Function fields and number fields

Soham

August 2016

Introduction

A *number field* is a finite extension $L/\mathbb{Q}$. A *function field* (over a finite field) is a finite extension of $\mathbb{F}_q(t)$.

Notation and conventions

1. For an infinite set, a property holds for *almost all* of its elements if it is satisfied by all but a finite number of elements.

2. Unless otherwise noted, p is an (integer) prime. In the same vein, $q = p^n$ for some prime p and positive power n.

3. We will write G_K for the absolute Galois group

$$G_K := \mathrm{Gal}(\overline{K}/K)$$

for K a (usually number) field.

Bibliography

[AW45] Emil Artin and George Whaples. "Axiomatic characterization of fields by the product formula for valuations". In: *Bull. Amer. Math. Soc.* 51.7 (July 1945), pp. 469–492. URL: http://projecteuclid.org/euclid.bams/1183507128.

[KKS00] Kazuya Kato, Nobushige Kurokawa, and Takeshi Saito. *Number Theory 1: Fermat's Dream*. 2000.

[Fre05] Edward Frenkel. "Lectures on the Langlands Program and Conformal Field Theory". In: *ArXiv High Energy Physics - Theory e-prints* (Dec. 2005). arXiv: hep-th/0512172.

[KKS11] Kazuya Kato, Nobushige Kurokawa, and Takeshi Saito. *Number Theory 2: Class Field Theory*. 2011.

[htt] Hurkyl (http://math.stackexchange.com/users/14972/hurkyl). *"Place" vs. "Prime" in a number field*. URL: http://math.stackexchange.com/q/201565.

Chapter 1

The structure of number fields

We will follow [Fre05] in this chapter. Throughout this chapter, when not otherwise noted, K and F will be number fields.

[KKS00] and [KKS11] are references for the material in this chapter.

1.1 Preliminaries from Galois theory

Denote by Fld_k the category of field extensions of k.

Theorem 1 (Fundamental theorem of Galois theory)**.** There is a functor

$$\mathrm{Gal}(-/k)\colon \mathsf{Fld}_k^{\mathsf{op}} \to \mathsf{Grp},$$

the *Galois group functor*.

Translated from the categorical language, there is an association

$$K/k \longleftrightarrow \mathrm{Gal}(K/k)$$

for every field extension K/k (or for every field K "over k"). This association is *functorial* in the sense that, for every k-morphism of fields $\phi : K/k \to L/k$, we have a commutative diagram

$$\begin{array}{ccc} K/k & \xrightarrow{\phi} & L/k \\ \downarrow & & \downarrow \\ \mathrm{Gal}(K/k) & \xleftarrow[\mathrm{Gal}(\phi)]{} & \mathrm{Gal}(L/k) \end{array}$$

1.1.1 Cyclotomic fields

Recall that the field of *cyclotomic numbers*, $\mathbb{Q}(\zeta_n)$, has Galois group

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$$

where $[n] \in \mathbb{Z}/n\mathbb{Z}$ acts as the n-th power map. This can be seen by noticing that the action of an element σ of the Galois group on the field is completely determined by where it sends ζ_n.

1.2 Class field theory

1.2.1 Abelian extensions

The study of general extensions of $\mathbb{Q}$ has proven technically challenging so far. While the fact that $\mathbb{Q}$ is a "nice" field means we have Galois theory at our disposal, arbitrary Galois extensions are too varied to be understood using field-theoretic methods alone.

However, the *abelian* extensions are a particularly tractable class of extensions, whose structure is completely given by the class field theory of number fields, or more generally, the class field theory of global fields (of which function fields are the other main example).

Definition 1. An *abelian* extension of $\mathbb{Q}$ is an extension $K/\mathbb{Q}$ with $\mathrm{Gal}(K/\mathbb{Q})$ abelian.

For instance, extensions like $\mathbb{Q}(i)$ are manifestly abelian. (TODO add examples and nonexamples)

Theorem 2 (Kronecker-Weber)**.** The maximal abelian extension $\mathbb{Q}^{\mathrm{ab}}$ of $\mathbb{Q}$ satisfies

$$\mathbb{Q}^{\mathrm{ab}} = \bigcup_n \mathbb{Q}(\zeta_n)$$

where, for $m|n$, we identify $\mathbb{Q}(\zeta_m)$ with the canonically given subfield of $\mathbb{Q}(\zeta_n)$.

