# Integral models of tori

Mikdad, D.

ضرار محمد المقداد

D. Mikdad

# Integral models of tori

Doctoraalscriptie, defended on 22 June 2007

*Supervised by: Prof. dr. H. W. Lenstra Jr.*


Mathematisch Instituut, Universiteit Leiden

# Table of contents

# Introduction

A year ago Professor Hendrik Lenstra asked me the following question.

**Question.** Let $T$ be a one dimensional torus over a number field $K$. Furthermore assume that $\lambda$ is a point in $T(K)$ and $\lambda^{\mathbf{Z}}$ is Zariski-dense in $T$, i.e. $\lambda^{\mathbf{Z}}$ is infinite. Is it true that the set

$$S = \{n \in \mathbf{Z}_{>0} : \nexists \text{ prime ideal } \mathfrak{p} \text{ of } \mathcal{O}_K \text{ such that } n = \text{order}(\lambda \bmod \mathfrak{p})\}$$

is finite?

In this Master's thesis we give a positive answer and provide a proof at the end of chapter three.

In chapter one we study group schemes, which are group objects in the category of schemes. In chapter two we study tori over fields since the tori we are interessted in are defined over a number field. A group scheme $G$ of multiplicative type over a field $K$ is called a torus if there exists an $r \in \mathbf{N}$ such that $G \otimes_K K_s \cong (\mathbf{G}_{m,K_s})^r$, where $K_s$ is separable closure of $K$. The integer $r$ is called the rank of the torus. Furthermore we make an integral model for tori. We do that because we want to know the primes for which these tori have *good reduction*. In chapter three we provide a proof using heights to a special version of the theorem of Zsigmondy. Then we prove the main theorem.

**Open problem.** Suppose now that we replace $T$ by a two dimensional torus over $K$. Furthermore assume that $\lambda = (\lambda_1, \lambda_2)$ is a point in $T(K)$ and $\lambda^{\mathbf{Z}}$ is Zariski-dense, is it true that the set

$$S = \{n \in \mathbf{Z}_{>0} : \nexists \text{ prime ideal } \mathfrak{p} \text{ of } \mathcal{O}_K \text{ such that } n = \text{order}((\lambda_1, \lambda_2) \bmod \mathfrak{p})\}$$

is infinite?

If we take $K$ equal to $\mathbf{Q}$, then the answer is yes for $T = \mathbf{G}_m \times \mathbf{G}_m$ and $\lambda = (a, b)$ provided that we assume the Ailon-Rudnick conjecture [1] is true.

**Conjecture.** [Ailon-Rudnick] If two non-zero integers $a$ and $b$ are multiplicatively independent with $\gcd(a-1, b-1) = 1$, then there are infinitely many integers $n \geq 1$ such that

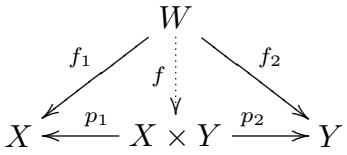
$$\gcd(a^n - 1, b^n - 1) = 1.$$

# 1 Group schemes

## ▶ Preliminaries

We begin this section by looking at the notion of a product in a category. We also treat functoriality and functor categories. The main reference of this section are the lecture notes of Professor Hendrik Lenstra, see [20].

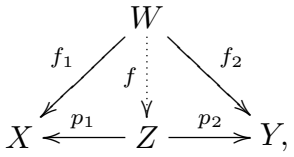
Suppose that we are given objects $X$ and $Y$ in a category $\mathcal{C}$. By a *product* of $X$ and $Y$, denoted by $X \times Y$, one means an object $Z$ in $\mathcal{C}$ together with morphisms $p_1 : Z \to X$ and $p_2 : Z \to Y$ such that $Z, p_1$, and $p_2$ satisfy the *universal property*: if $W$ is any object of $\mathcal{C}$ and $f_1 : W \to X$ and $f_2 : W \to Y$ are an arbitrary pair of morphisms, then there exists a unique morphism $f : W \to Z$ such that $f_1 = p_1 \circ f$ and $f_2 = p_2 \circ f$.



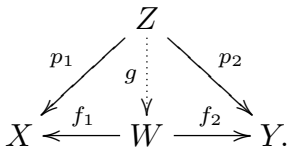

A product of two objects may not exist in a category. However, if it does, then this universal property guarantees that such an object with its projections to $X$ and $Y$, is essentially unique.

**Proposition 1.1.** *The product is uniquely determined by the universal property up to a unique isomorphism.*

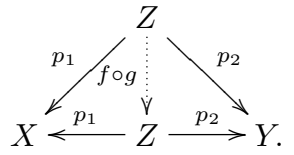
Proof. Suppose $W$ and $Z$ are both products of $X$ and $Y$, with corresponding projection morphisms $p_i$ and $f_i$ for $i = 1, 2$. Consider the corresponding diagrams




and




By assumption $Z$ is a product of $X$ and $Y$. So there exists a map $W \to Z$ such that $f_1 = p_1 \circ f$ and $f_2 = p_2 \circ f$. By similar argument, there is also a map $Z \to W$ such that $p_1 = f_1 \circ g$ and $p_2 = f_2 \circ g$. Consider the composition $f \circ g : Z \to Z$ . Then we have $p_1 \circ f \circ g = f_1 \circ g = p_1$, and $p_2 \circ f \circ g = f_2 \circ g = p_2$. Consider the diagram




By the universal property we have $f \circ g = \mathrm{Id}_Z$. By similar argument we have $g \circ f = \mathrm{Id}_W$. This shows that $Z$ and $W$ are canonically isomorphic.

Suppose that $(X_i)_{i\in I}$ is an arbitrary collection of objects in a category $\mathcal{C}$. By a product of the $X_i$ one means an object $V$ of $\mathcal{C}$ together with projection morphisms $p_i : V \to X$, for $i \in I$, such that for any object $U$ of $\mathcal{C}$, and any collection of morphisms $(f_i : V \to X_i)_{i\in I}$ in $\mathcal{C}$ there exists a unique morphism $f : U \to V$ such that for all $i \in I$ one has $f_i = p_i f$. Again a product of arbitrary collections of objects may not exist in a category. However, if it does, then using a similar argument as for products of two objects, one can show that a product is unique up to a unique isomorphism.

**Example.** Suppose we are given a collection of sets $(X_i)_{i\in I}$ of **Set**, the category of sets. We recall that the class of objects of **Set** is the class of all sets, and the morphisms are the usual maps of sets. A product of this collection in **Set** is defined as the cartesian product

$$\prod_{i\in I} X_i := \{(x_i)_{i\in I} | x_i \in X_i \text{ for all } i \in I\},$$

together with projection maps

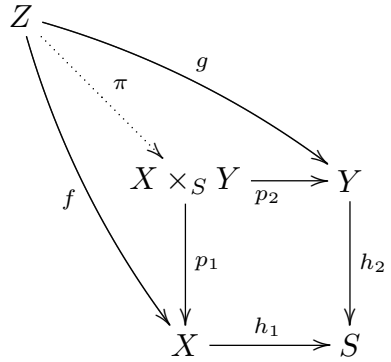
$$p_j : \prod_{i\in I} X_i \to X_j,\ p_j((x_i)_{i\in I}) := x_j.$$

Let $W$ be any set together with maps $f_i : W \to X_i$. One defines the unique map as

$$f : W \to \prod_{i\in I} X_i,\ f(w) = (f_i(w))_{i\in I}.$$

A *terminal object* of a category $\mathcal{C}$ is an object $S$ such that for any object $X$ of $\mathcal{C}$ there exists exactly one morphism $X \to S$ in $\mathcal{C}$. If a terminal object exists, then it is unique up to a unique isomorphism. It is sometimes denoted by 1. In **Set** the terminal objects are the one-element sets. In the category of schemes Spec **Z** is a terminal object, while in the category of schemes over $S$ the object $S$ is a terminal object.

Consider arbitrary objects $X, Y, S$ in a category $\mathcal{C}$. Let $h_1 : X \to S$ and $h_2 : Y \to S$ be morphisms in $\mathcal{C}$. By a *fibred product* of $X$ and $Y$, denoted by $X \times_S Y$, one means an object in $\mathcal{C}$ together with projection morphisms $p_1 : X \times_S Y \to X$ and $p_2 : X \times_S Y \to Y$ which make a commutative diagram with the given morphisms $h_1 : X \to S$ and $h_2 : Y \to S$ such that given any object $Z$ with morphisms $f : Z \to X$ and $g : Z \to Y$ that make a commutative diagram with the given morphisms $h_1 : X \to S$ and $h_2 : Y \to S$, there exists a unique morphism $\pi : Z \to X \times_S Y$ such that $f = p_1\pi$ and $g = p_2\pi$.




If a fibred product exists, then it is unique up to a unique isomorphism. If a category contains a terminal object $Z$ then the fibred product $X \times_Z Y$ is the ordinary product

$X \times Y$. In **Set** the fibred product $X \times_S Y$ is the set $\{(x, y) \in X \times_S Y \mid h_1(x) = h_2(y)\}$. Not all fibred products exist in the category of sets with one or two elements. Consider a set of two elements $\{a, b\}$. Suppose that $V$ is a fibred product of the one-element sets $\{a\}, \{b\}$ over $\{a, b\}$. Now $V$ is not empty, so it should contain at least one element. Let $c$ be an element of $V$. Then the map from $V$ to $\{a\}$ sends $c$ to $a$ and the map from $V$ to $\{b\}$ sends $c$ to $b$. This is a contradiction. So $V$ is not a fibred product.

Suppose we are given objects $A, B, C$ and $D$ in a category $\mathcal{C}$. One calls the commutative diagram

$$\begin{array}{ccc} A & \longrightarrow & B \\ \downarrow & \square & \downarrow \\ C & \longrightarrow & D \end{array}$$

*cartesian* if it satisfies the universal property of the fibred product of $B$ and $C$ over $D$. We emphasize that by putting a square in the centre.

Let $\mathcal{C}, \mathcal{D}$ be categories, and let $\mathcal{F}, \mathcal{G} : \mathcal{C} \to \mathcal{D}$ be covariant functors. Then a morphism of functors

$$\gamma : \mathcal{F} \to \mathcal{G}$$

consists of a morphism in $\mathcal{D}$

$$\gamma_T : \mathcal{F}(T) \to \mathcal{G}(T),$$

for all $T$ of $\mathcal{C}$ such that, for any morphism $f : T \to S$ in $\mathcal{C}$ the diagram

$$\begin{array}{ccc} \mathcal{F}(T) & \xrightarrow{\gamma_T} & \mathcal{G}(T) \\ \downarrow{\scriptstyle \mathcal{F}(f)} & & \downarrow{\scriptstyle \mathcal{G}(f)} \\ \mathcal{F}(S) & \xrightarrow{\gamma_S} & \mathcal{G}(S) \end{array} \tag{1}$$

commutes in $\mathcal{D}$. By $\mathrm{Ob}\,\mathcal{C}$ we mean the class of objects of $\mathcal{C}$. One says alternatively that the system $(\gamma_T)_{T \in \mathrm{Ob}\,\mathcal{C}}$ is *functorial* in $T$ if for every morphism $f : T \to S$ in $\mathcal{C}$ the above diagram commutes in $\mathcal{D}$. The functors $\mathcal{C} \to \mathcal{D}$ form the objects in a *category of functors*, denoted by $\mathrm{Fun}(\mathcal{C}, \mathcal{D})$. One has to be careful here since the collection of morphisms between two given functors can be too large to be a 'set'. We choose to ignore this set-theoretical problem.

Let $\mathcal{C}$ be a category, and let $X \in \mathrm{Ob}\,\mathcal{C}$. We define a contravariant functor $h_X$ from $\mathcal{C}$ to **Set**. The functor $h_X$ sends any object $T$ of $\mathcal{C}$ to the set

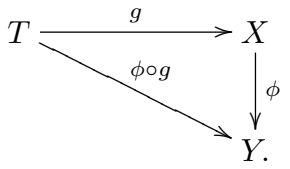
$$h_X(T) = \mathrm{Mor}(T, X)$$

of $T$-valued points of $X$ and sends a morphism $f : Y \to Z$ in $\mathcal{C}$ to

$$f^\star : g \mapsto g \circ f : h_X(Z) \to h_X(Y),$$

where $g : Z \to X$. One calls $h_X$ the functor of points of $X$. Any morphism $\phi : X \to Y$ defines a morphism of functors $\phi_\star : h_X \to h_Y$ defined by

$$\phi_{\star T} : g \mapsto \phi \circ g : h_X(T) \to h_Y(T).$$




We often just write $\phi_\star$ for $\phi_{\star T}$. So we have a covariant functor from $\mathcal{C}$ to $\mathrm{Fun}(\mathcal{C}, \mathbf{Set})$, the category of contravariant functors from $\mathcal{C}$ to **Set**. The morphisms of $\mathrm{Fun}(\mathcal{C}, \mathbf{Set})$ are morphisms of functors.

**Lemma 1.2.** *(*Yoneda.*) The functor $\mathcal{C} \to \mathrm{Fun}(\mathcal{C}, \mathbf{Set})$, which sends an object $X$ to $h_X$ and a morphism $\phi$ to $\phi_\star$, is fully faithful, i.e for all objects $X, Y$ of $\mathcal{C}$, the map*

$$\alpha : \mathrm{Mor}(X, Y) \to \mathrm{Mor}(h_X, h_Y)$$
$$\phi \mapsto \phi_\star = \phi \circ -,$$

*is a bijection.*

Proof. Let $\gamma \in \mathrm{Mor}(h_X, h_Y)$. Then for each $u$ and each $f \in h_X(u)$ the diagram (1) is commutative. Note that the covariant functors in the diagram (1) have to be replaced by contravariant ones. So $\gamma(u)(f) = \gamma_X(\mathrm{Id}_X) \circ f$. Hence $\gamma = \gamma_X(\mathrm{Id}_X) \circ - = \gamma(X)(\mathrm{Id}_X)_\star$.

