GRENOBLE 1

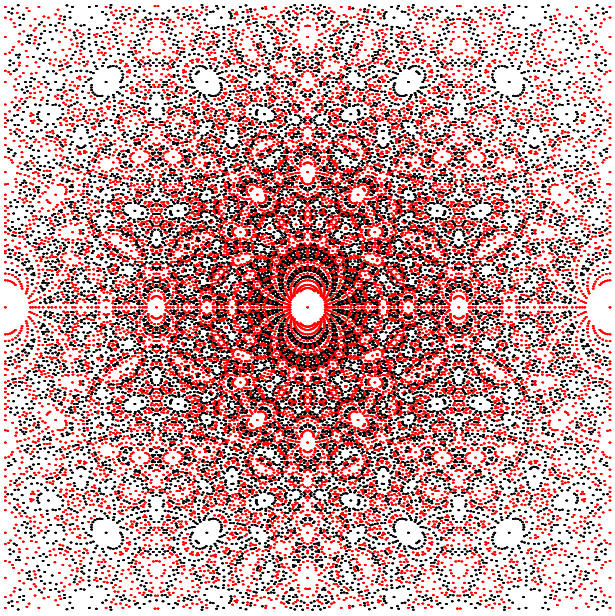
Master 2R Mathématiques

THÉORIE DES NOMBRES

Un recueil de brouillons

(12 Janvier 2014)

Emmanuel Peyre



Emmanuel Peyre
Institut Fourier, UFR de Mathématiques, UMR 5582, Université de Grenoble I et CNRS, BP 74, 38402 Saint-Martin d'Hères CEDEX, France.
E-mail : Emmanuel.Peyre@ujf-grenoble.fr
Url : http://www-fourier.ujf-grenoble.fr/~peyre/

Plan du cours

0) Introduction
- ½ Théorème de Fermat et structure d'anneaux d'entiers
- ✓ Principe de Hasse, les complétés, places
- ✓ analogue géométrique $\mathbb{P}^1_k \leftrightarrow \mathrm{Val}(\mathbb{Q})$.

1) Anneaux d'entiers (Réf. : SAMUEL, chapitre II)
- ✓ Intégralité
- ✓ clôture intégrale
- ✓ factoriel ⇒ intégralement clos
- ✓ Exemples : cas quadratique (TD)
- ✓ Norme, trace, discriminant.

2) Théorie de Galois (finie, Réf mon cours à l'ENS)

a) Analogue géométrique (Réf, SZAMUELY, chap. 3)
- ✓ Atlas complexe
- ✓ Surfaces de Riemann, morphismes,
- ✓ Structure locale, ramification, exemple
- ✓ Corps de fonctions d'une surface de Riemann.

b) Cadre algébrique
- ½ PU de la clôture algébrique
- ✓ degré de séparabilité
- ✓ Groupe de Galois,
- ✓ Théorème fondamental
- ✓ Exemples, cas cyclotomique (TD)
- – Application à Fermat. (Réf : HELLEGOUARC'H revu)

3) Anneaux de Dedekind (Ref : SAMUEL, chapitre III)

- ✓ Localisation d'un anneau (e.g. $\mathbb{Z}_{(p)}$; $A_{(\mathfrak{p})}$; $\mathbb{F}_q[G_p]$)
- ✓ Rappels sur les modules et les anneaux noethériens
- ✓ Compléments sur la trace et les extensions séparables.
- ✓ Définition
- ✓ Factorisation
- ✓ Stabilité par localisation et extension
- ✓ Image directe dans une extension, degré résiduel, ramification
- ✓ Lien avec le discriminant
- ✓ Le cas des extensions galoisiennes

4) Places d'un corps global (Réf : HASSE, Part II LANG, Algebra)

- ✓ Définition
- ✓ Exemples
- ✓ équivalence
- ✓ places d'un corps de nombres, d'un corps global
- ✓ Complété
- ✓ Exemples
- ✓ Théorème d'Ostrowski (sur $\mathbb{Q}$)
- ✓ Extension de corps
- ✓ Restriction
- ✓ formule du produit (zéros et pôles)

5) Classes d'idéaux (Ref : SAMUEL, ch. V)

- ✓ Plongement
- ✓ Finitude
- ✓ Hermite
- ✓ Dirichlet

6] Théorème des unités (Ref : Samuel, ch. IV)
✓ Le théorème
✓ Le cas des extensions quadratiques (TD + CC)
✓ Equation de Pell (TD + CC).

7] Local / Global
✓ Théorème des fonctions implicite } TD
✓ Lemme de Hensel
✓ Adèles, Idèles
✓ $\mathbb{A}_K / K$, $\mathbb{G}_m(\mathbb{A}_K)^1 / K^*$
✓ Principe de Hasse, approximation faible

8] Un peu de hauteur
✓ Hauteur normalisée
✓ Théorème de Northcott
[— Lemme de Siegel : non fait]

M2R
2013-2014
Semestre 1

Algebraic number theory

References

The first book on the list is a «must». Many of the proofs, I shall explain in this lecture will be taken from there. Easy to read, it is the best reference for Dedekind rings.

P. SAMUEL, Théorie algébrique des nombres, Hermann

The second reference contains more material, in particular about absolute values

S. LANG, Algebraic number theory, Graduate Texts in Mathematics 110, Springer-Verlag.

The third contains more advanced stuff, but its 1st chapters is extremly well written and give interesting results about completions of global fields

J.P. SERRE, Corps locaux, Hermann.

Outline of the lectures

1] Ring of integers, examples
2] Galois theory
3] Dedekind rings
4] Absolute values, places
5] Ideal classes
6] Units
7] Decomposition of prime ideals in an extension.
8] Local vs Global.
9] Heights

The problem is that some of you may have already taken lectures about some of this stuff,

like Galois theory, but not all of you. I hope you will not mind me going over this material again.

A Leitmotiv of this lecture is the analogy and the connections between

Arithmetics	Geometry
and more precisely	
$\mathbb{Z}$	$\mathbb{F}_p[T]$ ($\mathbb{C}[T]$) — $\mathbb{Z}/p\mathbb{Z}$, p prime
$\mathbb{Q}$	$\mathbb{F}_p(T)$ ($\mathbb{C}(T)$)
Field of "functions" over ???	Field of rational functions over $\mathbb{P}^1_{\mathbb{F}_p}$ $\mathbb{P}^1_{\mathbb{C}}$
???	Point on the projective line
Locally means ??	Locally means "in a small neighbourhood of point"
$K/\mathbb{Q}$ finite field extension	Covering $C \xrightarrow{\pi} \mathbb{P}^1$ curve surjective, with finite fibers, ...
??	ramification: $\mathbb{P}^1_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$, $(u:v) \mapsto (u^2:v^2)$, ramified at 0 and ∞

and so on... Most of the terminology comes from geometry and I shall try to explain why. The geometry was there before and was used as a source of inspiration. The aim of the "geometry of numbers" is to look at $\mathbb{Z}$ or $\mathbb{Q}$ has a geometric object.

Without more ado, let me start at the starting point:

I] Ring of integers

Prerequisite:
- Modules over a commutative ring
- Various tools of linear algebra:
- Fields extensions

If you need to refresh your memory about these topics, there is a book which starts at the very beginning and goes much further the material I shall need:

Reference
S. LANG, Algebra, Addison-Wesley.

1] Algebra over a commutative ring (Reminder)

Definition
Let A be a commutative ring. A unitary associative algebra over A (or simply A-algebra) is a ring B equipped with a ring homomorphism $\varphi_B : A \to B$ such that

$\zeta_B(A) \subset Z(B) = \{b \in B \mid \forall c \in B,\ bc = cb\}$ ← center of B

Remark

(i) This is a particular case of a more general notion:
An **algebra over A** is an A-module B equipped with a bilinear form (multiplication)

$$B \times B \longrightarrow B$$
$$(b_1, b_2) \mapsto b_1 b_2$$

In our case the A-module structure is given by

$$A \times B \longrightarrow B$$
$$(a, b) \mapsto ab = \zeta(a) b$$

(ii) Note that $\zeta_B(1_A) = 1_B$ by definition of a ring homomorphism.

Examples

- For $n \in \mathbb{N}$, $\mathcal{M}_n(A)$ algebra of square $n \times n$ matrices / A
- ζ if B is a commutative A-algebra which means that B is commutative as a ring corresponding to $\zeta_B : A \to B$ and C is a B algebra for $\zeta_C : B \to C$ then C equipped with $\zeta_C \circ \zeta_B$ is an A-algebra
- $A[X_1, \dots, X_n]$ algebra in n variables with coefficients in A

Definition

Let B and C be A-algebras; a morphism of A-algebras from B to C is

a ring homomorphism $\varphi : B \to C$ such that $\varphi \circ \varsigma_B = \varsigma_C$.

$$\begin{array}{ccc} & & C \\ & \nearrow^{\varsigma_B} & \uparrow \varsigma_C \\ A & & \end{array}$$

Example

Let $n \in \mathbb{N}$, $f_1, \dots, f_m \in A[X_1, \dots, X_n]$ and let B be a commutative A-algebra. There is a bijection

$$\mathrm{Mor}_{A\text{-alg}}\left(A[X_1, \dots, X_n]/(f_1, \dots, f_m), B\right) \to \{(x_1, \dots, x_n) \in B^n \mid \forall i, f_i(x_1, \dots, x_n) = 0\}$$

(the set on the right: geometric object)

↑ set of homomorphisms of A-algebras

$$\varphi \longmapsto (\varphi(X_1), \dots, \varphi(X_n))$$

Definition

A sub-algebra of an A-algebra B is a subring C of B such that $\varsigma_B(A) \subset C$. Then C equipped with $\varsigma_C : A \to C$, $a \mapsto \varsigma_B(a)$ is an A-algebra.

Example

- The intersection of a family of sub-algebras is a subalgebra.
- Let B be an A-algebra and $X \subset B$. The intersection of the subalgebras of B containing X is a sub-algebra of B; it is the smallest sub-algebra of B containing X and is called the sub-algebra of B generated by X. We denote by $A[a_1, \dots, a_n]$ the subalgebra generated by $\{a_1, \dots, a_n\} \subset B$

2) Polynomial division, roots (Reminder)

Proposition

Let A be a commutative ring

Let $F, G \in A[X]$ and assume the leading coefficient of G is invertible (in A)

$$G = \sum_{i=0}^{d} b_i X^i \text{ with } b_d \in A^*$$

Then

$\exists!\ (Q,R) \in A[X]^2$, $F = GQ + R$ with $\deg(R) < \deg(G)$ (*)

R: remainder of the division of F by G

Example

For any $F \in A[X]$, $F(a)$ is the remainder of the division of F by $(X-a)$.

Definition

Let $P \in A[X]$, $\alpha \in A$, $k \geq 1$, one says that

(i) α is root of order $\geq k$ of P iff $(X-\alpha)^k \mid P$

(ii) α ——— k of iff $(X-\alpha)^k \mid P$ and $(X-\alpha)^{k+1} \nmid P$.

Proposition

Let A be an integral domain (ie a commutative ring such that $\forall a,b \in A$, $ab = 0 \Rightarrow a = 0$ or $b = 0$.)

Let $P \in A[X] - \{0\}$, $a_1, \dots, a_r$ distinct elements of A, $k_1, \dots, k_r \in \mathbb{N} - \{0\}$

Then the following statements are equivalent:

(i) $\forall i \in \{1, \dots, r\}$, a_i is a root of order $\geq k_i$ of P

(ii) $\prod_{i=1}^{r} (X-a_i)^{k_i} \mid P$.

In that case $\sum_{i=1}^{r} k_i \leq \deg(P)$.

Definition

Let A be an integral domain

$P \in A[X]$ is said to be split if

$P = 0$ or $P = a \prod_{i=1}^{d} (X - a_i)$ with $a \in A - \{0\}$, $a_1, \dots, a_d \in A$.

Prop

Let $\sigma_i(X_1, \dots, X_d) = \sum_{1 \le j_1 < \dots < j_i \le d} \prod_{k=1}^{i} X_{j_k}$

i-th elementary symmetric polynomial in $X_1, \dots, X_d$, then

$$\prod_{i=1}^{d} (X - a_i) = \sum_{i=0}^{d} (-1)^i \sigma_i(a_1, \dots, a_d) X^{d-i}$$

(with $\sigma_0(a_1, \dots, a_d) = 1$)

Definition

A field $\mathbb{K}$ is said to be algebraically closed iff it satisfies the following equivalent statements

(i) Any $P \in \mathbb{K}[X]$ with $\deg(P) \geq 1$ has a root in $\mathbb{K}$

(ii) Any $P \in \mathbb{K}[X]$ is split

(iii) The irreductible polynomials in P are the polynomials of degree 1.

Example

$\mathbb{C}$ is algebraically closed

That's enough remainders for now, let us now turn to the main topic: ring of integers in a number field.

3) Integral elements

In this section A denotes a commutative ring

Definition

Let M be an A-module

(a) M is said to be *faithful* iff $\{a \in A \mid \forall m \in M,\ am = 0\} = \{0\}$

(b) M is said to be of finite type iff it satisfies the following equivalent statements:

(i) M is generated by a finite set of elements as an A-module

(ii) There exists an integer n and a surjective A-linear map $A^n \to M$.

Example

An A-algebra B is a faithful A-module iff the corresponding morphism $f : A \to B$ is injective.

We say that the A-algebra B is *faithful* if it is a faithful A-module

Theorem

Let B be an A-algebra, and let $b \in B$

The following statements are equivalent

(i) There exists $P \in A[X]$, $P = X^n + \sum_{i=0}^{n-1} a_i X^i$ such that $P(b) = 0$ Note that the leading coefficient has to be 1.

(ii) $A[b]$ is a A-module of finite type

(iii) There exists a subalgebra of B which contains b and which is an A-module of finite type

(iv) There exists a $A[b]$-faithful module M which is a A-module of finite type

Remark

Let B be an A-algebra and M be a B-module. M equipped with $A \times M \longrightarrow M$, $(a, m) \mapsto am = \rho(a)M$ is a A-module called the **A-module induced from M by restriction of scalars**. This let us see the $A[b]$ module M as an A-module.

Proof of the theorem

(i) $\Rightarrow$ (ii)

By the division of polynomials, the A-module $A[X]/(P)$ is a free A-module a basis of which is given by $(1, \overline{X}, \dots, \overline{X}^{n-1})$

Consider the morphism of algebras

$$ev_b : A[X] \longrightarrow B, \quad P \longmapsto P(b)$$

Since $(P) \subset \ker(ev_b)$ it induces a surjective morphism of A-modules

$$A^n \simeq A[X]/(P) \longrightarrow A[b]$$

$$(a_0, \dots, a_{n-1}) \longmapsto \sum_{i=0}^{n-1} a_i b^i$$

Thus $A[b]$ is an A-module of finite type.

(ii) $\Rightarrow$ (iii) take $C = A[b]$

(iii) $\Rightarrow$ (iv) take $M = C$ it is a $A[b]$ faithful module (since $A[b] \to C$ is injective) and is an A-module of finite type

It remains to prove that

(iv) $\Rightarrow$ (i)

Let M be an $A[b]$ faithful module and an A-module of finite type

Let $\{e_1, \dots, e_n\}$ a subset of M generating M as an A-module.

We may write

$$\begin{cases} be_1 = a_{1,1} e_1 + \dots + a_{1,n} e_n \\ \vdots \\ be_n = a_{n,1} e_1 + \dots + a_{n,n} e_n \end{cases}$$

Let $M = (a_{i,j})_{\substack{1 \le i \le n \\ 1 \le j \le n}} \in \mathcal{M}_n(A)$

Let $\varphi_B : A \to B$ be the natural morphism.

We get that

$$\begin{cases} b - \varphi_B(a_{1,1}) e_1 - \dots - \varphi_B(a_{1,n}) e_n = 0 \\ \vdots \\ -\varphi_B(a_{n,1}) e_1 - \dots + (b - \varphi_B(a_{n,n})) e_n = 0 \end{cases}$$

Let $N = bI_n - \varphi(M) \in \mathcal{M}_n(A[b]) \subset \mathcal{M}_n(B)$

Let $\tilde{N}$ = transpose of the comatrix of N $\left((-1)^{i+j} \det (n_{k,\ell})_{\substack{k \neq i \\ \ell \neq j}}\right)$

By a well-known formula in linear algebra

$$\tilde{N} N = N \tilde{N} = \det(N) I_n,$$

we put $d = \det(N) \in A[b]$.
For any $U = (u_{ij}) \in \mathcal{M}_n(A[b])$ we may define $\psi(U) : M^n \longrightarrow M^n$ $A[b]$-linear

$$(m_i)_{1\le i\le n} \longmapsto \left(\sum_{j=1}^{n} u_{ij} m_j\right)$$

It satisfies

$$\psi(UV) = \psi(U)\psi(V) \quad \text{for } U, V \in \mathcal{M}_n(A[b])$$

and

$$\psi(a I_n) = a\, Id_{M^n} \quad \text{for } a \in A[b]$$

Thus

$$d(e_1, \dots, e_n) = \psi(d I_n)(e_1, \dots, e_n)$$
$$= \psi(\tilde{N})\big(\underbrace{\psi(N)(e_1, \dots, e_n)}_{0}\big) = 0$$

Thus

$$d e_i = 0 \quad \text{for} \quad 1 \le i \le n$$

But then $\forall m \in M$, $dm = 0$
and since M is a faithful $A[b]$-module,

$$d = 0$$

Let $P = \det \begin{pmatrix} X - a_{1,1} & \cdots & -a_{1,n} \\ \vdots & \ddots & \vdots \\ -a_{n,1} & \cdots & X - a_{n,n} \end{pmatrix} \in A[X]$

satisfies
→ the leading coefficient of P is 1
→ $\Phi = P(b) = 0$ □

Definition
With notations as above, $b \in B$ is said to be integral over A iff it satisfies the conditions (i) to (iv) of the theorem.

Example
Let B be an A-algebra which is a A-module

an A-module of finite type (eg $\mathcal{H}_n(A)$) then any element of B is integral over A.

4) Integral closure

Proposition / Definition

Let A be a commutative ring and B be a commutative A-algebra. Then

$$\overline{A} = \{ b \in B \mid b \text{ is integral over } A \}$$

is a subalgebra of B called the integral closure of A in B.

Let me start with a remark:

Remark

Let B be a commutative A-algebra and C be a B-algebra, $\alpha \in C$. If α is integral over A it is integral over B.

Indeed, let $P = X^n + \sum_{i=0}^{n-1} a_i X^i \in A[X]$ such that $P(\alpha) = 0$, $\varphi_B(P) = X^n + \sum_{i=0}^{n-1} \varphi_B(a_i) X^i$ satisfies

$$\varphi_B(P)(\alpha) = b^n + \sum_{i=0}^{n-1} \varphi_B(a_i) b^i$$

$$= b^n + \sum_{i=0}^{n-1} a_i b^i = 0.$$

↑ by definition of the A-module structure on C

I am now to prove Lemmas:

Lemma 1

Let B be a commutative A-algebra and M be a B-module
If B is a A-module of finite type and M a B-module of finite type, then M is a A module of finite type

Proof.
Let $\{e_1, \dots, e_m\}$ generates the A-module B
Let $\{f_1, \dots, f_n\}$ ——— B ——— M
We want to prove that $\{e_i f_j,\ 1 \le i \le m, 1 \le j \le n\}$ generates the A-module M.
Let $x \in M$, we may write

$$x = \sum_{j=1}^{n} b_j f_j \quad \text{with } (b_1, \dots, b_n) \in B^n$$

and

$$b_j = \sum_{i=1}^{m} a_{i,j} e_i \quad \text{with } a_{ij} \in A \text{ for } \begin{matrix} 1 \le i \le m \\ 1 \le j \le n \end{matrix}$$

thus

$$x = \sum_{j=1}^{n} \sum_{i=1}^{m} a_{ij} e_i f_j \text{ as wanted } \square$$

Remark
If $(e_1, \dots, e_m)$ is a basis of the A-module B
and $(f_1, \dots, f_n)$ ——— B ——— M
then $(e_i f_j)_{\substack{1 \le i \le m \\ 1 \le j \le n}}$ ——— A ——— M.

Lemma 2

Let B a commutative A-algebra which is a A-module of finite type and let C be a B-algebra, let $x \in C$
If x is integral over B then $B[x]$ is an A-module of finite type (and x is integral over A).

Proof
Apply lemma 1 to the B-module $B[\alpha]$ $\square$
$\wedge$
C

Proof of the proposition
1) Check that for any $a \in A$,
$(X-a)(\varphi_B(a)) = 0$ in B
so $\varphi_B(A) \subset \tilde{A}$ and $0, 1_B \in \tilde{A}$
2) Let $\alpha, \beta \in \tilde{A}$
β is integral over A
By the remark it is integral over $A[\alpha]$
Thus $A[\alpha, \beta]$ is an A-module of finite type
Thus any element of $A[\alpha, \beta]$, including $\alpha+\beta$ and $\alpha\beta$ are integral over A.
Thus $\tilde{A}$ is a subring of B containing $\varphi_B(A)$ that is a subalgebra $\square$

Quick exercise
Show that $\sqrt{2}$, $\sqrt{3}$ are integral over $\mathbb{Z}$; find a polynomial in $\mathbb{Z}[X]$ with leading coefficient 1 which vanishes at $\sqrt{2}+\sqrt{3}$.

Remark
By induction on n, if $\alpha_1, \dots, \alpha_n \in \tilde{A}$ then the subalgebra $A[\alpha_1, \dots, \alpha_n] \subset B$ is a A-module of finite type.

Proposition — integral closure of the integral closure.

$$\widetilde{\widetilde{A}} = \widetilde{A}$$

Proof

Assume that $d \in B$ is integral over $\widetilde{A}$
let $P = X^d + \sum_{i=0}^{d-1} a_i X^i \in \widetilde{A}[X]$ be such that $P(\alpha) = 0$
By the last remark, $A[a_0, \dots, a_{d-1}]$
is an A-module of finite type
But $P \in A[a_0, \dots, a_{d-1}]$ and $P(\alpha) = 0$
so α is integral over $A[a_0, \dots, a_{d-1}]$
by lemma 2 it is integral over A. □

Definition

Let A be an integral domain
and let $K = Fr(A)$ be the fraction field of A.
One says that A is an integrally
closed ring if its integral closure of A
in K coincides with the image of A in K.

Proposition.

A factorial ring is integrally closed.

Proof

Any $\alpha \in K$ may be written as $\alpha = \frac{p}{q}$
with $p, q \in A$, $q \neq 0$ and $\gcd(p, q) = 1$
(factorial rings have gcd's !)
If α is integral over A, we may
choose

$$P := X^d + \sum_{i=0}^{d-1} a_i X^i \in A[X]$$

so that $P\left(\frac{p}{q}\right) = 0$ so

$$p^d + a_{d-1} q p^{d-1} + \cdots + a_0 q^d = 0$$

Thus $q \mid p^d$.

But since A is factorial, $gcd(p^d, q) = 1$

So $q \mid 1$ and $q \in A^*$

so $\frac{p}{q}$ is the image of $pq^{-1} \in A$ □

Example $\mathbb{Z}[i\sqrt{3}]$ is not factorial, but $\mathbb{Z}\left[i\frac{\sqrt{3}+1}{2}\right]$ is

5| The case of an algebra over a field

Let $\mathbb{K}$ be a commutative field.

Definition (Reminder)

Let B be a $\mathbb{K}$-algebra and $\alpha \in B$ be integral over $\mathbb{K}$ then the generator of the kernel of

$$ev_\alpha : \mathbb{K}[X] \to B$$
$$P \mapsto P(\alpha)$$

with leading coefficient one is called the minimal polynomial of α and is denoted by $\mu_\alpha^{\mathbb{K}}$ (or μ_α if $\mathbb{K}$ is clear from the context)

Definitions (Reminder)

* An extension of a field $\mathbb{K}$ is a $\mathbb{K}$-algebra which is a field, denoted $\mathbb{L}/\mathbb{K}$
* Let $\mathbb{L}$ be an extension of $\mathbb{K}$ and $\alpha \in \mathbb{L}$, α is said to be algebraic over $\mathbb{K}$ iff it is integral.
* Let $\mathbb{L}/\mathbb{K}$ be a field extension $[\mathbb{L} : \mathbb{K}]$ is the cardinal of a basis of the $\mathbb{K}$-vector space $\mathbb{L}$.

* L/K is said to be algebraic iff any element of L is algebraic over K.

Remark.

* If L/K is a finite extension it is algebraic
* If $\alpha \in L$ is algebraic over K then N_α^K is an irreducible polynomial in $K[X]$,

$$\overline{ev_\alpha} : K[X]/(N_\alpha^K) \longrightarrow K[\alpha] = K(\alpha)$$

is an isomorphism. In particular, we get

$$\deg(N_\alpha^K) = [K(\alpha) : K]$$

* For extensions $M/L/K$, one has

$$[M : K] = [M : L]\,[L : K]$$

the multiplicativity formula

Definition

If L/K is a finite extension and $\alpha \in L$, we get $m_\alpha : L \longrightarrow L$ K-linear, $x \longmapsto \alpha x$

We define

(a) χ_α^K = characteristic polynomial of m_α

(b) $Tr_{L/K}(\alpha) = Tr(m_\alpha)$ trace of α in L/K

(c) $N_{L/K}(\alpha) = \det(m_\alpha)$ Norm of α in L/K

Remarks

(i) N_α^K is also the minimal polynomial of m_α

(ii) $Tr_{L/K} : L \longrightarrow K$ is a K-linear map

(iii) $N_{L/K}(ab) = N_{L/K}(a)\, N_{L/K}(b)$ for $a, b \in K$

$N_{L/K}(\zeta_L(a)) = a^{[L:K]}$ for $a \in K$.

Definition

The $\mathbb{K}$ bilinear map

$$\mathbb{L} \times \mathbb{L} \to \mathbb{K}$$
$$(x, y) \mapsto \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(xy)$$

is called the trace form of $\mathbb{L}/\mathbb{K}$.

Theorem (Reminder)

Let $\mathbb{K}$ be a (commutative) field then

(a) There is an algebraic extension of $\mathbb{K}$ which is algebraically closed

(b) Any two such extensions of $\mathbb{K}$ are isomorphic as extensions of $\mathbb{K}$

An algebraic closure of $\mathbb{K}$ is an algebraic extension $\overline{\mathbb{K}}$ of $\mathbb{K}$ which is algebraically closed

Example

$\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} \mid \alpha \text{ is algebraic over } \mathbb{Q}\}$ is an algebraic closure of $\mathbb{Q}$

6) Number fields, ring of integers, discriminant

Definition

* A number field is a finite extension of $\mathbb{Q}$
* If $\mathbb{K}$ is an algebraic extension of $\mathbb{Q}$ then the ring of integers in $\mathbb{K}$, denoted by $\mathcal{O}_{\mathbb{K}}$ is the integral closure of $\mathbb{Z}$ in $\mathbb{K}$ [anneau des entiers] We also put $\overline{\mathbb{Z}} = \mathcal{O}_{\overline{\mathbb{Q}}}$

Lecture 1

Proposition

Let A be an integral domain, which is integrally closed.
Let $\mathbb{K}$ be the fraction field of A and let $\mathbb{L}$ be a finite extension of $\mathbb{K}$.
Let $\alpha \in \mathbb{L}$ be integral over A.
Then

$$\chi_\alpha^{\mathbb{K}} \in A[X], \quad \mu_\alpha^{\mathbb{K}} \in A[X],$$

In particular,

$$\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha) \in A \text{ and } N_{\mathbb{L}/\mathbb{K}}(\alpha) \in A$$

Proof.