1.2.2 A first look at Γ^{ab}

The Galois group of the maximal abelian extension, Γ^{ab}, is in fact the abelianization of the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ of $\mathbb{Q}$.[1] The Kronecker-Weber theorem allows us to apply $\mathrm{Gal}(-/\mathbb{Q})$ to get the following first description of the abelianized Galois group of $\mathbb{Q}$, noting that the union operation is the colimit in the category of sets, and contravariant functors like $\mathrm{Gal}(-/\mathbb{Q})$ "turn the arrows around":

$$\Gamma^{\mathrm{ab}} := \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}) \cong \varprojlim_n (\mathbb{Z}/n\mathbb{Z})^\times$$

[1] This holds for any field. (nice enough?)

Here the limit is taken with respect to the system of surjections

$$\pi_n^m \colon (\mathbb{Z}/n\mathbb{Z})^\times \to (\mathbb{Z}/m\mathbb{Z})^\times \text{for all } m|n$$

that sends, for instance, $[5] \in \mathbb{Z}/6\mathbb{Z}$ to $[1] \in \mathbb{Z}/3\mathbb{Z}$. This can be thought of as "throwing away" the information carried by the other factors (which is just 2 in this case).

What does an element of Γ^{ab} look like? By the definition of the inverse limit of a filtered set (TODO check this), an element of Γ^{ab} is a collection of elements

$$\alpha_n \in \mathbb{Z}/n\mathbb{Z}$$

compatible with the π_m^n, where by *compatibility* we mean that

$$m|n \implies \pi_n^m(\alpha_m) = \alpha_n.$$

1.2.3 Describing Γ^{ab} with p-adics

(fill in defns of $\mathbb{Z}_p$ and $\mathbb{Q}_p$ later)

We have the following classical result:

Theorem 3 (Chinese remainder theorem)**.** There exists an isomorphism

$$\mathbb{Z}/n\mathbb{Z} \cong \prod_p \mathbb{Z}/p^{\nu_p(n)}\mathbb{Z}.$$

Definition 2. We denote by

$$\hat{\mathbb{Z}} = \varprojlim_n \mathbb{Z}/n\mathbb{Z}$$

the *profinite completion* of $\mathbb{Z}$, where the limit is taken with respect to the natural system of surjections considered in the previous section.

Now note that

$$\begin{aligned}\hat{\mathbb{Z}} &= \varprojlim_n \mathbb{Z}/n\mathbb{Z} \\ &\cong \varprojlim_n \prod_p \mathbb{Z}/p^{\nu_p(n)}\mathbb{Z} \\ &\cong \prod_p \varprojlim_r \mathbb{Z}/p^r\mathbb{Z}\end{aligned}$$

which finally gives us

$$\hat{\mathbb{Z}} \cong \prod_p \mathbb{Z}_p.$$

Now observe that the Kronecker-Weber theorem can be understood as saying that $\Gamma^{\mathrm{ab}} \cong \hat{\mathbb{Z}}^\times$. Using the product expression for $\hat{\mathbb{Z}}$, we find that

$$\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}) \cong \prod_p \mathbb{Z}_p^\times.$$

1.3 Class field theory

The obvious next step is, given a number field $F/\mathbb{Q}$, to try to "upgrade" the Kronecker-Weber theorem and describe its maximal abelian extension F^{ab}.

No such analog is known. However, we do have a description of $\mathrm{Gal}(F^{\mathrm{ab}}/F)$, the abelianized Galois group of F, via class field theory.

1.3.1 Adeles and ideles

The special case of $F = \mathbb{Q}$

Define the ring of *integral adeles*

$$\mathbb{A}_{\mathbb{Z}} = \mathbb{R} \times \hat{\mathbb{Z}}$$

and the ring of *adeles* as

$$\mathbb{A}_{\mathbb{Q}} = \mathbb{A}_{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Q}.$$

We can put a topology on this: let $\hat{\mathbb{Z}}$ have the product topology inherited from the $\mathbb{Z}_p$, give $\mathbb{Q}$ the discrete topology, and let $\mathbb{R}$ have its usual topology. This makes $\mathbb{A}_{\mathbb{Q}}$ a topological ring, with a diagonal embedding $\mathbb{Q} \to \mathbb{A}_{\mathbb{Q}}$. There is a similar embedding $\mathbb{Q}^\times \to \mathbb{A}_{\mathbb{Q}}^\times$.