On the other hand, if $\gamma = \phi_\star$, then $\gamma_X(\mathrm{Id}_X) = \phi \circ \mathrm{Id}_X = \phi$. □

Suppose that $\mathcal{F} \in \mathrm{Fun}(\mathcal{C}, \mathbf{Set})$. Then $\mathcal{F}$ is called *representable* if there exists an object $X$ of $\mathcal{C}$ and an isomorphism of functors

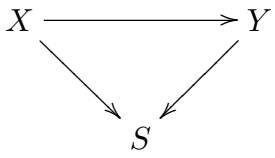
$$\mathcal{F} \xrightarrow{\sim} h_X$$

Yoneda's lemma shows that if $h_X \cong h_Y$ then $X \cong Y$.

### ▶ Fibred product of schemes

The general reference in this section is Hartshorne [14].

Let $S$ be a fixed scheme. An *$S$-scheme* is a scheme $X$ together with a morphism $X \to S$. A morphism of $S$-schemes between the $S$-schemes $X$ and $Y$ is a morphism $X \to Y$ such that the diagram




commutes.

**Theorem 1.3.** *The fibred product $X \times_S Y$ for any two schemes $X$ and $Y$ over a scheme $S$ exists, and is unique up to a unique isomorphism.*

Proof. Hartshorne [14], chapter II, §3, theorem 3.3. □

**Example.** Suppose $X, Y, S$ are affine schemes:

$$X = \mathrm{Spec}\ A, \quad Y = \mathrm{Spec}\ B, \quad S = \mathrm{Spec}\ C.$$

Then $X \times_S Y = \text{Spec } (A \otimes_C B)$.

**Example.** Let $f : X \to S$ be a morphism of schemes, and let $j : U \hookrightarrow S$ be an open immersion, i.e. $j$ induces an isomorphism of $U$ with an open subscheme of $S$. Then the diagram

$$\begin{array}{ccc} f^{-1}U & \longrightarrow & X \\ \downarrow & \square & \downarrow f \\ U & \longrightarrow & S \end{array}$$

is cartesian, i.e. $X \times_S U = f^{-1}U$.

**Definition.** Let $S$ be a scheme, and let $\mathbf{P}^n_{\mathbf{Z}}$ be the $n$-dimensional projective space over $\mathbf{Z}$. Then there exist unique morphisms

$$S \to \text{Spec } \mathbf{Z} \qquad \text{and} \qquad \mathbf{P}^n_{\mathbf{Z}} \to \text{Spec } \mathbf{Z}.$$

We define $\mathbf{P}^n_S = \mathbf{P}^n_{\mathbf{Z}} \times_{\text{Spec } \mathbf{Z}} S$. Then the following diagram

$$\begin{array}{ccc} \mathbf{P}^n_S & \longrightarrow & \mathbf{P}^n_{\mathbf{Z}} \\ \downarrow & \square & \downarrow \\ S & \longrightarrow & \text{Spec } \mathbf{Z} \end{array}$$

is cartesian.

**Definition.** Let $f : X \to S$ be a morphism of schemes, let $s \in S$, and let $\kappa(s)$ be the residue class field of $S$ at $s$. Then the *fibre* of $f$ at $s$ is defined by the cartesian diagram

$$\begin{array}{ccc} X_s & \longrightarrow & X \\ \downarrow & \square & \downarrow \\ \text{Spec } \kappa(s) & \longrightarrow & S. \end{array}$$

As a topological space, $X_s$ actually equals $f^{-1}s$ with the induced topology.

**Example.** Consider $A = \mathbf{Z}[X_1, \ldots, X_n]/(f_1, \ldots, f_m)$, where $f_i \in \mathbf{Z}[X_1, \ldots, X_n]$, and $X = \text{Spec } A$. Then $X$ is a scheme over $S = \text{Spec } \mathbf{Z}$. We can see it as the "variety" in the affine $n$-space over $\mathbf{Z}$ given by the equations $f_1 = 0, \ldots, f_m = 0$.

Let $p$ be a prime number. We want to calculate $X_p = \text{Spec } (A \otimes_{\mathbf{Z}} \mathbf{F}_p)$, i.e. $X_s$ for $s = (p) \in S$. We have an exact sequence

$$\begin{aligned} \mathbf{Z}[X_1, \ldots, X_n]^m \to \mathbf{Z}[X_1, \ldots, X_n] \to A \to 0 \\ (g_1, \ldots, g_m) \mapsto \sum_i g_i f_i. \end{aligned}$$

Tensoring with $\mathbf{F}_p$ we get

$$\begin{aligned} \mathbf{F}_p[X_1, \ldots, X_n]^m \to \mathbf{F}_p[X_1, \ldots, X_n] \to A \otimes_{\mathbf{Z}} \mathbf{F}_p \to 0 \\ (g_1, \ldots, g_m) \mapsto \sum_i g_i \overline{f_i}, \end{aligned}$$

where $\overline{f_i} = (f_i \bmod p)$.

So $X_p$ is the "variety" in the affine $n$-space over $\mathbf{F}_p$ given by the polynomials $(f_i \bmod p)$.

## ▶ Group objects

In this section we want to define the notion of group objects in a category. The main reference of this section is Bosch et al. [5].

Let $\mathcal{C}$ be a category. A *group functor* is an object $X$ and a factorization of the functor of points $h_X$ from the category of groups **Grp** to **Set** through the *forgetful functor* from **Grp** to **Set**. The functor from $\mathcal{C}$ to **Grp** is said to be a group functor because it sends any object $X$ of $\mathcal{C}$ to a group $\mathcal{F}(X)$, and a morphism $f \in \mathcal{C}$ to a group homomorphism $\mathcal{F}(f)$, while the functor from **Grp** to **Set** is called forgetful because it sends groups to their underlying sets and each homomorphism to itself (viewed as a map), and 'forgets' part of the structure.

We define a law of composition on an object $X$ of $\mathcal{C}$ by a morphism of functors $\gamma : h_X \times h_X \to h_X$. Therefore it consists of a morphism $\gamma_T : h_X(T) \times h_X(T) \to h_X(T)$ for all $T$ of $\mathcal{C}$ such that, for any $f : T \to S$ the diagram

$$\begin{array}{ccc} h_X(S) \times h_X(S) & \xrightarrow{\gamma_S} & h_X(S) \\ \downarrow{\scriptstyle h_X(f)\times h_X(f)} & & \downarrow{\scriptstyle h_X(f)} \\ h_X(T) \times h_X(T) & \xrightarrow{\gamma_T} & h_X(T) \end{array}$$

commutes. If $h_X(T)$ is a group under $\gamma_T$ for all $T$, then $\gamma$ defines on $h_X$ a structure of a group functor. Therefore $\gamma$ is said to be a group law.

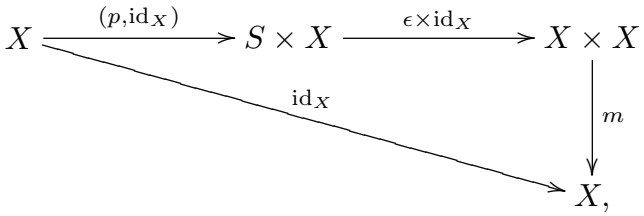
**Definition.** A group object in $\mathcal{C}$ is an object $X$ together with a multiplication $\gamma : h_X \times h_X \to h_X$ which is a group law.

Suppose now that $\mathcal{C}$ has finite products and a terminal object $S$. Let $X$ be a group object in $\mathcal{C}$ with $\gamma$ as group law. By Yoneda's lemma and because $h_{X\times X} \cong h_X \times h_X$ the law of composition $h_X \times h_X \to h_X$ corresponds to a morphism $m : X \times X \to X$. The unit element of each group $h_X(T)$ gives rise to a morphism of functors from $h_S$ to $h_X$. By Yoneda this corresponds to a morphism $\epsilon : S \to X$, which we call the *unit section* of $X$. A terminal object is needed as the source of the morphism $\epsilon$. The inverse map in each group $h_X(T)$ yields a functorial morphism from $h_X$ into $h_X$. By Yoneda this corresponds to a morphism $i : X \to X$ which we call the *inverse map* on $X$. The group axioms which are satisfied by $h_X(T)$ correspond to the commutativity of the following diagrams:

(i) *associativity*

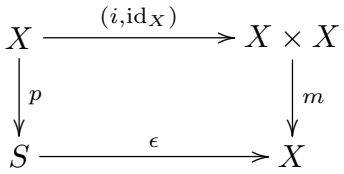
$$\begin{array}{ccc} X \times X \times X & \xrightarrow{m\times \mathrm{id}_X} & X \times X \\ \downarrow{\scriptstyle \mathrm{id}_X \times m} & & \downarrow{\scriptstyle m} \\ X \times X & \xrightarrow{m} & X \end{array}$$

(ii) *existence of a left-identity*

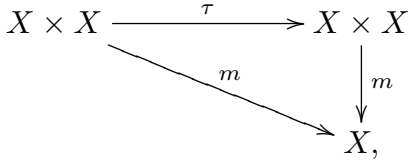



where $p : X \to S$ is the morphism from $X$ to the terminal object $S$.

(iii) *existence of a left-inverse*




(iv) *commutativity in case $h_X(T)$ are commutative groups*




where $\tau$ interchanges the factors.

**Proposition 1.4.** *The collection of group objects in a category $\mathcal{C}$ that admits fibred products and terminal objects, is in one-to-one correspondence with the collection of data $(X, m, \epsilon, i)$ where $X$ is an object of $\mathcal{C}$ and where*

$$m\colon X \times X \to X, \qquad \epsilon : S \to X, \qquad i : X \to X$$

*are morphisms in $\mathcal{C}$ such that the diagrams* (i), (ii), (iii) *are commutative. Furthermore a group object in $\mathcal{C}$ is commutative if and only if, in addition, the corresponding diagram* (iv) *is commutative.*

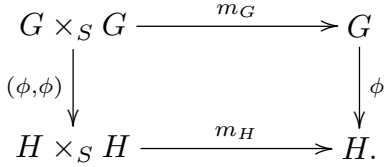
Proof. Bosch et al. [5], chapter IV, §1, proposition 3. □

### ▶ Group schemes

An $S$-group scheme is a group object in the category of $S$-schemes $\mathrm{Sch}/S$. A homomorphism of group schemes $G$ and $H$ over $S$ is an $S$-morphism $\phi : G \to H$ of schemes such that

$$\phi \circ m_G = m_H \circ (\phi \times \phi),$$

i.e. for all $T$ and $x, y \in G(T) : \phi(x, y) = \phi(x)\phi(y)$. We can express this in the commutative diagram



We denote the set of all homomorphisms of group schemes $G \to H$ by $\mathrm{Hom}_S(G, H)$.

Let $G$ be a group scheme over $S$, and $T$ be an $S$-scheme. Then $G_T = G \times_S T$ is a $T$-scheme because for any $T$-scheme $Y$ we have

$$G_T(Y) = \mathrm{Hom}_T(Y, G \times_S T) = \mathrm{Hom}_S(Y, G) = G(Y).$$

Hence $G_T$ has a group structure in the category of $T$-schemes and represents the same functor as the group scheme $G$ over $S$ but restricted to the category of $T$-schemes. We obtain $G_T$ from $G$ by *base change.*

Let $S$ be an affine scheme, i.e. $S = \mathrm{Spec}\ A$ for some ring $A$. A group scheme $G$ over $S$ is called an affine group scheme over $S$ if $G = \mathrm{Spec}\ B$ where $B$ is an $A$-algebra. The structure of $G$ is to be given by the $S$-morphisms:

$$\begin{aligned} m &: G \times_S G \to G, \\ \epsilon &: S \to G, \\ i &: G \to G. \end{aligned}$$

But since the category of affine schemes over $S$ is anti-equivalent to the category of algebras over $A$ (see Waterhouse [33]), the group structure of $G$ is determined by the corresponding $A$-algebra homomorphisms

$$\begin{aligned} m^\star &: B \to B \otimes_A B, \\ \epsilon^\star &: B \to A, \\ i^\star &: B \to B. \end{aligned}$$

The data $(A, B, f : A \to B, m^\star, \epsilon^\star, i^\star)$ form a so-called Hopf algebra.

**Example.** Let $\mathbf{G}_a$ be the covariant functor from the category of commutative rings **Crg** to the category of abelian groups **Ab** defined by $\mathbf{G}_a(R) = R^+$, where $R^+$ denotes the additive group of the commutative ring $R$. The functor $\mathbf{G}_a$ is representable by the affine scheme Spec $\mathbf{Z}[t]$, since $\mathrm{Hom}_{\mathbf{Crg}}(\mathbf{Z}[t], R) = R$, for any $R$. So $\mathbf{G}_a = \mathrm{Spec}\ \mathbf{Z}[t]$. We write down the group operations $m, i, \epsilon$. Let $m$ be the map that corresponds to the $\mathbf{Z}$-algebra homomorphism

$$m^\star : \mathbf{Z}[t] \to \mathbf{Z}[t] \otimes_{\mathbf{Z}} \mathbf{Z}[t],\ m^\star(t) = t \otimes 1 + 1 \otimes t.$$

Similarly we let $\epsilon$ and $i$ be the maps that correspond to the $\mathbf{Z}$-algebra maps

$$\begin{aligned} \epsilon^\star &: \mathbf{Z}[t] \to \mathbf{Z},\ \epsilon^\star(t) = 0, \\ i^\star &: \mathbf{Z}[t] \to \mathbf{Z}[t],\ i^\star(t) = -t. \end{aligned}$$

The affine group scheme $\mathbf{G}_a$ is called the additive group.

**Example.** Let $\mathbf{G}_m$ be the covariant functor from the category of commutative rings **Crg** to the category of abelian groups **Ab** defined by $\mathbf{G}_m(B) = B^\star$, where $B^\star$ denotes the multiplicative group of invertible elements of the commutative ring $B$. The functor $\mathbf{G}_m$ is representable by the affine scheme Spec $\mathbf{Z}[t, t^{-1}]$, since $\mathrm{Hom}_{\mathbf{Crg}}(\mathbf{Z}[t, t^{-1}], B) \overset{(1)}{=} B^\star$, where (1) follows from exercise 2.1 in §2, chapter II in Hartshorne [14]. Hence $\mathbf{G}_m =$

Spec $\mathbf{Z}[t,t^{-1}]$. Let $A=\mathbf{Z}[t,t^{-1}]$. We write down the group operations $m,i,\epsilon$. Let $m$ be the map that corresponds to the $\mathbf{Z}$-algebra homomorphism

$$m^\star : A \to A\otimes_{\mathbf{Z}} A,\ m^\star(t)=t\otimes t.$$

Similarly we let $\epsilon$ and $i$ be the maps that correspond to the $\mathbf{Z}$-algebra maps

$$\epsilon^\star : A\to \mathbf{Z},\ \epsilon^\star(t)=1,$$
$$i^\star : A\to A,\ i^\star(t)=t^{-1}.$$

The affine group scheme $\mathbf{G}_m$ is called the multiplicative group.

