èles1.2.59Adèlessubsection.1.2.5

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 $\mathbb{F}_q(t)$.

Number fields have been one of the main objects of study in algebraic number theory for many years. Function fields arise naturally in algebraic geometry, as the rings of global functions on smooth projective curves.

The analogy between these two classes of fields is deep and fascinating: in particular, there are instances of results being proven on one side and subsequently being transported to the other side. For instance, the classical subject of class field theory has an analog for function fields, called *geometric class field theory*.

Acknowledgements

This paper was supervised by David Roe, who also taught me a lot of number theory in my time at Mathcamp 2016, and encouraged me to work on this project. His guidance has been invaluable, and I have learned a lot from the fruitful conversations we have had.

I am indebted to Clifton Cunningham for introducing me to p-adic fields and adèles in a class on the character group of $\mathbb{Q}$, for referring me to [AW45], the paper which I have treated here, and for convincing me to work towards learning arithmetic geometry.

Thanks to Frank Dai for going through a draft of this paper.

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.

4. We use the computer science-inspired notation

$$A := B$$

to indicate that some piece of notation A is being defined to mean B.

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 Absolute Galois groups

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 (the Galois group is $\mathbb{Z}/2\mathbb{Z}$ in this case).

Definition 2. The *maximal abelian extension* of a field is the largest extension that has an abelian Galois group.

One of the crowning achievements of algebraic number theory is the following result, which shows us that $\mathbb{Q}^{\mathrm{ab}}$ can be understood in terms of "simple" extensions of $\mathbb{Q}$.

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 $\mathbb{Q}$. 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":

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

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, 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 p-adics

We briefly outline the construction of the p-adic fields $\mathbb{Q}_p$.

Consider the rings $\mathbb{Z}/p^n\mathbb{Z}$. In a way similar to what was done above (in fact, this is a special case), we can define projections

$$\pi_s^t \colon \mathbb{Z}/p^s\mathbb{Z} \to \mathbb{Z}/p^t\mathbb{Z} \text{ for all } m|n$$

We can then construct the inverse limit:

$$\mathbb{Z}_p = \varprojlim_r \mathbb{Z}/p^r\mathbb{Z}$$

There is an embedding $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$, by "taking successive remainders": define the sequence

$$t_n = t \pmod{p^n}$$

Then each such sequence $s(t) = (t_1, t_2, \cdots)$ is a p-adic integer.

Example 1. 35 embeds[1] into $\mathbb{Z}_2$ as the sequence

$$(1, 3, 3, 3, 3, 35, 35, 35, \ldots)$$

which, like all p-adics derived from $\mathbb{Z}$, eventually "stabilizes" when the modulus becomes large enough.

[1] **Wikipedia**.

We then define

$$\mathbb{Q}_p = \mathrm{Frac}(\mathbb{Z}_\mathrm{p})$$

which we can do since $\mathbb{Z}_p$ is an integral domain.

Algebraic number theory books treat this construction in more detail. For instance, chapter II of [Neu99] is an excellent reference.

1.2.4 Describing Γ^{ab} with p-adics

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 3. 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

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

1.2.5 Adèles

Define the ring of *integral adèles*

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

and the ring of *adèles* 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 $\mathbb{Q} \hookrightarrow \mathbb{A}_{\mathbb{Q}}$. There is a similar embedding $\mathbb{Q}^\times \hookrightarrow \mathbb{A}_{\mathbb{Q}}^\times$.

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

Adèles are related to *idèles*, which are a multiplicative analogue that we make use of in the next chapter.

Chapter 2

The Artin-Whaples characterization

2.1 Introduction

A striking piece of evidence in favor of the 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 either a number field or a function field.

We will follow the proof of the theorem, setting out the two axioms and showing that number fields and function fields satisfy them.

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 4. 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 5. 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 6. 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] sequence of lemmas (the proofs are somewhat "analytic" in nature and might be skipped on a first reading), culminating in a very useful approximation theorem.

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

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

Proof. Equivalent valuations can each be expressed as a power of the other. For inequivalence, there must be some α and β such that

$$|\alpha|_1 < 1 \leq |\alpha|_2$$
$$|\beta|_1 \geq 1 > |\beta|_2$$

We can then set $\gamma = \alpha/\beta$. □

[3] AW45, p. 471–2.

