102-107.

[Ku-S] Kunyavskii, B. and Skorobogatov, A., Weak approximation in algebraic groups and homogeneous spaces, Contemp., Math. **131** (1991), 447-551.

[Ma] Manin, Ju., Rational surfaces over perfect fields, Publ. Math. IHES, (1966), No. 30, 55-97.

[P-R] Platonov, V. and Rapinchuk, A., Algebraic Groups and Number Theory, Moscow: Nauka, 1991.

[Po] Popov, V., Picard groups of homogeneous spaces of linear algebraic groups, Izv.Akad.Nauk SSSR, Ser. Math. **38** (1974), No 2, 292-322.

[P-V] Popov, S. and Voskresenskii, V., Galois lattices and reductions of algebraic tori, Communicat. in algebra **29(9)** (2001), 3711-3726.

[Ro] Rosenlicht, M., Some rationality questions on algebraic groups, Ann.Mat. Pura Appl. **43** (1957), 25-50.

[Sa] Sansuc, J.-J., Groupe de Brauer et arithmétique des groupes algébriques linéaires sur un corps de nombres, J. reine angew. Math. **327** (1981), 12-80.

[Se] Serre, J.-P., Groupes algébriques et corps de classes, Hermann, Paris, (1959).

[V1] Voskresenskii, V., Picard groups of linear algebraic groups, Studies in Number Theory, Saratov Univ., (1969), No. 3, 7-16.

[V2] Voskresenskii, V., On the birational equivalence of linear algebraic groups, Soviet. Math. Dokl. **10** (1969), 1212-1215.

[V3] Voskresenskii, V., Stable equivalence of algebraic tori, Math. USSR Izv. **8** (1974), 1-7.

[V4] Voskresenskii, V., Algebraic tori, Nauka, Moscow, 1977.

[V5] Voskresenskii, V., Maximal tori without affect in semisimple algebraic groups, Math.Notes **44** (1988), 651-655.

[V-Ku] Voskresenskii, V. and Kunyavskii, B., On maximal tori of semisimple algebraic groups, Dep. VINITI 5.03.84, N 1269.

[V-Kl] Voskresenskii, V. and Klyachko, A., Toroidal Fano varieties and root systems, Math. USSR Izv. **24** (1985), No 2, 221-244.

[V-F] Voskresenskii, V. and Fomina, T., Integer structures in algebraic tori, Izv. RAN, Ser. Math. **59** (1995), No 5, 3-18.

[VKM] Voskresenskii, V., Kunjavskii, B. and Moroz, B., On integral models of algebraic tori, Algebra and Analysis **14** (2002), 46-70.