**Example.** Let $G=$ Spec $A$, where $A=\mathbf{Z}[x]/(x^n-1)$. Let Spec $\mathbf{Z}=S$. We want to show that $G$ is a group scheme over Spec $\mathbf{Z}$. As in the previous example we have to give the maps $m,i,\epsilon$. Now $G\times_S G=$ Spec $(A\otimes_{\mathbf{Z}} A)$. The map $m$ corresponds to a $\mathbf{Z}$-algebra homomorphism

$$m^\star : A\to A\otimes_{\mathbf{Z}} A,\ m^\star(x)=x\otimes x.$$

Similarly the maps $\epsilon$ and $i$ correspond to $\mathbf{Z}$-algebra maps

$$\epsilon^\star : A\to \mathbf{Z},\ \epsilon^\star(x)=1,$$
$$i^\star : A\to A,\ i^\star(x)=x^{n-1}.$$

Now for any scheme $X$ over Spec $\mathbf{Z}$ one has

$$\begin{aligned} h_G(X) &= \mathrm{Mor}_{\mathbf{Crg}}(A,\Gamma(X,\mathcal{O}_X)) \\ &= \{\alpha\in\Gamma(X,\mathcal{O}_X)^\star | \alpha^n=1\}. \end{aligned}$$

So there is a natural group law on $h_G$. We denote $G$ by $\mu_n$ and call it the group of $n$th roots of unity.

### ▶ Group rings

Let $R$ be a ring and let $G$ be a group. The group ring $R[G]$ of $G$ over $R$ consists of elements of the set

$$R[G]=\{\sum_{\sigma\in G} a_\sigma\sigma\colon a_\sigma\in R, a_\sigma=0 \text{ for all but finitely many } \sigma\in G\}.$$

Two elements $\sum_{\sigma\in G} a_\sigma\sigma$ and $\sum_{\sigma\in G} b_\sigma\sigma$ are equal in $R[G]$ if and only if for all $\sigma\in G$ we have $a_\sigma=b_\sigma$. The group ring $R[G]$ is a ring. The operations of addition and multiplication in $R[G]$ are given by

$$\sum_{\sigma\in G} a_\sigma\sigma+\sum_{\sigma\in G} b_\sigma\sigma=\sum_{\sigma\in G}(a_\sigma+b_\sigma)\sigma,$$

$$(\sum_{\sigma\in G} a_\sigma\sigma)(\sum_{\sigma\in G} b_\sigma\sigma)=\sum_{\rho\in G}\sum_{\sigma,\tau\in G,\sigma\tau=\rho}(a_\sigma b_\tau)\rho=\sum_{\rho\in G}\sum_{\sigma\in G}(a_\sigma b_{\sigma^{-1}\rho})\rho.$$

Note that $R$ can be viewed as a subring of $R[G]$

$$x\mapsto x\cdot 1\in R[G],$$

and if $R\neq 0$ then $G$ can be viewed as a subgroup in $R[G]^\star$

$$g\mapsto 1\cdot g\in R[G].$$

## ▶ Diagonalizable group schemes

Let $M$ be an abelian group, and let $\mathbf{Z}[M]$ be the group ring of $M$ over $\mathbf{Z}$. We define

$$D(M) = \text{Spec } \mathbf{Z}[M].$$

Let $S$ be a scheme. We define

$$D_S(M) = D(M)_S = D(M) \times_{\text{Spec } \mathbf{Z}} S.$$

We observe that the group ring $\mathbf{Z}[M]$ is a commutative ring since $M$ is an abelian group. So Spec $\mathbf{Z}[M]$ is well-defined. The set of $S$-valued points of $D(M)$ is

$$\begin{aligned} D(M)(S) &= \text{Mor}_{\mathbf{Sch}}(S, D(M)) \\ &\cong \text{Mor}_{\mathbf{Ring}}(\mathbf{Z}[M], \Gamma(S, \mathcal{O}_S)) \\ &\cong \text{Mor}_{\mathbf{Grp}}(M, \Gamma(S, \mathcal{O}_S)^\star). \end{aligned}$$

The first isomorphism follows from exercise 2.1 in §2, chapter II in Hartshorne [14], the second isomorphism is a standard fact about $\mathbf{Z}[M]$. In other words

$$D(M)(S) \cong \text{Mor}_{\mathbf{Grp}}(M, \mathbf{G}_m(S)).$$

We observe that the set $D(M)(S)$ has the structure of a commutative group, and the group structure is functorial in $S$. Hence $D(M)$ is a commutative group scheme.

Let $D$ be a functor from the category of commutative rings **Crg** to the category of abelian groups **Ab**. Then we have a commutative diagram

$$\begin{array}{ccc} {}_S\mathbf{Alg} & \xrightarrow{\text{Forgetful}} & \mathbf{Crg} \\ & \searrow^{D_S} & \downarrow D \\ & & \mathbf{Ab}. \end{array}$$

Hence $D_S$, the functor from the category of $S$-algebras ${}_S\mathbf{Alg}$ to the category of abelian groups **Ab**, is the composition of $D$ by the forgetful functor, and $D_S$ is a commutative group scheme because $D$ is a commutative group scheme.

**Definition.** Let $S$ be a scheme. A group scheme $G$ over $S$ is called *diagonalizable* if it is of the form $D_S(M)$ for some $M$.

We study the structure of the diagonalizable groups by looking at the structure of the groups $M$.

**Theorem 1.5.** (Structure theorem for finitely generated abelian groups) *Let $M$ be a finitely generated abelian group, i.e. there exist a finite subset $E$ of $M$ such that $M = \langle E \rangle$. Then there is an isomorphism*

$$M \cong (\mathbf{Z}/n_1\mathbf{Z}) \oplus (\mathbf{Z}/n_2\mathbf{Z}) \oplus \ldots \oplus (\mathbf{Z}/n_s\mathbf{Z}) \oplus \mathbf{Z}^r,$$

*where $n_i > 0$ for all $i$ and $n_1 | n_2 | \ldots | n_s$, with $r \geq 0, s \geq 0$. Furthermore, $M$ uniquely determines the $n_i$ and $r$.*

Proof. Lang [18], chapter I, §8. □

**Definition.** Let $S$ be a scheme. A group scheme $G$ over $S$ is of *finite type* over $S$ if the structure morphism $G \to S$ is of finite type.

**Lemma 1.6.** *Let $M, M'$ be abelian groups. Then*

$$D(M \oplus M') = D(M) \times_{\mathrm{Spec}\ \mathbf{Z}} D(M'),$$

$$D_S(M \oplus M') = D_S(M) \times_S D_S(M').$$

Proof. There is a natural isomorphism

$$\mathrm{Mor}_{\mathbf{Grp}}(M \oplus M', \Gamma(S, \mathcal{O}_S^\star)) \cong \mathrm{Mor}_{\mathbf{Grp}}(M, \Gamma(S, \mathcal{O}_S^\star)) \times \mathrm{Mor}_{\mathbf{Grp}}(M', \Gamma(S, \mathcal{O}_S^\star)).$$

So as functors $h_{D(M\oplus M')} \cong h_{D(M)} \times h_{D(M')}$. The isomorphism follows directly from Yoneda's lemma. □

By the Structure theorem for abelian groups we can write any finitely generated abelian group $M$ as

$$M \cong (\mathbf{Z}/n_1\mathbf{Z}) \oplus (\mathbf{Z}/n_2\mathbf{Z}) \oplus \ldots \oplus (\mathbf{Z}/n_s\mathbf{Z}) \oplus \mathbf{Z}^r$$

Then from the lemma above it follows that

$$D(M) = D(\mathbf{Z}/n_1\mathbf{Z}) \times D(\mathbf{Z}/n_2\mathbf{Z}) \times \ldots \times D(\mathbf{Z}/n_s\mathbf{Z}) \times D(\mathbf{Z})^r.$$

To understand $D(M)$, we only need to understand $D(\mathbf{Z})$ and $D(\mathbf{Z}/n\mathbf{Z})$, where $n$ is a positive integer. Now $D(\mathbf{Z}) \cong \mathbf{G}_m$, since the group ring $\mathbf{Z}[\mathbf{Z}]$ is isomorphic to $\mathbf{Z}[t, t^{-1}]$, and $D(\mathbf{Z}/n\mathbf{Z})$ is equal to $\mu_n$, the group of $n$th roots of unity, since

$$D(\mathbf{Z}/n\mathbf{Z})(S) \cong \{\alpha \in \Gamma(S, \mathcal{O}_S^\star) \,|\, \alpha^n = 1\},$$

where $S$ is a scheme.

A diagonalizable group scheme $D(M)$ is of finite type if and only if $M$ is finitely generated; in that case, $D(M)$ is a finite product of copies of $\mathbf{G}_m$ and $\mu_n$.

## 2 Integral models of tori

### ▶ Galois extension of rings

Let $B$ be a noetherian domain, and let $H$ be a finite subgroup of $\mathrm{Aut}(B)$. Let $A = B^H$, the subring of $B$ consisting of all elements which remain invariant under the action of $H$. The inclusion of $A$ in $B$ gives a morphism $p : \mathrm{Spec}\ B \to \mathrm{Spec}\ A$. Then for each $\mathfrak{p} \in \mathrm{Spec}\ A$, the group $H$ acts transitively on $p^{-1}\mathfrak{p}$, see Atiyah-MacDonald [2].

**Definition.** Let $\mathfrak{q} \in \mathrm{Spec}\ B$. Then the decomposition group of $\mathfrak{q}$ is

$$H_d(\mathfrak{q}) = \{h \in H \mid h\mathfrak{q} = \mathfrak{q}\}$$

and the inertia group of $\mathfrak{q}$ is

$$H_i(\mathfrak{q}) = \{h \in H_d(\mathfrak{q}) \mid h \text{ acts trivially on } \kappa(\mathfrak{q}),\ \text{the residue field at } \mathfrak{q}\}.$$

**Definition.** Let $A$ and $B$ be Dedekind domains. Then $B$ is a Galois ring extension of $A$ if $A \subset B$, $A = B^G$, where $G = \mathrm{Aut}(B/A)$, and the inertia group of $\mathfrak{q}$ is trivial for all $\mathfrak{q}$ in Spec $B$.

**Example.** Let $K$ be a field. Then Spec $K = \{(0)\}$, and the inertia group $H_i((0))$ is always trivial, since $\kappa((0)) = K$. So in this case the definition coincides with the classical one from finite Galois theory.

**Proposition 2.1.** *Suppose $B$ is a Dedekind domain and $A = B^H$. Then $A$ is a Dedekind domain.*

Proof. This proof is largely based on an original proof by Professor Hendrik Lenstra Jr.

By assumption $B$ is a domain. So $A$ is also a domain since it is contained in $B$. Now $B$ is integral over $A$ since every $b \in B$ is a zero of the polynomial $\prod_{\sigma \in H}(X - \sigma(b))$ which has invariant coefficients in $B$. This means that these coefficients are also in $A$. Note that $K$, the field of fractions of $A$, is contained in $L^H$, where $L$ is the field of fractions of $B$. Suppose that $x \in K$ is integral over $A$. Then it is certainly integral over $B$. So it is in $B$ since $B$ is integrally closed, but it is also invariant under $H$, so it is in $A$. Hence $A$ is integrally closed.

Choose $\mathfrak{q}$ a prime ideal of $B$ such that $\mathfrak{p} = \mathfrak{q} \cap A$, where $\mathfrak{p}$ is a prime ideal of $A$. Consider $A_\mathfrak{p}$, the localisation of $A$ at $\mathfrak{p}$. We claim that

$$A_\mathfrak{p} = B_\mathfrak{q} \cap K.$$

Let $x \in B_\mathfrak{q} \cap K$. Then $x = \sigma x \in \sigma B_\mathfrak{q} = B_{\sigma\mathfrak{q}}$, for all $\sigma \in H$. Hence

$$x \in \bigcap_{\sigma \in H} B_{\sigma\mathfrak{q}} = \bigcap_{\mathfrak{q}' \mid \mathfrak{p}} B_{\mathfrak{q}'} \overset{(*)}{=} \bar{A}_\mathfrak{p} = A_\mathfrak{p},$$

since $A$ and hence the $A_\mathfrak{p}$ is integrally closed; by $\bar{A}_\mathfrak{q}$ we mean the integral closure of $A_\mathfrak{q}$. So $B_\mathfrak{q} \cap K \subseteq A_\mathfrak{p}$. $(*)$ follows from corollary 5.22 in Atiyah-McDonald [2]). It is easy to see $A_\mathfrak{p} \subseteq B_\mathfrak{q} \cap K$. This proves the claim. Now we have

$$K^\star/A_\mathfrak{p}^\star \hookrightarrow L^\star/B_\mathfrak{q}^\star = \mathbf{Z}.$$

Hence $K^\star/A_\mathfrak{p}^\star \cong \mathbf{Z}$, since $A_\mathfrak{p}^\star \subset K^\star$. We see that $A_\mathfrak{p}$ is a discrete valuation ring. Hence $A_\mathfrak{p}$ is noetherian of dimension 1. Recall that $B$ is a Dedekind domain, i.e. an integrally closed noetherian domain of dimension 1.