Lemma 2. If $|\cdot|_1, |\cdot|_2, \ldots, |\cdot|_n$ are nontrivial and inequivalent, there is some α such that

$$|\alpha|_1 > 1$$

and, for all $i > 1$,

$$|\alpha|_i < 1.$$

This means that we can always find some α that distinguishes a particular valuation in a set of mutually inequivalent ones.

Proof. This is just an extension of the previous lemma, which can be considered to be the $n = 2$ case of this. We use induction on n, assuming we have found some γ such that

$$\begin{aligned} |\gamma|_1 &> 1 \\ |\gamma|_i &< 1, 1 < i \leq n-1 \end{aligned}$$

Now we apply the previous lemma to the set of valuations $\{|\cdot|_1, |\cdot|_n\}$ to get a δ such that $|\delta|_1 > 1$ and $|\delta|_n < 1$. There are two possible cases:

1. $|\gamma|_n \leq 1$. In this case, set $\alpha = \gamma^r \delta$. Then

   $$|\alpha|_1 = |\gamma^r|_1 |\delta|_1 > 1$$

   by construction. In addition, for r sufficiently large,

   $$|\alpha|_i < 1$$

   for $2 \leq i \leq n$, since whatever the valuation of δ at the other primes, the factor of $|\gamma|_i^r$ (which is known to be less than 1, by hypothesis) will eventually outweigh the factor of $|\delta|_i$ for r large enough.

2. If $|\gamma|_n > 1$, set

   $$\alpha = \frac{\gamma^r}{\gamma^r + 1}\delta$$

   so that we have

   $$|\alpha|_i = \frac{|\gamma|_i^r |\delta|_i}{|\gamma^r + 1|_i} \leq \frac{|\gamma|_i^r}{1 - |\gamma|_i^r}|\delta|_i$$

   for $2 \leq i \leq n-1$, and

   $$|\alpha|_n \leq \frac{|\gamma|_n^r}{|\gamma|_n^r - 1}|\delta|_n.$$

For r large enough, $|\alpha|_i < 1$ (since the numerator goes to 0 as $r \to \infty$) for $2 \leq i \leq n-1$.

Note that

$$\lim_{r\to\infty} \frac{|\gamma|_n^r}{|\gamma|_n^r - 1} = 1$$

(since $|\gamma|_n > 1$) so $|\alpha|_n < 1$ since $|\delta|_n < 1$ by hypothesis. Hence this satisfies the conditions of the theorem for $2 \leq i \leq n$.

For the case $i = 1$, observe that

$$|\alpha|_1 \geq \frac{|\gamma|_1^r}{1 + |\gamma|_1^r} |\delta|_1$$

so choosing a sufficiently large r gives us $|\alpha|_1 > 1$.

□

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

$$|\alpha - 1|_1 \leq \epsilon$$

and

$$|\alpha|_i \leq \epsilon \text{ for } i > 1.$$

Proof. Choose an appropriate γ according to the previous lemma, so that $|\gamma|_1 > 1$ and $|\gamma|_i < 1$ for $i > 1$. Set

$$\alpha = \frac{\gamma^r}{1 + \gamma^r}$$

Then

$$|\alpha - 1|_1 = \frac{1}{|1 + \gamma^r|_1} \leq \frac{1}{|\gamma|_1^r}^{4} \leq \epsilon$$

for r sufficiently large, while, for $i > 1$, we have

$$|\alpha|_i = \frac{|\gamma|_i^r}{|1 + \gamma^r|_i} \leq \frac{|\gamma|_i^r}{1 - |\gamma|_i^r} \leq \epsilon$$

(again, for r sufficiently large).

□

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

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

[4] The $|\cdot|_1$ in the denominator is just a $|\cdot|$ in the original paper, which I suspect is a typo since $|\cdot|$ hasn't been defined to mean anything at this point.