Let Ω be an algebraically closed extension of $\mathbb{L}$ and let $\alpha_1, \dots, \alpha_d$ be the roots of $\mu_\alpha^{\mathbb{K}}$ in Ω, counted with multiplicities. We have

$$\chi_\Omega(\mu_\alpha^{\mathbb{K}}) = \prod_{i=1}^{d} (X - \alpha_i) \text{ in } \Omega[X]$$

Let $P = X^n + \sum_{i=0}^{n-1} a_i X^i \in A[X]$ be such that $P(\alpha) = 0$.
By definition of the minimal polynomial,

$$\mu_\alpha^{\mathbb{K}} \mid P \text{ in } \mathbb{K}[X]$$

Thus $P(\alpha_i) = 0$ for $i \in \{1, \dots, d\}$ and $\alpha_1, \dots, \alpha_d$ are integral over A.
Since

$$\chi_\alpha(\mu_\alpha^{\mathbb{K}}) = \sum_{i=0}^{d} (-1)^i \sigma_i(\alpha_1, \dots, \alpha_d) X^{d-i},$$

the coefficients of $\mu_\alpha^{\mathbb{K}}$ are integral over A.
Since A is integrally closed,

$$\mu_\alpha^{\mathbb{K}} \in A[X].$$

Since $\mu_\alpha^{\mathbb{K}}$ is the minimal polynomial of m_α

By a result of linear algebra we know that

$$M_\alpha^{\mathbb{K}} \mid \chi_\alpha^{\mathbb{K}} \mid (M_\alpha^{\mathbb{K}})^{[\mathbb{L}:\mathbb{K}]}$$

Since $M_\alpha^{\mathbb{K}}$ is irreducible and $M_\alpha^{\mathbb{K}}$ and $\chi_\alpha^{\mathbb{K}}$ both have leading coefficient one, ($\chi_\alpha^{\mathbb{K}} = \det(X\,\mathrm{Id} - m_\alpha)$) we get

$$\chi_\alpha^{\mathbb{K}} = (M_\alpha^{\mathbb{K}})^r \quad \text{for some } r.$$

Thus

$$\chi_\alpha^{\mathbb{K}} \in A[X]$$

To finish the proof, it remains to note that:

$$\chi_\alpha^{\mathbb{K}} = X^n - \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha) X^{n-1} + \dots + (-1)^n N_{\mathbb{L}/\mathbb{K}}(\alpha)$$

where $n = [\mathbb{L}:\mathbb{K}]$. □

Remark

Since $\deg(\chi_\alpha^{\mathbb{K}}) = [\mathbb{L}:\mathbb{K}]$

and $\deg(M_\alpha^{\mathbb{K}}) = [\mathbb{K}(\alpha):\mathbb{K}]$

we get

$$\chi_\alpha^{\mathbb{K}} = (M_\alpha^{\mathbb{K}})^{[\mathbb{L}:\mathbb{K}(\alpha)]}.$$

and therefore

$$\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha) = [\mathbb{L}:\mathbb{K}[\alpha]]\,\mathrm{Tr}_{\mathbb{K}(\alpha)/\mathbb{K}}(\alpha)$$

and

$$N_{\mathbb{L}/\mathbb{K}}(\alpha) = N_{\mathbb{K}(\alpha)/\mathbb{K}}(\alpha)^{[\mathbb{L}:\mathbb{K}(\alpha)]}.$$

This remark gives also another way to compute the trace and the norm which may be useful

Proposition

Let $\mathbb{L}/\mathbb{K}$ be a finite extension and let $\alpha \in \mathbb{L}$. Let Ω be an extension of $\mathbb{K}$ which is algebraically closed and let $\alpha_1, \dots, \alpha_d$ be the roots of $M_\alpha^{\mathbb{K}}$ in Ω, counted with multiplicities,

then

$$\rho_{\mathfrak{L}}\left(\mathrm{Tr}_{\mathfrak{U}/\mathbb{K}}(\alpha)\right) = [\mathfrak{U}:\mathbb{K}(\alpha)] \sum_{i=1}^{d} \alpha_i$$

$$\rho_{\mathfrak{L}}\left(N_{\mathfrak{U}/\mathbb{K}}(\alpha)\right) = \left(\prod_{i=1}^{d} \alpha_i\right)^{[\mathfrak{U}:\mathbb{K}(\alpha)]}$$

Proof

$$\rho_{\mathfrak{L}}\left(N_{\alpha}^{\mathbb{K}}\right) = \prod_{i=1}^{d} (X - \alpha_i)$$

and

$$\chi_{\alpha}^{\mathbb{K}(\alpha)/\mathbb{K}} = N_{\alpha}^{\mathbb{K}}$$ and we apply the remark □

Example

Let A be an integral domain which is integrally closed and let $\mathbb{K} = \mathrm{Fr}(A)$. Let $\mathfrak{U}/\mathbb{K}$ be a quadratic extension, $\alpha \in \mathfrak{U}$. Then α is integral over A iff $\mathrm{Tr}_{\mathfrak{U}/\mathbb{K}}(\alpha) \in A$ and $N_{\mathfrak{U}/\mathbb{K}}(\alpha) \in A$

Indeed, the condition is necessary by the proposition and if $\mathrm{Tr}_{\mathfrak{U}/\mathbb{K}}(\alpha) \in A$ and $N_{\mathfrak{U}/\mathbb{K}}(\alpha) \in A$ then

$$\chi_{\alpha}^{\mathbb{K}} = X^2 - \mathrm{Tr}_{\mathfrak{U}/\mathbb{K}}(\alpha) X + N_{\mathfrak{U}/\mathbb{K}}(\alpha) \in A[X]$$

and $\chi_{\alpha}^{\mathbb{K}}(\alpha) = 0$. □

Lemma

Let A be an integral domain and let $\mathbb{K}$ be its fraction field. Let $\mathfrak{U}/\mathbb{K}$ a finite extension of $\mathbb{K}$ and let B be the integral closure of A in $\mathfrak{U}$.

Let $\alpha \in \mathfrak{U}$ then there exists $a \in A - \{0\}$ such that $\rho_{\mathfrak{L}}(a)\alpha \in B$

Remark

If we identify $\mathbb{K}$ with its image by φ_u this means that any $\alpha \in \mathbb{K}$ may be written as $\alpha = \frac{b}{a}$ with $b \in B$ and $a \in A - \{0\}$.

Proof

Let $P = \Psi_\alpha^{\mathbb{K}} = X^d + \sum_{i=0}^{d-1} u_i X^i$.
with $u_0, \dots, u_{d-1} \in \mathbb{K}$
Taking the product of the denominators of the u_i, we may write

$$u_i = \frac{a_i}{a} \quad \text{with } a_1, \dots, a_{d-1}, a \in A, a \neq 0$$

we then multiply P by a^d and get

$$(a\alpha)^d + \sum_{i=0}^{d-1} a^{d-1-i} a_i (a\alpha)^i = 0$$

Thus

$$a\alpha \in B. \quad \square$$

Definition

Let A be an integral domain and let $\mathbb{K} = Fr(A)$. A *fractional ideal* in $\mathbb{K}$ is a A-submodule I of $\mathbb{K}$ such that there exists $c \in A - \{0\}$ with $cI \subset A$.

Example

* If $\alpha \in \mathbb{K}$ then we denote by (α) the A submodule of $\mathbb{K}$ generated by α. It is a fractional ideal ideal
(Indeed we may write $\alpha = \frac{p}{q}$, $p, q \in A$, $q \neq 0$
then $q(\alpha) = (q\alpha) = (p) \subset A$)
Such a fractional ideal is said to be *principal*

* Any ideal of A is a fractional ideal of K.

To finish this section, it remains to define the discriminant. This terminology comes from quadratic forms, let me start with a quick reminder in that setting:

Definition (Reminder)

Let K be a field and E be a K vector space of finite dimension d. Let

$$\langle \cdot, \cdot \rangle : E \times E \to K$$

be a symmetric bilinear form.

Let $(e_1, \dots, e_d)$ be a basis of E.

The class of

$$\det\left(\left(\langle e_i, e_j \rangle \right)_{1 \le i,j \le d} \right)$$

in K / K^{*2} does not depend on the choice of the basis $(e_1, \dots, e_d)$ and is called the *discriminant* of the form B

(K^{*2} acts by multiplication on K.)

Remark

$K / K^{*2} = \{0\} \cup K^* / K^{*2}$ (group quotient)

Definition which generalizes the last one

Let A be an integral domain which is integrally closed

Let $K = \mathrm{Fr}(A)$ and L be a finite extension of K

Let B be the integral closure of A in L.

Let $d = [L : K]$.

Let $\mathfrak{b}$ be a fractional ideal in L

($\mathfrak{}$ german fraktur script)

Then ($\nearrow$ A-module generated by)

$$D_{B|A}(b) = \mathrm{Mod}_A\left\{ \mathrm{Det}\left(\left(\mathrm{Tr}(\ell_i \ell_j) \right)_{\substack{1 \le i \le d \\ 1 < j \le d}} \right), (\ell_1, \dots, \ell_d) \in b^d \right\}$$

is a fractional ideal of $\mathbb{K}$ called the discriminant of the fractional ideal b.

In particular, we define

$$D_{B/A} = D_{B|A}(B).$$

is called the discriminant of B over A.

Remark

If $A = \mathbb{Z}$, then we also call discriminant of $\mathbb{K}/\mathbb{Q}$ the unique integer $d_{\mathbb{K}/\mathbb{Q}} \in \mathbb{N}$ such that

$$(d_{\mathbb{K}/\mathbb{Q}}) = D_{G_{\mathbb{K}/\mathbb{Z}}}.$$

It turns out to be a very useful invariant for number fields.

Exercise

Compute it for quadratic extensions of $\mathbb{Q}$.

Proof of the fact that the discriminant is a fractional ideal.

For $\underline{\ell} = (\ell_1, \dots, \ell_d) \in \mathbb{K}^d$ let

$$Q_{\underline{\ell}} = \left(\mathrm{Tr}(\ell_i \ell_j) \right)_{\substack{1 \le i \le d \\ 1 < j \le d}}$$

Let $M = (m_{ij})_{1 \le i,j \le d} \in \mathcal{M}_d(\mathbb{K})$

We put $f_j = \sum_{i=1}^{d} m_{ij} e_i$ for $1 \le j \le d$.

$$\mathrm{Tr}(f_i f_j) = \sum_{\substack{1 \le k \le d \\ 1 \le \ell \le d}} m_{ki} \mathrm{Tr}(e_k e_\ell) m_{\ell j}$$

We get the usual formula for matrices of bilinear forms

$$Q_f = {}^t M \, Q_e \, M$$

Thus $\det(Q_f) = \det(M)^2 \det(Q_e)$

From that we can deduce the formula

$$\det(Q_{\alpha e}) = (N_{L/K}(\alpha))^2 \det(Q_e)$$

For $\alpha \in L$, $\alpha e = (\alpha e_1, \dots, \alpha e_d)$

Indeed,

→ if the family $(e_1, \dots, e_d)$ is related

$$\det(Q_{\alpha e}) = \det(Q_e) = 0$$

→ Otherwise $(e_1, \dots, e_d)$ is a basis of L over K and we take $M = \mathrm{Mat}_{(e_1, \dots, e_d)}(m_\alpha)$

$$N_{L/K}(\alpha) = \det(M).$$

Now choose $\alpha \in L$ such that $\alpha \mathfrak{b} \subset B$

For any $(e_1, \dots, e_d) \in \mathfrak{b}^d$,

$$N_{L/K}(\alpha)^2 \det(Q_e) = \det(Q_{\alpha e}) \in A. \quad \square$$

$\uparrow$

$\mathfrak{D}_d(A)$

From this proof we also get the following formula:

Proposition

$$D_{L/K}(\alpha \mathfrak{b}) = (N_{L/K}(\alpha))^2 D_{L/K}(\mathfrak{b})$$

for any fractional ideal $\mathfrak{b}$ of L and any $\alpha \in L$.

II Galois theory

I decided to start with the geometric analog so that it may help you get a better feeling of the corresponding algebraic notions in Algebraic Number Theory.

A) Riemann surfaces

1) Complex atlas

Since this is not the main topic of the lecture, I shall not go to the most general setting and skip various technical details, You may get more background from: T. SZAMUELY, Galois groups and fundamental groups, Cambridge Studies in advanced mathematics 117.

Definition

A topological space X is **Hausdorff** [séparé] iff For any $x \neq y$ in X, there exists open subsets U & V in X such that $x \in U$, $y \in V$.

Let X be a Hausdorff topological space. A **complex atlas** on X is given by

- $(U_i)_{i \in I}$ a covering of X by open subsets ($X = \bigcup_{i \in I} U_i$)
- for any $i \in I$ an homeomorphism $\varphi_i : U_i \to V_i \subset \mathbb{C}$ called **chart**

so that for any $i, j \in I$, the map $\varphi_j \circ \varphi_i^{-1} : \varphi_i(U_i \cap U_j) \to \varphi_j(U_i \cap U_j)$ is **holomorphic** (and, by exchanging i and j, we see that in fact its inverse function is also holomorphic)

This means that around each point of X one may find a "little" open subset which "is like a small disk on the complex plane.

Definition

Two complex atlases on X $\mathcal{A}$ given by $(U_i)_{i\in I}$ and $(\varphi_i)_{i\in I}$ and $\mathcal{A}'$ given by $(U_i)_{i\in I'}$ and $(\varphi'_i)_{i\in I'}$ are said to be equivalent iff $(U_i'')_{i\in \{1\}\times I \cup \{2\}\times I'}$ and $(\varphi_i'')_{i\in I\amalg I'}$ defined by

$$U_i'' = \begin{cases} U_j & \text{if } i=(1,j) \\ U'_j & \text{if } i=(2,j) \end{cases} \qquad \varphi_i'' = \begin{cases} \varphi_j & \text{if } i=(1,j) \\ \varphi'_j & \text{if } i=(2,j) \end{cases}$$

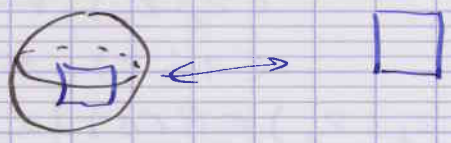
($I\amalg I'$ "formal" disjoint union)

is an atlas on X

Remark

(i) This is a equivalence relation on the set

(ii) Think of maps (in the usual sense) for areas of the earth



An atlas is a collection of maps so that there is a map for each area on the earth (But the map may be thought as a part of plane). Adding more maps does not change the earth (but only give a description which might be easier to use) You may also buy different atlases from different editors but the earth is the same.

Definition

A Riemann surface is a Hausdorff topological space endowed with an equivalence class of complex atlases.

Example

Let me give you two compact examples

a) The Riemann sphere $\mathbb{P}^1(\mathbb{C})$

$\mathbb{P}^1(\mathbb{C})$ = {1-dimensional vector subspaces in $\mathbb{C}^2$}.

$\mathbb{C}^2 - \{0\} \xrightarrow{\pi} \mathbb{P}^1(\mathbb{C})$; colon

$(z_1, z_2) \longmapsto \mathbb{C}(z_1, z_2) = (z_1 : z_2)$

$\mathbb{P}^1(\mathbb{C})$ is a topological space for the quotient topology :

$U \subset \mathbb{P}^1(\mathbb{C})$ open iff $\pi^{-1}(U)$ open in $\mathbb{C}^2 - \{0\}$

This is a Hausdorff topological space.

$U_1 = \{(z_1 : z_2) \in \mathbb{P}^1(\mathbb{C}) \mid z_1 \neq 0\} \xrightarrow[\varphi_1]{\sim} \mathbb{C}$ homeomorphism

$(z_1 : z_2) \longmapsto z_2/z_1$

$(1 : z) \longleftarrow z$

$U_2 = \{(z_1 : z_2) \in \mathbb{P}^1(\mathbb{C}) \mid z_2 \neq 0\} \xrightarrow[\varphi_2]{\sim} \mathbb{C}$

$(z_1 : z_2) \longmapsto z_1/z_2$

$$\varphi_2 \circ \varphi_1^{-1} : \underbrace{\varphi_1(U_1 \cap U_2)}_{\mathbb{C} - \{0\}} \longrightarrow \underbrace{\varphi_2(U_1 \cap U_2)}_{\mathbb{C} - \{0\}}$$

$$z \longmapsto 1/z$$

Topologically $\mathbb{P}^1(\mathbb{C})$ is homeomorphic to a sphere

When you remove one pole from the sphere, the remainder is homeomorphic to the complex plane.

b) The tores T_τ

Let $\tau \in \mathbb{C} - \mathbb{R}$
then the subgroup $\Lambda = \mathbb{Z} + \mathbb{Z}\tau \subset \mathbb{C}$ is a lattice in $\mathbb{C}$ and we consider $\pi : \mathbb{C} \to T = \mathbb{C}/\Lambda$ quotient group equipped with the quotient topology One may again show that it is an Hausdorff topological space.
Let $\varepsilon = \frac{1}{2} \min_{\lambda \in \Lambda - \{0\}} (|\lambda|)$ disk of center z and radius ε.)
Then for any $z \in \mathbb{C}$ we define $U_z = \pi(D(z,\varepsilon))$
$\pi_{|D(z,\varepsilon)} : D(z,\varepsilon) \to U_z$ is a homeomorphism and we put $\varphi_z = \pi^{-1}_{|D(z,\varepsilon)}$
Then
$(U_z)_{z \in \mathbb{C}}$, $(\varphi_z)_{z \in \mathbb{C}}$ defines an atlas on $\mathbb{C}/\Lambda$
Indeed
$$\varphi_{z'} \circ \varphi_z^{-1} : \varphi_z(U_z \cap U_{z'}) \to \varphi_{z'}(U_z \cup U_{z'})$$
$$u \longmapsto u + \lambda$$
for any $\lambda \in \Lambda$ such that $(D(z,\varepsilon) + \lambda) \cap D(z',\varepsilon) \neq \emptyset$
(there is either one such λ or none)
Topologically it looks like a ring doughnut

c) An open subset U in a Riemann surface with the restriction of the charts

Terminology

Let X be a Riemann surface. A complex chart of X is an homeomorphism φ from an open subset of X to an open subset of $\mathbb{C}$ which appears in one of the atlases of X.

2) Holomorphic maps

Definition

Let X and Y be Riemann surfaces a holomorphic map (or morphism) from X to Y is a continuous map $f: X \to Y$ such that for any open subsets $U \subset X$ and $V' \subset Y$ and any charts

$$\varphi : U \to V \text{ of } X \text{ and } \varphi' : U' \to V' \text{ of } Y,$$

$\varphi' \circ f \circ \varphi^{-1} : \varphi(f^{-1}(V') \cap U) \to V'$ is holomorphic

($f^{-1}(V') \cap U$ is $\hat{X}$)

(We check "locally" whether the map is holomorphic)

An holomorphic function on X is a holomorphic map

$$f : X \to \mathbb{C}$$

A meromorphic function on X is a holomorphic map $f : X \to \mathbb{P}^1(\mathbb{C})$ such that $f(X) \neq \{\infty\}$.

($\infty = (0:1)$)

Remark

One could also define a meromorphic function as a function $\varphi : X - S \to \mathbb{C}$,

with S a discrete subset of X so that $\varphi \circ g^{-1}$ is meromorphic for any chart g of X.

Examples a) $\mathbb{P}^1(\mathbb{C}) \xrightarrow{z^n} \mathbb{P}^1(\mathbb{C})$ $(u:v) \mapsto (u^n : v^n)$.

b) As above, let $\tau \in \mathbb{C} - \mathbb{R}$, $\Lambda = \mathbb{Z} + \mathbb{Z}\tau \subset \mathbb{C}$. The Weierstrass $\wp$ function is defined as

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda - \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$$

for $z \in \mathbb{C} - \Lambda$. It converges uniformly on any compact subset in $\mathbb{C} - \Lambda$, $\wp$ extends meromorphically to $\mathbb{C}$ and satisfies

(1) $\wp(z+\lambda) = \wp(z)$ for $z \in \mathbb{C}$, $\lambda \in \Lambda$

as well as

(2) $\wp(-z) = \wp(z)$ for $z \in \mathbb{C}$.

(Indeed $\wp'(z) = -2 \sum_{\omega \in \Lambda} \frac{1}{(z-\omega)^3}$ satisfies $\wp'(z+\lambda) = \wp'(z)$ for $\lambda \in \Lambda$, $z \in \mathbb{C}$ thus $\wp(z+\lambda) - \wp(z)$ does not depend on z, and ... $\wp(-\frac{1}{2}) = \wp(\frac{1}{2})$, $\wp(-\frac{\tau}{2}) = \wp(\frac{\tau}{2})$.)

It induces a holomorphic map

$$\wp : \mathbb{C}/\Lambda \longrightarrow \mathbb{P}^1(\mathbb{C}).$$

3) Local structure of holomorphic maps

Proposition

Let X and Y be Riemann surfaces

and let $f: X \to Y$ be a holomorphic map, which is not constant on any connected component of X.
Let $x \in X$ and $y = f(x)$.
Then there exists open subsets $U \subset X$ and $V \subset Y$ such that $x \in U$ and $y \in V$ and charts

$$\varphi: U \to W \subset \mathbb{C} \text{ and } \psi: V \to W' \subset \mathbb{C}$$

so that $f(U) \subset V$, $\varphi(x) = 0$, $\psi(y) = 0$ and

$$\psi \circ f \circ \varphi^{-1}: W \longrightarrow W'$$
$$z \longmapsto z^{e_x}$$

where $e_x \in \mathbb{N}$ does not depend on the choice of the charts.

Definition

e_x is called the ramification index of f at x. The points x for which $e_x > 0$ are called the branch points of f.

Remark

(i) The proposition implies that the set S_f of branch points is discrete in X.
(ii) Moreover the fibre $f^{-1}(y)$ is discrete in X for any $y \in Y$.

Sketch of the proof of the proposition

- Starting with any charts around x and y, by reducing the open subset around x and composing with translations in $\mathbb{C}$ it is is easy to get

$$\varphi: U \to W \quad \text{and} \quad \psi: V \to W'$$

such that $f(U) \subset V$, $\varphi(x) = 0$ and $\psi(y) = 0$
By definition of a holomorphic function from X to Y,
$\psi \circ f \circ \varphi^{-1} : W \to \mathbb{C}$
is holomorphic and $\psi \circ f \circ \varphi^{-1}(0) = 0$
Let e be the order of the zero of this function at 0, $e_x \geq 1$
and we may write
$$\psi \circ f \circ \varphi^{-1}(z) = c z^{e_x} H(z) \qquad c \in \mathbb{C}^*$$
where $H : W \to \mathbb{C}$ is holomorphic and $H(0) = 1$
Without loss of generality, reducing U if necessary, we may assume that $H(W) \subset \mathbb{C} - \mathbb{R}^-$
Choose γ so that $\gamma^{e_x} = c$
Let $\mathrm{Log} : \mathbb{C} - \mathbb{R}^- \to \mathbb{C}$
be the holomorphic function such that
$$\mathrm{Log}|_{\mathbb{R}^+_*} = \log \text{ and } \exp \circ \log = \mathrm{Id}_{\mathbb{C}-\mathbb{R}^-}$$
We define $h : W \to \mathbb{C}$
$$z \mapsto \gamma \exp\left(\frac{1}{e_x} \log H(z)\right)$$
$z \xrightarrow{\tau} z\,h(z)$ is holomorphic on W and $\tau'(0) = 1$; thus it is a diffeomorphism from a neighborhood of 0 to its image.
Using $\tau \circ \varphi$ instead of φ we get the wanted charts.
(Indeed $\psi \circ f \circ \varphi^{-1} \circ \tau^{-1}(z) = z^{e_x}$) □

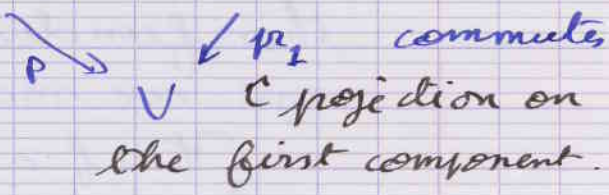
I need a bit of topological terminology.

Definition
Let X and E be topological spaces
a continuous map $p : E \to X$

is called <u>a cover of X</u> iff
for any $x \in X$ there exists a
neighbourhood V of x in X,
a set F equipped with discrete topology,
and a homeomorphism

$$\tau : p^{-1}(V) \to V \times F$$

such that



commutes,
p_1 projection on
the first component.

<u>Definition</u>

Let X and Y be topological spaces
a continuous map

$$f : X \to Y$$

is proper iff for any topological space Z
the image by

$$f \times Id_Z : X \times Z \to Y \times Z$$

of a closed subset of $X \times Z$ is a closed subset
of $Y \times Z$.

<u>Proposition</u>

If X is Hausdorff, $f : X \to Y$ is proper
iff it satisfies

(i) $f(Z)$ is closed for any closed Z in Y
(ii) $\forall y \in Y$, $f^{-1}(y)$ is compact.

<u>Proof</u> (omitted)

See N. Bourbaki Topology, Chap. I, §10, n°2
In fact, since I am only interested
in compact Riemann surface, I shall

not really need this notion of proper...

Corollary

Let X be compact topological space, and Y be a Hausdorff space
$f: X \to Y$ is proper iff it is continuous

So now I can state the proposition I was interested in:

Proposition

Let X and Y be Riemann surfaces and let $f: X \to Y$ be a non-proper holomorphic map, which is not constant on any connected component of X, assume Y is connected, Then f is surjective with finite fibers and the induced map $X - f^{-1}(f(S_f)) \to Y - f(S_f)$ is a cover of $Y - f(S_f)$; the cardinal of the fibres on $Y - f(S_f)$ is constant and is called the degree of f.

Proof In the case where X and Y are compact and connected.
By remarks (i) and (ii) S_f and the fibres $f^{-1}(y)$ are finite (since they are discrete in a compact space)
Using the proposition, $f(X)$ is open in Y and it is closed, thus $f(X) = Y$.
and the last statement follows from the definition of S_f and the proposition (we may have $S_f \subsetneq f^{-1}(f(S_f))$) □

Example

a) $P_n : \mathbb{P}^1(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$ define a cover
$(u:v) \mapsto (u^n : v^n)$

Lecture 2

$\mathbb{P}^1(\mathbb{C}) - \{0,\infty\} \longrightarrow \mathbb{P}^1(\mathbb{C}) - \{0,\infty\}$
and, outside $\{0,\infty\}$, all the fibers have cardinal n.

b) $\wp : \mathbb{C}/\Lambda \to \mathbb{P}^1(\mathbb{C})$ [exercise]
is a cover outside

$$\mathbb{C}/\Lambda[2] = \{p \in \mathbb{C}/\Lambda \mid 2p = 0\} \quad \text{2 torsion pts}$$
$$= \{\overline{0}, \overline{\frac{T}{2}}, \overline{\frac{\tau}{2}}, \overline{\frac{T}{2}+\frac{\tau}{2}}\}$$

and gives a cover

$$\mathbb{C}/\Lambda = \mathbb{C}/\Lambda[2] \to \mathbb{P}^1(\mathbb{C}) - \{0, \wp(\tfrac{T}{2}), \wp(\tfrac{\tau}{2}), \wp(\tfrac{T+\tau}{2})\}$$

with fibers of cardinal 2.

4) Back to field extensions

Lemma

a) Let X be a connected Riemann surface, the set $\mathcal{M}(X)$ of meromorphic functions on X is a field

b) Let X and Y be connected Riemann surfaces and let $f : X \to Y$ be a non-constant holomorphic map then

$$f^* : \mathcal{M}(Y) \to \mathcal{M}(X)$$
$$g \longmapsto g \circ f$$

is morphism of fields (so $\mathcal{M}(X)$ may be seen as an extension of $\mathcal{M}(Y)$).

Remark

Let $f, g \in \mathcal{M}(X)$, $f^{-1}(\infty), g^{-1}(\infty)$ are finite subsets of X and we may extend

$$f+g,\ fg : X - (f^{-1}(\infty) \cup g^{-1}(\infty)) \to \mathbb{C} \subset \mathbb{P}^1(\mathbb{C})$$
$$z \mapsto (1:z)$$

to meromorphic functions

$f+g, fg : X \to \mathbb{P}^1(\mathbb{C})$.

Proof

a) follows from the fact that for any connected open subset U of $\mathbb{C}$, the set of meromorphic functions on U is a field (You can check everything locally using charts).

b) Check locally using charts. □

Examples

a) The map $\mathbb{C}(T) \to \mathbb{C}(\mathbb{P}^1(\mathbb{C}))$

$P/Q \mapsto ((1:z) \mapsto (Q(z):P(z)))$

is an isomorphism of fields

Indeed it is a morphism of fields and if $f \in \mathbb{C}(\mathbb{P}^1(\mathbb{C}))$

Consider

$$\begin{array}{ccc} \mathbb{P}^1(\mathbb{C}) & \xrightarrow{f} & \mathbb{P}^1(\mathbb{C}) \\ \cup & & \cup \\ \mathbb{C} - f^{-1}(\infty) & \xrightarrow{\tilde{f}} & \mathbb{C} \end{array}$$

$\tilde{f}$ is either constant or meromorphic on $\mathbb{C}$ with a finite number of pole and zeroes

Let $p_1, \dots, p_m$ be its zeroes with multiplicities $\alpha_1 - \alpha_m$

and $q_1, \dots, q_n$ ——— poles ——— $\beta_1 - \beta_n$

$$h : z \mapsto \tilde{f}(z) \frac{\prod_{i=1}^{n} (z-q_i)^{\beta_i}}{\prod_{i=1}^{m} (z-p_i)^{\alpha_i}}$$ is an entire function on $\mathbb{C}$, write

$$h(z) = \sum_{n \in \mathbb{N}} a_n z^n$$

$h\left(\frac{1}{z}\right) = \sum_{n \geq 0} a_n z^{-n}$
has a finite pole at $z = 0$
thus $a_n = 0$ for n large enough
Therefore h is a polynomial with
no zeroes and has to be constant.

b) As before let $\tau \in \mathbb{C} - \mathbb{R}$ and $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$
$T = \mathbb{C}/\Lambda$
Then $\mathbb{C}(T) = \mathbb{C}(\wp, \wp')$ is the field generated by
Indeed, we only have to prove
that for any meromorphic function f
on $\mathbb{C}$ such that
$f(z+\lambda) = f(z)$ for $z \in \mathbb{C}$ and $\lambda \in \Lambda$
$f \in \mathbb{C}(\wp, \wp')$
We may write f as the sum of
an even and an odd function:

$$f(z) = \underbrace{\frac{f(z)+f(-z)}{2}}_{f_+} + \underbrace{\frac{f(z)-f(-z)}{2}}_{f_-}$$

Since $\wp$ is even, $\wp'$ is odd
and $f_-/\wp'$ is even. So it is enough
to prove that if f as above is even
then $f \in \mathbb{C}(\wp)$, for such an f $\operatorname{ord}_0 f = 0$ (2)
Let $D = \{x + y\tau,\ x \in [0,1[,\ y \in [0,1[\}$
Using the fact that f is even and
Λ are periods of f, we may find
$p_1, \dots, p_m$ and $q_1, \dots, q_n$ in $D - \{0\}$
such that, counting with multiplicities,
$p_1, \dots, p_m, -p_1, \dots, -p_m$ are the zeroes of f in D

and $q_1, \dots, q_n, \sigma(q_1), \dots, \sigma(q_n)$ its poles, $\sigma : D \to D$ being defined by $z + \tau(z) \in \Lambda$ for $z \in D$.