Consider a strictly increasing chain of ideals in $A$.

$$0 \neq \mathfrak{a}_0 \subset \mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \dots$$

Let $0 \neq \alpha \in \mathfrak{a}_0$. Then $\alpha \in B$, since $A \subset B$. We have

$$\mathfrak{a} = \mathfrak{b} \Leftrightarrow \forall \mathfrak{p} : \mathfrak{a}_\mathfrak{p} = \mathfrak{b}_\mathfrak{p}.$$

Note that the set

$$Z(\alpha) = \{\mathfrak{p} \in \operatorname{Spec} A : \alpha \in \mathfrak{p}\}$$

is finite. Choose $\mathfrak{p} \in Z(\alpha)$. Then there are finitely many $\mathfrak{q} \in B$ with $A \cap \mathfrak{q} = \mathfrak{p}$, say $\mathfrak{q}_1, \dots, \mathfrak{q}_n$, since $H$ acts transitively on the set

$$\{\mathfrak{q} \in \operatorname{Spec} B : A \cap \mathfrak{q} = \mathfrak{p}\}.$$

So $\alpha \in \mathfrak{p}$ is equivalent to $\alpha \in \mathfrak{q}_i$, for $i = 1, \dots, n$. Now for all $\mathfrak{p}$ we can choose $i_\mathfrak{p}$ such that for all $j \geq i_\mathfrak{p}$

$$(\mathfrak{a}_j)_\mathfrak{p} = (\mathfrak{a}_i)_\mathfrak{p},$$

since $A_\mathfrak{p}$ is noetherian. Then for all $\mathfrak{p} \notin Z(\alpha)$ and for all $j$ we have

$$(\alpha_i)_\mathfrak{p} = A_\mathfrak{p},$$

since $\alpha_i$, for $i = 1, \dots, n$, is a unit. Choose $i = \max i_\mathfrak{p}$. Then for all $j \geq i$, we have

$$(\mathfrak{a}_i)_\mathfrak{p} = (\mathfrak{a}_j)_\mathfrak{p},$$

for all $\mathfrak{p}$. This equivalent to

$$\mathfrak{a}_i = \mathfrak{a}_j.$$

This proves that $A$ is noetherian. So $A$ is an integrally closed noetherian domain of dimension 1. Hence $A$ is a Dedekind domain. □

**Example.** Let $B$ be a Dedekind domain, and let $L$ be its field of fractions. Then $H$ acts on $L$. By the previous proposition $A$ is also a Dedekind domain. Let $\mathfrak{q} \in \operatorname{Spec} B$ and $\mathfrak{p} = \mathfrak{q} \cap A \in \operatorname{Spec} A$. Then $A_\mathfrak{p} \subseteq B_\mathfrak{q}$. In $A_\mathfrak{p}$ we know that $A_\mathfrak{p}\mathfrak{p} = (\pi)$ for some $\pi \in A_\mathfrak{p}$.

We set $e(\mathfrak{q}/\mathfrak{p}) = v_\mathfrak{q}(\pi)$, the ramification index of $\mathfrak{q}$ over $\mathfrak{p}$. We say that $\mathfrak{p}$ is unramified if $e(\mathfrak{p}) = 1$ and $B/\mathfrak{q}$ is separable over $A/\mathfrak{p}$. Now

$$\#H_i(\mathfrak{q}) = e(\mathfrak{q}/\mathfrak{p})[B/\mathfrak{q} : A/\mathfrak{p}]_{\text{ins}},$$

where $[B/\mathfrak{q} : A/\mathfrak{p}]_{\text{ins}}$ is the inseparability degree, see Lang [18] chapter V, §6. So $B$ is Galois over $A$ if and only if $B$ is unramified over all prime ideals of $A$.

**Definition.** Let $A, B$ be as above. A group scheme $G$ over Spec $A$ is *split* over Spec $B$ if $G \times_{\operatorname{Spec} A} \operatorname{Spec} B$ is diagonalizable over Spec $B$.

**Proposition 2.2.** *Let $A \subset B$ be a finite Galois extension of rings with group $H = \mathrm{Gal}(B/A)$. Then there is an anti-equivalence of categories between the category of commutative group schemes over* Spec $A$ *split over* Spec $B$ *and the category of $H$-modules, i.e. abelian groups with $H$-action, given by*

$$G \mapsto \mathrm{Hom}_{\mathrm{Spec}\ B}(G_{\mathrm{Spec}\ B}, \mathbf{G}_{m,\mathrm{Spec}\ B}).$$

Proof. Grothendieck, et al., Proposition 1.1 in exposé X. □

### ► Tori over fields

Let $K$ be a field and let $\bar{K}$ be an algebraic closure of $K$. Let $G$ be a group scheme over $K$. Then $G$ is said to be of multiplicative type over $K$ if $G_{\bar{K}}$ is diagonalizable, i.e. $G_{\bar{K}} \cong \mathrm{Spec}\ (\mathbf{Z}[M] \otimes \bar{K})$, for some abelian group $M$. One calls $G$ split over an algebraic extension of fields $L/K$ if $G_L$ is diagonalizable.

**Lemma 2.3.** *Let $G$ be a group of multiplicative type over $K$, and let $K_s$ be a separable closure of $K$. Then $G \otimes_K K_s$ is diagonalizable.*

Proof. Demazure and Gabriel [9], Corollaire 3.5 in IV.§1. □

**Lemma 2.4.** *For every field $K$, the group of endomorphisms of the $K$-group scheme $\mathbf{G}_{m,K}$ is canonically isomorphic to $\mathbf{Z}$.*

Proof. We denote the collection of endomorphisms of $\mathbf{G}_m$ by End $\mathbf{G}_m$. By Yoneda's lemma

$$\mathrm{End}\ \mathbf{G}_m \cong \mathrm{End}_{_K\mathbf{Grp-Sch}}(\mathrm{Spec}\ K[X, X^{-1}], i, \epsilon, m),$$

where ${}_K\mathbf{Grp} - \mathbf{Sch}$ denotes the category of group schemes over $K$. We also have

$$\mathrm{End}_{_K\mathbf{Grp-Sch}}\ (\mathrm{Spec}\ K[X, X^{-1}], i, \epsilon, m) \cong \mathrm{End}_{\mathbf{Hopf-Alg}}\ (K[X, X^{-1}], i^\star, \epsilon^\star, m^\star),$$

since the functor Spec from the category of Hopf algebras to the category of group schemes is fully faithful (see Waterhouse [33]). First we consider all endomorphisms of $K[X, X^{-1}]$. Then we determine which ones are Hopf algebra endomorphisms. We know that

$$\mathrm{Hom}_{_K\mathbf{Alg}}(K[X, X^{-1}], K[X, X^{-1}]) \cong K[X, X^{-1}]^\star = \{\lambda X^r | r \in \mathbf{Z}, \lambda \in K^\star\},$$
$$f \mapsto f(X).$$

Hence the elements of $K[X, X^{-1}]^\star$ are of the form $\lambda X^r$, $(\lambda \in K^\star, r \in \mathbf{Z})$. Consider the ring homomorphism

$$f : K[X, X^{-1}] \to K[X, X^{-1}],$$
$$X \mapsto \lambda X^r, \lambda \in K^\star, r \in \mathbf{Z}.$$

Then $f$ is a homomorphism of Hopf algebras if the following diagrams are commutative, i.e. we have to check that $(f \otimes f) \circ m^\star = m^\star \circ f$, $f \circ i^\star = i^\star \circ f$ and $f \circ \epsilon^\star = \epsilon^\star \circ f$.

$$\begin{array}{ccc} K[X, X^{-1}] & \xrightarrow{m^\star} & K[X, X^{-1}] \otimes_K K[X, X^{-1}] \\ \downarrow f & & \downarrow f \otimes f \\ K[X, X^{-1}] & \xrightarrow{m^\star} & K[X, X^{-1}] \otimes_K K[X, X^{-1}]. \end{array}$$

$$\begin{array}{ccc} K[X,X^{-1}] & \xrightarrow{i^\star} & K[X,X^{-1}] \\ \downarrow f & & \downarrow f \\ K[X,X^{-1}] & \xrightarrow{i^\star} & K[X,X^{-1}]. \end{array}$$

$$\begin{array}{ccc} K[X,X^{-1}] & \xrightarrow{\epsilon^\star} & K \\ \downarrow f & & \downarrow f \\ K[X,X^{-1}] & \xrightarrow{\epsilon^\star} & K. \end{array}$$

We write down the $K$-algebra homomorphisms $m^\star, i^\star$ and $\epsilon^\star$.

$$\begin{gathered} m^\star : K[X,X^{-1}] \to K[X,X^{-1}] \otimes_K K[X,X^{-1}], \\ X \to X \otimes X. \end{gathered}$$

$$\begin{gathered} i^\star : K[X,X^{-1}] \to K[X,X^{-1}], \\ X \to X^{-1}. \end{gathered}$$

$$\begin{gathered} \epsilon^\star : K[X,X^{-1}] \to K, \\ X \to 1. \end{gathered}$$

Now

$$(f \otimes f)(m^\star(X)) = (f \otimes f)(X \otimes X) = (f(X) \otimes f(X)) = \lambda X^r \otimes \lambda X^r = \lambda^2 (X^r \otimes X^r),$$

and

$$m^\star(f(X)) = m^\star(\lambda X^r) = \lambda m^\star(X)^r = \lambda (X \otimes X)^r = \lambda X^r \otimes X^r.$$

So $(f \otimes f) \circ m^\star = m^\star(f(X))$ if and only if $\lambda = 1$. Similarly

$$f(i^\star(X)) = f(X^{-1}) = f(X)^{-1} = (\lambda X^r)^{-1} = X^{-r}\lambda^{-1},$$

and

$$i^\star(f(X)) = i^\star(\lambda X^r) = \lambda i^\star(X)^r = \lambda X^{-k}.$$

So $f \circ i^\star = i^\star \circ f$ if and only if $\lambda = \pm 1$. Finally

$$f(\epsilon^\star(X)) = f(1) = 1,$$

and

$$\epsilon^\star(f(X)) = \epsilon^\star(\lambda X^r) = \lambda \epsilon^\star(X)^r = \lambda.$$

So $f \circ \epsilon^\star = \epsilon^\star \circ f$ if and only if $\lambda = 1$. □

**Remark.** The above lemma also holds if we replace a field $K$ by a domain $D$.

**Definition.** Let $G$ be a group of multiplicative type over $K$, and let $K_s$ be a separable closure of $K$. Then $G$ is called a torus if there exists an $r \in \mathbf{N}$ such that $G \otimes_K K_s \cong (\mathbf{G}_{m,K_s})^r$. The integer $r$ is called the rank of the torus.

Let $T$ be a torus over $K$. We have the following isomorphism

$$\mathrm{Hom}_{K_s}(T_{K_s}, \mathbf{G}_{m,K_s}) \cong \mathbf{Z}^r.$$

This follows from:

$$\begin{aligned}\mathrm{Hom}_{K_s}(T_{K_s}, \mathbf{G}_{m,K_s}) &\cong \mathrm{Hom}_{K_s}(\mathbf{G}_{m,K_s}^r, \mathbf{G}_{m,K_s}) \\ &\cong \prod_{i=1}^{r} \mathrm{Hom}_{K_s}(\mathbf{G}_{m,K_s}, \mathbf{G}_{m,K_s})\end{aligned}$$

and lemma 2.4. We define the character group of $T$

$$X^\bullet(T) = \mathrm{Hom}_{K_s}(T_{K_s}, \mathbf{G}_m),$$

and the cocharacter group of $T$

$$X_\bullet(T) = \mathrm{Hom}_{K_s}(\mathbf{G}_m, T_{K_s}).$$

The character and cocharacter groups of $T$ are free abelian groups of rank $r$. They come together with a continuous action of $\mathrm{Gal}(K_s/K)$. We write $N = X^\bullet(T)$ and $\Gamma = \mathrm{Gal}(K_s/K)$.

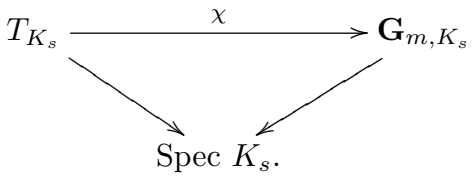
**Definition.** An action of $\Gamma$ on $N$ is called continuous if the map $\Gamma \times N \to N, (\sigma, x) \mapsto \sigma x$ is continuous. We endow $\Gamma$ with the Krull topology, $N$ with the discrete topology, and $\Gamma \times N$ with the product topology.

The functor $X_\bullet$ from the category of tori over $K$ to the category of free abelian groups of finite rank with continuous action of $\Gamma$-modules is an equivalence of categories, while the functor $X^\bullet$ is an anti-equivalence of categories. The action of the Galois group is given by a continuous homomorphism

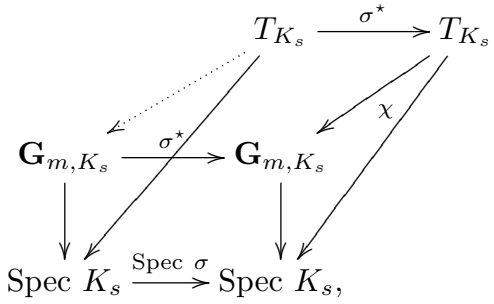
$$\phi : \Gamma \to \mathrm{Aut}_{\mathbf{Ab}}(N).$$

We endow $\mathrm{Aut}_{\mathbf{Ab}}(N)$ with the discrete topology for $N$ finitely generated. For each $\sigma \in \Gamma$ and $\chi \in X^\bullet(T)$ we want to explicitly describe the action $\sigma\chi$.

By definition we have a commutative diagram




To determine the action of $\Gamma$ on $X^\bullet(T)$ we base change the above diagram by Spec $\sigma$; we take the fibred product of $T_{K_s}$ and $\mathbf{G}_{m,K_s}$ via Spec $\sigma$.



We define the action $\sigma\chi = \sigma^{\star^{-1}}\chi\sigma^{\star}$. It is given by the dotted arrow in the above diagram.

**Proposition 2.5.** *Let $K_s$ be a separable closure of $K$. Then the functor $G \mapsto D(G)(K_s)$ induces an equivalence of categories between the category of groups $G$ of multiplicative type over $K$ and the category of continuous* $\mathrm{Gal}(K_s/K)$*-modules. Restricting this functor to the category of groups of multiplicative type which are of finite type over $K$ yields an equivalence of categories between the category of groups of multiplicative type which are of finite type over $K$ and the category of* $\mathrm{Gal}(K_s/K)$*-modules which are finitely generated as* $\mathbf{Z}$*-modules.*

Proof. Demazure and Gabriel [9], Corollaire 3.6 in IV.§1. □

To understand $T$ over $K$, we study $T$ over $K_s$ and describe how the Galois group acts. This is done explicitly using descent theory. A study of this topic is beyond the scope of this master's thesis. A good reference on this topic is Bosch et al. [5].