Proof. Let

$$M = \max\{|\alpha_i|_j : 1 \leq i, j \leq n\}$$

and choose γ_i such that

$$|1 - \gamma_i|_i < \frac{\epsilon}{nM}$$

and

$$|\gamma_i|_j < \frac{\epsilon}{nM} \text{ for } i \neq j.$$

Now set

$$\alpha = \sum_i \alpha_i \gamma_i.$$

Then we have $|\alpha - \alpha_i|_i < \epsilon$ for all i. To see this, assume without loss of generality that $i = 1$. Then

$$\alpha - \alpha_1 = \alpha_1(\gamma_1 - 1) + \sum_{i>1} \alpha_i \gamma_i$$

and, applying $|\cdot|_1$, we get

$$\begin{aligned} |\alpha - \alpha_1|_1 &\leq |\alpha_1|_1 |\gamma_1 - 1|_1 + \left| \sum_{i>1} \alpha_i \gamma_i \right|_1 \\ &\leq |\alpha_1|_1 |\gamma_1 - 1|_1 + \sum_{i>1} |\alpha_i|_i |\gamma_i|_i \\ &\leq \frac{\epsilon}{nM} \sum_i |\alpha_i|_1 \\ &\leq \epsilon. \end{aligned}$$

by the definition of M. □

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

$$P(\alpha) := \prod |\alpha|_i^{\nu_i} = 1$$

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

Proof. The argument follows quite naturally from our lemmas, which tell us that we can find elements of k with precisely determined valuations at a given set of primes.

Let $\nu_i \neq 0$. Choosing an x for which $|x|_i$ is sufficiently large and the other $|x|_j$ for $i \neq j$ are sufficiently close to 1 gives us the necessary contradiction in the form of an α such that $P(\alpha) > 1$. □

Theorem 1 "precludes the possibility that a finite number of valuations can ever be interrelated". Nevertheless, an infinite number of valuations *can* be interrelated in such a way – and this, claims [AW45], characterizes number fields and function fields.

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 Axiom 1: the valuation product formula

Axiom 1. There is a set M of pairs $(\mathfrak{p}, |\cdot|_\mathfrak{p} : k \to \mathbb{R}_{>0})$ 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

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

Notice that, since $|1+1|_{(\mathfrak{p})} > 1$ for archimedean $\mathfrak{p}$, M can only contain finitely many archimedean places.

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

Consider a set M defined as above. We define a vector space 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 7. 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 $k \hookrightarrow V_M$, which may very well be called a "diagonal embedding" (similarly to how $\mathbb{Q}$ has a natural inclusion into $\mathbb{A}_{\mathbb{Q}}$). Writing $i_{\mathfrak{p}}$ for the inclusion $k \to k_{\mathfrak{p}}$, this embedding is given by

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

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, the product of the two (possibly) infinite products being well-defined since an idèle has valuation 1 at almost every place. In this sense, idèles can be considered "measurable" elements of V_M.

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 with the $\mathfrak{p}$-component given by all $\mathfrak{c}$ such that

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

   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 defined by the coordinates of x.

   It is later shown that all valuations are either archimedean or discrete (in the sense defined in 2.2.2). If this is true, then for any collection of elements $x_{\mathfrak{p}} \in \mathbb{R}$, among all the elements of $k_{\mathfrak{p}}$, some $\alpha_{\mathfrak{p}} \in k_{\mathfrak{p}}$ will have the largest valuation not greater than $x_{\mathfrak{p}}$.

   Hence, we can, without loss of generality, replace our map x with an idèle $\mathfrak{a}$ and construct all vectors $\mathfrak{c}$ satisfying

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

   instead.

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[5]

although the definition itself is a a construction I have little motivation for. The purpose of this is mainly to enable the definition of a notion of "size" for the set of elements $\alpha \in k$ that are contained in a given $\mathfrak{a}$-parallelotope (where we are transparently considering elements of k as elements of V_M using the diagonal embedding), which gives us some information about $\mathfrak{a}$.

Definition 8. Given a "field of discourse" k, the order $O(S)$ of a set S 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.

Example 2 (A special case)**.** Consider the situation of a finite field k_0 of constants, and a k_0-vector space S (or, according to the original,

> should [...] our set be closed under addition and under multiplication by elements of k_0[6]

which implies a *finite-dimensional* vector space structure). Then, by the definition of the order for a finite base field, and noting that there exists a finite basis

$$B = \{b_1, \ldots, b_s\}$$

by assumption (where $s = \dim_{k_0} S$), we find that $O(S) = q^s$ is just the number of elements in S.

[5] AW45, p. 474.
[6] 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 $\mathsf{M}(\mathfrak{a})$.

Note that, for nonzero $\theta \in k$, $\mathsf{M}(\theta\mathfrak{a}) = \mathsf{M}(\mathfrak{a})$. This is because multiplying by θ changes the parallelotope of size $\mathfrak{a}$ into the parallelotope of size $\theta\mathfrak{a}$. This does not change the order (this can be seen by looking at the cases in the definition of order, noting that linear (in)dependence is not affected if all elements of a subset of a vector space are multiplied by a field element).