[$$\sigma(z) = \begin{cases} 1+\tau-z & \text{if } z = x+y\tau \text{ with } x, y \in]0,1[\\ 1-z & \text{if } z = x \text{ with } x \in]0,1[\\ \tau - z & \text{if } z = x\tau \text{ with } x \in]0,1[\\ 0 & \text{if } z = 0 \end{cases}$$]

$f \times \dfrac{\prod_{i=1}^{n} (p - p(q_i))}{\prod_{i=1}^{m} (p - p(p_i))} p^{n+m-n}$ is a holomorphic bounded function on $\mathbb{C}$ and thus constant □

Let me now prove that p and p' satisfy a polynomial equation

$$p(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda - \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$$

For $n \geq 3$ let

$$G_n(\Lambda) = \sum_{\omega \in \Lambda - \{0\}} \frac{1}{\omega^n} \quad \text{(this converges)}$$

$= 0$ if n is odd

then

$$p(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda - \{0\}} \sum_{k=1}^{+\infty} \frac{(k+1)}{\omega^{k+2}} z^k$$

$$= \frac{1}{z^2} + \sum_{k=1}^{\infty} (k+1) G_{k+2} z^k.$$

$$p'(z) = -\frac{2}{z^3} + \sum_{k=1}^{\infty} (k+2)(k+1) G_{k+3} z^k$$

Computing the first terms of the Laurent series we get that

$$p'(z)^2 - 4p(z)^3 + 60 G_4 p(z) + 140 G_6 = \underset{z \to 0}{O}(z^3)$$

Therefore

$$(*) \quad p'^2 - 4p^3 + 60 G_4 p + 140 G_6 = 0$$

Reference A. W. KNAPP Elliptic curves, chapter VI
or D HUSEMOLLER Elliptic curves, chapter 9.

Conclusion

(i) $\mathbb{C}(X)[Y]/(Y^2 - 4X^3 + 60G_4X + 140G_6) \xrightarrow{\sim} \mathbb{C}(\Pi)$

$X \longmapsto H$

$Y \longmapsto H'$

(ii) and $\wp : \Pi \to \mathbb{P}^1(\mathbb{C})$

induces

$$\mathbb{C}(X) \hookrightarrow \mathbb{C}(X)[Y]/(\quad)$$

so that

$\mathbb{C}(\Pi) / \mathbb{C}(\mathbb{P}^1(\mathbb{C}))$ is a quadratic extension.

Theorem

Let X and Y be compact connected Riemann surfaces and let

$$f : X \to Y$$

be a non-constant holomorphic map then $\mathbb{C}(X) / \mathbb{C}(Y)$ is a field extension of degree $\deg(f)$.

Proof. that $[\mathbb{C}(X) : \mathbb{C}(Y)] \leq d$.

We start with the following lemma

Lemma 1

Let X and Y be connected Riemann surfaces and let $f : X \to Y$ be a proper morphism

which is not constant and of degree d
then, for any $g \in \mathbb{C}(X)$
$$[\mathbb{C}(Y)(g) : \mathbb{C}(Y)] \leq d$$

Proof

We put $S = S_f \subset X$ and $T = f(S) \subset Y$,
Let $g \in \mathbb{C}(X)$, $S' = g^{-1}(\{\infty\})$, $T' = f(S')$
For any $y \in Y - T \cup T'$ we put
$$F_y(T) = \prod_{x \in f^{-1}(y)} (T - g(x)) \in \mathbb{C}[T]$$

F_y is a polynomial of degree d with lead coefficient 1
$$F_y(T) = T^d + \sum_{i=0}^{d-1} a_i T^i.$$

Let us prove that $a_i \in \mathbb{C}(Y)$ for $i \in \{0, \dots, d-1\}$
Let $y \in Y - T \cup T'$ and let $U \subset Y - T \cup T'$ be an open open neighbourhood so that there exists a homeomorphism
$$\varphi : f^{-1}(U) \xrightarrow{\sim} U \times \underbrace{f^{-1}(y)}_{\text{discrete topology}}$$
$$f \searrow \quad \swarrow p_1$$
$$U$$

For $x \in X_y = f^{-1}(y)$, let $U_x = \varphi^{-1}(U \times \{x\})$
then
$$f|_{U_x} : U_x \to U$$
is a holomorphic homeomorphism.
In local maps this implies that the derivative of f is everywhere different from 0 on U_x and $f|_{U_x}$ is a diffeomorphism.
$a_i|_U$ is obtained, up to sign, as the $(d-i)$-th symmetric polynomial in $\left(g \circ (f|_{U_x})^{-1}\right)_{x \in X_y}$.

Thus $a_i|_U$ is holomorphic

Take now $y \in T \cup T'$ and choose charts $\varphi_x : U_x \to W_x$ around $x \in X_y$

$\psi_y : V_y \to W_y$ around y.

as in the local description of holomorphic map. Without loss of generality, we may assume that

$V_y \cap T' \subset \{y\}$ in $W_x = W_y = D(0,\delta)$

for some $\delta \in \mathbb{R}_{>0}$. Of course, we have $\psi_y(y) = 0$.

Since y is meromorphic, there exists an integer N so that

$(\psi_y \circ f)^N \cdot g$ is holomorphic at x

for $x \in X_y$, and therefore bounded on

$\varphi_x^{-1}(D(0, \frac{\delta}{2}))$

It follows from the construction of a_i that

$\psi_y^{N(d-i)} a_i$ is bounded on $\psi_y^{-1}(D(0,\delta/2))$

By Riemann's removable singularity theorem $z \mapsto z^{N(d-i)}(a_i \circ \psi_y^{-1})$ has holomorphic extension to $D(0,\delta/2)$. and thus

$a_i \in \mathbb{C}(X)$ ☐

This concludes the proof of the lemma

Proof of $[\mathbb{C}(X) : \mathbb{C}[Y]] \leq d$

Since $\mathrm{char}(\mathbb{C}(Y)) = 0$, for any finite extension $\mathbb{L}$ of $\mathbb{C}(Y)$ there exists $\alpha \in \mathbb{L}$ such that $\mathbb{L} = \mathbb{C}(Y)(\alpha)$ (Every separable extension has a primitive element). So for any $\mathbb{L} \subset \mathbb{C}(X)$ which is a finite extension of $\mathbb{C}(Y)$

$[\mathbb{L} : \mathbb{C}(Y)] \leq d$.

is algebraic

If $\mathbb{C}(X)/\mathbb{C}(Y)$ were infinite, there would exist an infinite sequence $(\alpha_i)_{i\in\mathbb{N}}$ so that $\alpha_i \notin \mathbb{C}(Y)(\alpha_1, \dots, \alpha_{i-1})$ for $i \in \mathbb{N}$.
But then $[\mathbb{C}(Y)(\alpha_1, \dots, \alpha_i) : \mathbb{C}(Y)] \xrightarrow[i\to+\infty]{} +\infty$
which is absurd

Thus $\mathbb{C}(X)/\mathbb{C}(Y)$ is finite and
$[\mathbb{C}(X) : \mathbb{C}(Y)] \leq d$. □

The main difficulty to show that the degree is exactly d is to show that there are enough meromorphic functions on X.
In order to do that, we need the following very deep result of Riemann, which I shall not prove.

Riemann's existence theorem

Let X be a compact Riemann surface, let $x_1, \dots, x_n \in X$ and let $a_1, \dots, a_n \in \mathbb{P}^1(\mathbb{C})$
Then there exists a meromorphic function $f \in \mathbb{C}(X)$ such that

$$f(x_i) = a_i \quad \text{for } i \in \{1, \dots, n\}$$

Let me apply this to prove the following

[Reference] Corollary

Lemma 2

With the notations of the theorem, there exists $g \in \mathbb{C}(X)$ and an irreducible $P \in \mathbb{C}(Y)[T]$ such that $P(g) = 0$.

Proof

Take $y \in Y - T$ and let $X_y = f^{-1}(y)$.

By Riemann's existence theorem, there exists $g \in \mathbb{C}(X)$ such that
$\forall x, x' \in X_g$, $x \neq x' \Rightarrow g(x) \neq g(x')$
By Lemme 1, g is algebraic / $\mathbb{C}(t)$ of degree $\leq d$
Write $N_g^{\mathbb{C}(t)} = T^m + \sum_{i=0}^{m-1} a_i T^i$

with $a_i \in \mathbb{C}(t)$ for $i \in \{0, \dots, m-1\}$
The polynomial

$$T^m + \sum_{i=0}^{m-1} a_i(g) T^i \in \mathbb{C}[T]$$

vanishes at $g(x)$ for $x \in X_g$
and it has d different root
Therefore $d = m$. □

Reference for Riemann's existence theorem
O. FORSTER lectures on Riemann surfaces, Graduate texts in Mathematics 81 Springer-Verlag.

Corollary
Let X be a compact connected Riemann surface then $\mathbb{C}(X)$ is a finite extension of $\mathbb{C}(T)$.

Proof
Choose any meromorphic function $f \in \mathbb{C}(X)$
it gives a holomorphic map $f : X \to \mathbb{P}^1(\mathbb{C})$

Remark
Conversely, we shall see later on that for any finite extension $\mathbb{L}$ of $\mathbb{C}(T)$, there exists a compact connected Riemann surface X so that $\mathbb{L} \simeq \mathbb{C}(X)$

Warning $\deg_{\mathbb{C}} \mathbb{L} = 1 \not\Rightarrow \mathbb{L}$ finite extension of $\mathbb{C}(T)$.

B) Algebraic Galois theory.

1) Quick motivation and historical background

I think it is enlightening to realize that Galois theory started from the problem of solving polynomial equations using radicals

a) Equations of small degree

(i) degree 2 (Babylon - 18th century BC).

Solutions of $aX^2+bX+c=0$ are $\frac{-b+\sqrt{b^2-4ac}}{2a}$.

(ii) degree 3 (Del Ferro, Fontana, Cardano (XVIth century))

$X^3+aX^2+bX+c=0$

Write $Y=X+\frac{a}{3}$ get $Y^3+pX+q=0$ (*)

Look for a solution of the form

$$y=\sqrt[3]{t}+\sqrt[3]{u}$$

$$y^3=t+u+3\left(\sqrt[3]{t}+\sqrt[3]{u}\right)\left(\sqrt[3]{t+u}\right)$$

y solution of (*) $\Leftrightarrow (t+u+q)+\left(\sqrt[3]{t}+\sqrt[3]{u}\right)\left(3\sqrt[3]{t+u}+p\right)=0$

A sufficient condition for this to be 0 is

$$\begin{cases} t+u=-q \\ tu=-\left(\frac{p}{3}\right)^3 \end{cases}$$

we get $\{t,u\}=\left\{-\frac{q}{2}\pm\sqrt{\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3}\right\}$

and a solution of (*)

$$y=\sqrt[3]{-\left(\frac{q}{2}\right)+\sqrt{\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3}}+\sqrt[3]{-\left(\frac{q}{2}\right)-\sqrt{\left(\frac{q}{2}\right)+\left(\frac{p}{3}\right)^3}}$$

(iii) degree 4 (Ferrari 1565) As before, we can easily reduce to an equation of the form

$$Y^4+pY^2+qY+r=0 \qquad (*)$$

and assume $q\neq 0$ (otherwise we get an equation of degree in Y^2, easy to solve).

$(*) \Leftrightarrow \left[Y^2+\frac{p}{2}\right]^2 = -qY - r + \left(\frac{p}{2}\right)^2$

We want to write this as an equality between square of more simple expressions.

We introduce an extra variable u and write

$(*) \Leftrightarrow \left[Y^2+\frac{p}{2}+u\right]^2 = -qY - r + \left(\frac{p}{2}\right)^2 + 2uY^2 + pu + u^2$

$\overset{?}{=} \left(Q_u(Y)\right)^2$

where Q_u is a affine function in Y. We have no choice:

$$Q_u(Y) = \left(\sqrt{2u}\,Y - \frac{q}{2\sqrt{2u}}\right)^2$$

and we get the equation in u:

$$u^2 + pu + \left(\frac{p}{2}\right)^2 - r = \frac{q^2}{8u}$$

that is

$$u^3 + pu^2 + \left[\left(\frac{p}{2}\right)^2 - r\right]u - \frac{q^2}{8} = 0$$

(Since $q \neq 0$, 0 is not a solution of this equation)

Since this equation is of degree 3 we know how to solve it. It remains to solve

$$\left[Y^2+\frac{p}{2}+u\right]^2 = \left[\sqrt{2u}\,Y - \frac{q}{2\sqrt{2u}}\right]^2$$

$$\Leftrightarrow \quad Y^2+\frac{p}{2}+u = \varepsilon\left(\sqrt{2u}\,Y - \frac{q}{2\sqrt{2u}}\right)$$

with $\varepsilon \in \{-1, 1\}$. This gives 2 equations of degree 2 we know how to solve with radicals. And it was a big challenge to find formulas for higher degrees

Answer (Abel 1824, Galois 1832)

It is impossible to solve a general polynomial equation of degree 5 using radicals. (The problem was initially considered over $\mathbb{Q}$, but you can also consid

this problem over $\mathbb{C}(t)$.

b) Sketch of the proof of Galois (covered in modern terms.)

Let $P \in \mathbb{Q}[T]$, and consider

$$E_P = \{ \alpha \in \mathbb{C} \mid P(\alpha) = 0 \}.$$

And $K_P = \mathbb{Q}(E_P)$

Defines G_P as the automorphism group of the extension $K / \mathbb{Q}$

For any $\sigma \in G_P$, $\sigma(E_P) \subset E_P$

Moreover, if $\sigma_{|E_P} = Id_{E_P}$ then $\sigma = Id_K$.

So

$$G_P \subset \mathfrak{S}_{E_P} = \text{Permutation group of } E_P.$$

Example 1

$n \in \mathbb{N} - \{0\}$, $P = X^n - 1$

$E = \mu_n(\mathbb{C}) = \{1, \xi, \dots, \xi^{n-1}\}$ where $\xi = \exp\left(\frac{2i\pi}{n}\right)$

$K_P = \mathbb{Q}(\xi)$.

$\sigma \in G_P$ is caracterised by $\sigma(\xi) \in \{1, \xi, \dots, \xi^{n-1}\}$

and $\mathrm{ord}_{\mathbb{C}^*}(\sigma(\xi)) = \mathrm{ord}_{\mathbb{C}^*}(\xi) = n$

thus

$$\sigma(\xi) = \xi^k \text{ with } k \in \mathbb{Z}, \quad \gcd(k, n) = 1$$

we get on group isomorphism

$$G_P \xrightarrow{\sim} (\mathbb{Z}/n\mathbb{Z})^*$$
$$(\xi \mapsto \xi^k) \longleftrightarrow \overline{k}$$

Example 2

p prime, $a \in \mathbb{Q}^* - \mathbb{Q}^{*p}$

$P(X) = X^p - a$.

$\mathcal{E}_p = \{\lambda, \xi\lambda, \dots, \xi^{p-1}\lambda\}$ where ξ is a primitive p-th root of 1

$K_p = \mathbb{Q}(\lambda, \xi)$

$\sigma \in G_p$ is determined by

$$\begin{cases} \sigma(\xi) \text{ primitive } p\text{-th root of 1} \\ \sigma(\lambda)/\lambda \in \{1, \dots, \xi^{p-1}\}. \end{cases}$$

we get a group homomorphism

$$\begin{aligned} \psi : G &\longrightarrow (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})^* \\ \sigma &\longmapsto (a, b) / \begin{cases} \sigma(\lambda) = \xi^a \lambda \\ \sigma(\xi) = \xi^b. \end{cases} \end{aligned}$$

(Indeed the law group in $(\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})^*$ is given by:

$$(a_1, b_1)(a_2, b_2) = (a_1 + b_1 a_2, b_1 b_2)$$

$\sigma_1, \sigma_2 \in G_p$

$$\sigma_i(\lambda) = \xi^{a_i}\lambda, \quad \sigma_i(\xi) = \xi^{b_i} \quad i = 1, 2$$

then

$$\sigma_1 \circ \sigma_2(\xi) = \xi^{b_1 b_2} \text{ and}$$

$$\sigma_1 \circ \sigma_2(\lambda) = \sigma_1(\xi^{a_2}\lambda) = \xi^{b_1 a_2 + a_1}\lambda.)$$

More generally Galois proved the following result:

Theorem

Let $P \in \mathbb{Q}[X]$, the equation $P(X) = 0$ may be solved using radicals iff the group G_p is solvable, that is there exist subgroup

$$\{e\} = G_0 \triangleleft G_1 \dots \triangleleft G_{n-1} \triangleleft G_n = G_p$$

so that G_{i-1} is a normal subgroup of G_i and G_i / G_{i-1} is cyclic for $i \in \{1, \dots, n\}$.

Examples

Let us again consider the case of low degree equations:

(i) if $\deg P = 2$ $\quad G_P \subset S_2 = \mathbb{Z}/2\mathbb{Z}$ solvable

(ii) if $\deg P = 3$ $\quad G_P \subset S_3 \supset \mathbb{Z}/3\mathbb{Z} \triangle \mathbb{Z}/2\mathbb{Z}$ solvable

(A subgroup of a solvable group is solvable)

(Indeed $A_3 \cong \mathbb{Z}/3\mathbb{Z}$ and $S_3/A_3 \cong \mathbb{Z}/2\mathbb{Z}$)

(iii) if $\deg P = 4$ $\quad G_P \subset S_4$

$\{Id, (12)(34), (13)(24), (14)(23)\} \triangle A_4 \triangle S_4$

$\downarrow S$ $\qquad A_4/- \quad S_4/A_4$

$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. $\qquad \downarrow S \quad \downarrow S$

$\mathbb{Z}/3\mathbb{Z} \quad \mathbb{Z}/2\mathbb{Z}$

Thus S_4 is solvable as is G_P

(iv) In one of the exercise session, we shall see that

If $P = X^5 - 10X + 5$, $G \cong S_5$

$A_5 \subset S_5$, A_5 is a simple group

$\Rightarrow S_5$ is not solvable and therefore S_5 is not solvable. □

Let me mention an

Open problem (Inverse Galois problem).

Given G finite group is it possible to find an (explicit) $P \in \mathbb{Q}[X]$ such that

$$G_P \cong G.$$

This is known as the inverse Galois problem

Lecture 3

2) Extension of morphisms

In this section, $\mathbb{K}$ denotes a (commutative) field and $\overline{\mathbb{K}}$ an algebraic closure of $\mathbb{K}$ that is an algebraic extension of $\mathbb{K}$ which is algebraically closed.

Notation

For any algebraic extension $\mathbb{L}$ of $\mathbb{K}$, $\Sigma_{\mathbb{L}/\mathbb{K}}$ denotes the set of of morphisms of algebras from $\mathbb{L}$ to $\overline{\mathbb{K}}$

Lemma 1

Let $\mathbb{M}$, $\mathbb{L}$, $\mathbb{K}$ be algebraic extensions of $\mathbb{K}$ Assume that $\mathbb{M} = \mathbb{L}(\alpha)$ for some $\alpha \in \mathbb{M}$ and let $\sigma \in \Sigma_{\mathbb{L}/\mathbb{K}}$, then there is bijection

$$\{\tau \in \Sigma_{\mathbb{M}/\mathbb{K}} \mid \tau \circ \iota_{\mathbb{L}/\mathbb{K}} = \sigma\} \to \{\beta \in \overline{\mathbb{K}} \mid \sigma(P_\alpha^{\mathbb{L}})(\beta) = 0\}$$

$$\tau \longmapsto \tau(\alpha).$$

Proof

- For $\tau \in \Sigma_{\mathbb{M}/\mathbb{K}}$ such that $\tau \circ \iota_{\mathbb{L}/\mathbb{K}} = \sigma$

  Since $\iota_{\mathbb{L}/\mathbb{K}}(P_\alpha^{\mathbb{L}})(\alpha) = 0$, $\sigma(P_\alpha^{\mathbb{L}})(\tau(\alpha)) = 0$.

  Therefor this map is well defined and
- Since $\mathbb{M} = \mathbb{L}(\alpha)$ it is injective
- For $\beta \in \overline{\mathbb{K}}$ s.t such that $\sigma(P_\alpha^{\mathbb{L}})(\beta) = 0$

We get $\mathbb{K}[X]/(\Pi_\alpha \Psi)$ $\xrightarrow{ev_\beta}$ $\overline{\mathbb{K}}$

$\downarrow S$ $\qquad P \mapsto P(\beta)$ $\nearrow \tau$

$\mathbb{M} = \Psi(\alpha)$ $\qquad \square$

Proposition 1

Let $P \in \mathbb{K}[X]$ be irreducible

Then the following statements are equivalent:

$\Updownarrow$

(i) $\#\{\beta \in \overline{\mathbb{K}} \mid P(\beta) = 0\} \neq \deg(P)$

(ii) $P' = 0$

(iii) $\mathrm{char}(\mathbb{K}) = p > 0$ and there exists an irreducible $Q \in \mathbb{K}[X]$ such that $P(X) = Q(X^p)$

Proof

(i) $\Rightarrow$ (ii)

Assume that there exists $\beta \in \overline{\mathbb{K}}$ which is a root of P of order ≥ 2

Write $P = (X-\beta)^2 R$ for some $R \in \overline{\mathbb{K}}[X]$

Then $P(\beta) = P'(\beta) = 0$.

Since P irreducible and $P \in \mathrm{Ker}(ev_\beta) : \mathbb{K}[X] \to \overline{\mathbb{K}}$, $S \mapsto S(\beta)$

we get $\mathrm{Ker}(ev_\beta) = (P)$ and $P \mid P'$

Since $\deg(P') < \deg(P) - 1$, $P' = 0$

(ii) $\Rightarrow$ (i)

Let $\beta \in \overline{\mathbb{K}}$ be a root of P

$P = (X-\beta) R$

Since $P'(\beta) = 0$, $R(\beta) = 0$ and $(X-\beta)^2 \mid P$.

(ii) $\Rightarrow$ (iii)

Write $P = \sum_{i=0}^{d} a_i X^i$ with $a_d \neq 0$
we get $i a_i = 0$ for $i \in \{1, \dots, d\}$
If $\mathrm{char}(\mathbb{K}) = 0$ then $d a_d \neq 0$ absurd ↯
Thus $p = \mathrm{char}(\mathbb{K}) > 0$, p prime
If $a_i \neq 0$ in $\mathbb{K}$ then $i = 0$ in $\mathbb{K}$
then $p \mid i$

we may write

$$P = \sum_{i=0}^{d/p} a_{pi} X^{pi}$$

and $P(X) = Q(X^p)$ for $Q = \sum_{i=0}^{d/i} a_{pi} X^i$
If Q is reducible, so is P
(iii) ⇒ (ii)

$$Q(X^p)' = p X^{p-1} Q'(X^p) = 0. \quad \square$$

Corollary
If $\mathrm{char}(\mathbb{K}) = 0$ or $\mathbb{K}$ is a finite field
then for any irreducible $P \in \mathbb{K}[X]$

$$\#\{\beta \in \overline{\mathbb{K}} \mid P(\beta) = 0\} = \deg(P).$$

Proof
We only have to consider the case $\mathbb{K}$ finite
If $\mathbb{K}$ is finite

$$\mathrm{Fr}_p : \mathbb{K} \longrightarrow \mathbb{K}$$
$$a \mapsto a^p$$

is a morphism of fields, therefore injective and since $\mathbb{K}$ is finite surjective
If $Q = \sum_{i=0}^{m} a_i X^i \in \mathbb{K}[X]$
for any $i \in \{0, \dots, m\}$ let $b_i \in \mathbb{K}$ be such that $a_i = b_i^p$
Then

$$Q = \sum_{i=0}^{m} b_i^p X^i$$

and $Q(X^p) = \left(\sum_{i=0}^{m} b_i X^i\right)^p$ is not irreducible $\square$

Remark

More generally a field $\mathbb{K}$ is said to be perfect if one of the following conditions is satisfied.

(i) $\mathrm{char}(\mathbb{K}) = 0$ or

(ii) $\mathrm{char}(\mathbb{K}) = p > 0$ and $Fr : \mathbb{K} \to \mathbb{K}$, $x \mapsto x^p$ is surjective. The statement of the corollary is valid for any perfect field.

Example

$X^p - T \in \mathbb{F}_p(T)[X]$

is irreducible (by Eisenstein criterion applied to $\mathbb{F}_p[T]$, $p = T$) but in $\mathbb{F}_p(T)$

$$X^p - T = \left(X - \sqrt[p]{T}\right)^p$$

where $\sqrt[p]{T}$ is the unique p-th root of T in $\mathbb{F}_p(T)$.

Theorem (Reminder)

For any algebraic extension $\mathbb{L}/\mathbb{K}$, $\Sigma_{\mathbb{L}/\mathbb{K}}$ is finite.

Proof

- If $\mathbb{L}/\mathbb{K}$ is finite, we may choose $\alpha_1, \dots, \alpha_r \in \mathbb{L}$ so that $\mathbb{L} = \mathbb{K}(\alpha_1, \dots, \alpha_r)$ and the result follows from Lemma 1 by induction on r.
- If $\mathbb{L}/\mathbb{K}$ is infinite apply Zorn's lemma to the following ordered set:

  X is the set of $(\mathbb{M}, \sigma)$ where $\mathbb{M}$ is a subextension of $\mathbb{L}$ over $\mathbb{K}$ and $\sigma \in \Sigma_{\mathbb{M}/\mathbb{K}}$

with order
$(M,\sigma) \leq (M',\sigma')$ iff $M \subset M'$ and $\sigma'_{|M} = \sigma$.
□

Definition
Let L/K be an algebraic extension then the separable degree of L over K is
$$[L:K]_s = \# \Sigma_{L/K} \leq +\infty$$

N.B.
This does not depend on the choice of the algebraic closure $\overline{K}$: let $\overline{K}'$ be another algebraic closure of K: then there exists an isomorphism of K-extension

$$\sigma : \overline{K} \longrightarrow \overline{K}'$$

and
$$\Sigma_{L/K} \overset{\text{bij}}{\longleftrightarrow} \Sigma'_{L/K}$$
$$\tau \longmapsto \sigma \circ \tau$$

Example
If $L = K(\alpha)$ for some $\alpha \in L$
Then
$$[L:K]_s = \#\{p \in \overline{K} \mid \mu_\alpha^K(p) = 0\}$$
In particular if K is perfect
$$[L:K]_s = [L:K].$$

Theorem
Let M L/K be algebraic extension
then $[M:K]_s = [M:L]_s [L:K]_s$

and, in particular
$[M : K]_s$ is finite iff $[M : L]_s$ and $[L : K]_s$ are.

Proof
Consider the restriction map

$$\begin{aligned} res : \Sigma_{M/K} &\longrightarrow \Sigma_{L/K} \\ \tau &\longmapsto \tau_{|L} \end{aligned}$$

and choose $\sigma \in \Sigma_{L/K}$.
Using $\sigma : L \to \overline{K}$, $\overline{K}$ is an algebraic closure of L.
$res^{-1}(\sigma)$ is the set of morphisms of L-algebras from M to $\overline{K}$ where $\overline{K}$ structural morphism is σ. We get

$$\#\left(res^{-1}(\sigma)\right) = [M : L]_s$$

Here is use that this cardinal does not depend on the choice of the algebraic closure of L.
We get

$$\#\left(\Sigma_{M/K}\right) = [M : L]_s \cdot \#\left(\Sigma_{L/K}\right)$$

The last statement follows from the fact that $[M : L]_s \geq 1$ and $[L : K]_s \geq 1$. □

Definition
- The exponential characteristic of K is one if $char(K) = 0$ and p otherwise.
- Let $P \in K[X] - \{0\}$, P is said to be separable iff

$$\#\{x \in \overline{K} \mid P(x) = 0\} = \deg(P).$$

- Let L/K be an extension of fields and let $\alpha \in L$ be algebraic $/K$

Then α is separable over $\mathbb{K}$ iff $\mu_\alpha^{\mathbb{K}}$ is.

o Let $\mathbb{L}/\mathbb{K}$ be an algebraic extension. Then $\mathbb{L}/\mathbb{K}$ is separable iff any $\alpha \in \mathbb{L}$ is.