Notice that the quotient

$$\mathbb{A}_{\mathbb{Q}}/\mathbb{Q} \simeq \hat{\mathbb{Z}} \times (\mathbb{R}/\mathbb{Z})$$

is compact, since $\hat{\mathbb{Z}}$ is a profinite group and hence compact.

In the special case of $F = \mathbb{Q}$, the statement of class field theory is that $\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$ is isomorphic to the group of connected components of the quotient $\mathbb{A}_{\mathbb{Q}}^\times/\mathbb{Q}^\times$. With the previous statement, we see that

$$\mathbb{A}_{\mathbb{Q}}^\times/\mathbb{Q}^\times \simeq \mathbb{R}^{>0} \times \prod_p \mathbb{Z}_p^\times.$$

Since $\mathbb{R}^{>0}$ is very conencted, the group of connected components is isomorphic to $\prod_p \mathbb{Z}_p^\times$, thus verifying the Kronecker-Weber theorem.

More general settings

Now we generalize to arbitrary $F/\mathbb{Q}$.

Chapter 2

The Artin-Whaples characterization

2.1 Introduction

A striking piece of evidence in favor of our hypothesis that number fields and function fields are more similar than one might expect is given by [AW45], which proves the following theorem:

Theorem 4 (Main theorem of [AW45])**.** If a field satisfies the valuation product formula, and if one of those valuations is of a suitable type, then it is forced to be either a number field or a function field.

We will now examine the proof of the following theorem, essentially following the original in its development of the material.

2.2 Places and valuations

2.2.1 Valuations

A valuation on a field is a way to assign a "size" to its elements in a way that fits our usual expectations of how such functions should behave. For instance, we have the valuation

$$|\cdot| : \mathbb{C} \to \mathbb{R}$$

which is defined by the mapping

$$|a + ib| \mapsto \sqrt{a^2 + b^2}$$

for $a + ib \in \mathbb{C}$.

The properties this satisfies (nonnegativity, the triangle inequality, and so on) are abstracted by the following definition:

Definition 3. Let k be a field. A function $|\cdot| : k \to \mathbb{R}$ is called a *valuation* if it satisfies the following properties:[1]

1. $|\alpha| = 0 \iff \alpha = 0$
2. $\mathrm{Im}\,|\cdot| \subset \mathbb{R}^{>0}$
3. $|\alpha\beta| = |\alpha||\beta|$
4. $|\alpha + \beta| \leq |\alpha| + |\beta|$

If a valuation satisfies the following, it is called *nonarchimedean* (and *archimedean* otherwise):

3' $|\alpha + \beta| \leq \max(|\alpha|, |\beta|)$

2.2.2 Motivation for places

When working with number fields other than $\mathbb{Q}$, we find that there are "more primes" than we might expect. In a naive sense, of course, this is true: for instance, we have primes like $(1 + i)$ in $\mathbb{Q}(i)$.

More generally, we can look at a prime ideal in the ring of integers and consider the valuation it gives rise to.

For instance, $(3) \subset \mathbb{Z}[i]$ gives us the valuation

$$|x|_3 = |x|_{(3)} = 3^{-\nu_3(x)}$$

with, e.g. $|36|_3 = 3^{-2}$.

We might then decide to consider the valuations themselves as the fundamental objects. This is very useful: considering valuations allows us to recover a lot of data, like the prime ideals of the ring of integers, in a purely *field-theoretic* way, instead of having to worry about integral closures and so on.[2]

Of course, this on its own is not very useful, since there are many, many more possible valuations than there can be "generalized primes" (however one wishes to define that).

2.2.3 The equivalence relation on valuations

The solution is to define a notion of *equivalence* for valuations. One way to do it is by noticing the following:

Theorem 5. Every valuation on a field induces a metric on it.

A metric defines a metric space structure, and hence a topological space structure, on the field. We can now say that

Definition 4. Two valuations $|\cdot|_1$ and $|\cdot|_2$ are *equivalent* if they determine identical topological space structures on the field.