2.5.3 The ring of $\mathfrak{p}$-integers, and the norm

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 *ring of* $\mathfrak{p}$*-integers*).

Example 3. In the case of, say, $k = \mathbb{Q}$, the ring of (2)-integers is, as one might expect, $\mathbb{Z}_2$ (and so on).

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 $\mathfrak{p}$ (or $\mathfrak{p}\mathcal{O}_\mathfrak{p}$). Now we have a quotient field $\mathcal{O}_\mathfrak{p}/\mathfrak{p}$, and so on. The *order* of this field, if finite, is called the norm $\mathrm{Nm}(\mathfrak{p})$ 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

$$\mathrm{Nm}(\mathfrak{p}) = O(k^\mathfrak{p}) = q^f$$

where we put $f = [k^\mathfrak{p} : k_0]$ and q is the order of k_0, as before.

2.6 Axiom 2

Axiom 2. The set M of 1 contains at least one prime $\mathfrak{q}$, which is of one of the following types:

- discrete, with a quotient field of finite order $\mathrm{Nm}(\mathfrak{q})$
- 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
$$\|\alpha\|_\mathfrak{p} = \mathrm{Nm}(\mathfrak{p})^{-\nu}$$
where $\nu = |\alpha|_\mathfrak{p}$. This covers the case of function fields, since all valuations are nonarchimedean in that case.
- 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 square of the usual absolute value on $\mathbb{C}$. (This is not a valuation in the usual sense!)

This is called the *normed valuation at* $\mathfrak{p}$.

Note that in the case of $p \in \mathbb{Z}$ prime, the normed valuation corresponding to $(p) \in \operatorname{Spec} \mathbb{Z}$ is the usual p-adic valuation

$$|x|_p = p^{-\nu_p(x)}.$$

2.7 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 1 and 2 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 over 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 (1 transfers to subfields)**.** Let k be a field for which 1 holds, and F a subfield that does not exclusively comprise constants of k. Let N be the set of nontrivial divisors p of F that are divisible by some $\mathfrak{p}$ of M. Then 1 holds in F for N.

Proof. Let $p \in \mathsf{N}$, and $a \in F$ with $|a|_p > 1$. Then $|a|_{\mathfrak{p}} > 1$ for all $\mathfrak{p}|p$ (as can be seen by writing $p = \mathfrak{p}p'$).

Because of 1, there can only be a finite number of such $\mathfrak{p}|p$. We now define valuations

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

for $\alpha \in F$, noting that the products are finite and hence well-defined. The set of all such $|\cdot|_p$ satisfies 1. □

Lemma 5 (1 transfers to finite algebraic extensions)**.** Let k be a field for which 1 holds and K/k a finite algebraic extension. Let N be the set of all divisors $\mathfrak{n}$ of K that divide some $\mathfrak{m}$ of M. Then 1 holds in K for some subset $\mathsf{N}' \subset \mathsf{N}$.

Proof. Omitted. □

In fact, $\mathsf{N}' = \mathsf{N}$, but we do not demonstrate this here since it is not required for the proof (the existence of any set of places satisfying our criteria is sufficient).

2.7.1 The product formula exists for $\mathbb{Q}$ and $k(z)$

We now look at the special case of $K = k_1(z)$. The proof involves some interesting interaction between ring-theoretic ideals and valuation theory.

Theorem 8. A product formula of the type referred to in 1 exists for $K = k_1(z)$.

Proof. Consider a nontrivial valuation p of K that is trivial on k_1. p is nonarchimedean, and there are two possible cases (by Ostrowski's theorem[7]):

1. $|z|_p \leq 1$. This implies that $|f(z)|_p \leq 1$ for all polynomials in z, as can be seen by writing (omitting the p subscript to simplify the notation):

$$\begin{aligned} |f(z)| &= |a_n z^n + a_{n-1} z^{n-1} \cdots + a_0| \\ &\leq \max\left(|a_n||z|^n, |a_{n-1}||z|^{n-1}, \ldots, |a_0|\right) \\ &\leq \max\left(|z|^n, |z|^{n-1}, \ldots, 1\right) \\ &\leq 1. \end{aligned}$$

   Here we use the triviality of $|\cdot|_p$ when restricted to k_1, and the nonarchimedeanness of the valuation, to bound the valuation above.