### ▶ Integral models of tori

Let $K$ be a number field. Let $T$ be a torus over $K$. We want to reduce modulo primes of $K$, i.e. modulo maximal ideals of $\mathcal{O}_K$. To do this we construct a model of $T$ over a non-empty open subset $U$ of $\mathcal{O}_K$.

**Definition.** Let $X = \mathrm{Spec}\ A$, for some Dedekind domain $A$, and let $Y$ be an $X$-scheme. Let $G$ be a finite group acting on the right on $Y$ via $X$-automorphisms. Then $Y$ is called a Galois cover with group $G$ if $Y$ is an integral scheme which is finite over $X$ (so $Y$ is affine and hence is the spectrum of a domain $B$), if $X$ is a quotient of $Y$ by the action of $G$ in the category of schemes, and if the inertia group is trivial for all $\mathfrak{q}$ in Spec $B$. If $f : Y \to X$ is a Galois cover, then we write $\mathrm{Gal}(Y/X) = \mathrm{Aut}_X(Y)$.

**Lemma 2.6.** *Let $U$ be a non-empty open subscheme of* Spec $\mathcal{O}_K$*, let $V$ over $U$ be a Galois cover, and let $L$ be the field of rational functions on $V$. Then $L/K$ is a finite Galois extension and $V$ is a non-empty open subset of* Spec $\mathcal{O}_L$*.*

Proof. Let $L$ be the field of rational functions on $V$. Let $\xi$ be the generic point of $V$, so that $L = \mathcal{O}_{V,\xi}$. By assumption $V$ over $U$ is a Galois cover. So there is a finite surjective map $\lambda : V \to U$. We have a diagram

$$\begin{array}{ccc} \tilde{U} & \xrightarrow{\subseteq} & \tilde{X} = \mathrm{Spec}\ \mathcal{O}_L \\ \downarrow & & \downarrow \\ U & \xrightarrow{\subseteq} & X = \mathrm{Spec}\ \mathcal{O}_K, \end{array}$$

where $\tilde{U}$ is the normalisation of $U$ in $L$, and $\tilde{X}$ the normalisation of $X$ in $L$. For $V$ being normal is equivalent to $\mathcal{O}_{V,x}$ being a discrete valuation ring for $x \in V$. We now apply theorem 2.24, §2.14, chapter II, Iitaka [16], to conclude that $\tilde{U} = V$, and $V \subseteq \mathrm{Spec}\ \mathcal{O}_L$.

Any isomorphism of $V$ over $U$ maps $\xi$ to itself, so it induces an automorphism of $L = \mathcal{O}_{V,\xi}$. Therefore, there is a map

$$\mathrm{Gal}(V/U) \to \mathrm{Gal}(L/K).$$

This is an isomorphism. Indeed, let $U_i = \text{Spec } A_i$, $i \in \{1, \dots n\}$ be an affine open cover of $U$, and let $V_i$ be the normalisation of $U_i$ in $L$. Then $V_i = \text{Spec } B_i$, where $B_i$ denotes the integral closure of $A_i$ in $L$. We extend each $\sigma \in \text{Gal}(L/K)$ to $\sigma^\star \in \text{Gal}(V/U)$ in the following way. First we extend $\sigma$ to an element $\sigma_i^\star \in \text{Gal}(V_i/U_i)$ for all $i$ as follows: if $x \in B_i$ is integral over $A_i$, then $\sigma x$ is integral over $A_i$. So $\sigma$ restricts to an isomorphism $\sigma_i : B_i \xrightarrow{\sim} B_i$. Now we apply the Spec-functor to get $\sigma^\star$. Then we glue all elements $\sigma_i^\star$ to get $\sigma^\star$.

**Definition.** A group scheme $\tilde{T}$ over an non-empty open subset $U$ of Spec $\mathcal{O}_K$ is called a torus if there exists a Galois cover $V \to U$ such that $\tilde{T} \times_U V$ is isomorphic to $\mathbf{G}_{m,V}^r$ for some $r \in \mathbf{Z}_{\geq 0}$.

**Definition.** A model of a torus $T$ over $K$ consists of
i) a non-empty open subset $U$ of Spec $\mathcal{O}_K$;
ii) a torus $\tilde{T}$ over $U$ such that

$$\tilde{T}_K = \tilde{T} \times_U \text{Spec } K$$

is isomorphic to $T$.
We denote a model of $T$ by $(U, \tilde{T})$.

**Definition.** For each torus $T$, a maximal model is $(U, \tilde{T})$ such that if $(U', \tilde{T}')$ is any other model then $U' \subseteq U$ and $\tilde{T}' \cong \tilde{T}_{|U'} = \tilde{T} \times_U U'$.

**Theorem 2.7.** *Every torus $T$ has a maximal model, and it is unique up to isomorphism.*

We prove the theorem later on. We now introduce some definitions and prove a proposition which we need in the proof of the theorem above.

**Definition.** A splitting field of a torus $T$ over $K$ is a field extension $L/K$ such that $T_L \cong \mathbf{G}_{m,L}$ for some $r$. A minimal splitting field exists.

**Proposition 2.8.** *Let $T$ be a torus over a field $K$, and let $K_s$ be a separable closure of $K$. Then there exists a unique Galois extension $M/K$ with $M \subseteq K_s$ such that $M$ is a splitting field of $T$, and such that if $L \subseteq K_s$ is any other Galois extension that is a splitting of $T$, then $M \subset L$.*

Proof. We recall that $T$ is uniquely determined by

$$X^\bullet = \text{Hom}_{K_s}(T_{K_s}, \mathbf{G}_{m,K_s}) \quad (\cong \mathbf{Z}^r)$$

with the action

$$\text{Gal}(K_s/K) \to \text{Aut}_{\mathbf{Ab}}(X^\bullet). \qquad (*)$$

If $L$ is any subfield of $K_s$, containing $K$, then $T_L$ is a torus over $L$ split over $K_s$. So $T_L$ is determined by $X^\bullet$ and the action

$$\text{Gal}(K_s/L) \to \text{Aut}_{\mathbf{Ab}}(X^\bullet). \qquad (**)$$

Note that the diagram

$$\begin{array}{ccc} \mathrm{Gal}(K_s/L) & \xrightarrow{\quad\subseteq\quad} & \mathrm{Gal}(K_s/K) \\ & \searrow \quad \swarrow & \\ & \mathrm{Aut}_{\mathbf{Ab}}(X^\bullet). & \end{array}$$

commutes. Note also that $T_L \cong \mathbf{G}_{m,L}^r$ if and only if $(**)$ is the trivial action. By the diagram we see that this is true if and only if $\mathrm{Gal}(K_s/L)$ is contained in the kernel of $(*)$. We call this kernel $H$ and let $M = K_s^H$. By Galois theory

$$\mathrm{Gal}(K_s/L) \subseteq H \Leftrightarrow M \subseteq L,$$

we see that

$$T \text{ is split over } L \Leftrightarrow M \subseteq L.$$

We call $M$ the *minimal splitting field* of $T$; by definition it is unique.

We now prove theorem 2.7.

Proof. We first construct the maximal model. Let $M$ be the minimal splitting field of $T$. Let $V_T$ be the maximal open subset of Spec $\mathcal{O}_M$ where the morphism Spec $\mathcal{O}_M \to$ Spec $\mathcal{O}_K$ is unramified, i.e. $V_T$ consists of the generic point and all primes of $\mathcal{O}_M$ not ramified over $\mathcal{O}_K$.

Let $U_T$ be the image of $V_T$ in Spec $\mathcal{O}_K$. Then the morphism $V_T \to U_T$ is Galois and

$$\mathrm{Gal}(M/K) \cong \mathrm{Gal}(V_T/U_T).$$

Therefore, the action of $\mathrm{Gal}(M/K)$ on

$$X^\bullet(T) = \mathrm{Hom}_M(T_M, \mathbf{G}_{m,M}) \quad (\cong \mathbf{Z}^r)$$

induces an action of $\mathrm{Gal}(V_T/U_T)$ on $X^\bullet$. By proposition 2.2 the $\mathrm{Gal}(V_T/U_T)$-module $X^\bullet$ corresponds to a unique torus $\tilde{T}$ over $U_T$, split over $V_T$. We first check that $(U_T, \tilde{T})$ is indeed a model, i.e. $\tilde{T} \times_{U_T} \mathrm{Spec}\ K \cong T$. Consider the diagram

$$\tilde{T} \longmapsto X^\bullet(\tilde{T})$$

$$\begin{array}{ccccc} \tilde{T} & & \{\text{Tori over } U \text{ split over } V\} & \xrightarrow{\sim} & \{\mathrm{Gal}(V/U) - \mathrm{mod}\} & & N \\ \downarrow & & \downarrow & & \downarrow \wr & & \downarrow \\ \tilde{T}_K & & \{\text{Tori over } K \text{ split over } L\} & \xrightarrow{\sim} & \{\mathrm{Gal}(L/K) - \mathrm{mod}\}. & & \iota(N) \end{array}$$

$$T \longmapsto X^\bullet(T)$$

The right vertical arrow is induced by the isomorphism $\iota : \mathrm{Gal}(L/K) \xrightarrow{\sim} \mathrm{Gal}(V/U)$.

By the construction of $\tilde{T}$ we have $X^\bullet(T) = \iota(X^\bullet(\tilde{T}))$ To prove that $\tilde{T}_K = T$, it suffices to show that the above diagram commutes. By this we mean that there exists a natural isomorphism

$$\varphi : \iota(X^\bullet(\tilde{T})) \to X^\bullet(\tilde{T}_K).$$

We construct this map as an isomorphism of groups. Let $D$ be a domain and let $r \geq 0$. Then we have an isomorphism of groups $\mathbf{Z}^r \xrightarrow{\sim} \mathrm{Hom}(\mathbf{G}_{m,D}^r, \mathbf{G}_{m,D})$, given by $(n_1, \ldots, n_r) \mapsto ((x_1, \ldots, x_r) \mapsto \prod_{i=1}^r x_i^{n_i})$. By lemma 2.4 we have $X^\bullet(\tilde{T}) = \mathrm{Hom}_V(\tilde{T} \otimes V, \mathbf{G}_{m,V}) \cong \mathbf{Z}^r$ and $X^\bullet(\tilde{T}_K) = \mathrm{Hom}_L(\tilde{T}_K \otimes L, \mathbf{G}_{m,L}) \cong \mathbf{Z}^r$. Hence the following diagram commutes and $X^\bullet(\tilde{T}) \cong X^\bullet(\tilde{T}_K)$ as groups.

$$\begin{array}{ccc} X^\bullet(\tilde{T}) & \xrightarrow{\sim} & X^\bullet(\tilde{T}_K) \\ & {\scriptstyle\sim}\nwarrow \quad \nearrow{\scriptstyle\sim} & \\ & \mathbf{Z}^r. & \end{array}$$

The Galois action is compatible. Hence the following diagram is commutative and we have an isomorphism of the Galois modules $\iota(X^\bullet(\tilde{T}))$ and $X^\bullet(\tilde{T}_K)$.

$$\begin{array}{ccc} X^\bullet(\tilde{T}) & \xrightarrow{\sim} & X^\bullet(\tilde{T}_K) \\ \downarrow{\scriptstyle\sigma} & & \downarrow{\scriptstyle\sigma_K} \\ X^\bullet(\tilde{T}) & \xrightarrow{\sim} & X^\bullet(\tilde{T}_K). \end{array}$$

We claim that $(U_T, \tilde{T})$ is the maximal model.

Suppose that $(U', \tilde{T}')$ is any other model. Let $V' \to U'$ be a Galois cover such that

$$\tilde{T}' \times_{U'} V' \cong \mathbf{G}_{m,V'}^r.$$

Then $V'$ is an open subset of Spec $\mathcal{O}_L$ for some $L \supseteq K$, and $L$ is a splitting field of $T$. So $M \subseteq L$.

The morphism Spec $\mathcal{O}_L \to$ Spec $\mathcal{O}_K$ factors through Spec $\mathcal{O}_M$. Because $V' \to U'$ is unramified, it factors through $V_T$:

$$\begin{array}{ccc} V' & \longrightarrow & V_T \\ \downarrow & & \downarrow \\ U' & \xrightarrow{\subseteq} & U_T \end{array}$$

So $U' \subseteq U_T$.

From the argument below lemma 2.6, it follows that

$$\mathrm{Gal}(L/K) \cong \mathrm{Gal}(V'/U'),$$
$$\mathrm{Gal}(M/K) \cong \mathrm{Gal}(V_T/U_T).$$

There is a commutative diagram

$$\begin{array}{ccc} \mathrm{Gal}(L/K) & \longrightarrow & \mathrm{Aut}_{\mathbf{Ab}}(\mathrm{Hom}_L(T_L, \mathbf{G}_{m,L}) \\ \downarrow{\scriptstyle\cong} & & \downarrow{\scriptstyle\cong} \\ \mathrm{Gal}(V'/U') & \longrightarrow & \mathrm{Aut}_{\mathbf{Ab}}(\mathrm{Hom}_{V'}(\tilde{T}'_{V'}, \mathbf{G}_{m,V'})) \end{array}$$

The upper map factors as

$$\begin{array}{ccc} \mathrm{Gal}(L/K) & \longrightarrow & \mathrm{Aut}_{\mathbf{Ab}}(\mathrm{Hom}_L(T_L, \mathbf{G}_{m,L})) \\ \downarrow{\scriptstyle \text{restriction}} & & \downarrow{\scriptstyle \cong} \\ \mathrm{Gal}(M/K) & \longrightarrow & \mathrm{Aut}_{\mathbf{Ab}}(\mathrm{Hom}_M(T_M, \mathbf{G}_{m,L})) \end{array}$$

Therefore, the bottom map factors as

$$\begin{array}{ccc} \mathrm{Gal}(V'/U') & \longrightarrow & \mathrm{Aut}_{\mathbf{Ab}}(\mathrm{Hom}_{V'}(\tilde{T}_{V'}, \mathbf{G}_{m,V'})) \\ \downarrow & & \downarrow{\scriptstyle \cong} \\ \mathrm{Gal}(V_T/U_T) & \longrightarrow & \mathrm{Aut}_{\mathbf{Ab}}(\mathrm{Hom}_{V_T}(T_{V_T}, \mathbf{G}_{m,V_T})) \end{array}$$

This means that

$$\tilde{T}' \cong \tilde{T}_{|U'}.$$

**Definition.** Let $T$ be a torus over $K$. Denote by $U_T$ the maximal open subset of $\mathrm{Spec}\ \mathcal{O}_K$ which consists of the generic point and all unramified primes in a minimal splitting field $M$. For each closed point $\mathfrak{p} \in U_T$, the reduction of $T$ modulo $\mathfrak{p}$ is

$$\tilde{T}_{\mathfrak{p}} = \tilde{T} \times_{U_T} \mathrm{Spec}\ \kappa(\mathfrak{p}).$$

We say that $T$ has *good reduction* at a nonzero prime ideal $\mathfrak{p} \in U_T$ if $\tilde{T}_{\mathfrak{p}}$ is a torus over $U_T$. We say that $T$ has *good reduction* if it has good reduction at every $\mathfrak{p}$. We say that $T$ has *bad reduction* at $\mathfrak{p}$ if $\mathfrak{p} \notin U_T$.