[1] AW45, section 1.

[2] I realised the importance of this thanks to [htt].

Another way to do it is as follows: first, notice that raising an absolute value to any power less than 1 gives rise to another absolute value. We can, hence, define two absolute values to be equivalent if there is some power $c \in (0,1)$ for which

$$|\cdot|_1 = |\cdot|_2^c$$

.

These two definitions of *equivalent* are actually equivalent!

Definition 5. An equivalence class of valuations is called a *prime place*, or simply a *place* for short.

The (nontrivial) places of $\mathbb{Q}$ can be classified as follows:

- the nonarchimedean ones, which correspond to p-adic valuations and hence to prime ideals (p) in the ring of integers $\mathbb{Z}$ of $\mathbb{Q}$ (and thus to the p-adic fields arising as completions of $\mathbb{Q}$ under these valuations)
- the archimedean ones, which correspond to embeddings of $\mathbb{Q}$ into $\mathbb{R}$ or $\mathbb{C}$ ("real" and "complex" embeddings)

In general, a field may have many archimedean places, corresponding to different embeddings into $\mathbb{R}$ or $\mathbb{C}$.

2.3 The proof

2.3.1 A finite set of valuations

We now look at a *finite* set of (nontrivial, inequivalent) valuations $|\cdot|_i$. We have the following[3] results:

Lemma 1. If $|\cdot|_1$ and $|\cdot|_2$ are two inequivalent valuations, there is some γ such that

$$|\gamma|_1 < 1 \text{ and } |\gamma|_2 > 1.$$

Lemma 2. If $|\cdot|_i$ are inequivalent, there is some α such that

$$|\alpha|_1 > 1 \text{ and } |\alpha|_{i>1} < 1.$$

Lemma 3. If $|\cdot|_i$ are inequivalent, for every $\epsilon > 0$, there is an α such that

$$|\alpha - 1|_1 \leq 1 \text{ and } |\alpha|_{\nu>1} \leq 1.$$

Theorem 6 (Approximation theorem)**.** Given pairs $(|\cdot|_i, \alpha_i)$, with the $|\cdot|_i$ inequivalent, then for every $\epsilon > 0$ there is some α with

$$|\alpha - \alpha_i|_i < \epsilon.$$

[3] AW45, p. 471–2.

Corollary 1. If $|\cdot|_i$ are nontrivial and inequivalent, then any identity of the form

$$\prod |\alpha|_i^{\nu_i} = 1$$

with $0 \neq \alpha \in k$ implies that the ν_i are all 0.

Theorem 1 "precludes the possibility that a finite number of valuations can ever be interrelated".

2.4 The product formula

We now come to the product formula referred to in 4. Recall that it states that a field satisfying two particular axioms with respect to the valuations defined on it must either be a number field or a function field.

We will now look at the two axioms of the theorem.

2.4.1 The valuation product formula

Axiom 1. There is a set M of pairs $(\mathfrak{p}, |\cdot|_\mathfrak{p})$ such that, for any $0 \neq \alpha \in k$,

- $|\alpha|_\mathfrak{p} = 1$ for almost all $\mathfrak{p}$
- Extending the product over all primes,

$$\prod_\mathfrak{p} |\alpha|_\mathfrak{p} = 1$$

For instance, for $6 \in \mathbb{Q}$, the product looks like

$$|6|_{(0)} \cdot |6|_{(2)} \cdot |6|_{(3)} = 6 \cdot 2^{-1} \cdot 3^{-1} = 1$$

We have mentioned earlier that to any prime $\mathfrak{p}$, we can associate infinitely many equivalent valuations on k. This axiom allows us to choose one particular valuation as a distinguished representative of its equivalence class.

2.4.2 Idèles

We associate to M a space of vectors V_M, whose elements are vectors of the form

$$v = (v_\mathfrak{p})_\mathfrak{p}, \text{where } v_\mathfrak{p} \in k_\mathfrak{p}.$$

We will simplify notation by writing $|v|_\mathfrak{p}$ for $|v_\mathfrak{p}|_\mathfrak{p}$.