   Now let $p(z)$ be a polynomial of the minimal possible degree such that $|p(z)|_p < 1$ holds. If $g(z)$ is another such polynomial, we use the division algorithm in $k_1(z)$ to get

$$g(z) = p(z)h(z) + r(z)$$

   where $\deg r(z) < \deg p(z)$. Rewriting the above relation as

$$r(z) = g(z) - p(z)h(z)$$

   gives us $|r(z)|_p < 1$, which implies $r(z) = 0$.

   Now let $\phi \in K$ be some polynomial in z and write

$$\phi(z) = \varphi(z) \cdot p(z)^\nu$$

   where φ contains no factors of $p(z)$ in the numerator or denominator (which means that $\nu = |\phi|_p$, so the $p(z)^\nu$ factor "captures" the $p(z)$-term).

   To find the normed valuation $\|\cdot\|_p$ in this case, we have to determine the degree of the quotient field $L := k_1(z)/p(z)$ over the base field K. We know that

$$[L : K] = f := \deg p(z)$$

[7] Con.

so that we have $\mathrm{Nm}(p) = q^f$ and

$$\|\phi(z)\|_p = q^{-\nu f}.$$

2. If $|z|_p > 1$ then we replace z by $y := 1/z$.

   Then $|y|_p < 1$ and this reduces to our previous case. Now, the lowest-degree polynomial in y is just y, so there is only one such prime divisor p of this kind. We will denote it p_∞.

   Let $\phi(z) = g(z)/h(z)$, and set $m := \deg g(z), n := \deg h(z)$. We then have

$$\phi(z) = y^{n-m}\frac{g_1(y)}{h_1(y)}$$

   where neither g_1 nor h_1 are divisible by y. Then

$$\|\phi(z)\|_{p_\infty} = q^{m-n}.$$

We can construct a product formula connecting this set of valuations, or a subset, in the form

$$\prod_p \|\phi(z)\|_p^{\lambda(p)} = 1$$

where the $\lambda(p)$ are nonnegative constants.

Now we substitute $\phi(z) = p(z)$ with $p(z)$ irreducible. There can only be two possible factors in the product formula that are not equal to 1: the one corresponding to p itself, and the p_∞ factor at infinity. Writing out the expression (omitting the factors of 1 corresponding to all the other primes), we have

$$q^{f\lambda(p)}q^{-f\lambda(p_\infty)} = 1$$

so $\lambda(p) = \lambda(p_\infty)$. Since the choice of p was arbitrary, we conclude that

$$\lambda(p_1) = \lambda(p_2) = \cdots = \lambda(p_\infty)$$

and we may as well set them all equal to 1. Now we define a volume function V as before on the idèles of $k_1(z)$:

$$V(\phi(z)) = \prod_p \|\phi(z)\|_p$$

This is obviously multiplicative and satisfies $V(1/f) = 1/V(f)$.

The multiplicativity of the V-function, together with the observation that $V(p(z)) = 1$ for all irreducible $p(z)$, allows us to conclude the result

$$V(\phi(z)) = 1$$

for all nonzero $\phi(z) \in k_1(z)$.

□

We now treat the case of $\mathbb{Q}$, which is analogous.

Theorem 9. A product formula of the type referred to in 1 exists for $\mathbb{Q}$.

Proof. From Ostrowski's theorem, any valuation on $\mathbb{Q}$ is either

1. the standard absolute value $|\cdot| = \|\cdot\|_{p_\infty}$, corresponding to the "prime at infinity" p_∞, or

2. one of the ordinary p-adic valuations $|\cdot|_p$ on $\mathbb{Q}$, given by

$$|a|_p = p^{-\nu}$$

where $\nu := \nu_p(a)$ is the p-valuation of a, i.e. the exponent of p in the expression

$$a = p^\nu \cdot \frac{s}{t} \text{ where } p \nmid s, t.$$

We again consider a hypothetical product formula

$$\prod_p \|a\|_p^{\lambda(p)} = 1$$

as before, and substitute an irreducible $p \in \mathbb{Z}$ (which is just a prime). This gives us

$$p^{-\lambda(p)} \cdot p^{\lambda(p_\infty)} = 1$$

and we again have $\lambda(p) = \lambda(p_\infty)$. Again, since we chose p arbitrarily, this holds for all primes p and we get

$$\lambda(p_1) = \lambda(p_2) = \cdots = \lambda(p_\infty)$$

where we can again assume $\lambda(p_i) = 1$ for all i. We construct a volume function in exactly the same way as before to complete the proof of the product formula for $\mathbb{Q}$.