**Lemma 2.9.** *Let $K$ be a field of characteristic not equal to 2. For each $m \in K^\star \setminus (K^\star)^2$ we define a $K$-algebra $A_m = K[u,v]/(u^2 - mv^2 - 1)$ and an affine scheme $T_m = \mathrm{Spec}\ A_m$ with the following morphisms:*

*(i)* $\mu = \mathrm{Spec}\ \mu^\star$, *where* $\mu^\star$ *denotes the $K$-algebra homomorphism*

$$\begin{aligned} \mu^\star : A_m &\to A_m \otimes_K A_m, \\ u &\mapsto u \otimes u + mv \otimes v, \\ v &\mapsto u \otimes v + v \otimes u. \end{aligned}$$

*(ii)* $\iota = \mathrm{Spec}\ \iota^\star$, *where* $\iota^\star$ *denotes the $K$-algebra homomorphism*

$$\begin{aligned} \iota^\star : A_m &\to A_m, \\ u &\mapsto u, \\ v &\mapsto -v. \end{aligned}$$

*(iii)* $\epsilon = \mathrm{Spec}\ \epsilon^\star$, *where* $\epsilon^\star$ *denotes the $K$-algebra homomorphism*

$$\begin{aligned} \epsilon^\star : A_m &\to K, \\ u &\mapsto 1, \\ v &\mapsto 0. \end{aligned}$$

*Then $T_m$ is a torus of rank 1 over $K$ for each $m$. Moreover, if $T$ is an arbitrary torus of rank 1 over $K$, then $T$ is isomorphic to $\mathbf{G}_{m,K}$ or to a torus of the form $T_m$.*

Proof. Let $m \in K^\star \backslash (K^\star)^2$, and let $L$ be the quadratic field extension $L = K(\sqrt{m})$. Then tensoring $A_m$ with $L$ over $K$ one gets an $L$-algebra $A_m \otimes_K L = L[u,v]/(u^2 - mv^2 - 1)$, which is isomorphic to the $L$-algebra $L[x,y]/(xy-1)$ of the split torus $\mathbf{G}_{m,L}$. This isomorphism is given by $u \mapsto (x+y)/2$ and $v \mapsto (y-x)/(2\sqrt{m})$. The data $(\mu, \iota, \epsilon)$ are under this isomorphism in one-to-one correspondence with the $(\mu, \iota, \epsilon)$ of $\mathbf{G}_{m,L}$. Hence $T_m$ is group scheme over $L$ since $\mathbf{G}_{m,L}$ is group scheme over $L$. Moreover $T_m$ is a group scheme over $K$ since $L/K$ is faithfully flat. We have shown that $T_m$ is isomorphic over $L/K$ to the split torus $\mathbf{G}_{m,L}$. Hence $T_m$ is a torus of rank 1 over $K$.

We compute the Galois module of $T_m$. Recall that a torus is uniquely determined by its character group with the action

$$\mathrm{Gal}(L/K) \to \mathrm{Aut}_{\mathbf{Ab}}(X^\bullet(T_m)).$$

From a previous lemma it follows that $X^\bullet(T_m) = \mathbf{Z}$. Hence $\mathrm{Aut}_{\mathbf{Ab}}(\mathbf{Z}) = \{\pm 1\}$. Consider the generator $\chi$ of the character group of $T_m$ given by

$$\chi = \mathrm{Spec}\ (L[x,y]/(xy-1) \xrightarrow[\chi^\star]{\sim} A_m),$$

where the $L$-algebra isomorphism $\chi^\star$ is given by

$$\begin{aligned} x &\mapsto u - \sqrt{m}v, \\ y &\mapsto u + \sqrt{m}v. \end{aligned}$$

The Galois group $\mathrm{Gal}(L/K)$ is cyclic of order 2, and the nontrivial element $\sigma$ sends $\sqrt{m}$ to $-\sqrt{m}$.

We calculate the action of $\sigma\chi$ of $\mathrm{Gal}(L/K)$ on the character group of $T_m$. Consider the diagram

$$\begin{array}{ccc} L[x,y]/(xy-1) & \xrightarrow[\sim]{\chi^\star} & A_{m,L} \\ {\scriptstyle\sim}\downarrow{\scriptstyle\sigma} & & {\scriptstyle\sim}\downarrow{\scriptstyle\sigma} \\ L[x,y]/(xy-1) & \xrightarrow[\sim]{\sigma\chi^\star} & A_{m,L}. \end{array}$$

Now

$$\begin{aligned} \sigma\chi^\star(x) &= \sigma(\chi^\star(\sigma^{-1}(x))) \\ &= \sigma(\chi^\star(x)) \\ &= \sigma(u - \sqrt{m}v) \\ &= u + \sqrt{m}v. \end{aligned}$$

Similarly we see that $\sigma\chi^\star(y) = u - \sqrt{m}v$. So the nontrivial element of the Galois group acts on the character group of $T_m$ via multiplication by $-1$.

Let $T$ be an arbitrary torus of rank 1 over $K$. Then the character group $X^\bullet(T)$ of $T$ is isomorphic to $\mathbf{Z}$. The automorphism group of $X^\bullet(T)$ is $\{\pm 1\}$. The image of the map

$$\phi : \mathrm{Gal}(K_s/K) \to \mathrm{Aut}(X^\bullet(T))$$

giving the action is isomorphic to a quotient of the Galois group. The image must contain one or two elements since $\mathrm{Aut}(\mathbf{Z})$ is a group of order 2. If $T$ splits, i.e. $T \cong \mathbf{G}_m$,

then $\#\mathrm{im}(\phi) = 1$. If $T$ does not split, then $\#\mathrm{im}(\phi) = 2$. In that case $L/K$ must be a quadratic field extension, where $L = K_s^{\ker(\phi)}$. Let $\alpha \in L \setminus K$, then $\alpha^2 + p\alpha + q = 0$, for certain $p, q \in K$. Put $\beta = \alpha + p/2$. Then $\beta^2 = \alpha^2 + p\alpha + p^2/4 = -q + p^2/4$. Note that $L = K(\alpha) = K(\beta)$. So $\beta^2 = m$, with $m = (p^2 - 4q)/4$. Hence $L/K$ is of the form $L = K(\sqrt{m})$ with $m \in K^\star \setminus (K^\star)^2$. The Galois group of the splitting field $L/K$ of $T$ is cyclic of order 2. So the nontrivial element $\sigma$ of the Galois group acts on the character group $X^\bullet(T)$ of $T$ by multiplication by $-1$. Hence $T$ must be isomorphic to a torus of the form $T_m$. □

**Lemma 2.10.** *Let $K$ be a field of characteristic 2. For each $a \in K$, $a$ not of the form $b^2 + b$ with $b \in K$, we define a $K$-algebra $B_a = K[x, y]/(x^2 + xy + ay^2)$ and an affine scheme $T_a = \mathrm{Spec}\ B_a$ with the following morphisms:*

*(i) $\mu = \mathrm{Spec}\ \mu^\star$, where $\mu^\star$ denotes the $K$-algebra homomorphism*

$$\begin{aligned} \mu^\star : B_a &\to B_a \otimes_K B_a, \\ x &\mapsto x \otimes x + ay \otimes y, \\ y &\mapsto x \otimes y + y \otimes x + y \otimes y. \end{aligned}$$

*(ii) $\iota = \mathrm{Spec}\ \iota^\star$, where $\iota^\star$ denotes the $K$-algebra homomorphism*

$$\begin{aligned} \iota^\star : B_a &\to B_a, \\ x &\mapsto x + y, \\ y &\mapsto y. \end{aligned}$$

*(iii) $\epsilon = \mathrm{Spec}\ \epsilon^\star$, where $\epsilon^\star$ denotes the $K$-algebra homomorphism*

$$\begin{aligned} \epsilon^\star : B_a &\to K, \\ x &\mapsto 1, \\ y &\mapsto 0. \end{aligned}$$

*Then $T_a$ is a torus of rank 1 over $K$ for each $a$. Moreover, if $T$ is an arbitrary torus of rank 1 over $K$, then $T$ is isomorphic to $\mathbf{G}_{m,K}$ or to a torus of the form $T_a$.*

Proof. The proof goes along the same lines as above. □

# 3 Main theorem

## ▶ Result

We state here the main theorem of this Master's thesis.

**Theorem 3.1.** *Let $T$ be a one-dimensional torus defined over a number field $K$, and let $\lambda$ be a point in $T(K)$. Assume furthermore that $\lambda^{\mathbf{Z}}$ is Zariski-dense in $T$, i.e. $\lambda^{\mathbf{Z}}$ is infinite. Then the set*

$$S = \{n \in \mathbf{Z}_{>0} : \nexists \text{ prime ideal } \mathfrak{p} \text{ of } \mathcal{O}_K \text{ such that } n = order(\lambda \bmod \mathfrak{p})\}$$

*is finite.*

We will provide a proof of the main theorem at the end of this chapter. In the next section we consider the theorems of Zsigmondy and Schinzel since they are related to the main theorem.

## ▶ Theorem of Zsigmondy

Let $a, b$ be relatively prime integers with $|a| > |b| > 0$. A prime is called a primitive prime divisor of $a^n - b^n$ if it divides this number but does not divide $a^k - b^k$ for $0 < k < n$. A. Bang [3] proved in 1886 that there exists a constant $M > 0$ such that for each non-zero rational number $x$, $x \neq \pm 1$, and every integer $n > M$, there exists a prime number $p$ such that the order of $x$ modulo $p$ equals $n$. In 1892, K. Zsigmondy stated and proved a stronger version [35].

**Theorem 3.2.** [Zsigmondy] *Let $a, b$ be coprime integers with $a > b > 0$. Then for $n > 1$ $a^n - b^n$ has always a primitive prime divisor unless*
*(i) $a = 2, b = 1$ and $n = 6$; or*
*(ii) $a + b = 2^k$ for some integer $k$ and $n = 2$.*

Proof. Zsigmondy [35].

We state the analogue of Zsigmondy's theorem in algebraic number fields.

**Theorem 3.3.** [Schinzel] *Let $K$ be an algebraic number field, $A$, $B$ integers of $K$ such that $(A, B) = 1, AB \neq 0$, and $A/B$ of degree $d$ is not a root of unity. Then for every $d \in \mathbf{Z}_{>0}$, there exists a constant $n_0(d)$ such that for $n > n_0(d)$, $A^n - B^n$ has a prime ideal factor that does not divide $A^m - B^m$ for $m < n$.*

Proof. Schinzel [26]. Note that the theorem is best possible up to the order of the function $n_0(d)$; an absolute constant cannot be expected since for $A = \sqrt[d]{2}, B = 1, A^d - B^d = 1$ has no primitive divisor.

## ▶ Height functions and absolute values

In this section we present a brief introduction to height functions and valuations. We only state results that we need in the next section in which we prove —using heights— a special version of the theorem of Zsigmondy. A good reference to the theory of height functions is Hindry and Silverman [15]. For more details about valuations and algebraic number theory in general we refer to Neukirch [22] or Cassels and Fröhlich [7].

An absolute value on a number field $K$ is a function

$$|\cdot| : K \to \mathbf{R}_{\geq 0}$$
$$x \mapsto |x|$$

satisfying the following properties

(i) $|x| = 0 \Leftrightarrow x = 0$,
(ii) $|xy| = |x| \cdot |y|$ for all $x, y \in K$,
(iii) $\exists \alpha > 0$ such that for all $x, y \in K$, $|x + y|^\alpha \leq |x|^\alpha + |y|^\alpha$,
(iv) $\exists x_0 \in K$ with $|x_0| \neq 0, |x_0| \neq 1$.

An absolute value $|\cdot|$ on $K$ is called non-archimedean if (iii) can be replaced by the stronger inequality

$$|x + y| \leq \max(|x|, |y|) \quad \text{for } x, y \in K;$$

otherwise it is called archimedean.

Two absolute values $|\cdot|_1$ and $|\cdot|_2$ on $K$ are called equivalent if there is $\alpha > 0$ such that for $x \in K$, $|x|_2 = |x|_1^\alpha$. An equivalence class of absolute values on $K$ is called a place of $K$. A place is called infinite if it consists of archimedean absolute values, and finite otherwise. We denote by $\mathcal{M}_K$ the collection of places of $K$. Note that an absolute value $|\cdot|$ on $K$ induces a Hausdorff topology on $K$ in which a basis for the neighbourhoods of $x$ is given by the sets $\{y \in K : |y - x| < r\}$, for $x \in K$ and $r > 0$. Two absolute values on $K$ are equivalent if and only if they induce the same topology. Similarly to the construction of $\mathbf{R}$ from $\mathbf{Q}$, we can construct the completion of $K$ with respect to an absolute value $|\cdot|$, and $|\cdot|$ can be extended to a continuous absolute value on the completion. Equivalent absolute values give rise to the same completion, and therefore it makes sense to speak about the completion of $K$ at a place. The completion of $K$ at a place $v$ is denoted by $K_v$. We mention that if $v$ is infinite then $K_v \cong \mathbf{R}$ or $\mathbf{C}$.