Definition 6. A vector $(v_\mathfrak{p})$ of this form is an *idèle* if

- $v_\mathfrak{p} \neq 0$ for all $\mathfrak{p}$
- $v_\mathfrak{p} = 1$ for almost all $\mathfrak{p}$

There is a natural embedding $k \hookrightarrow V_M$, reminiscent of diagonal embeddings: writing $i_\mathfrak{p}$ for the inclusion $k \to k_\mathfrak{p}$,

$$\alpha \mapsto (i_\mathfrak{p}(\alpha))_\mathfrak{p}$$

2.4.3 The volume of an idèle

For each idèle $\mathfrak{a}$, define

$$V(\mathfrak{a}) = \prod_{\mathfrak{p}} |\mathfrak{a}|_{\mathfrak{p}}$$

This function is obviously multiplicative.

1. For elements α coming from k via the embedding, notice that we have, via the product formula 2.4,

$$V(\alpha) = \prod_{\mathfrak{p}} |\mathfrak{a}|_{\mathfrak{p}} = 1.$$

   This gives

$$V(\alpha\mathfrak{a}) = V(\alpha)V(\mathfrak{a}) = V(\mathfrak{a}).$$

2. A map $\mathfrak{p} \mapsto x_{\mathfrak{p}} \in \mathbb{R}$, with $x_{\mathfrak{p}} = 1$ for almost all $\mathfrak{p}$, gives a set of vectors

$$|\mathfrak{c}|_{\mathfrak{p}} \leq |\mathfrak{a}|_{\mathfrak{p}}$$

   which we call the parallelotope with dimensions $x_{\mathfrak{p}}$ or even simply x. In this case, the number $V(\mathfrak{a})$ can be thought of as the "volume" of the parallelotope.

2.5 Other notions

2.5.1 The order of a set

[AW45] defines a notion of *order*, stating that it

> [unites] different types of fields[4]

although the definition itself is a a construction I have little motivation for.

Given a "field of discourse" k, the order of a set of elements is defined as follows:

1. If k has an archimedean valuation, then the order of a set is its the number of elements.

2. If all the valuations of k are nonarchimedean, there is some field of constants $k_0 \subset k$. (For instance, if $k = \mathbb{F}_q(\sqrt{t})$, $k_0 = \mathbb{F}_q$.) The order of a set is then defined to be q^s, where we define q and s as follows:

   (a) If k_0 is finite, q is its number of elements. Otherwise, q is an arbitrary fixed number greater than 1.

   (b) s is the number of elements in the set that are linearly independent over k_0.

[4] AW45, p. 474.

2.5.2 The M-function

The order of a set of elements contained in the parallelotope of size $\mathfrak{a}$ will be denoted $M(\mathfrak{a})$. Note that, for nonzero $\theta \in k$, $M(\theta\mathfrak{a}) = M(\mathfrak{a})$ since multiplying by θ changes the parallelotope of size $\mathfrak{a}$ into the parallelotope of size $\theta\mathfrak{a}$ and does not change the order.

2.5.3 The ring of $\mathfrak{p}$-integers

The set of elements $\alpha \in k$ for which $|\alpha|_\mathfrak{p} \leq 1$ forms a ring, which we denote $\mathcal{O}_\mathfrak{p}$. The subset of $\mathcal{O}_\mathfrak{p}$ with $|\alpha|_\mathfrak{p} < 1$ forms an ideal in this ring, which, by abuse of notation, is also denoted $\mathfrak{p}$. Now we have a quotient field $\mathcal{O}_\mathfrak{p}/\mathfrak{p}$, and so on. The *order* of this field is called the norm $N\mathfrak{p}$ of $\mathfrak{p}$. For instance, if there is a constant field $k_0 \subseteq k^\mathfrak{p} = \mathcal{O}_\mathfrak{p}/\mathfrak{p}$, we have

$$N\mathfrak{p} = (\#k_0)^{[k^\mathfrak{p}:k_0]}$$

2.6 Axiom 2

The set M of **??** contains at least one prime $\mathfrak{q}$, which is either

- discrete, with a finite quotient field of finite order $N\mathfrak{q}$
- archimedean, with $k_\mathfrak{q} = \mathbb{R}$ or $\mathbb{C}$

Note that, by Ostrowski's theorem, the second part of the condition on archimedean places is superfluous.