Remark p. 58

Proposition 2

Let $\mathbb{L}/\mathbb{K}$ be a finite extension, Then

$$[\mathbb{L}' : \mathbb{K}]_s \mid [\mathbb{L} : \mathbb{K}]$$

and $[\mathbb{L}/\mathbb{K}) / [\mathbb{L}' : \mathbb{K}]_s$ is a power of the exponential characteristic of $\mathbb{K}$.

Moreover $\mathbb{L}/\mathbb{K}$ is separable iff

$$[\mathbb{L} : \mathbb{K}]_s = [\mathbb{L} : \mathbb{K}].$$

Proof

o If $\mathbb{L} = \mathbb{K}(\alpha)$ let $\sum_{i=0}^{d} a_i X^i = \mu_\alpha^{\mathbb{K}}$, $a_d \neq 0$

Assume $p = \text{char}(\mathbb{K}) > 0$ and put

$$r = \max \{ t \mid \{ i \mid a_i \neq 0 \} \subset p^t \mathbb{Z} \}$$

then

$$\mu_\alpha^{\mathbb{K}} = \sum_{i=0}^{d/p^r} a_{p^r i} X^{p^r i} = Q(X^{p^r})$$

where $Q = \sum_{i=0}^{d/p^r} a_{p^r i} X^i$ is irreducible and (by definition of r), $Q' \neq 0$.

Let $\beta \in \overline{\mathbb{K}}$

$$\mu_\alpha^{\mathbb{K}}(\beta) = 0 \Leftrightarrow Q(\beta^{p^r}) = 0$$

But $\overline{\mathbb{K}}$ is perfect:

$$\text{Fr} : \overline{\mathbb{K}} \to \overline{\mathbb{K}} \quad \text{is injective}$$
$$x \mapsto x^p$$

and since $\overline{\mathbb{K}}$ is algebraically closed, surjective

Thus $\{ \beta \in \overline{\mathbb{K}} \mid \mu_\alpha^{\mathbb{K}}(\beta) = 0 \} \to \{ \delta \in \overline{\mathbb{K}} \mid Q(\delta) = 0 \}$

$$\beta \mapsto \beta^{p^r}$$

is bijective

and $\#\{\gamma \in \overline{\mathbb{K}} \mid Q(\gamma) = 0\} = \deg Q = \frac{\deg(P)}{p^e}$

Then $[\mathbb{L} : \mathbb{K}]_s = \deg Q$

and $[\mathbb{L} : \mathbb{K}] / [\mathbb{L} : \mathbb{K}]_s = p^e$ (if $\mathrm{char}(\mathbb{K}) = 0$, $[\mathbb{L} : \mathbb{K}] = [\mathbb{L} : \mathbb{K}]_s$)

- If $\mathbb{L} = \mathbb{K}(\alpha_1, \dots, \alpha_n)$ put $\mathbb{K}_i = \mathbb{K}(\alpha_1, \dots, \alpha_i)$
  $[\mathbb{L} : \mathbb{K}] = [\mathbb{K}_n : \mathbb{K}_{n-1}] \times \cdots \times [\mathbb{K}_1 : \mathbb{K}_0]$
  is a multiple of
  $[\mathbb{L} : \mathbb{K}]_s = [\mathbb{K}_n : \mathbb{K}_{n-1}]_s \times \cdots \times [\mathbb{K}_1 : \mathbb{K}_0]_s$
  and $[\mathbb{L} : \mathbb{K}] / [\mathbb{L} : \mathbb{K}]_s$ is a power of p.
- If $\mathbb{L}/\mathbb{K}$ is separable so is α_i over $\mathbb{K}_{i-1}$ (remark) and $[\mathbb{L} : \mathbb{K}]_s = [\mathbb{L} : \mathbb{K}]$
- Let $\alpha \in \mathbb{L}$

$$\begin{array}{ccccc} [\mathbb{L} : \mathbb{K}] & = & [\mathbb{L} : \mathbb{K}(\alpha)] & & [\mathbb{K}(\alpha) : \mathbb{K}] \\ \vee | & & \vee | & & \vee | \\ [\mathbb{L} : \mathbb{K}]_s & = & [\mathbb{L} : \mathbb{K}(\alpha)]_s & & [\mathbb{K}(\alpha) : \mathbb{K}]_s \end{array}$$

If $[\mathbb{L} : \mathbb{K}] = [\mathbb{L} : \mathbb{K}]_s$, then $[\mathbb{K}(\alpha) : \mathbb{K}] = [\mathbb{K}(\alpha) : \mathbb{K}]_s$
that is

$$\deg(N_\alpha^{\mathbb{K}}) = \#\{\beta \in \overline{\mathbb{K}} \mid N_\alpha^{\mathbb{K}}(\beta) = 0\}$$

and α is separable. □

Definition

If $\mathbb{L}/\mathbb{K}$ is a finite extension
the inseparable degree of $\mathbb{L}/\mathbb{K}$ is

$$[\mathbb{L} : \mathbb{K}]_i = [\mathbb{L} : \mathbb{K}] / [\mathbb{L} : \mathbb{K}]_s$$

it is a power of the exponential characteristic of $\mathbb{K}$.

Corollary 1 / Definition

If $\mathbb{L}/\mathbb{K}$ is an algebraic extension

$$\Pi = \{\alpha \in \mathbb{L} \mid \alpha \text{ is separable } /\mathbb{K}\}$$

is a subfield of $\mathbb{L}$, called the relative separable closure of $\mathbb{K}$ in $\mathbb{L}$

Remark

Let $\mathbb{M}/\mathbb{L}/\mathbb{K}$ be field extensions
Let $\alpha \in \mathbb{M}$ be algebraic over $\mathbb{K}$
Since

$$P_\alpha^{\mathbb{L}} \mid P_\alpha^{\mathbb{K}}$$

if α is separable over $\mathbb{K}$ it is separable over $\mathbb{L}$.

Proof of Corollary 1

- Let $\alpha, \beta \in \mathbb{L}$ be separable over $\mathbb{K}$.
Then, by the remark, β is separable over $\mathbb{K}(\alpha)$
Thus

$$[\mathbb{K}(\alpha):\mathbb{K}]_s = [\mathbb{K}(\alpha):\mathbb{K}]$$

and $[\mathbb{K}(\alpha,\beta):\mathbb{K}(\alpha)]_s = [\mathbb{K}(\alpha,\beta):\mathbb{K}(\alpha)]$
Hence $[\mathbb{K}(\alpha,\beta):\mathbb{K}]_s = [\mathbb{K}(\alpha,\beta):\mathbb{K}]$
By the last proposition, $\mathbb{K}(\alpha,\beta)/\mathbb{K}$ is separable
Thus $\alpha+\beta$ and $\alpha\beta$ are separable over $\mathbb{K}$
- Similarly we may prove that if $\alpha \in \mathbb{L} \setminus \{0\}$ is separable over $\mathbb{K}$, so is α^{-1}. □

Notation

Let $\mathbb{M}/\mathbb{K}$ be a field extension
and let $\mathbb{L}, \mathbb{L}' \subset \mathbb{M}$ be sub extensions of $\mathbb{M}$
(that is subalgebras which are subfields).
then $\mathbb{L}\mathbb{L}' = \mathbb{K}(\mathbb{L} \cup \mathbb{L}') \subset \mathbb{M}$
is called the compositum of the fields

Corollary 2

Let $\mathbb{M}/\mathbb{K}$ be a field extension
and let $\mathbb{L}$ and $\mathbb{L}'$ be sub extensions of $\mathbb{M}$
Assume that $\mathbb{L}/\mathbb{K}$ and $\mathbb{L}'/\mathbb{K}$ are separable

then $L_1 L_2 / K$ and $L_1 \cap L_2 / K$ are separable

Proof

If L_1 and L_2 are contained in the subfield separable closure of K in M so is $L_1 L_2$. □

Proposition 3

Let $M / L / K$ be field extensions
Let $\alpha \in M$
Assume that L / K is separable
and that α is **algebraic and separable** over L
Then α is separable over K

Proof

Write $\psi_L^\alpha = X^d + \sum_{i=0}^{d-1} a_i X^i$ with $a_i \in L$ for $i \in \{0, \dots, d-1\}$
Then $\psi_L^\alpha \in K(a_0, \dots, a_{d-1})[X]$ is irreducible
(otherwise it would be reducible over L)
Thus $\psi^\alpha_{K(a_0, \dots, a_{d-1})} = \psi_L^\alpha$
and α is separable over $K(a_0, \dots, a_{d-1})$
$[K(a_0, \dots, a_{d-1}, \alpha) : K]_s = [K(a_0, \dots, a_{d-1}, \alpha) : K(a_0, \dots, a_{d-1})]_s \times$
$\times [K(a_0, \dots, a_{d-1}) : K]_s = [K(a_0, \dots, a_{d-1}, \alpha) : K]$
So α is separable over K. □

Corollary

Let $M / L / K$ be **algebraic** extensions
M / K is separable iff M / L and L / K are

Proof

$\Rightarrow$ Remark above
$\Leftarrow$ Proposition □

Proposition 4

Let L/K be a finite extension. Let L' be the relative separable closure of K in L. Then

$$[L' : K] = [L : K]_s$$

Proof

- $[L' : K] = [L' : K]_s \mid [L : K]_s$ gives $[L' : K] \leq [L : K]_s$.
- Let $\alpha \in L$ and remember the proof of proposition 2: there exists $r \geq 0$ and $Q \in K[X]$ irreducible with $Q' = 0$ such that $\mu_\alpha^K = Q(X^{p^r})$. It follows that $\beta = \alpha^{p^r} \in L'$ and $\mu_\alpha^{L'} \mid X^{p^r} - \beta = (X - \alpha)^{p^r}$ in $L[X]$. Let $\overline{L'}$ be an algebraic closure of L'. For any $\sigma \in \Sigma_{L/L'}$, $\sigma(\alpha)$ is the unique p^r-th root of the image of β in $\overline{L'}$. In other words $\sigma(\alpha)$ is independent of σ. There is only one possible value for $\sigma(\alpha)$ since it is true for any $\alpha \in L$.

$$\#\Sigma_{L/L'} = 1$$

and $[L : L']_s = 1$ □.

Note that for any $\alpha \in L$, there is $r \geq 0$ such that $\alpha^{p^r} \in L'$. Purely inseparable extensions (ie extensions with $[L : K]_s = 1$) are obtained using p-th roots of elements of the field.

Theorem

Let $\mathbb{L}/\mathbb{K}$ be a finite separable extension
Then
there exists $\alpha \in \mathbb{L}$ such that $\mathbb{L} = \mathbb{K}(\alpha)$

Proof

- If $\mathbb{K}$ is finite, then $\mathbb{L}$ is finite
  Then $\mathbb{L}^*$ is cyclic, choose a generator α of $\mathbb{L}^*$
- Otherwise $\mathbb{K}$ is infinite
  Take $\alpha, \beta \in \mathbb{L}$ and consider $\mathbb{L}' = \mathbb{K}(\alpha, \beta)$

$$P(X) = \prod_{\substack{\sigma, \sigma' \in \Sigma_{\mathbb{L}'/\mathbb{K}} \\ \sigma \neq \sigma'}} (\sigma(\alpha) + X\sigma(\beta) - \sigma'(\alpha) - X\sigma'(\beta)) \in \mathbb{K}[X]$$

For any $\sigma, \sigma' \in \Sigma_{\mathbb{L}'/\mathbb{K}}$ such that $\sigma \neq \sigma'$
either $\sigma(\alpha) \neq \sigma'(\alpha)$ or $\sigma(\beta) \neq \sigma'(\beta)$
Thus $P \neq 0$.
Since $\mathbb{K}$ is infinite, there exists $c \in \mathbb{K}$
such that $P(c) \neq 0$.
Let $\gamma = \alpha + c\beta$

$$P(c) = \prod_{\substack{\sigma, \sigma' \in \Sigma_{\mathbb{L}'/\mathbb{K}} \\ \sigma \neq \sigma'}} (\sigma(\gamma) - \sigma'(\gamma)) \neq 0$$

ie $\forall \sigma, \sigma' \in \Sigma_{\mathbb{L}'/\mathbb{K}}$, $\sigma \neq \sigma' \Rightarrow \sigma(\gamma) \neq \sigma'(\gamma)$
We get $\Sigma_{\mathbb{L}'/\mathbb{K}} \xrightarrow{\text{Res}} \Sigma_{\mathbb{K}(\gamma)/\mathbb{K}}$ is injective
So

$$[\mathbb{L}:\mathbb{K}] \geq [\mathbb{K}(\gamma):\mathbb{K}] \geq [\mathbb{K}(\gamma):\mathbb{K}]_s \geq [\mathbb{L}':\mathbb{K}]_s = [\mathbb{L}':\mathbb{K}]$$

since $\mathbb{L}'/\mathbb{K}$ is $\nearrow$ separable.

So $\mathbb{K}(\alpha, \beta) = \mathbb{K}(\gamma)$

- Write $\mathbb{L} = \mathbb{K}(\alpha_1, \dots, \alpha_r)$, by induction on r

we get that there exists $\delta \in \mathbb{L}$ such that $\mathbb{L} = \mathbb{K}(\delta)$. □

Remark

(2) False for inseparable extensions
$\mathbb{F}_p(T,U)(\sqrt[p]{T}, \sqrt[p]{U}) / \mathbb{F}_p(T,U)$

(2) There are separable extensions of degree p / $\mathbb{F}_p(T)$
eg $\mathbb{F}_p(T)[X]/(X^p - X - T)$ / $\mathbb{F}_p(T)$.

3) Splitting fields and normal extensions

In this section $\mathbb{K}$ denotes a field and $\overline{\mathbb{K}}$ an algebraic closure of $\mathbb{K}$

Definition.
Let $(P_i)_{i\in I}$ be a family of polynomials over $\mathbb{K}$.
A splitting field for $(P_i)_{i\in I}$ is an extension $\mathbb{L}$ of $\mathbb{K}$ which satisfies the following two conditions
(i) $\forall i \in I$, P_i splits over $\mathbb{L}$
(ii) $\mathbb{L}$ is generated (as a $\mathbb{K}$-extension) by the roots of the polynomials P_i, ie
$$\mathbb{L} = \mathbb{K}(\{\alpha \in \mathbb{L} \mid \exists i \in I, P_i(\alpha) = 0\})$$
In particular $\mathbb{L}/\mathbb{K}$ is algebraic

Proposition 1
Let $(P_i)_{i\in I} \in \mathbb{K}[X]^I$, then
(i) There exists a unique subextension $\mathbb{L}$ of $\overline{\mathbb{K}}$ which is a splitting field of $(P_i)_{i\in I}$

(ii) Let L' be a splitting field for $(P_i)_{i\in I}$ then

$$\forall \sigma \in \Sigma_{L'/K},\ \sigma(L') = L$$

In particular L' is isomorphic to L as a K extension

Proof :

- Let $\mathcal{E} = \{\lambda \in \bar{K} \mid \exists i \in I,\ P_i(\lambda) = 0\}$
  By definition of the splitting field $L = K(\mathcal{E})$ is the unique subextension of $\bar{K}$ which is a splitting field for $(P_i)_{i\in I}$.
- If $\sigma \in \Sigma_{L'/K}$ then L' and $\sigma(L') \subset \bar{K}$ are isomorphic has K-extensions therefore $\sigma(L')$ is a splitting field for $(P_i)_{i\in I}$
  By (i), $\sigma(L') = L$.
- We know that $\Sigma_{L'/K} \neq \emptyset$. □

Example

p prime, $q = p^r$ for some $r \geq 1$
any field of cardinal q is a splitting field for $X^q - X$ over $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Proposition 2 Definition

An algebraic extension L/K is said to be normal iff it satisfies one of the following equivalent conditions:

(i) $\forall \sigma, \sigma' \in \Sigma_{L/K},\ \sigma(L) = \sigma'(L)$
(ii) $\forall P \in K[X]$ be irreducible, if P has a root in L then P splits over L
(iii) L is a splitting field for a family of polynomials in $K[X]$

(i) ⇒ (ii)

Let P be an irreducible element of $\mathbb{K}[X]$ and let α be a root of P in $\mathbb{L}$ (I assume that P has such a root)

$$\Sigma_{\mathbb{L}/\mathbb{K}} \xrightarrow{\text{res}} \Sigma_{\mathbb{K}(\alpha)/\mathbb{K}} \longrightarrow \{\beta \in \overline{\mathbb{K}} \mid P(\beta) = 0\} = \mathcal{E}_P$$

$$\sigma \longmapsto \sigma(\alpha)$$

is surjective. So for any $\beta \in \mathcal{E}_P$ there exists $\sigma_\beta \in \Sigma_{\mathbb{L}/\mathbb{K}}$ such that $\sigma_\beta(\alpha) = \beta$

Fix $\sigma \in \Sigma_{\mathbb{L}/\mathbb{K}}$

By (i) $\forall\, \beta \in \mathcal{E}_P$ $\sigma_\beta(\mathbb{L}) = \sigma(\mathbb{L})$

so $\beta \in \sigma(\mathbb{L})$

Since $\mathbb{K} \subset \overline{\mathbb{K}}$ is algebraically closed, P splits in $\overline{\mathbb{K}}$ that is P may be written as

$$c \prod_{\beta \in \mathcal{E}_P} (X - \beta)^{m_\beta} \quad \text{in } \overline{\mathbb{K}}[X]$$

where $c \in \mathbb{K}$ is the leading coefficient of P.

Then the image of P in $\mathbb{L}[X]$ is

$$\sigma^{-1}\Big(c \prod_{\beta \in \mathcal{E}_P} (X-\beta)^{m_\beta}\Big) = c \prod_{\beta \in \mathcal{E}_P} (X - \sigma^{-1}(\beta))^{m_\beta}$$

and P splits over $\mathbb{L}$.

(ii) ⇒ (iii)

$\mathbb{L}$ is the splitting field of $\big(P^{\mathbb{K}}_\alpha\big)_{\alpha \in \mathbb{L}}$.

(iii) ⇒ (i)

By proposition 1. □

Examples

a) $\overline{\mathbb{K}}/\mathbb{K}$ is normal

b) $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ is not

Indeed $\mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{R} \subset \mathbb{C}$.

$$\mathbb{Q}(\sqrt[4]{2}) \xrightarrow{\sigma'} \mathbb{Q}(i\sqrt[4]{2}) \subset \mathbb{C}$$
$$\cong \uparrow \sigma \qquad \cong \uparrow s$$
$$\mathbb{Q}[T]/(T^4-2)$$

$\mathrm{Im}(\sigma) \neq \mathrm{Im}(\sigma')$

(and X^4-2 does not split over $\mathbb{Q}(\sqrt[4]{2})$

$X^4-2 = (X-\sqrt[4]{2})(X+\sqrt[4]{2})(X^2+\sqrt{2})$)

irreducible decomposition.

Proposition 2

Let M/K be an extension of fields and L, L' be subextensions of M

If L/K and L'/K are normal

$L \cap L'/K$ and LL'/K are as well

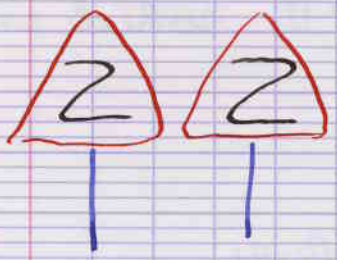
Proof

- $L \cap L'/K$ normal by (ii)
- Let $\sigma, \sigma' \in \Sigma_{LL'/K}$.

  $\sigma_{|L}, \sigma'_{|L} \in \Sigma_{L/K}$ and $\sigma_{|L'}, \sigma'_{|L'} \in \Sigma_{L'/K}$

  $\sigma(LL') = \sigma(L)\sigma(L') = \sigma'(L)\sigma'(L') = \sigma'(LL')$

  and apply (i) $\square$



Let $M/L/K$ be field extensions

a) One may have

M/L and L/K normal but M/K not normal

b) One may have

M/K normal and L/K not normal!

Examples.

a) $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ splitting field of $X^2-\sqrt{2}$ normal

$\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ ——— X^2-2 ———.

But $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ is not normal!

b) $\mathbb{Q}(i, \sqrt[4]{2})/\mathbb{Q}$ splitting field of x^4-2 normal
$\mathbb{Q}(i, \sqrt[4]{2})/\mathbb{Q}(\sqrt[4]{2})$ splitting field of x^2+1 —
But $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ is not.

Definition

Let $\mathbb{L}/\mathbb{K}$ be an algebraic extension
Let $\mathbb{L}^n$ be the splitting field of $(\mu_\alpha^{\mathbb{K}})_{\alpha \in \mathbb{L}}$ over $\mathbb{K}$. $\mathbb{L}^n$ is called a normal closure of $\mathbb{L}$ over $\mathbb{K}$

Properties

a) $\mathbb{L}^n$ is a normal extension of $\mathbb{K}$

b) There is a morphism of extensions

$$\sigma : \mathbb{L} \to \mathbb{L}^n$$

and we may consider $\mathbb{L}^n$ as a $\mathbb{L}$ extension.

d) For any extension $\mathbb{M}$ of $\mathbb{L}$ which is normal over $\mathbb{K}$, there exists a morphism of $\mathbb{L}$ extensions from $\mathbb{L}^n$ to $\mathbb{M}$.
We may think of $\mathbb{L}^n$ as «the» smallest extension of $\mathbb{L}$ which is normal over $\mathbb{K}$

Proof

a) $\mathbb{L}^n$ is a splitting field.

b) Choose $\tau \in \Sigma_{\mathbb{L}/\mathbb{K}}$ and $\tau' \in \Sigma_{\mathbb{L}^n/\mathbb{K}}$
Then

$$\tau'(\mathbb{L}^n) = \mathbb{K}\left(\{\beta \in \overline{\mathbb{K}} \mid \exists \alpha \in \mathbb{L},\ \mu_\alpha^{\mathbb{K}}(\beta) = 0\}\right)$$

for any $\alpha \in \mathbb{L}$, $\mu_\alpha^{\mathbb{K}}(\tau(\alpha)) = 0$
Thus $\tau(\mathbb{L}) \subset \tau'(\mathbb{L}^n)$
and $\tau'^{-1} \circ \tau : \mathbb{L} \to \mathbb{L}^n$

is a morphism of $\mathbb{K}$ extensions

c) We keep the notations of b)
$\overline{\mathbb{K}}$ equipped with τ is an algebraic Closure of $\mathbb{L}$.
Choose $\tau' \in \Sigma_{\mathbb{M}/\mathbb{L}}$
For any $\alpha \in \mathbb{L}$, $N_{\mathbb{L}}^{\mathbb{K}}(\tau'(\alpha)) = 0$ and $\tau'(\alpha) \in \tau''(\mathbb{M})$ which is normal over $\mathbb{K}$.
Therefor $N_{\mathbb{L}}^{\mathbb{K}}$ splits in $\tau''(\mathbb{M})$
and $\{\beta \in \overline{\mathbb{K}} \mid N_{\mathbb{L}}^{(\mathbb{K})}(\beta)\} \subset \tau''(\mathbb{M})$
We get $\tau'(\mathbb{L}^n) \subset \tau''(\mathbb{M})$
and $\tau''^{-1} \circ \tau' : \mathbb{L}^n \to \mathbb{M}$.

Note

You could consider all algebraic extensions of $\mathbb{K}$ as sub-extension of $\overline{\mathbb{K}}$ and consider only sub extensions of $\overline{\mathbb{K}}$

4) Galois extensions

As before $\overline{\mathbb{K}}$ is an algebraic closure of a field $\mathbb{K}$
The Galois extensions are the one for which the Galois groups behaves as expected.

Definition

An algebraic extension $\mathbb{L}/\mathbb{K}$ is said to be Galois iff it is separable and normal

Examples

1) Let $\mathbb{K}^s = \{\alpha \in \overline{\mathbb{K}} \mid \alpha$ is separable over $\mathbb{K}\}$
$\mathbb{K}^s$ is called a separable closure of $\mathbb{K}$

- $\mathbb{K}^s/\mathbb{K}$ is separable
- Let $\alpha \in \mathbb{K}^s$, $\Pi_\alpha^{\mathbb{K}}$ is separable
  $\{\beta \in \mathbb{K} \mid \Pi_\alpha^{\mathbb{K}}(\beta) = 0\} \subset \mathbb{K}^s$
  Thus $\mathbb{K}^s$ is the splitting field of the set of irreducible separable polynomials in $\mathbb{K}[X]$.
  $\mathbb{K}^s/\mathbb{K}$ is normal.

2) If $\mathrm{char}(\mathbb{K}) = 0$ Galois $\Leftrightarrow$ normal
3) If $P \in \mathbb{Q}[X]$ $\mathbb{K}_P/\mathbb{Q}$ is Galois !
4) If $\mathbb{K}$ is finite any extension of $\mathbb{K}$ is Galois.

Proposition

$\mathbb{M}/\mathbb{K}$ an extension
Let $\mathbb{L}$ and $\mathbb{L}'$ be subextensions of $\mathbb{M}$
If $\mathbb{L}/\mathbb{K}$ and $\mathbb{L}'/\mathbb{K}$ then Galois
so are $\mathbb{L} \cap \mathbb{L}'/\mathbb{K}$ and $\mathbb{L}\mathbb{L}'/\mathbb{K}$.

It follows from the corresponding result for Galois and normal extensions.

Lecture 4

Proposition

If $\mathbb{L}/\mathbb{K}$ is a separable extension
$\mathbb{L}^n/\mathbb{K}$ is a Galois extension.

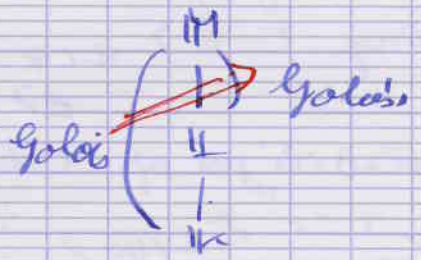
Proof

$\mathbb{L}^n = \mathbb{K}(\{\beta \in \mathbb{L}^n \mid \exists \alpha \in \mathbb{L},\ \underbrace{\Pi_{\mathbb{K}}^{\alpha}(\beta)}_{\text{separable}}\})$
Thus $\mathbb{L}^n/\mathbb{K}$ is separable. □

Lecture 4

Proposition

If M / L / K are algebraic extensions and M / K is Galois then M / L is Galois



⚠ Warning (Reminder): only true implication in that setting.

Proof

- Done: separable
- If M is the splitting field of $(H_i)_{i \in I}$ / K it is — of $(H_i)_{i \in I}$ / L.

Lecture 6

5| Galois groups

Definition

Let L / K be a Galois extension (finite or infinite). Then the Galois group of L / K is the automorphism group of the K-extension L

Proposition

If L / K is Galois; let $\tau_0 \in \Sigma_{L/K}$, the map

$$\mathrm{Gal}(L/K) \to \Sigma_{L/K}, \quad \sigma \mapsto \tau_0 \circ \sigma$$

is a bijection; In particular if L / K is Galois and finite $\#\,\mathrm{Gal}(L/K) = [L : K]$

Proof

- $\mathrm{Gal}(L/K) \times \Sigma_{L/K} \longrightarrow \Sigma_{L/K}$
  $(\sigma, \tau) \longmapsto (\tau \circ \sigma^{-1})$
  is an action of $\mathrm{Gal}(L/K)$ on the set $\Sigma_{L/K}$
- Since any $\tau \in \Sigma_{L/K}$ is injective
  $\tau \circ \sigma^{-1} = \tau \Rightarrow \sigma = \mathrm{Id}_L$
  So the stabilizer of τ is trivial.
- If $\tau, \tau' \in \Sigma_{L/K}$, $\tau(L) = \tau'(L)$
  $\tau'^{-1} \circ \tau \in \mathrm{Gal}(L/K)$
  and $\tau \circ (\tau'^{-1} \circ \tau)^{-1} = \tau'$

Therefore there is exactly one orbit.
(the action of $\mathrm{Gal}(L/K)$ on $\Sigma_{L/K}$ is simply transitive).
About the last statement
- $\#\mathrm{Gal}(L/K) = [L:K]_s = [L:K]$. □

Fundamental theorem of Galois theory

Let M/K be a finite Galois extension.
Then the map

$$\{L \text{ subextension of } M\} \longrightarrow \{H \text{ subgroup of } \mathrm{Gal}(M/K)\}$$
$$M^H \longleftarrow H$$
$$L \longmapsto \mathrm{Gal}(M/L)$$

is a bijection, strictly decreasing for the order of inclusion. (It reverses the inclusions)
Moreover L/K is Galois iff $\mathrm{Gal}(M/L) \triangleleft \mathrm{Gal}(M/K)$
"normal" "normal"
And in that case the restriction induces

$$\mathrm{Gal}(M/K) \longrightarrow \mathrm{Gal}(L/K)$$
$$\sigma \longmapsto \sigma_{|L}$$

and a group isomorphism
$$Gal(M/K)/Gal(M/L) \xrightarrow{\sim} Gal(L/K)$$

We get a complete dictionnary between group and field extensions

Dictionnary

Fields	Groups
subextension of M	subgroup of G
L/K Galois	$H \lhd G$
$L \cap L'$	$\langle H, H' \rangle$
$L L'$	$H \cap H'$
$[M:L]$	$\# H$
$[L:K]$	$[Gal(M/K) : H]$

Let's start the proof of the theorem with a few remarks

Remarks

- M/K Galois $\Rightarrow$ M/L Galois and $Gal(M/L) = \{\sigma \in Gal(M/K) \mid \sigma_{|L} = Id_L\}$ is a subgroup of $Gal(M/K)$.
- for $H \subset Gal(M/K)$
$$M^H = \{m \in M \mid \forall h \in H,\ h(m) = m\} \subset M$$
subextension.