Let $K = \mathbf{Q}$. We have on $\mathbf{Q}$ an archimedean absolute value given by

$$|x|_\infty = \max\{x, -x\}.$$

Further, for every prime number $p$ we have the $p$-adic absolute value given by

$$|x|_p = p^{-\mathrm{ord}_p(x)},\ x \in \mathbf{Q}^\star,\ |0|_p = 0,$$

where $\mathrm{ord}_p(x)$ is the unique integer such that

$$x = p^{\mathrm{ord}_p(x)} \cdot \frac{a}{b},\ a, b \in \mathbf{Z},\ p \not| ab.$$

Note that $\mathrm{ord}_p$ (with the convention $\mathrm{ord}_p(0) = \infty$) defines a discrete valuation on $\mathbf{Q}$. By a theorem of Ostrowski (Neukirch [22]) every absolute value on $\mathbf{Q}$ is equivalent to either $|\cdot|_\infty$ or $|\cdot|_p$ for some prime $p$. Thus we may identify $\mathcal{M}_\mathbf{Q}$ with $\{\infty\} \cup \{\text{primes}\}$.

Now let $K$ be any algebraic number field. Let $K'/K$ be an extension of number fields, and let $v \in \mathcal{M}_K$, and $w \in \mathcal{M}_{K'}$, we write $w|v$ if the restriction of $w$ to $K$ is $v$. For $v \in \mathcal{M}_K$, let $|\cdot|_v$ be the absolute value in $v$ extending one of the absolute values $|\cdot|_\infty$, $|\cdot|_p$ ($p$ primes) on $\mathbf{Q}$ defined above, and define the normalized absolute value $||\cdot||_v$ by

$$||x||_v = |x|_v^{n_v} \quad \text{for } x \in K,$$

where $n_v$ is the local degree of $v$ and is equal to $[K_v : \mathbf{Q}_v]$.

**Proposition 3.4.** *Let $K'/K$ be an extension of number fields.*
*(i)* (Degree formula) *For each place $v$ of $K$ we have*

$$\sum_{w \in \mathcal{M}_{K'}, w|v} [K'_w : K_v] = [K' : K].$$

*(ii)* (Product formula) *For any $x \in K^\star$ we have*

$$\prod_{v \in \mathcal{M}_K} ||x||_v = 1,$$

*where $|| \cdot ||_v$ is the normalized absolute value and $||x||_v = |x|_v^{n_v}$.*

Proof. Neukirch [22] for (i) chapter III, §1 and Hindry [15] for (ii), proposition B1.2, §B.1. □

Let $K$ be any number field, and let $\mathcal{M}_K$ be its set of places. Let $P = (x_0 : \ldots : x_n) \in \mathbf{P}^n(K)$ be a rational point in the $n$-dimensional projective space over $K$. We want to measure the size of $P$. Therefore we define the height of $P \in \mathbf{P}^n(K)$ relative to $K$ by

$$H_K(P) = \prod_{v \in \mathcal{M}_K} \max\{||x_0||_v, ||x_1||_v, \ldots, ||x_n||_v\}.$$

If we take the logarithm of $H_K(P)$, then we have the logarithmic height $h_K(P)$. We define $v(\cdot) = \log |\cdot|_v$. We write

$$h_K(P) = \log H_K(P) = \sum_{v \in \mathcal{M}_v} -n_v \min\{v(x_0), v(x_1), \ldots, v(x_n)\}.$$

The height function of $P$ is well-defined on $K$. It is independent of the choice of homogeneous coordinates. To see that we only have to apply the product formula mentioned above. The next lemma will enable us to define a height function that is independent of the field.

**Lemma 3.5.** *Let $K'/K$ be a finite extension of number fields. then*

$$H_{K'}(P) = H_K(P)^{[K':K]}.$$

Proof. This follows easily if we apply the degree formula to calculate the height. □

We define the absolute multiplicative height $H$ on $\mathbf{P}^n(\bar{\mathbf{Q}})$ as follows: given $P \in \mathbf{P}^n(\bar{\mathbf{Q}})$, take any number field $K$ such that $P \in \mathbf{P}^n(K)$ and put

$$H(P) = H_K(P)^{\frac{1}{[K:\mathbf{Q}]}}.$$

Then define the absolute logarithmic height or Weil height $h : \mathbf{P}^n(\bar{\mathbf{Q}}) \to \mathbf{R}_{\geq 0}$ by

$$h(P) = \log H(P).$$

The height function $h$ is invariant under the action of the Galois group $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$, i.e. if $P \in \mathbf{P}^n(\bar{\mathbf{Q}})$ and $\sigma \in \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$, then $H(\sigma(P)) = H(P)$.

**Example.** Let $P$ be a rational point $\in \mathbf{P}^n(\mathbf{Q})$. Then $P = (x_0 : x_1 : \ldots : x_n)$, where $x_0, x_1, \ldots, x_n \in \mathbf{Z}$ and $\gcd(x_0, x_1, \ldots, x_n) = 1$. The height of $P$ is $H(P) = \max\{|x_0|, \ldots, |x_n|\}$.

## ▶ Special version of Zsigmondy's theorem

**Theorem 3.6.** *Let $\alpha \in \mathbf{Q}^\star$, $\alpha \neq \pm 1$. Then for all but finitely many $n \in \mathbf{Z}_{>0}$, there is a prime $p$ such that the order of $\alpha$ modulo $p$ is exactly $n$.*

**Remark.** In the proof below, we used suggestions by dr. Jan-Hendrik Evertse.
Proof. The absolute height function $H$ defined above on $\mathbf{P}^1(\mathbf{Q})$ becomes

$$H(x_0 : x_1) = \prod_{p \in M_{\mathbf{Q}}} \max(|x_0|_p, |x_1|_p), \quad \text{for } (x_0; x_1) \in \mathbf{P}^1(\mathbf{Q}).$$

For every automorphism $A$ of $\mathbf{P}^1$ defined over $\mathbf{Q}$ there are constants $C_1, C_2 > 0$ depending only on $A$ such that

$$C_1 H(P) \leq H(AP) \leq C_2 H(P),$$

for all $P \in \mathbf{P}^1(\mathbf{Q})$, see Corollary 5.8, chapter VIII in [27]. In particular there are $C_1, C_2$ such that

$$\begin{aligned} C_1 H(x_0 \colon x_1) &\leq H(x_0 + x_1 \colon x_1) \\ &\leq C_2 H(x_0 \colon x_1). \end{aligned} \tag{1}$$

Now on $\mathbf{G}_m(\mathbf{Q}) = \mathbf{Q}^\star$ we define the height functions

$$\begin{aligned} h(\alpha) &= \log(H(\alpha^{-1} \colon 1)) \\ &= \log(H(1 : \alpha)) \end{aligned}$$

and

$$g(\alpha) = h(\alpha - 1).$$

By (1) we know that $|g - h| \leq C$ for some constant $C$. Note that

$$h(\alpha) = \log(\max\{1, |\alpha^{-1}|\}) + \sum_p \log(\max\{1, |\alpha^{-1}|_p\})$$

and

$$\begin{aligned} h_\infty(\alpha) &= \log(\max\{1, |\alpha^{-1}|\}) = \max\{0, -\log|\alpha|\} \\ h_p(\alpha) &= \log(\max\{1, |\alpha^{-1}|_p\}) \\ &= \max\{0, \log(p)\,\mathrm{ord}_p(\alpha)\}, \end{aligned}$$

for every prime $p$. Hence

$$h(\alpha) = h_\infty(\alpha) + \sum_p h_p(\alpha).$$

We also set

$$v_p(\alpha) = \log(p)\,\mathrm{ord}_p(\alpha) \in \log(p)\,\mathbf{Z}.$$

Similarly, with

$$g_\infty(\alpha) = h_\infty(\alpha - 1) \quad \text{and} \quad g_p(\alpha) = h_p(\alpha - 1), (p \,\text{prime})$$

we have

$$\begin{aligned} g(\alpha) &= g_\infty(\alpha) + \sum_p g_p(\alpha) \\ &= \max\{0, -\log|\alpha^{-1}|_p\} + \max\{0, \log(p)\,\mathrm{ord}_p(\alpha-1)\} \end{aligned}$$

Note that for every prime $p$ we have:

$$g_p(\alpha) > 0 \Leftrightarrow \mathrm{ord}_p(\alpha-1) > 0.$$

A simple calculation shows that $h(\alpha^n) = nh(\alpha)$. We now want to know $g(\alpha^n)$. Therefore we state and prove the following lemma.

**Lemma 3.7.** *Let $p$ be a prime number, and let $\alpha \in \mathbf{Z}_p = \{\alpha \in \mathbf{Q} | \mathrm{ord}_p(\alpha) \geq 0\}$. Furthermore let $n$ be a positive integer. If $p > 2$ and $\mathrm{ord}_p(\alpha-1) \geq 1$ or if $p = 2$ and $\mathrm{ord}_p(\alpha-1) \geq 2$, then*

$$g_p(\alpha^n) = g_p(\alpha) + v_p(n).$$

Proof. It suffices to prove the lemma for $n$ a prime number, since we can write each integer uniquely as a product of primes. Write $\alpha = \beta + 1$. Then $\mathrm{ord}_p(\beta) \geq 1$ if $p > 2$ and $\mathrm{ord}_p(\beta) \geq 2$ if $p = 2$. Now

$$\alpha^n = (1+\beta)^n = 1 + n\beta + \binom{n}{2}\beta^2 + \ldots + \binom{n}{n-1}\beta^{n-1} + \beta^n = 1 + \gamma_n.$$

If $n \neq p$, then $\mathrm{ord}_p(\alpha^n - 1) = \mathrm{ord}_p(\beta)$. If $n = p$, then $\mathrm{ord}_p(\gamma_n) > \mathrm{ord}_p(n\beta)$. So $\mathrm{ord}_p(\alpha^n - 1) = \mathrm{ord}_p(n\beta) = \mathrm{ord}_p(\beta) + 1$. Hence in all cases

$$\mathrm{ord}_p(\alpha^n - 1) = \mathrm{ord}_p(\alpha - 1) + \mathrm{ord}_p(n),$$

which translates into $g_p(\alpha^n) = g_p(\alpha) + v_p(n)$. □

The theorem holds for $\alpha$ if and only if it holds for $\alpha^{-1}$. So, replacing $\alpha$ by $\alpha^{-1}$ if necessary, we may assume that $|\alpha| > 1$. Then $\log(|\alpha^n|) > 0$, so $h_\infty(\alpha^n) = 0$. Also for $n \gg 0$, we have $|\alpha^n - 1| > 1$, so $g_\infty(\alpha^n) = 0$.

Therefore, for $n \gg 0$,

$$g(\alpha) = \sum_{p \in \{\text{primes}\}} g_p(\alpha) \qquad \text{and} \qquad h(\alpha) = \sum_{p \in \{\text{primes}\}} h_p(\alpha).$$

Let $\{q_1, \ldots, q_r\}$ be the set of primes dividing $n$. Suppose that $n$ does not occur as the order of $\alpha$ for a prime $p$. Then for every prime $p$, there is $q_i \in \{q_1, \ldots, q_r\}$ such that $\alpha^{n/q_i} \equiv 1 \bmod p$ which is equivalent to $g_p(\alpha^{n/q_i}) > 0$. Without loss of generality we may assume that $\{q_1, \ldots, q_s\}$ are the primes among $\{q_1, \ldots, q_r\}$ such that for each $q_i \in \{q_1, \ldots, q_s\}$ there is a prime $p$ with $\alpha^{n/q_i} \equiv 1 \bmod p$. First we assume that $n$ is odd or $n$ is even and $\mathrm{ord}_2(\alpha - 1) \geq 2$.

**Claim:**

$$\begin{aligned} g_p(\alpha^n) = \sum_{i=1}^{r} g_p(\alpha^{\frac{n}{q_i}}) - \sum_{1 \leq i < j \leq r} g_p(\alpha^{\frac{n}{q_i q_j}}) \\ + \ldots + (-1)^{r-1} g_p(\alpha^{\frac{n}{q_1 \cdots q_r}}). \end{aligned}$$

We have for any distinct primes $q_{i_1}, \ldots, q_{i_r}$ dividing $n$,

$$g_p(\alpha^n) = g_p(\alpha^{\frac{n}{q_{i_1}\cdots q_{i_r}}}) + v_p(q_{i_1}\ldots q_{i_r}).$$

So

$$\begin{aligned} g_p(\alpha^n) &= \binom{s}{1} g_p(\alpha^n) - \binom{s}{2} g_p(\alpha^n) + \ldots + (-1)^s \binom{s}{s} g_p(\alpha^n) \\ &= \sum_{i=1}^{s} \left( g_p(\alpha^{\frac{n}{q_i}}) + v_p(q_i) \right) - \sum_{1\le i_1<i_2\le s} \left( g_p(\alpha^{\frac{n}{q_{i_1}q_{i_2}}}) + v_p(q_{i_1}q_{i_2}) \right) \\ &\qquad + \ldots + (-1)^s \left( g_p(\alpha^{\frac{n}{q_1\cdots q_s}}) + v_p(q_1\ldots q_s) \right) \\ &= \sum_{i=1}^{s} g_p(\alpha^{n/q_i}) - \sum_{1\le i_1< i_2 \le s} g_p(\alpha^{\frac{n}{q_{i_1}q_{i_2}}}) + \ldots + (-1)^{s-1} g_p(\alpha^{\frac{n}{q_1\cdots q_s}}). \end{aligned}$$

The claim follows since the other terms are 0. Using the claim, summing over all $p$,

$$\begin{aligned} g(\alpha^n) = \sum_{q|n} g(\alpha^{\frac{n}{q}}) - \sum_{q_1,q_2|n} g(\alpha^{\frac{n}{q_1q_2}}) \\ + \ldots + (-1)^r g(\alpha^{\frac{n}{q_1\cdots q_r}}). \end{aligned}$$

This implies that for some constant $C > 0$,

$$\begin{aligned} h(\alpha^n) - C \le \sum_{q|n} h(\alpha^{\frac{n}{q}}) - \sum_{q_1,q_2|n} h(\alpha^{\frac{n}{q_1q_2}}) \\ + \ldots + (-1)^r h(\alpha^{\frac{n}{q_1\cdots q_r}}) \\ + 2^{\omega(n)} C. \end{aligned}$$

Hence

$$\begin{aligned} n\,h(\alpha) - C \le \sum_{q|n} \frac{n}{q} h(\alpha) - \sum_{q_1,q_2|n} \frac{n}{q_1q_2} h(\alpha) \\ + \ldots + (-1)^r \frac{n}{q_1\ldots q_r} h(\alpha) \\ + 2^{\omega(n)} C. \end{aligned}$$

So

$$\left( n - n\sum_{q|n} \frac{1}{q} + n \sum_{q_1,q_2|n} \frac{1}{q_1q_2} + \ldots + (-1)^r n \frac{1}{q_1\ldots q_r} \right) h(\alpha) \le C(2^{\omega(n)} + 1).$$

Hence

$$\left( n \prod_{q|n} (1 - \frac{1}{q}) \right) h(\alpha) \le C(2^{\omega(n)} + 1).$$

Now

$$\prod_{q|n}(1-\frac{1}{q}) = \phi(n)/n \geq \frac{C'}{\log\log n}, \qquad 2^{\omega(n)} \leq \mathrm{e}^{C''\frac{\log n}{\log\log n}},$$

for some constants $C^{'}, C^{''} > 0$, see Hardy and Wright, Introduction to the Theory of Numbers. So

$$C'\frac{n}{\log\log n}\,h(\alpha) \leq \mathrm{e}^{\frac{C''\log n}{\log\log n}}.$$

Since $\alpha \neq \pm 1$, we have $h(\alpha) > 0$. Hence $n$ is bounded.