□

Having proven the theorem for the cases $K = \mathbb{Q}$ and $K = k_1(z)$ is sufficient for us to conclude the main result, since we can transport our proofs to arbitrary finite algebraic extensions of these base fields using the lemmas demonstrated previously.

2.7.2 Putting it all together

Theorem 10. 1 holds in the case of $\mathbb{Q}$ and that of $K = k_1(z)$ for k_1 an arbitrary field.

The set 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 theorem 4. The fact that all valuations of M satisfy 2 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 k_0 of constants in case 2 of 7.

Proof. Assume that p is trivial on k_1. Then it will also be trivial on any algebraic extension of k_1.

Hence we need only show that any element $a \in k_0$ is algebraic with respect to k_1. If a were transcendental with respect to k_1, then from the minimal polynomial of a over $k_1(z)$, we find that z would have to be algebraic with respect to $k_1(a)$.

Since $k_1(c)$ is in k_0, this would mean that z is in k_0. This would imply that $k \subseteq k_0$, and p would be trivial on all of k – which is a contradiction. □

2.8 Characterizing fields by the product formula

In this section, k is an arbitrary field with a set of valuations M satisfying axioms 1 and 2. We will prove that it is of one of the two types mentioned before.

2.8.1 Definitions

Consider a prime $\mathfrak{p}$ satisfying Axiom 2. We will need to distinguish $|\alpha|_\mathfrak{p}$ and $\|\alpha\|_\mathfrak{p}$ (the normed valuation corresponding to $\mathfrak{p}$).

We define $\rho(\mathfrak{p}) > 0$, $\rho(\mathfrak{p}) \in \mathbb{R}$ by writing

$$|\alpha|_\mathfrak{p} = \|\alpha\|_\mathfrak{p}^{\rho(\mathfrak{p})}$$

Let K[8] refer to the following subfield of k:

1. If M has archimedean valuations, then $K := \mathbb{Q}$. In this case we set

$$\|a\|_{p_\infty} = |a|,$$

the ordinary absolute value on $\mathbb{R}$.

[8]The R that the original uses is slightly confusing.

2. In the other case, as we have seen before, k has a field of constants k_0. It cannot contain any algebraic extension of k_0 since any valuation trivial on k_0 would also be trivial on that extension.

   Let z be any element of k not in k_0. Then $K = k_0(z)$ is a transcendental extension of k_0. We will refer to elements of $k_0[z]$ as the "integers" of $k_0(z)$.

   $\|a\|_{p_\infty}$, in this case, will refer to the particular valuation found during the proof of 8 which has $\|z\|_{p_\infty} > 1$.

In both cases, $\mathfrak{p}_\infty$ is some divisor in M that divides p_∞. Since the product formula, when applied to elements of K, reduces to the formula of the main theorem (TODO LINK), there must be at least one such $\mathfrak{p}_\infty$ (since all other valuations are less than 1 for $\alpha \in K$, but the product must be equal to 1). The other primes are called *finite*.

For elements $a \in K$, the valuations $|\cdot|_{p_\infty}$ and $\|\cdot\|_{p_\infty}$ are equivalent. We define $\lambda(\mathfrak{p}_\infty) > 0$ by

$$|a|_{\mathfrak{p}_\infty} = \|a\|_p^{\lambda(\mathfrak{p}_\infty)}$$

The idea behind the proof is to show that k is a finite extension of K.