So both maps are well defined

- By definition they are both decreasing
- $\# Gal(M/L) = [M:L]$

So these maps are strictly decreasing and therefore injective.

We want to prove that the composite maps

are the identity maps.

Lemma

If M/L is a Galois extension, then $M^{Gal(M/L)}$ is the image of L in M

Proof

Fix an algebraic closure $\overline{L}$ of L.

Let $\alpha \in M^{Gal(M/L)}$, By proposition 1 for any $\sigma, \sigma' \in \Sigma_{M/L}$, $\sigma(\alpha) = \sigma'(\alpha)$

Since

$$\Sigma_{M/L} \xrightarrow{\text{surj}} \Sigma_{L(\alpha)/L} \xrightarrow{\text{bij}} \{\beta \in \overline{L} \mid \Psi_\alpha^L(\beta) = 0\}$$
$$\sigma \longmapsto \sigma(\alpha)$$

is surjective, Ψ_α^L has a single root in $\overline{L}$

Since α is separable over L, $\deg \Psi_\alpha^L = 1$, ie $\alpha \in L$. ☐

Theorem (Artin)

Let M be a field and let G be a finite subgroup of the automorphism group of the field M and let

$$L = M^G$$

Then M/L is a Galois extension and

$$Gal(M/L) = G.$$

In particular $[M : L] = \#G$

Remark

This completes the proof of the bijection in the fundamental theorem of Galois theory.

Proof of Artin's theorem.

- Let $\alpha \in M$ and let $G.\alpha$ be the orbit of α under the action of G.

We define

$$P_\alpha = \prod_{\beta \in G.\alpha} (X - \beta) \in \mathbb{M}[X]$$

G acts on $\mathbb{M}(X)$ by $\sigma \left(\sum_{i \in \mathbb{N}} a_i X^i \right) = \sum_{i \in \mathbb{N}} \sigma(a_i) X^i$
for $\sigma \in G$ and $\sum_{i \in \mathbb{N}} a_i X^i \in \mathbb{M}[X]$.

$$\mathbb{M}[X]^G = \left\{ \sum_i a_i X^i \in \mathbb{M}[X] \mid \forall \sigma \in G, \forall i \in \mathbb{N}, \sigma(a_i) = a_i \right\}$$
$$= \mathbb{L}[X].$$

Here $\sigma(P_\alpha) = \prod_{\beta \in G.\alpha} (X - \sigma(\beta)) = P_\alpha$

$\sigma \mapsto \sigma(\beta)$ is a bijection of $G.\alpha$

Thus $P_\alpha \in \mathbb{L}[X]$ and $P_\alpha(\alpha) = 0$.

- $P_\alpha^{\mathbb{K}} \mid P_\alpha$ the roots of which are simple
  Thus α is separable / $\mathbb{L}$.
- $\mathbb{M}$ is the splitting field of $(P_\alpha)_{\alpha \in \mathbb{M}}$
  So $\mathbb{M}/\mathbb{L}$ is Galois.
- $G \subset Gal(\mathbb{M}/\mathbb{L})$ by definition of $\mathbb{L}$
  For any $\alpha \in \mathbb{M}$,
  $$[\mathbb{L}(\alpha) : \mathbb{L}] \leq \deg(P_\alpha^{\mathbb{K}}) \leq \deg(P_\alpha) \leq \#G.$$

Then we can apply we used to prove that the degree of the field extension for a morphism of Riemann surfaces is the degree of the morphism.

Let $\mathbb{L} \subset \mathbb{L}' \subset \mathbb{M}$ be a subfield of $\mathbb{M}$.
If $\mathbb{L}'/\mathbb{L}$ is finite, it is separable
and thus $\exists \alpha \in \mathbb{L}'$ such $\mathbb{L}' = \mathbb{L}(\alpha)$
and $[\mathbb{L}' : \mathbb{L}] \leq \#G$.
As before we conclude (since $\mathbb{M}/\mathbb{L}$ is algebraic)
that $[\mathbb{M} : \mathbb{L}] \leq \#G$.

Therefore $\# Gal(M/L) = [M:L] \leq \# G$
and $G = Gal(M/L)$. □

If we want to prove the converse for normal subgroups

Lemma

Let M/K be a Galois extension
Let L be a subextension of M
and let $\sigma \in Gal(M/K)$.
Then

$$Gal(M/\sigma(L)) = \sigma\, Gal(M/L)\, \sigma^{-1}$$

Proof

$Gal(M/L) = \{ g \in Gal(M/K) \mid g_{|L} = Id_L \}$
and $g_{|L} = Id_L \iff \sigma g \sigma^{-1}_{|\sigma(L)} = Id_{\sigma(L)}$. □

End of the proof of the fundamental theorem

- Assume L/K is Galois
  Choose $\tau_0 \in \Sigma_{M/L}$
  Since L/K is normal,
  $\forall \sigma \in Gal(M/K)$, $\underbrace{\tau_0 \circ \sigma_{|L}}_{\in \Sigma_{L/K}}(L) = \tau_{0|L}(L)$
  Since τ_0 is injective, we get $\Sigma_{L/K}$-that
  $\forall \sigma \in Gal(M/K)$, $\sigma(L) = L$
  and by the lemma, $Gal(M/L)$ is normal in $Gal(M/K)$
- If $Gal(M/L)$ is normal in $Gal(M/K)$
  then by the lemma and the bijectivity,
  $(*)$ $\forall \sigma \in Gal(M/K)$, $\sigma(L) = L$.
  Let $\sigma, \sigma' \in \Sigma_{L/K}$ Choose $\tau, \tau' \in \Sigma_{M/K}$

such that $\tau_{|L} = \sigma$ and $\tau'_{|L} = \sigma'$, $\tau'(M) = \tau(M)$

$\tau' \circ \tau \in Gal(M/K)$

$\sigma'(L) = \tau'(L) = \tau'(\tau^{-1} \circ \tau(L)) = \tau(L) = \sigma(L)$

$\tau^{-1}(L)$

Thus L/K is normal

Since M/K is separated so is L/K

thus L/K is Galois

o Assume that L/K is Galois

We have a morphism of groups

$Rés : Gal(M/K) \longrightarrow Gal(L/K)$

$\sigma \longmapsto \sigma_{|L}$

By definition, its kernel is $Gal(M/L)$

It remains to prove that it is surjective which follows from the following statement:

Proposition

Let M/K be a Galois extension and let L be a subextension of M

For any morphism $\varphi : L \to M$ of K extensions there exists $\sigma \in Gal(M/K)$ such that $\sigma_{|L} = \varphi$.

Proof

Choose $\tau_0 \in \Sigma_{M/K}$,

$\tau_0 \circ \varphi : L \to \overline{K}$

extends to $\tau' \in \Sigma_{M/K}$, $\tau'_{|L} = \tau_0 \circ \varphi$

Since M/K is Galois $\tau'(M) = \tau_0(M)$

and $\sigma = \tau_0^{-1} \circ \tau' \in Gal(M/K)$

satisfies $\sigma_{|L} = \varphi$. □

Corollary 1

Let M/K be a Galois extension and let $\alpha \in M$, then

$$Gal(M/K)\cdot\alpha = \{\beta \in M \mid P_\alpha^K(\beta) = 0\}$$

Proof

$\subset$ $\forall \sigma \in Gal(M/K)$ $\quad P_\alpha^K(\sigma(\alpha)) = 0$

$\supset$ Let β be a root of P_α^K in M

$$\begin{array}{ccc} \varphi: K(\alpha) & \xrightarrow{\sim} & K(\beta) \\ & \nwarrow \quad \nearrow & \\ & K[X]/(P_\alpha^K) & \end{array}$$

φ extends to $\sigma \in Gal(M/K)$. $\square$

Reminder

P_α^K splits in M since M/K is normal and in $M[X]$

$$P_\alpha^K = \prod_{\{\beta \in M \mid P_\alpha^K(\beta) = 0\}} (X - \beta)$$

(P_α^K has simple roots α separable $/K$)

Corollary 2

Let M/K be a finite Galois extension. Then for any $\alpha \in M$

$$\chi_\alpha^K = \prod_{\sigma \in Gal(M/K)} (X - \sigma(\alpha))$$

$$Tr_{M/K}(\alpha) = \sum_{\sigma \in Gal(M/K)} \sigma(\alpha)$$

$$N_{M/K}(\alpha) = \prod_{\sigma \in Gal(M/K)} \sigma(\alpha)$$

Proof

$$\chi_\alpha^{\mathbb{K}} = \left(\prod_{\beta \in \mathbb{M} \mid N_\alpha^{\mathbb{K}}(\beta) = \alpha} (X - \beta) \right)^{[\mathbb{M} : \mathbb{K}(\alpha)]}$$

$$= \left(\prod_{\beta \in Gal(\mathbb{M}/\mathbb{K}).\alpha} (X - \beta) \right)^{\#Gal(\mathbb{M}/\mathbb{K})_\alpha}$$

Where

$$Gal(\mathbb{M}/\mathbb{K})_\alpha = \{ \sigma \in Gal(\mathbb{M}/\mathbb{K}),\ \sigma(\alpha) = \alpha \}$$
$$= Gal(\mathbb{M}/\mathbb{K}(\alpha))$$

But

$$\sigma(\alpha) = \sigma'(\alpha) \Leftrightarrow \sigma'^{-1} \circ \sigma \in Gal(\mathbb{M}/\mathbb{K})_\alpha.$$

The proof of the other assertions is similar. □

Examples

a) (Reminder)

Cyclotomic extension

ξ primitive n^{th} root of 1

$Gal(\mathbb{Q}(\xi)/\mathbb{Q}) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^*$

b) **Finite fields**

Let $\mathbb{K}$ be a finite field

and let $\mathbb{L}$ be a finite extension of $\mathbb{K}$

We put $d = [\mathbb{L} : \mathbb{K}]$ $(\#\mathbb{L} = \#\mathbb{K}^d)$

Theorem told you that $\mathbb{L}/\mathbb{K}$ is Galois

Proposition

$Gal(\mathbb{L}/\mathbb{K})$ is cyclic generated by

$$Fr_{\#\mathbb{K}} : \mathbb{L} \longrightarrow \mathbb{L}$$
$$x \longmapsto x^{\#\mathbb{K}}$$

Proof

- Let $p = \operatorname{char} \mathbb{K}$, $\#\mathbb{K}$ is a power of p

and $Fr_{\#\mathbb{K}} = (Fr_p)^q$ is an automorphism of $\mathbb{L}$

$\forall x \in \mathbb{K}$, $x^{\#\mathbb{K}} = x$ then $Fr_{\#\mathbb{K}|\mathbb{K}} = Id_{\mathbb{K}}$ and therefore $Fr_{\#\mathbb{K}} \in Gal(\mathbb{L}/\mathbb{K})$.

- Since $Fr_{\#\mathbb{L}} = Id_{\mathbb{L}}$, $(Fr_{\#\mathbb{K}})^d = Id_{\mathbb{L}}$.

More generally if $1 \leq k \leq d$

$$\mathbb{L}^{(Fr_{\#\mathbb{K}})^k} = \{x \in \mathbb{L} \mid x^{(\#\mathbb{K})^k} = x\}$$

is a subfield of $\mathbb{L}$ of cardinal $\leq \#\mathbb{K}^k$ and is $\neq \mathbb{L}$ if $k < d$

Thus $\mathrm{ord}_{Gal(\mathbb{L}/\mathbb{K})}(Fr_{\#\mathbb{K}}) = d$. □

Important remark

Let A be an integral domain
Let $\mathbb{K} = Fr(A)$ and let $\mathbb{L}$ be a Galois extension of $\mathbb{K}$
Let B be the integral closure of $\mathbb{K}$
then

$$\forall \sigma \in Gal(\mathbb{L}/\mathbb{K}),\ \sigma(B) = B$$

Therefore the Galois group acts on all sets related to the ring B like the set of invertible elements in B or the set of prime ideals in B.

III Dedekind rings

1) Localization of rings

Definition

Let A be a commutative ring and let $S \subset A$ be such that

$\forall x, y \in S, \quad xy \in S ; \quad 1 \in S$

On $A \times S$ we define two internal laws $+, \times$ by $(a,s) + (a',s') = (as' + a's, ss')$ and $(a,s) \times (a',s') = (aa', ss')$ and an equivalence relation

$(a,s) \sim (a',s') \Leftrightarrow \exists s'' \in S, \; as's'' = a'ss''$

For $a, a' \in A$ and $s, s' \in S$.

Then $+, \times$ are compatible with $\sim$ and the quotient $A \times S / \sim$ equipped with the induced laws $+, \times$ and the map

$$\varphi : A \to A \times S / \sim$$
$$a \mapsto \overline{(a,1)}$$

is a commutative A-algebra called the localization of A at S and is denoted by $A[S^{-1}]$

For $(a,s) \in A \times S$, we write $\frac{a}{s} = \overline{(a,s)}$

Proof

See the construction of $\mathbb{Q}$:

$\sim$ is transitive

$$(a_1, s_1) \sim (a_2, s_2) \sim (a_3, s_3)$$

Choose s', s'' so that

$$a_1 s_2 s' = a_2 s_1 s' \quad \text{and} \quad a_2 s_3 s'' = a_3 s_2 s''$$

Then $a_1 s_3 \times \underbrace{s_2 s' s''}_{\in S} = a_2 s_1 s_3 s' s'' = a_3 s_1 \times s_2 s' s''$

ν is compatible with $+$

$(a_1, s_1) \nu (a_2, s_2)$ $(a_1', s_1') \nu (a_2', s_2')$

Choose $s, s' \in S$ such that

$a_1 s_2 s = a_2 s_1 s$ and $a_1' s_2' s' = a_2' s_1' s'$

$(a_1 s_1' + a_1' s_1) s_2 s_2' s s' = (a_2 s_2' + a_2' s_2) s_1 s_1' s s'$

□

Remarks

- $g(a) = 0$ iff $\exists s \in S \mid as = 0$

  Indeed $(a, 1) \nu (0, 1) \Leftrightarrow \exists s \in S \quad as = 0s = 0$

- In particular

  $A[S^{-1}] = \{0\} \Leftrightarrow g(1) = 0$

  iff $0 \in S$.

- If A is an integral domain and $0 \notin S$, then g is injective

  In fact $A[S^{-1}]$ is then isomorphic to

  $\{x \in Fr(A) \mid \exists s \in S, \ xs \in A\}$

  $= "A[S^{-1}]"$ the subalgebra of $Fr(A)$ generated by S^{-1}

Examples

a) If A is an integral domain

$Fr(A) = A[(A - \{0\})^{-1}]$

b) If A is an integral domain $x \in A - \{0\}$

$A\left[\frac{1}{x}\right] = A\left[\{x^n, n \in \mathbb{N}\}^{-1}\right]$

c) If A is a commutative ring and p a prime ideal of A

By definition of a prime ideal $S = A - p$ satisfies $\forall x, y \in S, \ xy \in S$.

$A_{(p)} = A[(A-p)^{-1}]$ is called the "localization at p" of A.

Particular cases

- Let Ω be a non-empty connected subset of $\mathbb{C}$ and let $p \in \Omega$.
  Let $\mathcal{H}(\Omega)$ be the ring of holomorphic functions
  $$ev_p : \mathcal{H}(\Omega) \to \mathbb{C}, \quad f \mapsto f(p)$$
  is a surjective map of $\mathbb{C}$-algebras and $\mathfrak{p} = \ker(ev_p)$ is a prime (in fact maximal) ideal in $\mathcal{H}(\Omega)$. $\mathcal{H}(\Omega)_{\mathfrak{p}} = \mathcal{H}(\Omega)_{(p)}$ may be identified with the ring of meromorphic functions on Ω which are holomorphic in a neighbourhood of p (But this neighbourhood is not fixed.)
- Let $\mathbb{K}$ be a field and $f_1, \dots, f_m \in \mathbb{K}[X_1, \dots, X_n]$. Let $A = \mathbb{K}[X_1, \dots, X_n]/(f_1, \dots, f_m)$ and let $\mathbb{L}$ be a $\mathbb{K}$ extension.
  Remember
  $$\underset{\mathbb{K}\text{-Alg}}{\mathrm{Mor}}(A, \mathbb{L}) \overset{\text{bij}}{\leftrightarrow} \{(\lambda_1, \dots, \lambda_n) \in \mathbb{L}^n \mid f_i(\lambda_1, \dots, \lambda_n) = 0 \text{ for } i \in \{1, \dots, m\}\}.$$
  $$\| \quad V(\mathbb{L})$$
  fix $(\lambda_1, \dots, \lambda_n) \in V(\mathbb{L})$ the corresponding morphism is $A \xrightarrow{\varphi} \mathbb{L}$ is a morphism of $\mathbb{K}$-algebras
  $$\overline{g} \mapsto g(\lambda_1, \dots, \lambda_n)$$
  $\ker(\varphi)$ is a prime ideal in A.

(Exercice : Any prime ideal in A may be described in that way for a well chosen $\mathbb{K}$ and φ).

$A_p = A_{(p)}$: "rational functions on V defined at p". geometric object.

Proposition 1

Let A be a commutative ring and $S \subset A$ such that $\forall x, y \in S$, $xy \in S$, $1 \in S$. Let $\varphi : A \to A[S^{-1}]$ be the structural morphism. The map $J \mapsto \varphi^{-1}(J)$ induces a bijection from the set of ideals of $A[S^{-1}]$ to the set of ideals I of A such that

$\forall a \in A, \forall s \in S, \quad sa \in I \Rightarrow a \in I$.

Proof

- Let J be an ideal of $A[S^{-1}]$ and $I = \varphi^{-1}(J)$, then I is an ideal of A (general property for ring morphisms)

  If $a \in A$, $s \in S$ if $sa \in I$

  $\varphi(sa) = s\,\varphi(a) \in J$

  $\varphi(a) = s^{-1}(s\,\varphi(a)) \in J \Rightarrow a \in I$.

- Let I be as above, and let J be the ideal of $A[S^{-1}]$ generated by $\varphi(I)$

  $I \subset \varphi^{-1}(J)$

  Let $a \in \varphi^{-1}(J)$

  We may write $\varphi(a) = \sum_{i=1}^{n} \frac{\varphi(a_i)}{s_i}$

  with $a_1, \dots, a_n \in I$ and $s_1, \dots, s_n \in S$.

  Then $\varphi(a) = \sum_{i=1}^{n} \varphi\left(a_i \prod_{j \neq i} s_j\right) \Big/ \prod_{i=1}^{n} s_i$

ie $(a,1) \sim \left(\sum_{i=1}^{n} a_i \prod_{j\neq i} s_j, \prod_{i=1}^{n} s_i\right)$

ie $\exists\, s \in S$, $a \prod_{i=1}^{n} s_i \cdot s = \left(\sum_{j=1}^{n} a_i \prod_{j\neq i} s_j\right) s \in I$

Thus $a \in I$.

$$I = g^{-1}(J)$$

- Let J be an ideal of $A[S^{-1}]$ let $I = g^{-1}(J)$

$$J \supset g(I)$$

and thus contains the ideal generated by $g(I)$

Let $a \in J$ we may write as $\frac{g(a)}{s}$

for $a \in A$ and $s \in S$, $g(a) = s\,\frac{g(a)}{s} \in J$

thus $a \in I$ and J is the ideal generated by $g(I)$. □

Reminder (general property of commutative rings)

Let A and B be commutative rings and $g : A \to B$ a morphism of rings that $\mathfrak{p}$ be a prime ideal of B

Then $g^{-1}(\mathfrak{p})$ is a prime ideal of A

Proof

$A/g^{-1}(\mathfrak{p}) \hookrightarrow B/\mathfrak{p}$ integral domain

Proposition 2

The bijection of proposition 1 induces a bijection from the set of prime ideals of $A[S^{-1}]$ to the set of prime ideals of A

$S \cap \mathfrak{p} = \emptyset$

Reminder

The spectrum of A

$\mathrm{Spec}(A) = \{$ prime ideals of $A\}$

is equipped with the Zariski topology defined by its closed subsets of the form

$$V(X) = \{\mathfrak{p} \in \mathrm{Spec}(A) \mid \forall x \in X,\ x \in \mathfrak{p}\}$$

for $X \subset A$.

We get a bijection

$$\mathrm{Spec}(A[S^{-1}]) \leftrightarrow \bigcup_{a \in S} \underbrace{\mathrm{Spec}(A) - V(a)}_{\text{open in } A.}$$

and $A[S^{-1}]$ may be thought as the "union" of the rings of functions on these open subset.
(hence the terminology of localization)

Proof

- Let $\mathfrak{p}$ be a prime ideal of A
  If $\forall a \in A, \forall s \in S \quad as \in \mathfrak{p} \Rightarrow a \in \mathfrak{p}$
  then (since $1 \notin \mathfrak{p}$), $S \cap \mathfrak{p} = \emptyset$
  Conversely if $S \cap \mathfrak{p} = \emptyset$
  $\forall a \in A, \forall s \in S, \ as \notin \mathfrak{p} \Rightarrow a \in \mathfrak{p}$.
- Let $\mathfrak{p}$ be as above, and $\mathfrak{q}$ be the ideal of $A[S^{-1}]$ generated by $\varphi(\mathfrak{p})$
  Let $\overline{S}$ be the image of S in $A/\mathfrak{p}$
  The morphism

$$A/\mathfrak{p} \longrightarrow A[S^{-1}]/\mathfrak{q}$$

induces an isomorphism

$$A[S^{-1}]/\mathfrak{q} \cong A/\mathfrak{p}\,[\overline{S}^{-1}]$$

$$\subset Fr(A/\mathfrak{p})$$

and thus $\mathfrak{q}$ is a prime ideal of $A[S^{-1}]$. □

Corollary 1

The bijection of proposition 2 defines a bijection from $Spec(A_{(p)})$ to $\{q \in Spec(A) \mid q \subset p\}$

Proof

$A - p \cap q = \emptyset \iff q \subset p$

Example

p prime in $\mathbb{Z}$

The ideals in $\mathbb{Z}_{(p)}$ are $\{0\}$, $p\mathbb{Z}_{(p)}$ and $\mathbb{Z}_{(p)}$

Definition

A commutative ring is said to be <u>local</u> iff it has a unique maximal ideal

Corollary 2

$A_{(p)}$ is local with maximal ideal $pA_{(p)}$

2) Noetherian rings and modules

Definition / Proposition

Let A be a ring (not necessarily commutative)

Let M be an A-module.

Then M is <u>noetherian</u> iff it satisfies the following equivalent statements

(i) Any **sub-module** of M is of finite type

(ii) Any increasing sequence of submodules of M is stationnary

(iii) Any non empty set of submodules

If of M has a maximal element

Proof -

(i) $\Rightarrow$ (ii)

Let $(M_i)_{i \in \mathbb{N}}$ be an increasing sequence of submodules of M

$N = \bigcup_{i \in \mathbb{N}} M_i$ is a submodule of M

submodule generated by

$N = Mod(a_1, \dots, a_n)$, $a_i \in N$.

for $i \in \{1, \dots, n\}$, there exists $m_i \in \mathbb{N}$ such that $a_i \in M_{m_i}$

Let $m = \max\{m_1, \dots, m_n\}$

and $n \geq m$

$N \subset M_m \subset M_n \subset N$.

(ii) $\Rightarrow$ (iii)

Let X be a non-empty set of submodules of M which has no maximal element

for ~~Every submodule~~ $N \in X$ there exists $N' \in X$ such that $N \subsetneq$

so we may construct a strictly increasing sequence of elements of X

absurd. ↯

(iii) $\Rightarrow$ (i)

Let N be a submodule of M and let X be the set of finitely generated submodules of N

Let N' be a maximal element in X

it is a submodule of N
it is generated by a finite set $\{x_1, \dots, x_m\}$
Let $x \in N$
$N' \subset \mathrm{Mod}(x, x_1, \dots, x_m) \in X$
Since N' is maximal
$N' = \mathrm{Mod}(x, x_1, \dots, x_m)$
and $x \in N'$
Thus
$$M \subset N'. \quad \square$$

Def
A ring is noetherian if it is noetherian as an A-module.

Remark
If A is commutative this means that assertions (i) – (iii) apply to the ideals of A.

Example
Proposition
Let M be an A-module and N be a submodule of M. M is noetherian if and only if N and M/N are noetherian

Proof
$\Rightarrow$) submodules of N are submodules of M and there is an increasing bijection from the submodules of M containing N and the submodules of M/N.

For the converse let us prove the following

Lemma

Let M be a A-module, let N, P and Q be submodules of M such that $P \subset Q$,

$$N \cap P = N \cap Q \text{ and } N + P = N + Q$$

then

$$P = Q.$$

Proof.

Let $x \in Q$ $\quad x \in N + Q = N + P$.

Therefore $x = n + p$ with $n \in N$, $p \in P \subset Q$

$$n \in N \cap Q = N \cap P$$

we get $x \in P$. □

Proof of $\Leftarrow$)

Let (P_n) be an increasing sequence of submodules of M,

Let $P'_n = N \cap P_n$, $P''_n = N + P_n / N$ for $n \in \mathbb{N}$

There exists n_0 (resp n_1) such that

$$P'_n = P'_{n_0} \text{ for } n \geq n_0$$

(resp. $P''_n = P''_{n_1}$ for $n \geq n_1$)

let $m = \max(n_0, n_1)$

for $n \geq m$ one has

$$\begin{cases} N \cap P_n = N \cap P_m \\ N + P_n = N + P_m \\ P_n \supseteq P_m \end{cases}$$

Apply the lemma, we get $P_n = P_m$. □

Corollary 1

Let M be a A-module and let $(M_i)_{i \in I}$ be a finite family of submodules of M

a) If M_i is noetherian for $i \in I$, so is $\sum_{i \in I} M_i$

b) if M/M_i is noetherian for $i \in I$ so is $M / \bigcap_{i \in I} M_i$.

Proof

By induction on $\# I$ it is enough to prove it for $I = \{1, 2\}$.

$$(M_1 + M_2)/M_1 \simeq M_2 / M_1 \cap M_2$$

a) $(M_1 + M_2)/M_1$ and M_1 are noetherian so is $M_1 + M_2$

b) M/M_2 and $M_2 / M_1 \cap M_2$ are noetherian

$\Downarrow$

$$\left(M / M_1 \cap M_2\right) / \left(M_2 / M_1 \cap M_2\right)$$

□

Corollary 2

Let $(M_i)_{i \in I}$ be a finite family of noetherian A-modules

$\bigoplus_{i \in I} M_i$ is noetherian.

Corollary 3

Let A be a noetherian ring.

Any A-module of finite type is noetherian.

Proof

It is a quotient of A^n. □

Example
Any principal ring is noetherian.

Theorem (Hilbert)
If A is a commutative noetherian ring so is $A[T]$

Proof
Let I be an ideal of $A[T]$

$$\varphi_n : A[T] \longrightarrow A \quad \text{morphism}$$
$$\sum_{n\in\mathbb{N}} a_n T^n \mapsto a_n$$

of A-modules, $A[T]_n = \{P \in A[T] \mid \deg P \leq n\}$

Since $TI \subset I$ we have that $(\varphi_n(I \cap A[T]_n))_{n\in\mathbb{N}}$ is an increasing sequence of ideals

Let $N \in \mathbb{N}$ be such that

$$a_n = a_N \quad \text{for } n \geq N.$$

The ideals a_N are of finite type.

Choose $r_0, \dots, r_N$, $f_{i,j} \in I$ for $0 \leq i \leq N$, $1 \leq j \leq r_i$ such that

(i) $\deg f_{i,j} = i$

(ii) $a_i = (\varphi_i(f_{i,1}), \dots, \varphi_i(f_{i,r_i}))$

for $i \in \{0, \dots, N\}$

Let us prove that

$$I = (f_{i,j} \;\; 0 \leq i \leq N, \; 1 \leq j \leq r_i)$$

It is enough to prove that for $d \in \mathbb{N}$,

$$I \cap A[T]_d \subset (f_{i,j} : 0 \leq i \leq N, \; 1 \leq j \leq r_i) + I \cap A[T]_{d-1}$$

Let $\sum_{i=1}^{r_N} b_j f_{d-N,j} = T^{d-N} f_{d-N,i}$ for $1 \leq j \leq r_N$ if $d \geq N$

enough to prove
$I \cap A[T]_d = \mathrm{Mod}_A(f_{d,j};\ 1 \le j \le n_d) + I \cap A[T]_{d-1}$
Let $f \in I \cap A[T]_d$

$$\varphi_d(f) = \sum_{j=1}^{n_d} \lambda_j \varphi_j(f_{d,j})$$

$$f - \sum_{j=1}^{n_d} \lambda_j f_{d,j} \in I \cap A[T]_{d-1} \quad . \square$$

Proposition

Let A be a noetherian ring and let $\varphi : A \to B$ be a surjective morphism of rings then B is noetherian.