There remains the case that $n$ is even and $\mathrm{ord}_2(\alpha - 1) = 1$. Put $n = 2n'$ and $\alpha' = \alpha^2$. Then $\mathrm{ord}_2(\alpha' - 1) \geq 3$ and by applying the above argument to $\alpha', n'$ instead of $\alpha, n$ we obtain that $n'$ is bounded.

► **Proof of the main theorem**

We first consider the case $K = \mathbf{Q}$.

**Lemma 3.8.** *Let $T$ be a torus over $\mathbf{Q}$ isomorphic to the multiplicative group $\mathbf{G}_m$, and let $\lambda \in T(\mathbf{Q})$ be such that $\lambda^{\mathbf{Z}}$ is Zariski-dense in $T$. Then the set*

$$\{n \in \mathbf{Z}_{\geq 0} \mid \textit{there is no prime } p \textit{ such that the order of } \lambda \textit{ in } \mathbf{F}_p^\star \textit{ is } n\}$$

*is finite.*

Proof. Let $\lambda \in \mathbf{G}_m(\mathbf{Q}) = \mathbf{Q}^\star$ with $\lambda \notin \{\pm 1\}$. Write $\lambda = a/b$ with $a, b \in \mathbf{Z}$ and gcd($a$,$b$)=1. Note that $\lambda^m \equiv 1 (\mathrm{mod}\ p)$ if and only if $a^m - b^m \equiv 0 (\mathrm{mod}\ p)$. Let $n$ be a sufficiently large positive integer. Then by theorem 3.6 there is a prime $q_n$ which divides $a^n - b^n$ but does not divides $a^m - b^m$ for $1 \leq m < n$. Hence,

$$\begin{gathered}\lambda^n \equiv 1 \ (\mathrm{mod}\ q_n) \\ \text{and} \\ \lambda^m \not\equiv 1 \ (\mathrm{mod}\ q_n) \ \text{ for } 1 \leq m < n.\end{gathered}$$

But this just means that the order of $\lambda$ in $\mathbf{F}_{q_n}^\star$ is $n$. Therefore the set

$$\{n \in \mathbf{Z}_{\geq 1} \mid \text{there is no prime } p \text{ such that the order of } \lambda \text{ in } \mathbf{F}_p^\star \text{ is } n\}$$

is finite.

We now prove the main theorem.

Proof of the main theorem. Let $T$ be a one-dimensional torus defined over $K$ and $L$ the splitting field of $T$. Let $U$ be the biggest open subset of Spec $\mathcal{O}_K$ above which $L$ is unramified. Note that $U$ exists since there are finitely many primes above which a finite extension of number fields ramifies. Let $\tilde{T}$ be the unique torus defined over $U$ such that $\tilde{T}_K = \tilde{T} \times_U \mathrm{Spec}\ K \cong T$. Let $V := U \times_{\mathrm{Spec}\ \mathcal{O}_K} \mathrm{Spec}\ \mathcal{O}_L$, i.e. $V$ consists of all primes of $\mathcal{O}_L$ lying over $U$. By definition of $U$ and $V$, the diagram

$$\begin{array}{ccc} V & \xrightarrow{\subseteq} & \mathrm{Spec}\ \mathcal{O}_L \\ \downarrow & \square & \downarrow \\ U & \xrightarrow{\subseteq} & \mathrm{Spec}\ \mathcal{O}_K \end{array}$$

is cartesian. We know that $\tilde{T} \times_U V \cong \mathbf{G}_{m,V}$, by theorem 2.7, since $\tilde{T}$ is a model of $T_L \cong \mathbf{G}_{m,L}$. Let $\mathfrak{q}$ be a prime ideal of $\mathcal{O}_K$. Then for any prime ideal $\mathfrak{p}$ of $\mathcal{O}_L$ with $\mathfrak{q} = \mathfrak{p} \cap \mathcal{O}_K$, we have a commutative diagram

$$\begin{array}{ccc} \mathcal{O}_K & \longrightarrow & \mathcal{O}_K/\mathfrak{q} \\ \Big\downarrow{\scriptstyle \text{incl.}} & & \Big\downarrow \\ \mathcal{O}_L & \longrightarrow & \mathcal{O}_L/\mathfrak{p} \end{array}$$

Applying the Spec-functor reverses the arrows. So we have

$$\begin{array}{ccccc} \operatorname{Spec} \mathcal{O}_L/\mathfrak{p} & \hookrightarrow & V & \xrightarrow{\subseteq} & \operatorname{Spec} \mathcal{O}_L \\ \Big\downarrow & & \Big\downarrow & & \Big\downarrow \\ \operatorname{Spec} \mathcal{O}_K/\mathfrak{q} & \hookrightarrow & U & \xrightarrow{\subseteq} & \operatorname{Spec} \mathcal{O}_K \end{array}$$

We reduce $T$ modulo $\mathfrak{q}$, a prime of $\mathcal{O}_K$. That is by definition

$$\tilde{T}_\mathfrak{q} = \tilde{T} \times_{\operatorname{Spec} \mathcal{O}_K} \operatorname{Spec} \mathcal{O}_K/\mathfrak{q}.$$

Now consider what happens if we change base by Spec $\mathcal{O}_L/\mathfrak{p}$ to Spec $\mathcal{O}_K/\mathfrak{q}$, then we have

$$\begin{aligned} \tilde{T}_\mathfrak{q} \times_{\operatorname{Spec} \mathcal{O}_K/\mathfrak{q}} \operatorname{Spec} \mathcal{O}_L/\mathfrak{p} &\cong (\tilde{T} \times_U V) \times_V \operatorname{Spec} \mathcal{O}_L/\mathfrak{p} \\ &\cong \mathbf{G}_{m,V} \times_V \operatorname{Spec} \mathcal{O}_L/\mathfrak{p} \\ &\cong \mathbf{G}_{m,\mathcal{O}_L/\mathfrak{p}}. \end{aligned}$$

Hence

$$\begin{aligned} \tilde{T}_\mathfrak{q}(\mathcal{O}_K/\mathfrak{q}) &\subseteq \tilde{T}_\mathfrak{q}(\mathcal{O}_L/\mathfrak{p}) \\ &= \tilde{T}_\mathfrak{q} \times_{\operatorname{Spec} \mathcal{O}_K/\mathfrak{q}} \operatorname{Spec} \mathcal{O}_L/\mathfrak{p}(\mathcal{O}_L/\mathfrak{p}) \\ &\cong \mathbf{G}_{m,\mathcal{O}_L/\mathfrak{p}}(\mathcal{O}_L/\mathfrak{p}). \end{aligned}$$

Let $\lambda \in T(K) = \tilde{T}(K)$. Then $\lambda \in \mathbf{G}_{m,V}(L)$, since

$$\begin{aligned} \tilde{T}(K) &\subseteq \tilde{T}(L) \\ &= (\tilde{T} \times_U V)(L) \\ &= \mathbf{G}_{m,V}(L). \end{aligned}$$

By Schinzel's theorem there is a prime ideal $\mathfrak{p}$ of $\mathcal{O}_L$ such that

$$\begin{aligned} n &= \operatorname{order}(\, \overline{\lambda} \in (\tilde{T} \times_U V)_\mathfrak{p}(\mathcal{O}_L/\mathfrak{p}) \,) \\ &= \operatorname{order}(\, \overline{\lambda} \in \ (\tilde{T}_\mathfrak{q} \times_{\operatorname{Spec} \mathcal{O}_K/\mathfrak{q}} \operatorname{Spec} \mathcal{O}_L/\mathfrak{p})\ (\mathcal{O}_L/\mathfrak{p}) \,) \\ &= \operatorname{order}(\, \overline{\lambda} \in \tilde{T}_\mathfrak{q}(\mathcal{O}_K/\mathfrak{q}) \,), \end{aligned}$$

where $\mathfrak{q} = \mathfrak{p} \cap \mathcal{O}_K$.

# References


[1] N. Ailon, Z. Rudnick, *Torsion points on curves and common divisors of $a^k - 1$ and $b^k - 1$*, Acta Arith. **113** (2004), 31–38.

[2] M.F. Atiyah, I.G. MacDonald, *Introduction to commutative algebra*, Addison-Wesley, 1969.

[3] A. Bang, *Taltheoretiske undersogelser*, Tidskrift f. Math. **(5) 4** (1886), 31–38 and 130–137.

[4] A. Borel, *Linear Algebraic Groups*, Springer Graduate Texts in Mathematics, vol. 126, 1991.

[5] S. Bosch, W. Lütkebohmert, M. Raynaud, *Néron models*, Springer Ergebnisse der Mathematik und ihrer Grenzgebiete, vol. 21, 1990.

[6] Y. Bugeaud, P. Corvaja, U. Zannier, *An upper bound for the G.C.D. of $a^n - 1$ and $b^n - 1$*, Math. Z. **243** (2003), 79–84.

[7] J. W. S. Cassels, *Global fields*, Algebraic number theory, J. W. S. Cassels and A. Fröhlich eds., Academic press, 1967, 42–84.

[8] J. Cheon, S. Hahn, *The orders of the reductions of a point in the Mordell-Weil group of an elliptic curve*, Acta Arith. **88** (1999), 219–222.

[9] M. Demazure, P. Gabriel, *Groupes algébriques*, North-Holland Publ. Co., 1970

[10] D. Eisenbud, J. Harris, *The geometry of schemes*, Springer Graduate Texts in Mathematics, vol. 197, 2000.

[11] A. Grothendieck, *Éléments de géométrie algébrique. I. Le langage des schémas*, Inst. Hautes Études Sci. Publ. Math.(1960), no. 4, 228.

[12] A. Grothendieck (ed.) et al., *Revêtements étales et groupe fondamental (SGA 1)*, Springer Lecture Notes in Mathematics, vol. 224, 1971.

[13] A. Grothendieck, M. Demazure, et al., *Schémas en groupes (SGA 3)*, Springer Lecture Notes in Mathematics, vol. 151, 1970.

[14] R. Hartshorne, *Algebraic geometry*, Springer Graduate Texts in Mathematics, vol. 52, 1977.

[15] M. Hindry, J. H. Silverman, *Diophantine geometry, an introduction*, Springer Graduate Texts in Mathematics, vol. 201, 2000.

[16] S. Iitaka, *Algebraic geometry, an introduction to birational geometry of algebraic varieties*, Springer Graduate Texts in Mathematics, vol. 76, 1986.

[17] K. Ireland, M. Rosen, *A classical introduction to modern number theory*, Springer Graduate Texts in Mathematics, vol. 84, 1990.

[18] S. Lang, *Algebra*, Springer Graduate Texts in Mathematics, vol. 211, 2002.

[19] S. Lang, *Algebraic number theory*, Springer Graduate Texts in Mathematics, vol. 110, 1986.

[20] H. W. Lenstra Jr., *Galois theory for schemes*, Lecture notes, UC Berkeley, 1997.

[21] H. W. Lenstra Jr., *Primality testing*, Mathematics and computer science, J.W. Bakker et al. (eds.), CWI Monographs, 1986, 269–287.

[22] J. Neukirch, *Algebraic number theory*, Springer Grundlehren der mathematischen Wissenschaften, vol. 322, 1999.

[23] T. Ono, *Arithmetic of algebraic tori*, Annals of Mathematics **74** (1961), 101–139.

[24] B. Poonen, *Rational points on varieties*, Lecture notes, UC Berkeley, 2003.

[25] S. S. Shatz, *Group schemes, formal groups, and p-divisible groups*, Arithmetic Geometry, G. Cornell and J. H. Silverman eds., Springer-Verlag, 1986, 29–78.

[26] A. Schinzel, *Primitive divisors of the expression $A^n - B^n$ in algebraic number fields*, J. Reine Angew. Math. **268** (1974), 27–33.

[27] J. H. Silverman, *The arithmetic of elliptic curves*, Springer Gruadate Texts in Mathematics, vol. 106, 1986.

[28] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Springer Graduate Texts in Mathematics, vol. 151, 1994.

[29] J. H. Silverman, *Common divisors of $a^n - 1$ and $b^n - 1$ over function fields*, New York Journal of Math. **10** (2004), 37–43.

[30] J. H. Silverman, *The theory of height functions*, Arithmetic Geometry, G. Cornell and J. H. Silverman eds., Springer-Verlag, 1986, 151–166.

[31] P. Stevenhagen, *Number rings*, Lecture notes, Universiteit Leiden, 2004.

[32] V. E. Voskresenskii, *Algebraic groups and their birational invariants*, American Mathematical Society, Translations of Mathematical Monographs, vol. 179, 1998.

[33] W. C. Waterhouse, *Introduction to affine group schemes*, Springer Graduate Texts in Mathematics, vol. 66, 1979.

[34] M. Weissman, *Algebraic groups and automorphic forms*, Lecture notes, UC Berkeley, 2003.

[35] K. Zsigmondy, *Zur Theorie der Potenzreste*, Monatsh. f. Math. **3** (1892), 265–284.