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

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

2. 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.

[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

Adeles

1.1 Preliminaries from Galois theory

We will let K be a number field. 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.*

In particular, this means that given a k-automorphism $K \to L$, we get a morphism of Galois groups

$$\mathrm{Gal}(L/k) \to \mathrm{Gal}(K/k)$$

since any automorphism of L fixes K.

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.

1.2 Class field theory

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 $\mathbb{Q}(\zeta_n)$.

In particular, we may now apply $\mathrm{Gal}(-/\mathbb{Q})$ to get the following:

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

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

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

that sends, for instance, $[5] \in \mathbb{Z}/6\mathbb{Z}$ to $[1] \in \mathbb{Z}/3\mathbb{Z}$.

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

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

1.2.1 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 1. 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 $\mathbb{Q}^imes \to \mathbb{A}_{\mathbb{Q}}^imes$.

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 $\mathbb{A}_{\mathbb{Q}}^imes/\mathbb{Q}^imes$. With the previous statement, we see that

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

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 2. 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. $\operatorname{Im} |\cdot| \subset \mathbb{R}^{>0}$
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: the finite places of a field are in one-to-one correspondence with the prime ideals of its ring of integers. [htt]

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

2.2.3 The equivalence relation on places

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 3. Two valuations $|\cdot|_\mathfrak{p}$ and $|\cdot|_\mathfrak{q}$ are *equivalent* if they determine identical topological space structures on the field.

[1] AW45, section 1.

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!

2.3 The proof

2.3.1 Lemmas

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

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

- If $| \cdot |_i$ are inequivalent, there is some α such that

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

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

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

2.3.2 Approximation theorem

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

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

2.3.3 Corollary

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. This "precludes the possibility that a finite number of valuations can ever be interrelated", to paraphrase the original, but maybe an infinite number of valuations is okay?

2.4 The product formula

2.4.1 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

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

2.4.2 Idles

We associate to M a space of vectors $v = (v_{\mathfrak{p}})_{\mathfrak{p}}$, where $v_{\mathfrak{p}} \in k_{\mathfrak{p}}$. We will write $|v|_{\mathfrak{p}}$ for $|v_{\mathfrak{p}}|_{\mathfrak{p}}$.

Definition

A vector of this form is an idele if

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

Embedding

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

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

"Volume"

For each idele $\mathfrak{a}$, define

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

1. For elements coming from k via the embedding, notice that we have $V(\alpha) = 1$. This gives
$$V(\alpha\mathfrak{a}) = V(\mathfrak{a})$$
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 $|c|_{\mathfrak{p}} \leq |\mathfrak{a}|_{\mathfrak{p}}$ which we call the parallelotope with dimensions x.

Order

The order of a set of elements is defined as follows:

1. If k has an archimedean valuation, then order is the number of elements.
2. If not, there is some field of constants $k_0 \subset k$. 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. s is the number of elements in the set that are linearly independent over k_0.

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.

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

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

2.4.3 Axiom 2

The set M of 2.4.1 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 $\mathbb{C}$

2.4.4 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.

2.4.5 Theorem 2

We can construct M such that both 2.4.1 and 2.4.3 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 $/k_1$)

Lemma 4

Lemma 5

Lemma 6

2.5 Characterizing fields by the valuation product formula

2.5.1 (Main) theorem 3

If a field satisfies 2.4.1 and 2.4.3, it is of one of the two types in 2.4.5. Furthermore, 2.4.3 is satisfied for every place $\mathfrak{p}$.

2.6 Parallelotopes

2.6.1 Theorem 4

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

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

2.6.2 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 ideles $\mathfrak{a}$ 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.