Proof

$J \mapsto \varphi^{-1}(J)$ is an increasing bijection from the set of left ideals of B to the set of left ideals of A containing $\ker(\varphi)$ (left ideal of A = A-submodule of A). $\square$

Corollary

Let A be a commutative noetherian ring and let B be a finitely generated A-algebra then B is noetherian.

Proof

B is a quotient of $A[X_1, \dots, X_n]$. $\square$

Proposition

Let A be a commutative noetherian ring and let $S \subset A$ be such that $\forall x, y \in S \; xy \in S$. Then $A[S^{-1}]$ is noetherian.

Proof

Follows from the description of ideals of $A[S^{-1}]$. □

3) Application to integral closure

I read a few additional results about trace forms and separable extensions.

Proposition

Let L/K be a separable extension and $\overline{K}$ be an algebraic closure of K. Then for any $\alpha \in L$

$$\mathrm{Tr}_{L/K}(\alpha) = \sum_{\sigma \in \Sigma_{L/K}} \sigma(\alpha).$$

Proof

- If $L = K(\alpha)$, $\Sigma_{L/K} \longrightarrow \{\beta \in \overline{K} \mid \mu_\alpha^K(\beta) = 0\}$, $\sigma \longmapsto \sigma(\alpha)$ is bijective and the formula is true.
- In general

$$\mathrm{Res}: \Sigma_{L/K} \longrightarrow \Sigma_{K(\alpha)/K}, \quad \sigma \longmapsto \sigma_{|K(\alpha)}$$

is surjective and all the fibres have

corollaire $[L : K(\alpha)]_s = [\Omega : K(\alpha)]$

and

$$\sum_{\iota \in E} \left(\mathrm{Tr}_{\Omega/\iota K}(\alpha) \right) = [L : K(\alpha)] \sum_{\beta \in \{\beta \in \iota K \mid N_{\iota K}^{K}(\beta) = 0\}} \beta$$

$$= [L : K(\alpha)] \sum_{\sigma \in \Sigma_{K(\alpha)/K}} \sigma(\alpha)$$

$$= \sum_{\sigma \in \Sigma_{L/K}} \sigma(\alpha). \quad \square$$

Proposition (linear independance of characters)

Let G be a group and let K be a field

$$\mathrm{Hom}_{\mathrm{Grp}}(G, K^*)$$

seen as a subset of K^G is free over K

Proof

Take a non trivial relation

$$\lambda_1 \chi_1 + \cdots + \lambda_n \chi_n = 0$$

with $\chi_1, \ldots, \chi_n \in \mathrm{Hom}_{\mathrm{Grp}}(G, K^*)$, $(\lambda_1, \ldots, \lambda_n) \in K^n$ and n minimal. In particular $\chi_1 \neq \chi_2$ and $\lambda_i \neq 0$

Choose $g \in G$ such that $\chi_1(g) \neq \chi_2(g)$

Since

$$\forall h \in G \quad \lambda_1 \chi_1(h) + \cdots + \lambda_n \chi_n(h) = 0 \quad \times \chi_1(g)$$

one has

$$\forall h \in G \quad \lambda_1 \chi_1(g) \chi_1(h) + \cdots + \lambda_n \chi_n(g) \chi_n(h) = 0 \quad \times 1$$

We get

$$\lambda_2 \underbrace{(\chi_1(g) - \chi_2(g))}_{\neq 0} \chi_2 + \cdots + \lambda_n (\chi_1(g) - \chi_n(g)) \chi_n = 0$$

contradicts the minimality of n thanks to $\square$

Corollary

Let K and L be fields $\mathrm{Hom}_{\mathrm{Field}}(K, L)$ is a free

subset of $\mathbb{L}^{\mathbb{K}}$

Proof
Take $G = \mathbb{K}^\times$. □

Lecture 5

Corollary
Let $\mathbb{L}/\mathbb{K}$ be a finite separable extension of degree d and let $(e_1, \dots, e_d)$ be a basis of $\mathbb{L}$ as a $\mathbb{K}$ vector space
Write $\{\sigma_1, \dots, \sigma_d\} = \Sigma_{\mathbb{L}/\mathbb{K}}$
then
$$\det\left(\sigma_i(e_j)\right)_{1\le i,j\le d} \neq 0$$

Proof
If $\det\left(\sigma_i(e_j)\right)_{1\le i,j\le d} = 0$
there exists $(\lambda_1, \dots, \lambda_d) \in \overline{\mathbb{K}}^d$ such that
$\forall j \in \{1, d\}$ $\sum_{i=1}^{d} \lambda_i \sigma_i(e_j) = 0$
But then $\sum_{i=1}^{d} \lambda_i \sigma_i = 0$ Absurd. □

Formula
Let us keep the notations of the Corollary.
Then the discriminant of the trace form verifies
$$\det\left(\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(e_i e_j)\right)_{1\le i,j\le d} = \left|\det\left(\sigma_i(e_j)\right)_{1\le i,j\le d}\right|^2$$

Proof
Write $U = \left(\sigma_i(e_j)\right)_{1\le i,j\le d}$.
The (i,j) coefficient of ${}^t\!U\,U$ is
$$\sum_{\sigma\in\Sigma_{\mathbb{L}/\mathbb{K}}} \sigma(e_i)\sigma(e_j) = \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(e_i e_j)$$
By the first proposition of § 3. □

Proposition

Let L/K be a finite extension of fields
the following assertions are equivalent
(i) L/K is separable
(ii) The trace form $(x,y) \mapsto Tr_{L/K}(xy)$ is non degenerate
(iii) $Tr_{L/K} \neq 0$ (ie $\exists x \in L$, $Tr_{L/K}(x) \neq 0$).

Proof

(i) $\Rightarrow$ (ii) Formula + corollary
(ii) $\Rightarrow$ (iii)
$\neg$(i) $\Rightarrow$ $\neg$(iii)
Assume that L/K is not separable, $p = char(K) > 0$
Let $\alpha \in L$ let $E = \{ \beta \in \overline{K} \mid \beta \text{ conj. to } \alpha \}$
Write

$$\chi_K(\mu_\alpha^K) = \left(\prod_{\beta \in E} (X - \beta) \right)^{p^r}$$

Then

$$\chi_K\left(Tr_{L/K}(\alpha)\right) = [L : K(\alpha)]\, p^r \left(\sum_{\beta \in E} \beta \right)$$

- If α is separable then
  $p \mid [L : K]_i \mid [L : K(\alpha)]$ and $Tr_{L/K}(\alpha) = 0$
- Otherwise $r \geq 1$ and $Tr_{L/K}(\alpha) = 0$. □

Theorem

Let A be an integral, integrally closed ring.
and let $K = Fr(A)$ and L be a finite extension of K
Let B the integral closure of A
Then if L/K is separable
B is contained in A sub-module of L
which is free of rank $[L : K]$.

Proof -

We have seen that

$$\forall x \in L,\ \exists a \in A,\ ax \in B$$

Thus we may choose a basis $(e_1, \dots, e_d)$ of the K vector space L such that

$$(e_1, \dots, e_d) \in B^d.$$

Since $Tr_{L/K}$ is not degenerate we may find a basis $(f_1, \dots, f_d)$ of L over K such that

$$Tr_{L/K}(e_i f_j) = \delta_{i,j} = \begin{cases} 1 \text{ if } i=j \\ 0 \text{ otherwise} \end{cases}$$

For any submodule M of L let

$$M^* = \{ x \in L \mid \forall y \in M \quad Tr_{L/K}(xy) \in A \}$$

We have

$$\left(\sum_{i=1}^{d} A e_i \right)^* = \sum_{i=1}^{d} A f_i$$

and $\quad M \subset N \Rightarrow N^* \subset M^*$

Therefore

$$(*) \qquad \sum_{i=1}^{d} A f_i \supset B^* \supset B \supset \sum_{i=1}^{d} A e_i \qquad \square$$

↑ Because $Tr_{L/K}(B) \subset A$

Corollary 1

We keep the hypothesis of the theorem

a) If moreover A is noetherian then B is noetherian

b) If A is principal then B is a free A-module of rank d, and any non zero fractional ideal in L is a free A-module of rank d.

Proof -

a) B is an A submodule of an A module

of finite type

b) To prove the statement for B itself we use (*) and the following theorem about principal rings

Theorem (Reminder)

Let A be a principal ring
Let M be a free A-module of rank n
Let N be a submodule of M
Then there exists an integer $r \leq n$,
elements $a_1, \dots, a_r \in A$ with $a_1 | a_2 | \dots | a_r \neq 0$
and a basis $(e_1, \dots, e_r)$ of M such that

$$N = \sum_{i=1}^{r} A\, a_i e_i$$

End of the proof of the Corollary

It remains to prove the statement about the fractional ideals

Let $H \subset L$ be a fractional ideal
Choose $c \in B - \{0\}$ such that $cH \subset B$
and $b \in H - \{0\}$
Then

$$bB \subset H \subset c^{-1}B$$

free of rank d/A

Remark

If $(e_1, \dots, e_d)$ is a basis of H as an A-module

$$D_{L/K}(H) = (\det(\mathrm{Tr}_{L/K}(e_i e_j)))$$

In particular if $(e_1, \dots, e_d)$ is a basis of B as A-module

$$\Delta_{B/A} = (\det(\mathrm{Tr}_{L/K}(e_i e_j))$$

4) Dedekind rings

Definition

A ring A is said to be a Dedekind ring if it is integral (hence commutative), integrally closed, noetherian, and any non zero prime ideal of A is maximal.

Example

Principal rings. We shall see more interesting examples later on.

Definition

(99) Let A be an integral ring and let $K = Fr(A)$ let a, b be fractional ideals in K for A then

$$ab = \left\{ \sum_{i=1}^{n} x_i y_i,\ n \in \mathbb{N},\ (x_1, \dots, x_n) \in a^n, (y_1, \dots, y_n) \in b^n \right\}$$

is a fractional ideal in K for A called the product of a and b

Proof

It is a A-module since it contains 0, is stable by sums and multiplication by elements of A,

Let $\alpha \in A \setminus \{0\}$, $\beta \in A \setminus \{0\}$ such that $\alpha a \subset A$, $\beta b \subset A$ then

$$\alpha \beta ab \subset A. \quad \square$$

Notation

We denote by $\mathcal{F}(A)$ the set of nonzero

fractional ideals in $\mathbb{K}$ for A and by $\mathcal{H}(a)$ the set of nonzero principal fractional ideals.

We equip these sets with the product of ideals.

$\mathcal{P}(A)$ is the set of non zero prime ideals in A.

Remarks

(i) For any $a, b \in \mathbb{K}$,

$$(a).(b) = (ab)$$

↑ product of fractional ideals

(ii) $\mathcal{I}(A)$ is a commutative monoid.

The product is:

a) associative

b) admits A has a unit element

c) commutative.

(100)

Remark

The Krull dimension of a ring A is

$\dim_{Krull}(A) = \min\{r \mid \exists \underbrace{P_0, \dots, P_r}_{r+1} \text{ prime ideals of } A, P_0 \subsetneq P_1 \subsetneq \dots \subsetneq P_r\}$

the last condition of the definition is equivalent to $\dim_{Krull}(A) \leq 1$. ($\dim_{Krull}(A) = 0 \Leftrightarrow A$ is a field)

(eg $(0) \subsetneq (X_1) \subsetneq \dots \subsetneq (X_1, \dots, X_n)$ démontre que $\dim_{Krull}(\mathbb{K}[X_1, \dots, X_n]) \geq n$ en fait elle est egale à n)

Theorem

Let A be a Dedekind ring,

a) For any fractional ideal α for A, there exists a unique map $\mathfrak{P} \mapsto v_{\mathfrak{P}}(\alpha)$ from $\mathcal{P}(A)$ to $\mathbb{Z}$ such that.

(i) $\{ \mathfrak{p} \in P(A) \mid v_{\mathfrak{p}}(\alpha) \neq 0 \}$ is finite

(ii) $\alpha = \prod_{\mathfrak{p} \in P(A)} \mathfrak{p}^{v_{\mathfrak{p}}(\alpha)}$

(b) $\mathcal{I}(A)$ is a group, the inverse of a fractional ideal $\mathfrak{a} \neq (0)$ being $\mathfrak{a}^{-1} = \{ x \in Fr(A) \mid x\mathfrak{a} \subset A \}$.

Notation

The quotient $\mathcal{I}(A) / \mathcal{H}(A)$ is called the ideal class group of A and I denote it by $Cl(A)$

Remark (connexion to Honvel's lecture)

On may also see this group as the Picard group of $Spec(A)$. I shall come back to that later on. You should also be aware of the fact that it is finite for ring of integers, one of the purpose of this lecture shall be to prove this finiteness.

Let me start the proof of the theorem with a first lemma.

Lemma 1

Let A be a commutative ring and let $\mathfrak{p}$ be a prime ideal of A and $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ be ideals of A. If $\mathfrak{a}_1 \dots \mathfrak{a}_n \subset \mathfrak{p}$ then there exists $i \in \{1, \dots, n\}$ such that $\mathfrak{a}_i \subset \mathfrak{p}$

Proof

Assume $\alpha_i \not\subset \mathfrak{p}$ for $i \in \{1, \dots, n\}$
choose $a_i \in \alpha_i - \mathfrak{p}$ for $i \in \{1, \dots, n\}$
then $\prod_{i=1}^{n} a_i \in \prod_{i=1}^{n} \alpha_i$ but $\prod_{i=1}^{n} a_i \notin \mathfrak{p}$. □

Lemma 2

Let A be an integral ring
and $\alpha \neq (0)$ be a fractional ideal with respect to A
then α^{-1} is a fractional ideal.

Proof

α^{-1} is a A submodule of $Q(A)$
and for any $a \in \alpha$, $a \alpha^{-1} \subset A$.
write $a = \frac{p}{q}$, $p, q \in A$, then
$p \alpha^{-1} = q a \alpha^{-1} \subset A$. □

Remark

$\alpha \alpha^{-1}$ is an ideal in A.

Lemma 3

If α is invertible in $\mathcal{I}(A)$ then its
inverse is α^{-1}.

Proof

Let $\mathfrak{b}$ be an inverse for α
Then
$$\mathfrak{b}\alpha = A.$$
Thus $\mathfrak{b} \subset \alpha^{-1}$
$A = \mathfrak{b}\alpha \subset \alpha^{-1}\alpha \subset A$
We get $\alpha^{-1}\alpha = A$ and $\alpha^{-1} = \alpha^{-1}\alpha\mathfrak{b} = \mathfrak{b}$. □

Lemma 4

Let A be an integral, noetherian ring. Any non-zero ideal of A contains a product of non zero prime ideals.

Proof

Let $\mathcal{E}$ be the set of non zero ideals in A which do not contain any product of non zero prime ideals.

- Let $\mathfrak{b} \in \mathcal{E}$; we want to prove that there exists $\mathfrak{b}' \in \mathcal{E}$ such that $\mathfrak{b} \subsetneq \mathfrak{b}'$.

$\mathfrak{b}$ is not a prime ideal, $\mathfrak{b} \neq (0)$ otherwise it contains the product of 1 prime ideal. and $\mathfrak{b} \neq A$ (otherwise it would contain a maximal ideal which would be prime). If would be the product of 0 prime ideals (for a field)

Therefore, we may choose $x, y \in A$ such that

$$x, y \notin \mathfrak{b} \quad \text{and} \quad xy \in \mathfrak{b}.$$

Set $\mathfrak{b}_1 = \mathfrak{b} + Ax$, $\mathfrak{b}_2 = \mathfrak{b} + Ay$

we get

$$\mathfrak{b} \subsetneq \mathfrak{b}_1, \quad \mathfrak{b} \subsetneq \mathfrak{b}_2 \quad \mathfrak{b}_1 \mathfrak{b}_2 \subset \mathfrak{b}.$$

Assume that $\mathfrak{b}_1 \notin \mathcal{E}$ and $\mathfrak{b}_2 \in \mathcal{E}$

Then $\exists\, \mathfrak{p}_1, \dots, \mathfrak{p}_r, \mathfrak{q}_1, \dots, \mathfrak{q}_s \neq (0)$ prime ideals of A such that

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r \subset \mathfrak{b}_1 \quad \text{and} \quad \mathfrak{q}_1 \cdots \mathfrak{q}_s \subset \mathfrak{b}_2$$

Then

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r \mathfrak{q}_1 \cdots \mathfrak{q}_s \subset \mathfrak{b}_1 \mathfrak{b}_2 \subset \mathfrak{b}$$

absurd! We may take $\mathfrak{b}' = \mathfrak{b}_1$ or $\mathfrak{b}_2$.

- Then we may construct a sequence $(\mathfrak{b}_k)_{k \in \mathbb{N}} \in \mathcal{E}^{\mathbb{N}}$ such that $\forall k \in \mathbb{N}$ $\mathfrak{b}_k \subsetneq \mathfrak{b}_{k+1}$

On choose $\mathfrak{b}$ maximal in $\mathcal{E}$!

this contradict the hypothesis that A is noetherian. □.

Lemma 5

Let A be a Dedekind ring which is not a field and $\mathfrak{m}$ be a maximal ideal of A then

$$\mathfrak{m}\,\mathfrak{m}^{-1} = A$$

Proof

We have seen that $\mathfrak{m}\,\mathfrak{m}^{-1} \subset A$. (ideal)

Moreover $1 \in \mathfrak{m}^{-1}$ so $\mathfrak{m} \subset \mathfrak{m}\mathfrak{m}^{-1} \subset A$

Therefore

$$\mathfrak{m} = \mathfrak{m}\,\mathfrak{m}^{-1} \quad \text{or} \quad A = \mathfrak{m}\,\mathfrak{m}^{-1}$$

Let us assume that

$$\mathfrak{m} = \mathfrak{m}\,\mathfrak{m}^{-1}$$

Then let $x \in \mathfrak{m}^{-1}$

$$x\,\mathfrak{m} \subset \mathfrak{m} \quad \text{and for any } n \in \mathbb{N},\ x^n\,\mathfrak{m} \subset \mathfrak{m}$$

Let $d \in \mathfrak{m} - \{0\}$

$$\forall\, n \in \mathbb{N},\ x^n d \in A.$$

Thus $d\,A[x] \subset A$.

and $dA[x]$ (and therefore $A[x]$) is finitely generated A modules since A is noetherian.

Thus x is integral over A

But A is integrally closed

We get $x \in A$ and $\mathfrak{m}^{-1} \subset A$

We know that $A \subset \mathfrak{m}^{-1}$

Therfore $\mathfrak{m}^{-1} = A$.

Let $a \in \mathfrak{m} - \{0\}$.

By lemma 4 we may choose $p_1, \dots, p_n \in P(A)$

with r minimal so that

$$\prod_{i=1}^{r} p_i \subset (a) \subset \mathfrak{m}$$

Thus, by lemma 1, by permuting the p_i we may assume that

$$p_1 \subset \mathfrak{m}$$

Since A is Dedekind, p_1 is maximal,

$$p_1 = \mathfrak{m}.$$

Let $b = p_2 \cdots p_r$. $(a) \supset \mathfrak{m} b$.

Since r is minimal, $b \notin (a)$

Let $b \in b - (a)$

$$\mathfrak{m} b \subset \mathfrak{m} b \subset (a)$$

Thus $\frac{b}{a} \mathfrak{m} \subset A$.

and $\frac{b}{a} \subset \mathfrak{m}^{-1}$

but $b \notin (a)$ and $\frac{b}{a} \notin A$.

We get a contradiction $\lightning$

therefore $\mathfrak{m}\mathfrak{m}^{-1} = A$. $\square$

Lemma 6 Let A be a Dedekind ring, any ideal a in A, $a \neq (0)$ may be written as a product of prime ideals.

Proof

The proof is quite similar to the proof of lemma 6 (but uses lemma 5 which uses lemma 6).

Let $\mathcal{E}$ be the set of non zero ideals in A which might not be written as a product of prime ideals.

If $\mathcal{E} \neq \phi$ let $b \in \mathcal{E}$ be a maximal element (b exists since A is noetherian)

So before $b \neq A$, $b \neq (0)$, b is not prime.
Let m be a maximal ideal such that $b \subset m$.
$b \subset b m^{-1} \subset A$. is an ideal
if $b m^{-1} = \prod_{i=1}^{n} p_i$ then $b = m \prod_{i=1}^{n} p_i$.

So $b m^{-1} \in \mathcal{E}$ thus $b = b m^{-1}$
let $x \in m^{-1}$ and $d \in b - \{0\}$
$\forall n \in \mathbb{N}$ $x^n d \in A$ as above.
thus $d A[x] \subset A \Rightarrow x \in A$
we get $m^{-1} = A$ absurd $\lightning$
So $\mathcal{E} = \emptyset$. □.

Proof of the theorem

a) Lemma 6 proves the existence
let us check that such a decomposition is unique:

$$\prod_{p \in \mathcal{P}(A)} p^{m_p} = \prod_{q \in \mathcal{P}(A)} q^{n_p}$$

with $(m_p)_{p \in \mathcal{P}(A)}$, $(n_p)_{p \in \mathcal{P}(A)} \in \mathbb{Z}^{(\mathcal{P}(A))}$

Reminder

> A a ring, M a A-module
> X a set
> $M^{(X)} = \{(m_x)_{x \in X} \in M^X \mid \{x \in X \mid m_x \neq 0\}$ is finite$\}$

Then, since any $q \in \mathcal{P}(A)$ is invertible (Lemma 5)

$$\prod_{p \in \mathcal{P}(A)} p^{(m_p - n_p)} = A.$$

and moving negative powers to the right

$$\prod_{p \in \mathcal{P}(A)} p^{\max(0, m_p - n_p)} = \prod_{p \in \mathcal{P}(A)} p^{\max(0, n_p - m_p)}$$

which we may write as

$$p_1^{m_1} \cdots p_r^{m_r} = q_1^{n_1} \cdots q_s^{n_s}$$

with $m_1, \dots, m_r, n_1, \dots, n_s \in \mathbb{N}_{>0}$

$$\{p_1, \dots, p_r\} \cap \{q_1, \dots, q_s\} = \emptyset \qquad (*)$$

Moreover we may assume that $r = \max(r, s)$

If such a relation exists with $r \geq 1$ we choose one with r minimal

Then $p_1^{m_1} \cdots p_r^{m_r} \in p_1 \subsetneq A$

implies that $s \geq 1$

$$p_1^{m_1} \cdots p_r^{m_r} \in q_1$$

by lemma 1 there exists i such that

$$p_i \subset q_1$$

But p_i is maximal and $p_i \neq q_1$ which contradicts $(*)$.

b) Let $a \in S(A)$, we may write

$$a = \prod_{p \in P(A)} p^{v_p(a)}$$

it has an inverse namely

$$\prod_{p \in P(A)} p^{-v_p(a)}$$

Thus $S(A)$ is a group and the expression of the inverse is given by lemma 2.

Corollary

The map

$$\mathbb{Z}^{(P(A))} \longrightarrow S(A)$$

$$(m_p)_{p \in P(A)} \longmapsto \prod_{p \in P(A)} p^{m_p}$$

is a group isomorphism.

Remark

(a) Let $K = \mathrm{Fr}(A)$

The group morphism

$$K^* \longrightarrow \mathbb{Z}^{(\mathcal{P}(A))}$$
$$x \longmapsto (v_{\mathfrak{p}}(x))_{\mathfrak{p} \in \mathcal{P}(A)}$$

($v_{\mathfrak{p}}(x) = v_{\mathfrak{p}}(z)$)

is injective

(and a group isomorphism if and only if A is principal).

(b)* X a variety / k

$X^{(1)}$ is the set of irreducible hypersurfaces in X

There is an exact sequence

$$(**) \quad 0 \to k(X)^* \xrightarrow{\text{div}} \bigoplus_{\mathfrak{p} \in X^{(1)}} \mathbb{Z} \longrightarrow \mathrm{Pic}(X) \to 0$$
$$f \longmapsto (v_{\mathfrak{p}}(f))_{\mathfrak{p} \in X^{(1)}}$$

Picard group

The Picard group is a fundamental invariant of a variety and might be described in many ways

Ex A is a Dedekind ring and $X = \mathrm{Spec}(A)$

$\mathcal{P}(A) \to X^{(1)}$ is bijective

$\mathfrak{p} \mapsto \{\mathfrak{p}\}$

and $(**)$ may be written as

$$0 \to K^* \to \mathbb{Z}^{(\mathcal{P}(A))} \to \mathrm{Pic}(\mathrm{Spec}(A)) \to 0$$

we get $\mathrm{Pic}(\mathrm{Spec}(A)) \simeq Cl(A)$

Reference

HARTSHORNE, Algebraic geometry, Chapter II, §6. *

(c) The group isomorphism

$$\mathbb{Z}^{(\mathcal{P}(A))} \longrightarrow \mathcal{I}(A)$$
$$(m_{\mathfrak{p}})_{\mathfrak{p} \in \mathcal{P}(A)} \longmapsto \prod_{\mathfrak{p} \in \mathcal{P}(A)} \mathfrak{p}^{m_{\mathfrak{p}}}$$

is decreasing for the partial orders

$$(m_{\mathfrak{p}})_{\mathfrak{p} \in \mathcal{P}(A)} \leq (n_{\mathfrak{p}})_{\mathfrak{p} \in \mathcal{P}(A)} \Leftrightarrow \forall \mathfrak{p} \in \mathcal{P}(A),\ m_{\mathfrak{p}} \leq n_{\mathfrak{p}}$$

and $\subset$. This gives the following formula:

(i) $\mathfrak{a} \subset \mathfrak{b} \iff \forall p \in \mathcal{P}(A) \quad v_p(\mathfrak{a}) \geq v_p(\mathfrak{b})$

(ii) $v_p(\mathfrak{a} \cap \mathfrak{b}) = \max(v_p(\mathfrak{a}), v_p(\mathfrak{b}))$

(iii) $v_p(\mathfrak{a}+\mathfrak{b}) = \min(v_p(\mathfrak{a}), v_p(\mathfrak{b}))$.

5) Stability by localization and extension

Chinese remainder theorem. p 110 - 111

Proposition 1

Let A be an **integrally closed ring**.
And let $S \subset A$ be such that $1 \in S$ and $\forall x, y \in S$, $xy \in S$, $0 \notin S$.
Then $A[S^{-1}]$ is a **integrally closed ring**.

Proof

Since $0 \notin S$, $A[S^{-1}]$ is integral,
Let us prove it is integrally closed.
If $x \in Fr(A)$ is integral over $A[S^{-1}]$
Write

$$x^d + \sum_{i=0}^{d-1} \frac{a_i}{s_i} x^i = 0$$

Using $s = \prod_j s_j$ and $b_i = a_i \left(\prod_{j \neq i} s_j\right)^{d-1-i} s$
we get

$$x^d + \sum_{i=0}^{d-1} \frac{a_i}{s^{d-i}} x^i = 0$$

and

$$(sx)^d + \sum_{i=0}^{d-1} a_i (sx)^i = 0$$

Thus sx is integral over A
and $sx \in A$. Therefore $x \in A[S^{-1}]$. $\square$

Theorem 1

Let A be Dedekind ring
and let $S \subset A$ be such that $1 \in S$ and $\forall x, y \in S$ $xy \in S$

then $A[S^{-1}]$ is a Dedekind ring.

Proof
- integral and integrally closed: done
- noetherian: done.
- $\dim_{\text{Krull}}(A[S^{-1}]) \leq 1$ follows from the description of prime ideals in $A[S^{-1}]$. □

Theorem 2
Let A be a Dedekind ring and let $K = Fr(A)$
Let L be a finite separable extension of K
and let B be the integral closure of A in L
Then B is a Dedekind ring.

Proof
- $B \subset L$ is integral
- An integral closure is integrally closed
- Since L/K is separable, B is noetherian
- Let us now check the Krull dimension:
  Let q be a non zero prime ideal of B.
  and let $p = \xi^{-1}(q)$ prime ideal of A.
  Let $x \in q - \{0\}$
  and write
  $$N_x^K = x^d + \sum_{i=0}^{d-1} a_i x^i \in A[x]$$
  $\xi(a_0) \in q$ then $a_0 \in p$.
  Therefore a_0 is a maximal ideal in A.
  Then B/q is an A/p-algebra, integral since q is prime. Find k_p
  Let $x \in B/q - \{\bar{0}\}$ be the class of an element $b \in B$.

and let $P = \sum_{k=0}^{n} a_k X^k \in A[X]$, $\bar{P}$ its image in $A/\mathfrak{p}[X]$
Then $\bar{P} \neq 0$ and $\bar{P}(x) = 0$
Thus x is algebraic over $K_{\mathfrak{p}}$
and $K_{\mathfrak{p}}[x]$ is a field
Thus x is invertible in $K_{\mathfrak{p}}[x] \subset B/\mathfrak{q}$
We have proven that $B/\mathfrak{q}$ is a field,
$\mathfrak{q}$ is maximal. □

Corollary
For any number field K,
$\mathcal{O}_K$ is a Dedekind ring.