2.6.1 Another valuation

For $\alpha \neq 0$, define a valuation as follows:

- For $\mathfrak{p} \not| \infty$ set
$$||\alpha||_\mathfrak{p} = \frac{1}{N\mathfrak{p}^\nu}$$
where $\nu = \mathrm{Ord}_\mathfrak{p}(\alpha)$.
- If $k = \mathbb{R}$, $||\cdot||_\mathfrak{p}$ is defined to be the standard absolute value.
- If $k = \mathbb{C}$, $||\cdot||_\mathfrak{p}$ is set to be the squared absolute value.

2.6.2 Number fields and function fields work

We next come to the following theorem, which tells us that number fields and function fields satisfy the two axioms stated above:

Theorem 7. We can construct M such that both **??** and 2.6 hold for the following fields:

- a number field, i.e., a finite extension $K/\mathbb{Q}$
- a field of algebraic functions over any field k_1 (that is, a finite extension $K/k_1(z)$ with z transcendental $/k_1$)

In the second case, the field of constants $k_0 \subset k$ consists of all elements of k algebraic over k_1.

The proof of this is done through a sequence of lemmas.

Lemma 4. Let k be a field for which 1 holds, and F a subfield that does not exclusively comprise constants of k. Let $\mathfrak{N}$ be the set of nontrivial divisors (???) p of F that are divisible by some $\mathfrak{p}$ of $\mathfrak{M}$. Then 1 holds in F for $\mathfrak{N}$.

Lemma 5. Let k be a field for which 1 holds and K/k a finite algebraic extension. Let $\mathfrak{N}$ be the set of all divisors $\mathfrak{P}$ of K that divide some $\mathfrak{p}$ of $\mathfrak{M}$. Then 1 holds in K for some subset $\mathfrak{N}' \subset \mathfrak{N}$.

In fact, $\mathfrak{N}' = \mathfrak{N}$, but this is postponed to the next section.

Lemma 6. 1 holds in the case of $\mathbb{Q}$ and that of $K = k_1(z)$. The set $\mathfrak{M}$ of valuations is the set of all valuations in the case of $\mathbb{Q}$, and the set of valuations trivial on k_1 in the latter case. The product formula is of the form

$$\prod_p ||a||_p = 1$$

or a power, and there is no other relation between these valuations.

From the last two lemmas, we see that 1 holds for the fields of (??? thm2). The fact that all valuations of $\mathfrak{M}$ satisfy **??** follows from the fact that this is true in $\mathbb{Q}$ and hence in a finite extension $k/\mathbb{Q}$.

It remains to prove the statement about the field fe 0 of constants.

If p is trivial on k it is also trivial on an algebraic extension of ki. Hence we need only show that any constant c of ko is algebraic with respect to ki. If on the contrary c were transcendental with respect to ki then from the equation c satisfied with respect to ki(z) it follows that z would be algebraic with respect to ki(c). Since ki(c) is in ko, this would mean that z is in ko. So all of k would be in fe 0 , contradicting the fact that no p of 9J is trivial on k.

2.7 Characterizing fields by the product formula

2.7.1 (Main) theorem 3

If a field satisfies **??** and 2.6, it is of one of the two types in **??**. Furthermore, 2.6 is satisfied for every place $\mathfrak{p}$.

2.8 Parallelotopes

2.8.1 Theorem 4

There are positive C, D such that for all idèles $\mathfrak{a}$ we have

$$CV(\mathfrak{a}) < M(\mathfrak{a}) \leq \max(1, DV(\mathfrak{a}))$$

2.8.2 Definitions

Let U be the multiplicative group of "absolute units", that is, $x \in k$ is in U if $||x||_{\mathfrak{p}} = 1$ for all $\mathfrak{p}$.

- If there is a constant field k_0, $U = {k_0}^{\times}$.
- "In case order means number of elements, U must be a finite group since it is contained in the parallelotope of size 1, so U consists of all roots of unity in k.

Now select a finite set S of primes that contains all the archimedean primes. By $\mathfrak{a}_S$ we mean the idèles $\mathfrak{a}$ such that $|\mathfrak{a}| = 1$ for all $\mathfrak{p} \notin S$. As one might expect, $e_{\mathfrak{p}} \in k$ which belong to $\mathfrak{a}_S$ are called S-units.