2.8.2 The proof

Lemma 6. Let

- $\mathfrak{q}$ be a prime satisfying 2
- S be a set of elements of k, with order $M > 1$
- x be an upper bound on $\mathfrak{q}$-valuations for elements of S, that is,

$$|\alpha|_{\mathfrak{q}} \leq x \text{ for all } \alpha \in \mathsf{S}$$

Then there exists an element $\theta \in k$ with the following properties:

- $\theta \neq 0$
- θ is either a difference of two elements of S, or, if there is a field of constants k_0, a k_0-linear combination of elements of S
- For some constant $A_{\mathfrak{q}}$ (depending only on $\mathfrak{q}$),

$$|\theta|_{\mathfrak{q}} \leq A_{\mathfrak{q}} \cdot \frac{x}{M^{\rho(\mathfrak{q})}}$$

Proof. Omitted. □

Lemma 7. Let M be the order of the set of elements $\alpha \in k$ contained in a parallelotope of dimensions $x_{\mathfrak{p}}$. If $\mathfrak{q}$ is a prime satisfying 2, we can find some $B_{\mathfrak{q}}$ depending on $\mathfrak{q}$ such that either $M = 1$ (which happens if the set only contains $\alpha = 0$), or

$$M \leq B_{\mathfrak{q}} \left(\prod_{\mathfrak{p}} x_{\mathfrak{p}} \right)^{1/\rho(\mathfrak{q})}$$

Proof. Assume $M > 1$. Note that the $\mathfrak{q}$-component of the idèle x is an upper bound on $\mathfrak{q}$-valuations, so by 6, there is a $\theta \neq 0$ satisfying

$$|\theta|_{\mathfrak{q}} \leq A_{\mathfrak{q}} \cdot \frac{x_{\mathfrak{p}}}{M^{\rho(\mathfrak{q})}}$$

For the other $\mathfrak{p} \in \mathsf{M}$ we estimate θ to get

$$|\theta|_{\mathfrak{p}} \leq \begin{cases} x_{\mathfrak{p}}, & \mathfrak{p} \text{ nonarchimedean} \\ 4^{\rho(\mathfrak{p})} \cdot x_{\mathfrak{p}}, & \mathfrak{p} \text{ archimedean} \end{cases}$$

Substituting into the product formula, we get

$$1 \leq \frac{D_{\mathfrak{q}} \prod_{\mathfrak{p}} x_{\mathfrak{p}}}{M^{\rho(\mathfrak{q})}}$$

and rearranging gives

$$M \leq D_{\mathfrak{q}}^{1/\rho(\mathfrak{q})} \cdot \left(\prod_{\mathfrak{p}} x_{\mathfrak{p}} \right)^{1/\rho(\mathfrak{q})}$$

and we are done.

□

Lemma 8. If $\alpha_1, \alpha_2, \ldots, \alpha_l \in k$ are linearly independent over K, and if y is some nonzero integer of K, we can construct a certain set S of elements α such that

- $|\alpha|_{\mathfrak{p}} \leq a_{\mathfrak{p}} = \max\left(|\alpha_1|_{\mathfrak{p}}, |\alpha_2|_{\mathfrak{p}}, \ldots, |\alpha_l|_{\mathfrak{p}}\right)$
- $|\alpha|_{\mathfrak{p}_\infty} \leq B \cdot |y|_{\mathfrak{p}_\infty}$ for a certain constant B.
- If there is a field of constants k_0, then S is a k_0-vector space.
- The order of S satisfies
$$O(\mathsf{S}) > \|y\|_{p_\infty}^{l}$$

Proof. Omitted. □

Lemma 9. The degree $n := [k : K]$ is finite; every $\mathfrak{p}$ of M satisfies 2, and we have

$$n \leq \frac{1}{\rho(\mathfrak{p})} \cdot \sum_{\mathfrak{p}_\infty} \lambda(\mathfrak{p}_\infty)$$

for all $\mathfrak{p}$[9].

Proof. Omitted. □

With this, we have completed the proof of the following result:

Theorem 11. If k is a field that satisfies 1 and 2, it is an extension of either

- $K = \mathbb{Q}$, the field of rational numbers, or
- $K = k_0(z)$, the field of rational functions in one variable z over the field of constants k_0 of k

of finite degree n.

M consists of all extensions of the standard valuations on K (which we know from Ostrowski's theorem). We can, after raising all the valuations in the product formula to some fixed power, assume they are normed. We have

$$\sum_{\mathfrak{p}|p} n(\mathfrak{p}) = n$$

for all $p \in K$.

[9]The original writes p here.

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.

[Neu99] Jürgen Neukirch. *Algebraic Number Theory*. Springer Berlin Heidelberg, 1999. DOI: 10.1007/978-3-662-03983-0. URL: http://dx.doi.org/10.1007/978-3-662-03983-0.

[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.

[Con] Keith Conrad. "Ostrowski's theorem for $F(T)$". In: (). URL: http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/ostrowskiF(T).pdf.

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