Remark
The proof of the theorem also shows that for any $\mathfrak{q} \in \mathcal{P}(B)$,
$f^{-1}(\mathfrak{q}) = "\mathfrak{q} \cap A" \in \mathcal{P}(A)$.
and $B/\mathfrak{q}$ is an extension of $A/\mathfrak{p}$.

Proposition (Chinese remainder theorem)
Let A be a Dedekind ring.
and let $\mathfrak{a}$ be an ideal of A, then
$$A/\mathfrak{a} \xrightarrow{\sim} \prod_{\mathfrak{p} \in \mathcal{O}(A)} A/\mathfrak{p}^{\nu_{\mathfrak{p}}(\mathfrak{a})}$$
is an isomorphism of rings

This is a particular case of a more general statement:

Theorem
Let A be a commutative ring
and let $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ be ideals in A such that
$$\forall i, j \in \{1, \dots, n\} \quad i \neq j \Rightarrow \mathfrak{a}_i + \mathfrak{a}_j = A$$

Then the product of the projection maps
$$A \longrightarrow A/\mathfrak{a}_i$$
induces an isomorphism of rings
$$A/\bigcap_{i=1}^{n} \mathfrak{a}_i \longrightarrow \prod_{i=1}^{n} A/\mathfrak{a}_i.$$

Reference : LANG Algebra

Proof of the proposition

- Let $\mathfrak{p}, \mathfrak{q} \in \mathcal{P}(A)$ $\mathfrak{p} \neq \mathfrak{q}$ and $m, n \in \mathbb{N}_{>0}$
  By the previous formula $\mathfrak{p}^m + \mathfrak{q}^n = A$.
- Let $\mathfrak{p}_1, \dots, \mathfrak{p}_r \in \mathcal{P}(A)$, $\#\{\mathfrak{p}_1, \dots, \mathfrak{p}_r\} = r$
  $m_1, \dots, m_r \in \mathbb{N}$
  By the previous formula
  $$\bigcap_{i=1}^{r} \mathfrak{p}_i^{m_i} = \prod_{i=1}^{r} \mathfrak{p}_i^{m_i} . \square$$

6] Push forward of ideals in an extension.

In this section
- A is a Dedekind ring, $K = \mathrm{Fr}(A)$
- L is a finite separable extension of K
- B is the integral closure of A in L

Proposition 1
$\mathfrak{a} \longmapsto \mathfrak{a}B$ defines a morphism of groups $\rho^{L}_{L/K} : \mathcal{I}(A) \longrightarrow \mathcal{I}(B)$.

Proof
- $\mathfrak{a}B$ is the B submodule of L generated by the images of $\mathfrak{a}$ in L.
- If $\mathfrak{a}$ is an A-ideal such that $0 \neq \mathfrak{a} \subset A$ then $0 \neq \mathfrak{a}B \subset B$,

If $a, b \in \mathcal{I}(A)$, we have

$$a B . b B = a b B$$

since this is the B submodule of L generated by

$$\{ \rho_{L/K}(xy),\ x \in a,\ y \in b \}. \square$$

Since the group $\mathcal{I}(A)$ is generated by the prime ideals of A to describe this morphism it suffices to give the image of prime ideals.

Lemma 1

Let $\mathfrak{p} \in \mathcal{P}(A)$ and $\mathfrak{q} \in \mathcal{P}(B)$

$$v_{\mathfrak{q}}(\mathfrak{p} B) > 0 \iff \rho_{L/K}^{-1}(\mathfrak{q}) = \mathfrak{p}$$

Proof

$$\begin{aligned} v_{\mathfrak{q}}(\mathfrak{p} B) > 0 &\overset{\text{Formulae}}{\iff} \mathfrak{p} B \subset \mathfrak{q} \\ &\iff \mathfrak{p} . 1_L \subset \mathfrak{q} \\ &\iff \mathfrak{p} \subset \rho_{L/K}^{-1}(\mathfrak{q}) \\ &\iff \mathfrak{p} = \rho_{L/K}^{-1}(\mathfrak{q}) . \square \end{aligned}$$

Notation

We write $\mathfrak{q} \mid \mathfrak{p}$ for $v_{\mathfrak{q}}(\mathfrak{p} B) > 0$.

If $\mathfrak{q} \mid \mathfrak{p}$ we put

$$f_{\mathfrak{q}/\mathfrak{p}} = [B/\mathfrak{q} : A/\mathfrak{p}]$$

it is called the residual degree of $\mathfrak{q}$ over A.

and

$$e_{\mathfrak{q}/\mathfrak{p}} = v_{\mathfrak{q}}(\mathfrak{p} B)$$

is called the ramification index of $\mathfrak{q}$ over A

Notations

For any algebra A over a field k
Write

$$[A:k] = \dim_k(A)$$

Proposition 2

$[L:K] = [B/\mathfrak{p}B : A/\mathfrak{p}] = \sum_{\mathfrak{q}|\mathfrak{p}} e_{\mathfrak{q}/\mathfrak{p}} f_{\mathfrak{q}/\mathfrak{p}}$
for any $\mathfrak{p} \in P(A)$

Lecture 6

Remark

$$A \xrightarrow{\varphi} B \xrightarrow{\pi} B/\mathfrak{p}B$$

π projection map

Since $\mathfrak{p} \in \ker(\varphi)$ we get $\bar{\varphi} : A/\mathfrak{p} \to B/\mathfrak{p}B$
and thus an $A/\mathfrak{p}$-algebra structure on $B/\mathfrak{p}B$

Definition

A *discrete valuation ring* is an integral ring R which is integrally closed, noetherian and has a unique non-zero prime ideal $\mathfrak{m}_R$.

Example

If A is a Dedekind ring and $\mathfrak{p} \in P(A)$
The ring $A_{(\mathfrak{p})}$ has a unique non zero prime ideal

$$\mathfrak{m}_{\mathfrak{p}} = \mathfrak{p} A_{(\mathfrak{p})}.$$

Remark

A discrete valuation ring R
is a Dedekind ring and we get an isomorphism

$$v_{\mathfrak{m}_R} : \mathcal{G}(R) \xrightarrow{\sim} \mathbb{Z}$$

Definition

Let $\mathbb{K}$ be a field. A <u>discrete valuation</u> on $\mathbb{K}$ is a map

$$v : \mathbb{K} \longrightarrow \mathbb{Z} \cup \{+\infty\}$$

such that

(i) $v^{-1}(\{+\infty\}) = \{0\}$

(ii) $\forall x, y \in \mathbb{K}$, $v(xy) = v(x) + v(y)$

(iii) $\forall x, y \in \mathbb{K}$ $v(x+y) \geq \min(v(x), v(y))$

with the usual conventions

$+\infty + \alpha = +\infty$, $\min(+\infty, \alpha) = \alpha$.

Remark

a) v is said to be trivial if $v(\mathbb{K}^*) = \{0\}$

b) If v is a non trivial discrete valuation, $v(\mathbb{K}^*) = d\mathbb{Z}$ for some $d > 0$

$$v' = \frac{1}{d} v$$

is a surjective discrete valuation

Example

Let R be a discrete valuation ring and $\mathbb{K} = Fr(R)$

$$v_R : \mathbb{K} \longrightarrow \mathbb{Z} \cup \{+\infty\}$$

$$x \longmapsto \begin{cases} +\infty & \text{if } x = 0 \\ v_{\mathfrak{m}_R}((x)) & \text{otherwise} \end{cases}$$

is a discrete valuation and $R = \{x \in \mathbb{K} \mid v_R(x) \geq 0\}$

Lemma 2

Let $\mathbb{K}$ be a field and let v be a discrete valuation on $\mathbb{K}$

Then
$R = \{ x \in \mathbb{K} \mid v(x) \geq 0 \}$
is a **euclidean** ring with a unique maximal ideal
$\mathfrak{m}_R = \{ x \in \mathbb{K} \mid v(x) > 0 \}$.

Remarks
a) In particular any discrete valuation ring is principal.
c] With the notation of Lemma 2: if v is not trivial, A is a discrete valuation ring.
b] If A is a Dedekind ring and $p \in P(A)$, $A_{(p)}$ is principal

Terminology
With the notation of Lemma 2; an element of π of $\mathfrak{m}_R$ such that $\pi \notin \mathfrak{m}_R^2$ is called a local parameter for v.

Proof of Lemma 2
o since $\forall x \in \mathbb{K}$, $v(x) \geq 0 \Leftrightarrow x \in R$ we have that
$\forall a, b \in R$, $a \mid b \Leftrightarrow v(a) \leq v(b)$
If v is trivial $R = \mathbb{K}$ is principal
otherwise
$v : R - \{0\} \to \mathbb{N}$
is a euclidean map: let $a, b \in R$, $b \neq 0$
if $v(a) < v(b)$, $a = b \times 0 + a$, if $v(a) > v(b)$, $a = b\frac{a}{b} + 0$.

- let I be an ideal of R
  If $I \neq \{0\}$, let
  $$n = \min(v(I - \{0\}))$$
  and let $x \in I$ be such that $v(x) = n$
  Then $I = (x) = \{x \in R \mid v(x) \geq n\}$
  Thus π_R is the unique maximal ideal of R. □

Let me now get back to Proposition 2.

Lemma 3

With notation as in proposition 2
For any $\mathfrak{q} \in P(B)$ and any $n \in \mathbb{N}$
$\mathfrak{q}^n/\mathfrak{q}^{n+1}$ is a $B/\mathfrak{q}$ vector space of dimension one

Proof

- $\mathfrak{q}^n/\mathfrak{q}^{n+1}$ is a B-module
But
$$\mathfrak{q} \subset \{b \in B \mid \forall\, x \in \mathfrak{q}^n/\mathfrak{q}^{n+1},\ bx = 0\}$$
we get a morphism
$$B/\mathfrak{q} \to \mathrm{End}_{\mathbb{Z}}(\mathfrak{q}^n/\mathfrak{q}^{n+1})$$
which defines the $B/\mathfrak{q}$ vector space structure on $\mathfrak{q}^n/\mathfrak{q}^{n+1}$
- subspaces of $\mathfrak{q}^n/\mathfrak{q}^{n+1}$
  = B-submodules of $\mathfrak{q}^n/\mathfrak{q}^{n+1}$
  $\leftrightarrow$ B submodules $\mathfrak{b}$ of B such that $\mathfrak{q}^{n+1} \subset \mathfrak{b} \subset \mathfrak{q}^n$
  bij = ideals $\mathfrak{b}$ of B
  = $\{\mathfrak{q}^n, \mathfrak{q}^{n+1}\}$ (factorisation of ideals)
So $\mathfrak{q}^n/\mathfrak{q}^{n+1}$ has exactly two subspaces $\{0\}$ and itself.

Thus $\dim_{B/\mathfrak{q}} (\mathfrak{q}^n/\mathfrak{q}^{n+1}) = 1$. □

Lemma 4

The integral closure of $A_{(\mathfrak{p})}$ in L is $B\left[S_{L/K}(A-\mathfrak{p})^{-1}\right]$

Proof

Let $x \in L$ be integral over $A_{(\mathfrak{p})}$
We may write its minimal polynomial over K as

$$x^d + \sum_{i=0}^{d-1} \frac{a_i}{s^{d-i}} x^i$$

with $a_0, \dots, a_{d-1} \in A$ and $s \in A - \mathfrak{p}$
(see the proof of proposition 1).
Then $sx \in B$. □

Proof of proposition 2

- Put $A' = A_{(\mathfrak{p})}$ $\quad B' = B\left[S_{L/K}(A-\mathfrak{p})^{-1}\right]$

$A_{(\mathfrak{p})}/\mathfrak{p}A_{(\mathfrak{p})} \supseteq \underbrace{A/\mathfrak{p}}_{\text{field}}\left[\overline{(A-\mathfrak{p})}^{-1}\right] \simeq A/\mathfrak{p}$

and since $B\mathfrak{p} \cap S_{L/K}(A-\mathfrak{p}) = \emptyset$ $\left(\mathfrak{p} = S_{L/K}^{-1}(\mathfrak{p}B)\right)$

$B'/\mathfrak{p}B' \supseteq B/\mathfrak{p}B\left[\underbrace{S_{L/K}(A-\mathfrak{p})^{-1}}_{\text{invertible}}\right]$

$\supseteq B/\mathfrak{p}B$

So it is enough to prove the first equality for A' and B' (By Lemma 4, B' is the integral closure of the Dedekind ring A' in L).
But since A' is principal, B' is a free A' module of rank $d = [L:K]$

Let $(e_1, \dots, e_d)$ be a basis of B' over A'
Let π be a local parameter for A'
(ie $\pi \in \mathfrak{M}_{A'}$, $\mathfrak{M}_{A'} = (\pi)$).
$\mathfrak{p} B' = (\pi e_1, \dots, \pi e_d)$
Then $(\bar{e}_1, \dots, \bar{e}_d)$ is a basis
of the $A/\mathfrak{p}$ module $B/\mathfrak{p}B$.
$[B/\mathfrak{p}B : A/\mathfrak{p}] = [L : K]$.

- For the second equality,
by the Chinese remainder theorem,

$$B/\mathfrak{p}B \xrightarrow{\sim} \prod_{\mathfrak{q}|\mathfrak{p}} B/\mathfrak{q}^{e_{\mathfrak{q}/\mathfrak{p}}}$$

we have a sequence of $A/\mathfrak{p}$ vector
spaces in $B/\mathfrak{q}^{e_{\mathfrak{q}/\mathfrak{p}}}$:

$$(0) \subset \mathfrak{q}^{e_{\mathfrak{q}/\mathfrak{p}}-1}/\mathfrak{q}^{e_{\mathfrak{q}/\mathfrak{p}}} \subset \dots \subset B/\mathfrak{q}^{e_{\mathfrak{q}/\mathfrak{p}}}$$

the successive quotient, by lemma 3
are isomorphic to $\mathfrak{q}^{i-1}/\mathfrak{q}^i \xrightarrow{\sim} B/\mathfrak{q}$
as $A/\mathfrak{p}$ vector spaces

$$\dim_{A/\mathfrak{p}} (B/\mathfrak{q}) = f_{\mathfrak{q}/\mathfrak{p}}$$

we get

$$[B/\mathfrak{p}B : A/\mathfrak{p}) = \sum_{\mathfrak{q}|\mathfrak{p}} e_{\mathfrak{q}/\mathfrak{p}} f_{\mathfrak{q}/\mathfrak{p}} \quad \square$$

Remark
Let $\bar{\pi}$ be a local parameter for $A_{(\mathfrak{p})}$.
$\mathfrak{p} A_{(\mathfrak{p})} = (\pi)$
Let $\mathfrak{q} \in \mathfrak{O}(B)$ such that $\mathfrak{q}|\mathfrak{p}$

$$\mathfrak{p} B_{(\mathfrak{q})} = \left(\prod_{\mathfrak{q}|\mathfrak{p}} \mathfrak{q}^{e_{\mathfrak{q}/\mathfrak{p}}}\right) B_{(\mathfrak{q})}$$

$$= \mathfrak{q}^{e_{\mathfrak{q}/\mathfrak{p}}} B_{(\mathfrak{q})} = \left(\mathfrak{q} B_{(\mathfrak{q})}\right)^{e_{\mathfrak{q}/\mathfrak{p}}}$$

So $\pi B_{(\mathfrak{q})} = (\mathfrak{q} B_{(\mathfrak{q})})^{e_{\mathfrak{q}/\mathfrak{p}}}$

In other words

$$e_{q/p} = v_{B(q)}(\pi)$$

Example

Let X be a compact connected Riemann surface and fix $f \in \mathbb{C}(X)$ which induces

$$f^{\#} : \mathbb{C}(T) \longrightarrow \mathbb{C}(X)$$
$$T \longmapsto f$$

Let $A = \mathbb{C}[T]$ and let B be the integral closure of A in $\mathbb{C}(X)$.

- for any $x \in X$, I define

$$v_x : \mathbb{C}(X) \longrightarrow \mathbb{Z} \cup \{+\infty\}$$
$$g \longmapsto \begin{cases} +\infty \text{ if } g = 0 \\ \max\{n \in \mathbb{Z} \mid (t^{-n} g)(x) \in \mathbb{C}\} \end{cases}$$

where $\varphi : U \to \mathbb{C}$ is a chart at x such that $\varphi(x) = 0$.

v_x is a discrete valuation on $\mathbb{C}(X)$ non trivial by Riemann existence theorem

- $B \subset \{g \in \mathbb{C}(X) \mid v_x(g) \geq 0\}$
$\Leftrightarrow f(x) \neq \infty$

Indeed

$\Rightarrow$: $f \in B$ $\quad v_x(f) \geq 0$, $\quad f(x) \neq \infty$

$\Leftarrow$ Let $g \in B$ and assume $f(x) \in \mathbb{C}$

$$g \in B \Rightarrow g^n + \sum_{i=0}^{n-1} P_i(f)\, g^i = 0.$$

for some $P_i \in \mathbb{C}[T]$

$v_x(P_i(f)) \geq 0$

So $v_x\left(\sum_{i=0}^{n-1} P_i(f)\, g^i\right) \geq \min(0, (n-1)\, v_x(g))$ if $v_x(g) \geq 0$

$\|$

$v_x(g^n) = n\, v_x(g)$

$v_x(g) \geq 0$.

- $\mathbb{C} \xleftrightarrow{\text{bij}} \mathbb{C}(\mathbb{C}[T])$
  $a \longmapsto (T-a)$

Remark (i) p. 123 ↦ Lecture 7 (+ exam)

- Let $y \in \mathbb{C} \subset \mathbb{P}^1(\mathbb{C})$ $\quad f^{-1}(\{y\}) = X_y \subset X$
  Choose charts for $x \in X_y$ and y

$$\begin{array}{ccccc} U_x & \xrightarrow{\sim} & W_x & \subset & \mathbb{C} \\ \downarrow & & x \longmapsto 0 \downarrow & & \downarrow z \\ U & \longrightarrow & W & \subset & \mathbb{C} \\ & & y \longmapsto 0 & & z \end{array} \qquad z \mapsto z^{e_x}$$

Then

$$d = \deg(f) = \sum_{x \in X_y} e_x = [\mathbb{C}(X) : \mathbb{C}(T)]$$

(indeed $f^{-1}(U \to \{0\}) \to U - \{0\}$ is a cover of degree $\sum_{x \in X_y} e_x$).

- On the other hand

$$[\mathbb{C}(X) : \mathbb{C}(T)] = \sum_{\eta \mid (T-y)} e_{\eta/(T-y)}\, f_{\eta/(T-y)}$$

$$f_{\eta/(T-y)} = [B/\eta : \mathbb{C}[T]/(T-y)] = 1$$

$\mathbb{C}[T]/(T-y) \xrightarrow{\sim} \mathbb{C}$

we get

$$[\mathbb{C}(X) : \mathbb{C}(T)] = \sum_{\eta \mid (T-y)} e_{\eta/(T-y)}$$

There is a technical point –

- Let $\mathfrak{q} \in \mathcal{P}(B)$ such that $\mathfrak{q} \mid (T-y)$ we want to prove that $\exists\, x \in X_y$ such that
$$\mathfrak{q} = \{ g \in B \mid v_x(g) \geq 1 \}$$
- Take $g_1, g_2 \in \mathfrak{q}$ let us show that $\exists\, h \in \mathfrak{q}$, $\forall x \in X_y$ $\quad h(x) = 0 \Leftrightarrow g_1(x) = 0$ and $g_2(x) = 0$
Put $h = g_1 + \lambda g_2$ with $\lambda \in \mathbb{C}^*$
if $g_1(x) g_2(x) \neq 0$, $\quad h(x) = 0 \Leftrightarrow \lambda = -\dfrac{g_1(x)}{g_2(x)}$
So we may choose $\lambda \in \mathbb{C}^*$ so that
$\forall x \in X_y$, $\quad g_1(x) g_2(x) \neq 0 \Rightarrow h(x) \neq 0$
Such h satisfies the condition
- Assume
$$\{ x \in X_y \mid \forall h \in \mathfrak{q},\ h(x) = 0 \} = \emptyset$$
Then we may find $h \in \mathfrak{q}$ such that
$\forall x \in X_y$, $h(x) \neq 0$.
- Remember that $\exists\, a_0, \dots, a_{d-1} \in \mathbb{C}(T)$,
$$T^d + \sum_{i=0}^{d-1} a_i(z) T^i = \prod_{x \in X_z} (T - h(x))$$
for any $z \notin \phi(S_\phi) \cup \{\dots\}$ continuously given
$$T^d + \sum_{i=0}^{d-1} a_i(z) T^i = \prod_{x \in X_z} (T - h(x))^{e_x}$$
for any $z \notin f(h^{-1}(\infty))$. Since $a_0, \dots, a_{d-1}$ are defined at y, $a_i \in A_{((T-y))}$ and multiplying h by an element of
$$\mathbb{C}[T] - (T-y)$$
(ie not vanishing at y), we may assume
$$a_0, \dots, a_{d-1} \in A.$$
Then
$$a_0 \in h B \cap A \subset \mathfrak{q} \cap A = (T-y)$$
but $a_0(y) \neq 0$ absurd !

So any $\mathfrak{q} \subset \{g \in B \mid v_x(g) \geq 0\}$ for some $x \in X_y$, since $\mathfrak{q}$ is maximal they are equal.

- This means that v_x is a multiple of the valuation defined by $B_{(\mathfrak{q})}$

$$e_{\mathfrak{q}/(T-y)} = v(f-y) \mid v_x(f-y) = e_x$$

But the sums are equal so we get

$$e_{\mathfrak{q}/(T-y)} = e_x.$$

Corollary.

Let v be a discrete valuation, surjective on $\mathbb{C}(X)$ then there exists $x \in X$ such that

$$v = v_x.$$

Proof.

Either $v(f) \geq 0$ or $v\left(\frac{1}{f}\right) \geq 0$

Up to using $\frac{1}{f}$ instead of f we may assume $v(f) \geq 0$. Then

Then since

$$B_v = \{g \in \mathbb{C}(X) \mid v(g) \geq 0\}$$

is principal and hence integrally closed,

$$B \subset B_v.$$

and $\mathfrak{q} = \{g \in B \mid v(g) \geq 1\}$ is a non zero prime ideal in B

The previous proof shows that $\exists x \in X$

$$\mathfrak{q} = \{g \in B \mid v_x(g) \geq 1\}$$

Since v and v_x are surjective

we have

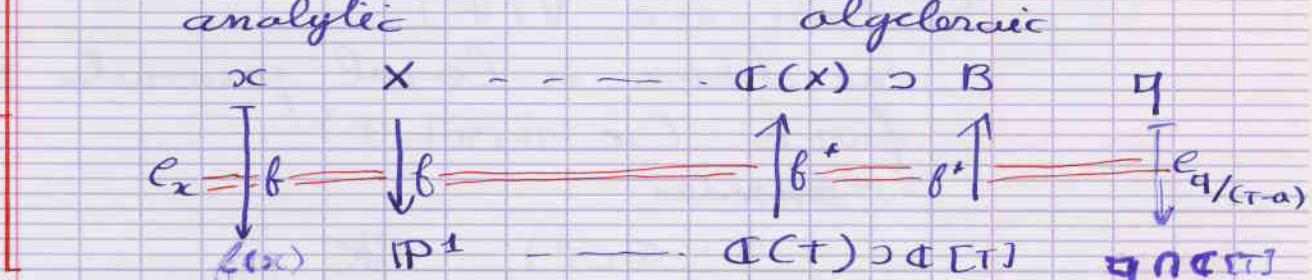
$$\mathfrak{q}^n = \{g \in B \mid v_x(g) \geq n\} = \{g \in B \mid v(g) \geq n\}$$

and $v_{|B} = v_{x|B} \Rightarrow v = v_x$. □

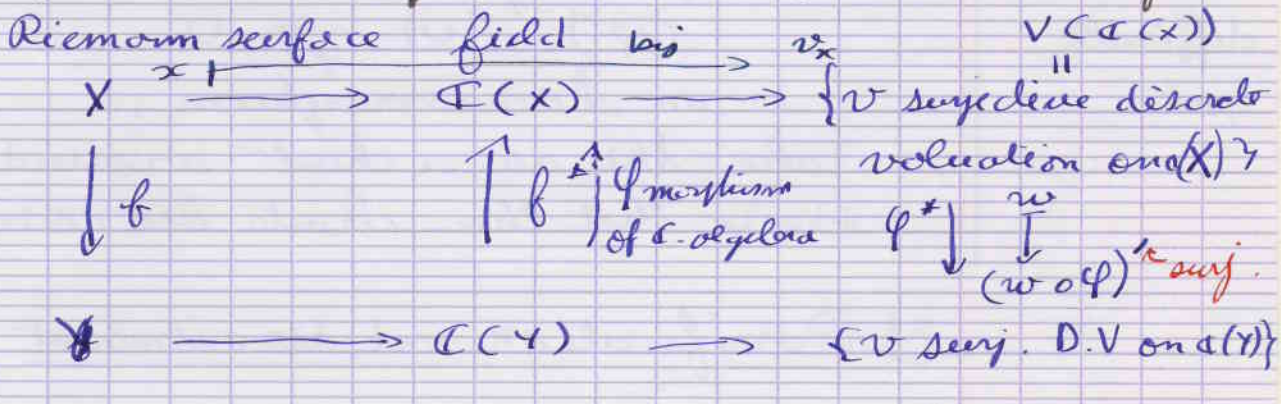
Remarks

p. 120

(i) We may translate



(ii) We can begin to construct the functor from $\mathbb{C}$-algebras which are isomorphic to finite extensions of $\mathbb{C}(T)$ to Riemann surfaces



$(f^*)^* = f$.

It remains to define a structure of Riemann surface on $V(\mathbb{C}(X))$ I do not wish to give you all the details

Sketch: $\mathbb{K}$ $\mathbb{C}$-algebra, finite extension of $\mathbb{C}(T)$.

a) For any morphism of $\mathbb{C}$-algebra

$\varphi \ \mathbb{C}(T) \to \mathbb{K}$

get $V(\mathbb{K}) \xrightarrow{\varphi^*} \mathbb{P}^1(\mathbb{C})$.

We equip $V(\mathbb{K})$ with the coarsest

topology such that all φ^A are continuous (ie generated by the open subsets $(\varphi^*)^{-1}(U)$ for $U \subset \mathbb{P}^1(\mathbb{C})$ open).

b) Take $v \in V(K)$
and choose a local parameter $\pi \in K$ for v. (ie $v(\pi)=1$)
Consider

$$\varphi : \mathbb{C}(t) \longrightarrow K$$
$$t \longmapsto \overline{\pi}$$

($v(\pi)=1 \Rightarrow \pi$ is not algebraic $/\mathbb{C}$).

difficult part

Prove that there is an open neighbourhood U of 0 in $\mathbb{P}^1(\mathbb{C})$ such that

$$(\varphi^*)^{-1}(U) \xrightarrow{\varphi^*} U$$

is an homéomorphism.
Take this as a chart around x.
Prove that these charts are compatible.

7) Ramification and discriminant

We keep the notations of § 6.

Definition
Let $\mathfrak{p} \in \mathcal{P}(A)$ and $\mathfrak{q} \in \mathcal{P}(B)$ such that $\mathfrak{p} | \mathfrak{q}$
We say that $K \subset L$ is unramified at $\mathfrak{q}$ if and only if

$$e_{\mathfrak{q}/\mathfrak{p}} = 1 \text{ and } B/\mathfrak{q} \text{ is separable over } A/\mathfrak{p}$$

it is said to be ramified otherwise

Remark
The second condition is automatic

if $A/\mathfrak{p}$ is finite (eg if k is a number field and $A = \mathcal{O}_k$).

Theorem

Let $\mathfrak{p} \in \mathcal{P}(A)$ then there exists $\mathfrak{q} \in \mathcal{P}(B)$, $\mathfrak{q}|\mathfrak{p}$ such that L/k is ramified at $\mathfrak{q}$ if and only if

$$\mathfrak{p} \mid d_{B/A}$$

d discriminant of B over A.

Corollary

The set of $\mathfrak{q} \in \mathcal{P}(B)$ such L/k is ramified at $\mathfrak{q}$ is finite.

Definition.

Let k be a field and let R be a commutative ring / a finite dimensional k-algebra and $x \in R$ a k algebra which is a free A-module of finite rank

$m_x : R \to R$ is k-linear

$x \mapsto \alpha x$

We define (S. did it for a finite extension but we may do it for any algebra of finite dimension)

a) χ_α^k : characteristic polynomial of m_α

b) $\mathrm{Tr}_{R/k}(\alpha) = \mathrm{Tr}(m_\alpha)$

c) $N_{R/k}(\alpha) = \det(m_\alpha)$.

Lemma 1

Let $\mathfrak{p} \in \mathcal{P}(A)$, then the diagram

$$\begin{array}{ccc} B & \longrightarrow & B/\mathfrak{p}B \\ \downarrow{\scriptstyle \mathrm{Tr}_{L/k}} & & \downarrow{\scriptstyle \mathrm{Tr}_{(B/\mathfrak{p}B)/(A/\mathfrak{p})}} \\ A & \longrightarrow & A/\mathfrak{p} \end{array}$$

$A/\mathfrak{p}$ algebra of finite dimension

commutes.

Proof –

Reminder:

Let $A' = A_{(p)}$ $\quad B' = B\left[\frac{1}{g_{L/K}(L-p)}\right]$

Then B' is the integral closure of A' in L and

$$A/p \cong A'/pA', \quad B/pB \cong B'/pB'$$

It is enough to prove the result for A' and B'.

But A' is principal so B' is a free A' module of dimension $d = [L:K]$

Let $(e_1, \dots, e_d)$ be a basis of the A'-module B'

Then $(\bar{e}_1, \dots, \bar{e}_d)$ is a basis of the A/p vector space B'/pB'

Let $\alpha \in B \subset B'$

$$\overline{\mathrm{Mat}_{(e_1,\dots,e_d)}(m_\alpha)} = \mathrm{Mat}_{(\bar{e}_1,\dots,\bar{e}_d)}(\bar{m}_\alpha)$$

We take the trace $\square$

Remark

The same proof works for $N_{L/K}(\alpha)$ and $\chi_{L/K}(\alpha)$. (But not for the minimal polynomial)

Lemma 2

Let k be a field and let R be a commutative k-algebra of finite dimension. Assume $x \in R$ is nilpotent, then x belongs to the kernel of the Trace bilinear form

$$\begin{aligned} \mathrm{tr}_{R/k} : R \times R &\to k \\ (y, y') &\to \mathrm{Tr}_{R/k}(yy') \end{aligned}$$

(that is $\mathrm{tr}_{R/k}(xy) = 0$ for any $y \in k$)

Proof

Let $n \geq 1$ be such that $x^n = 0$

Then for any $y \in R$, $(xy)^n = x^n y^n = 0$

and $(m_{xy})^n = m_{(xy)^n} = 0$

So m_{xy} is nilpotent,

$$\mathrm{tr}_{R/k}(xy) = \mathrm{Tr}(m_{xy}) = 0. \quad \square$$

Lemme 3

Let R_1 and R_2 be finite dimensional algebras over k then

$$\mathrm{tr}_{R_1 \times R_2/k}((x,y)) = \mathrm{Tr}_{R_1/k}(x) + \mathrm{Tr}_{R_2/k}(y)$$

for any $(x, y) \in R_1 \times R_2$.

The bilinear form $\mathrm{tr}_{R_1 \times R_2/k}$ is degenerate iff $\mathrm{tr}_{R_1/k}$ or $\mathrm{tr}_{R_2/k}$ is

Proof

Choose a basis $\underline{e}$ of R_1/k and $\underline{f}$ of R_2/k

this gives a basis $(\underline{e}, \underline{f})$ of $R_1 \times R_2$

$$\mathrm{Mat}_{(\underline{e},\underline{f})}(m_{(xy)}) = \begin{pmatrix} \mathrm{Mat}_{\underline{e}}(m_x) & 0 \\ 0 & \mathrm{Mat}_{\underline{e}}(m_y) \end{pmatrix}$$

$$\mathrm{Mat}_{(\underline{e},\underline{f})}(\mathrm{tr}_{R_1 \times R_2/k}) = \begin{pmatrix} \mathrm{Mat}_{\underline{e}}(\mathrm{tr}_{R_1/k}) & 0 \\ 0 & \mathrm{Mat}_{\underline{f}}(\mathrm{tr}_{R_2/k}) \end{pmatrix}$$

$\square$

inutile here [Proposition

Let k be a field, k'/k be a finite extension and let R be a finite dimensional k' algebra. Then

$$Tr_{R/k} = Tr_{k'/k} \circ Tr_{R/k'}$$

and

$$N_{R/k} = N_{k'/k} \circ N_{R/k'}$$

Proof

Let $\underline{e} = (e_1, \dots, e_m)$ be a basis of k' over k

Let $\underline{f} = (f_1, \dots, f_n)$ be a basis of R over k'

Then $\underline{e}\underline{f} = (e_i f_j)_{\substack{1 \le i \le m \\ 1 \le j \le n}}$ is a basis of R over k

Let $\alpha \in R$. Let $(\alpha_{i,j})_{\substack{1 \le i \le n \\ 1 \le j \le n}} = Mat_{\underline{f}}(m_\alpha)$

Then

$$Mat_{\underline{e}\underline{f}}(m_\alpha) = \begin{pmatrix} Mat_{\underline{e}}(m_{\alpha_{11}}) & \cdots & \\ \vdots & \ddots & \vdots \\ & \cdots & Mat_{\underline{e}}(m_{\alpha_{n,n}}) \end{pmatrix}$$

We get

$$Tr_{R/k}(\alpha) = \sum_{i=1}^{n} Tr_{k'/k}(m_{\alpha_{i,i}}) = Tr_{k'/k}\left(m_{\sum_{i=1} \alpha_{ii}}\right)$$

$$= Tr_{k'/k}\left(Tr_{R/k'}(\alpha)\right).$$

For the norm I need a

Technical lemma

Define

$$D = Det\begin{pmatrix} X_{1,1} & \cdots & X_{1,n} \\ \vdots & & \vdots \\ X_{n,1} & \cdots & X_{n,n} \end{pmatrix} \in \mathbb{Z}[X_{1,1}, X_{1,2}, \dots, X_{n,n}]$$

Let k be a commutative ring

and let $(M_{i,j})_{\substack{1\le i\le n\\ 1\le j\le n}} \in \mathcal{M}_m(R)$

such that $M_{ij}M_{k,\ell} = M_{k,\ell}M_{ij}$ for any $1\le i,j,k,\ell\le n$

Then

$$\mathrm{Det}\begin{pmatrix} M_{11} & \cdots & M_{1n} \\ \vdots & & \vdots \\ M_{n1} & \cdots & M_{nn} \end{pmatrix} = \mathrm{Det}\big(D(M_{1,1}, M_{1,2}, \dots, M_{n,n})\big)$$

($mn \times mn$ matrix; $m \times m$ matrix)

has a meaning only if these matrices commute

Proof –

By induction on n

True if $n = 0$ or 1

Define $D_{ij} = (-1)^{i+j}\,\mathrm{Det}\begin{pmatrix} X_{1,1} & \cdots & X_{1,j-1} & X_{1,j+1} & \cdots & X_{1,n} \\ \vdots & & \vdots & \vdots & & \vdots \\ X_{i-1,1} & \cdots & X_{i-1,j-1} & X_{i-1,j+1} & \cdots & X_{i-1,n} \\ X_{i+1,1} & \cdots & X_{i+1,j-1} & X_{i+1,j+1} & \cdots & X_{i+1,n} \\ \vdots & & \vdots & \vdots & & \vdots \\ X_{n,1} & \cdots & X_{n,j-1} & X_{n,j+1} & \cdots & X_{n,n} \end{pmatrix}$

Then

$$(*)\quad \delta_{ij}\,D(X_{1,1}, X_{1,2}, \dots, X_{n,n}) = \sum_{k=1}^{n} X_{ik}\,D^{jk}(X_{1,1}, \dots, X_{n,n})$$

We put $N_{ij} = M_{ij} + \delta_{ij}TI_m \in \mathcal{M}_m(R[T])$

$N_{ij}N_{k\ell} = N_{k\ell}N_{ij}$ for any $i,j,k,\ell \in \{1,\dots,n\}$.

Let $P = D(N_{1,1}, N_{1,2}, \dots, N_{n,n}) \in \mathcal{M}_{mn}(R[T])$

We put $N'_{ij} = P_{ij}(N_{1,1}, N_{1,2}, \dots, N_{n,n}) \in \mathcal{M}_m(R[T])$

$$U = \begin{pmatrix} N'_{11} & 0 & \cdots & 0 \\ \vdots & I_n & & \vdots \\ N'_{n1} & 0 & \cdots & I_n \end{pmatrix} \qquad N = \begin{pmatrix} N_{11} & \cdots & N_{1n} \\ \vdots & & \vdots \\ N_{n1} & \cdots & N_{nn} \end{pmatrix}$$

By $(*)$

$$NU = \begin{pmatrix} P & N_{12} & \cdots & N_{1n} \\ 0 & \vdots & & \vdots \\ \vdots & \vdots & & \vdots \\ 0 & N_{n,2} & \cdots & N_{n,n} \end{pmatrix}$$

We get

$$\mathrm{Det}(N)\ \mathrm{Det}(U) = \mathrm{Det}(P)\ \mathrm{Det}\begin{pmatrix} N_{22} - N_{2n} \\ 1 \\ N_{n,2} - N_{n,n} \end{pmatrix}$$

By induction hypothesis

$$= \mathrm{Det}(P)\ \mathrm{Det}\left(D^{(n)}(N_{2,2}, N_{2,3}, -D_{n,n})\right)$$

$$= \mathrm{Det}(P)\ \mathrm{Det}(U)$$

But $\mathrm{Det}\begin{pmatrix} N_{22} - N_{2n} \\ N_{n2} - N_{n,n} \end{pmatrix}$ is a polynomial of degree $(n-1)m$ with leading coefficient 1. So we may consider euclidean division by this polynomial, the quotient is unique; we get

$$\mathrm{Det}(N) = \mathrm{Det}(P) \text{ in } R(t)$$

Taking the value at 0 we get

$$\mathrm{Det}(M) = \mathrm{Det}(D(M_{1,1}, -, M_{n,n})). \square$$

End of the proof of lemma 4

Use that $R \longrightarrow \mathrm{Mat}_n(k')$ is a morphism of rings, $\alpha \longmapsto \mathrm{Mat}(m_\alpha)$

$$\mathrm{Det}\left(\mathrm{Mat}_{k'}(m_\alpha)\right) = \mathrm{Det}\left(D\left(\mathrm{Mat}_k(m_{\alpha_{1,1}}), \mathrm{Mat}_k(m_{\alpha_{n,n}})\right)\right)$$

$$= \mathrm{Det}\left(\mathrm{Mat}_k\left(D(m_{\alpha_{1,1}}, -, m_{\alpha_{n,n}})\right)\right)$$

$$= \mathrm{Det}\left(\mathrm{Mat}_k\left(m_{D(\alpha_{1,1}, -, \alpha_{n,n})}\right)\right)$$

$$= N_{k'/k}\left(D(\alpha_{1,1}, -, \alpha_{n,n})\right)$$

$$= N_{k'/k}\left(N_{R/k'}(\alpha)\right). \square$$

Proof of the Theorem

- We put $K_\mathfrak{p} = A/\mathfrak{p}$ field and $R = B/\mathfrak{p}B$ finite dimensional $K_\mathfrak{p}$ algebra

Let us prove that the bilinear $\mathrm{tr}_{R/K_\mathfrak{p}}$ is degenerate if and only if there exists $\mathfrak{q}|\mathfrak{p}$ such that $\mathfrak{q}$ is ramified in L/K.

Since

$$R \cong \prod_{\mathfrak{q}|\mathfrak{p}} B/\mathfrak{q}^{e_{\mathfrak{q}|\mathfrak{p}}}$$

By lemma 3 $\mathrm{tr}_{R/k}$ is degenerate if and only if one of the $\mathrm{tr}_{B/\mathfrak{q}^{e_{\mathfrak{q}|\mathfrak{p}}}}$ is

if $e_{\mathfrak{q}|\mathfrak{p}} \geq 2$ let $x \in \mathfrak{q}/\mathfrak{q}^{e_{\mathfrak{q}|\mathfrak{p}}} - \{0\}$

$x^{e_{\mathfrak{q}|\mathfrak{p}}} = 0$ in $B/\mathfrak{q}^{e_{\mathfrak{q}|\mathfrak{p}}}$
so x is nilpotent and the form is degenerate (lemma 2)

If $e_{\mathfrak{q}|\mathfrak{p}} = 1$ and $B/\mathfrak{q}$ is not separable over $K_\mathfrak{p}$, then $\mathrm{tr}_{(B/\mathfrak{q})/K_\mathfrak{p}} = 0$ is degenerate

If $e_{\mathfrak{q}|\mathfrak{p}} = 1$ and $B/\mathfrak{q}$ is separable then $\mathrm{tr}_{(B/\mathfrak{q})/K_\mathfrak{p}}$ is not degenerate.

The claim is proven.

- If the form $\mathrm{tr}_{R/K_\mathfrak{p}}$ is degenerate for any $\lambda_1, \dots, \lambda_d \in R$

$$\det\left(\mathrm{tr}_{R/K_\mathfrak{p}}(\lambda_i \lambda_j)_{\substack{1 \leq i \leq d \\ 1 \leq j \leq d}}\right) = 0$$

By lemma 1, for any $e_1, \dots, e_d \in B$

$$\det\left(\mathrm{Tr}_{L/K}(e_i e_j)_{\substack{1\le i\le d\\ 1\le j\le d}}\right)$$

$$= \det\left(\mathrm{Tr}_{R/K_{\mathfrak{p}}}(\bar{e}_i \bar{e}_j)_{\substack{1\le i\le d\\ 1\le j\le d}}\right) = 0$$

and $d_{B/A} \subset \mathfrak{p}$

○ If the form is non-degenerate

Let $\lambda_1, \dots, \lambda_d$ be a basis of R over $K_{\mathfrak{p}}$

$$\det\left(\mathrm{Tr}_{R/K_{\mathfrak{p}}}(\lambda_i \lambda_j)_{\substack{1\le i\le d\\ 1\le j\le d}}\right) \neq 0$$

Choose $e_1, \dots, e_d \in B$ so that $\bar{e}_i = \lambda_i$ for $i \in \{1, \dots, d\}$

We get

$$\det\left(\mathrm{Tr}_{L/K}(e_i e_j)_{\substack{1\le i\le d\\ 1\le j\le d}}\right) \neq 0$$

So

$$\det\left(\mathrm{Tr}_{L/K}(e_i e_j)_{\substack{1\le i\le d\\ 1\le j\le d}}\right) \notin \mathfrak{p}$$

and $d_{B/A} \notin \mathfrak{p}$. □

§3 The case of Galois extension

In this §,

- A is a Dedekind ring, $K = \mathrm{Fr}(A)$
- L is a finite Galois extension of K
- B is the integral closure of A in L
- $G = \mathrm{Gal}(L/K)$

Remark

G acts on $\{\mathfrak{q} \in \mathcal{P}(B) \mid \mathfrak{q} \mid \mathfrak{p}\}$ for any $\mathfrak{p} \in \mathcal{P}(A)$

Proposition 1

Let $\mathfrak{p} \in \mathcal{P}(A)$. G acts transitively on $\{\mathfrak{P} \in \mathcal{P}(B) \mid \mathfrak{P} | \mathfrak{p}\}$.

Proof.

Let $\mathfrak{P}, \mathfrak{P}' \in \{\mathfrak{P} \in \mathcal{P}(B) \mid \mathfrak{P} | \mathfrak{p}\}$

Assume that

$$\forall \sigma \in G, \ \sigma(\mathfrak{P}) \neq \mathfrak{P}'$$

By the Chines remainder theorem, we choose

$$x \in B$$

such that

$x \in \mathfrak{P}'$ and $x \notin \sigma(\mathfrak{P})$ for any $\sigma \in G$.

ie $\sigma(x) \notin \mathfrak{P}$ for $\sigma \in G$

Then $N_{L/K}(x) = \prod_{\sigma \in G} \sigma(x) \in \mathfrak{P}' \cap A = \mathfrak{p}$

But $\prod_{\sigma \in G} \sigma(x) \notin \mathfrak{P} \cap A = \mathfrak{p}$ absurd $\lightning$. $\square$

Corollary

Let $\mathfrak{p} \in \mathcal{P}(A)$, let $\mathfrak{P}, \mathfrak{P}' \in \mathcal{P}(B)$ such that $\mathfrak{P}|\mathfrak{p}, \mathfrak{P}'|\mathfrak{p}$

then

$$e_{\mathfrak{P}/\mathfrak{p}} = e_{\mathfrak{P}'/\mathfrak{p}} \quad \text{and} \quad f_{\mathfrak{P}/\mathfrak{p}} = f_{\mathfrak{P}'/\mathfrak{p}}$$

Proof.

Let $\sigma \in G$, $\sigma(\mathfrak{P}B) = \mathfrak{p}B$

then $e_{\sigma(\mathfrak{P})/\mathfrak{p}} = e_{\mathfrak{P}/\mathfrak{p}}$

and σ induces $\overline{\sigma}: B/\mathfrak{P} \xrightarrow{\sim} B/\sigma(\mathfrak{P})$

so $f_{\sigma(\mathfrak{P})/\mathfrak{p}} = f_{\mathfrak{P}/\mathfrak{p}}$ $\square$

Corollary 2 Let $p \in P(A)$.
If we put $r_p = \#\{q \in P(B) \mid q|p\}$
and $e_p = e_{q/p}$ $f_p = f_{q/p}$ for any $q|p$
then $d = [L:K] = \sum_p e_p f_p g_p$.

Notation
Let $p \in P(A)$, $q \in P(B)$ be such that $q|p$
the decomposition group of q is

$$D_q = \{\sigma \in G \mid \sigma(q) = q\}$$

It is a subgroup of G (the fixator of q)
As stated before
For any $\sigma \in D_q$ σ induces

$$\overline{\sigma} : B/q \to B/q$$

which is an automorphism of the A/p algebra B/q. We get a morphism of groups

$$r_q : D_q \to \mathrm{Aut}(B/q).$$

The inertia group $I_q^{A/p} = \ker(r_q)$

Proposition 2 We keep the same notations
The field extension $(B/q)/(A/p)$ is normal and r_q is surjective.

In general if A/p is not perfect (char 0 or finite) this extension may be not separable.

Proof of proposition 2
0 Take $a \in B/q$
Let $\tilde{a} \in B$ be a lifting of a to B ($\overline{\tilde{a}} = a$).

Then

$$\prod_{\sigma \in G} (X - \sigma(\tilde{a})) \in (B[X])^G$$

and therefore is the image of $P \in A[X]$.
The image of P in $B/\mathfrak{q}[X]$ is

$$\prod_{\sigma \in G} (X - \overline{\sigma(\tilde{a})}) \text{ is split}$$

Let $Q_a = \overline{P}$ be the image of P in $A/\mathfrak{p}[X]$
Then

$\overline{P}(a) = 0$ and $\overline{P}$ splits in $B/\mathfrak{q}[X]$

Thus $B/\mathfrak{q}$ is the splitting field of a family $(Q_a)_{a \in B/\mathfrak{q}}$ over $A/\mathfrak{p}$.

Lemma

Let $\mathbb{L}/\mathbb{K}$ be a normal extension and let $\mathbb{L}'$ be the separable closure of $\mathbb{K}$ in $\mathbb{L}$. Then $\mathbb{L}'/\mathbb{K}$ is Galois and the restriction map

$$\text{res} : \text{Aut}_{\mathbb{K}}(\mathbb{L}) \longrightarrow \text{Gal}(\mathbb{L}'/\mathbb{K})$$

is an isomorphism of groups

Proof

- $\mathbb{L}'/\mathbb{K}$ is separable
  Let $P \in \mathbb{K}[X]$ be irreducible and $a \in \mathbb{L}'$ be such $P(a) = 0$
  Then $P = \lambda \Pi_a^{\mathbb{K}}$ for $\lambda \in \mathbb{K}^*$ and P is separable.
  P splits over $\mathbb{L}$, let $b \in \mathbb{L}$ be such $P(b) = 0$
  Then b is separable over $\mathbb{K}$, $b \in \mathbb{L}'$
  So P splits over $\mathbb{L}'$ and $\mathbb{L}'/\mathbb{K}$ is normal.

- Choose an algebraic closure $\overline{k}$ of k and $\tau_0 \in \Sigma_{L/k}$
Let $\sigma \in Gal(L'/k)$ we want to show that there exist a unique
$$\tau \in Aut_k(L)$$
such that $\tau(x) = \sigma(x)$ for any $x \in L'$

* $\tau_0 \circ \sigma \in \Sigma_{L'/k}$ extends to $\tau' \in \Sigma_{L/k}$

Since L/k is normal, $\tau_0(L) = \tau'(L)$
and $\tau_0^{-1} \circ \tau' \in Aut_k(L)$
$\tau_0^{-1} \circ \tau'(x) = \tau_0^{-1} \circ \tau_0 \circ \sigma(x) = \sigma(x)$
for $x \in L'$.

* If $\tau, \tau' \in Aut_k(L)$ satisfy $\tau_{|L'} = \tau'_{|L'} = \sigma$
Let $a \in L$, there exist $s \geq 0$
such that
$$a^{p^s} \in L'$$
(where p is the exponential characteristic of k)
Then $\tau(a)$ (resp $\tau'(a)$) is the unique p^s-th root of $\sigma(a)$ in L.
Thus $\tau(a) = \tau'(a)$. □

End of the proof of proposition 2

- Let $(B/q)'$ be the separable closure of (A/p) in (B/q).
Let $a \in (B/q)'$ be such that
$$(B/q)' = (A/p)(a)$$
It exists since $(B/q)'$ is separable over A/p
We may assume $a \neq 0$.

Let $P = \mu_a^{A/\mathfrak{p}} \in A/\mathfrak{p}[X]$ $\deg(P) = [(B/\mathfrak{q})' : A/\mathfrak{p}]$

Then (P comes from $A/\mathfrak{p}[X]$, vanishes at a)

$$\chi_{(B/\mathfrak{q})'/(A/\mathfrak{p})}(P) \mid \prod_{\sigma \in Gal((B/\mathfrak{q})'/(A/\mathfrak{p}))} (X - \sigma(a))$$

$\deg [(B/\mathfrak{q})' : A/\mathfrak{p}]$

so

$$\chi_{(B/\mathfrak{q})'/(A/\mathfrak{p})}(P) = \prod_{\sigma \in \mathrm{Aut}_{A/\mathfrak{p}}(B/\mathfrak{q})} (X - \sigma(a))$$

Using the chinese remainder theorem, we pick $b \in B$ such that

(i) $\bar{b} = a$ in $B/\mathfrak{q}$

(ii) $b \in \sigma(\mathfrak{q})$ for $\sigma \in G - D_{\mathfrak{q}}$

(Indeed $\{\sigma(\mathfrak{q}), \sigma \in G\}$ is a finite set of maximal ideals in B).

Then let $Q \in A[X]$ be the polynomial such that

$$\chi_{L/K}(Q) = \prod_{\sigma \in G} (X - \sigma(b))$$

$$\bar{Q}(a) = 0$$

Therefore $P \mid \bar{Q}$

So for any $\sigma \in \mathrm{Aut}_{A/\mathfrak{p}}(B/\mathfrak{q})$, there exists $\tau \in G$ such that

$$\overline{\tau(b)} = \sigma(a) \neq 0$$

Therefore $\tau(b) \notin \mathfrak{q}$

ie $b \notin \tau^{-1}(\mathfrak{q})$ thus $\tau^{-1} \notin G - D_{\mathfrak{q}}$ by (ii)

ie $\tau^{-1} \in D_{\mathfrak{q}}$ and $\tau \in D_{\mathfrak{q}}$.

We have (since a generates $(B/\mathfrak{q})'$.

$$r(\tau)|(B/\mathfrak{q})' = \sigma|(B/\mathfrak{q})'$$

Thus $r(\tau) = \sigma$. □

Corollary

We get an isomorphism of groups

$$D_{\mathfrak{q}} / I_{\mathfrak{q}} \xrightarrow{\sim} \mathrm{Gal}((B/\mathfrak{q})'/(A/\mathfrak{p}))$$

Notation

Put $f'_{\mathfrak{q}/\mathfrak{p}} = [B/\mathfrak{q} : A/\mathfrak{p}]_s$ (even if L/K is not Galois)

and $e'_{\mathfrak{q}/\mathfrak{p}} = [B/\mathfrak{q} : A/\mathfrak{p}]_i$ which is a power of the exponential characteristic.

and, in the Galois case,

$$e'_{\mathfrak{p}} = e'_{\mathfrak{q}/\mathfrak{p}} \qquad f'_{\mathfrak{p}} = f'_{\mathfrak{q}/\mathfrak{p}}$$

NB.

L/K unramified at $\mathfrak{q}$ iff $e'_{\mathfrak{q}/\mathfrak{p}} e_{\mathfrak{q}/\mathfrak{p}} = 1$

Proposition

In the Galois case, if $\mathfrak{p} \in \mathcal{P}(A)$

$$d = [L:K] = e_{\mathfrak{p}} e'_{\mathfrak{p}} f'_{\mathfrak{p}} g_{\mathfrak{p}}.$$

and for $\mathfrak{q} | \mathfrak{p}$, $\mathfrak{q} \in \mathcal{P}(B)$

$$\# D_{\mathfrak{q}} = e_{\mathfrak{p}} e'_{\mathfrak{p}} f'_{\mathfrak{p}}$$

$$\# I_{\mathfrak{q}} = e_{\mathfrak{p}} e'_{\mathfrak{p}}.$$

Proof

follows from last corollary and proposition 1

Remark

L/K is unramified at $\mathfrak{q}$ iff $\mathfrak{R}_{\mathfrak{q}}$ is an isomorphism

IV Absolute values, Places

1) Motivation

$$\begin{array}{ccc} \{\text{prime numbers}\} & \overset{bij}{\longleftrightarrow} & \mathrm{Spec}(\mathbb{Z}) \\ \updownarrow & & \updownarrow \text{Analogy} \\ \mathbb{C} & \overset{bij}{\longleftrightarrow} & \mathrm{Spec}(\mathbb{C}[T]) \\ \cap & & \cap \\ \text{compact } \mathbb{P}^1(\mathbb{C}) & \overset{bij}{\longleftrightarrow} & \{\text{surj. discr. val on } \mathbb{C}(T)\} \end{array}$$

and there is a «magic» formula for any compact connected Riemann surface and any $f \in \mathbb{C}(X)$,

$$\sum_{x \in X} v_x(f) = 0 .$$

(Exercise : prove it for $\mathbb{P}^1(\mathbb{C})$).
There is no similar formula for elements of $\mathbb{Q}$!

Grothendieck :
Points are missing in $\mathrm{Spec}(\mathbb{Z})$.

2) Absolute values

Definition.
Let K be a field. An absolute value on K is a map

$$|\cdot| : K \longrightarrow \mathbb{R}_{\geq 0}$$
$$x \longmapsto |x|$$

which satisfies the following condition

(i) $\forall x \in \mathbb{K}$, $|x| = 0 \Leftrightarrow x = 0$

(ii) $\forall x, y \in \mathbb{K}$, $|xy| = |x||y|$

(iii) $\forall x, y \in \mathbb{K}$ $|x+y| \leq |x| + |y|$

$|.|$ is said to be non-archimedean if, moreover,

(iii') $\forall x, y \in \mathbb{K}$ $|x+y| \leq \max(|x|, |y|)$

Lecture 8

Examples

a) $\mathbb{K} \longrightarrow \mathbb{R}$

$$x \longmapsto |x| = \begin{cases} 0 \text{ if } x = 0 \\ 1 \text{ otherwise} \end{cases}$$

is a non-archimedean absolute value which is said to be trivial.

b) If $v : \mathbb{K} \longrightarrow \mathbb{Z} \cup \{+\infty\}$ is a discrete valuation and $\alpha \in \mathbb{R}_{>0}$ $\alpha > 1$ then

$$|x|_v = \alpha^{-v(x)}$$

is a non-archimedean absolute value on $\mathbb{K}$.

c) On $\mathbb{Q}$ we have the usual absolute value

$$|x|_\infty = \max(x, -x) \in \mathbb{R}$$

and for any prime p the absolute value $|.|_p$ associated to $v_{(p)}$

$$\left|\frac{a}{b} p^n\right|_p = p^{-n}$$

if $a, b \in \mathbb{Z} - (p)$, $n \in \mathbb{Z}$.

Definition.

Let $\mathbb{K}$ be a field and let $|.|$ be an absolute value on $\mathbb{K}$

then $d(x,y) = |x-y|$ defines a distance on $\mathbb{K}$, and the corresponding topology on $\mathbb{K}$ is called the topology defined by $|\cdot|$.

Absolute values $|\cdot|$ and $|\cdot|'$ on $\mathbb{K}$ are said to be dependent if they define the same topology on $\mathbb{K}$.

Proposition 1

Let us equip $\mathbb{K}$ with the topology defined by an absolute value $|\cdot|$ then $\mathbb{K}$ is a topological field :

(i) $+ : \mathbb{K}\times\mathbb{K} \to \mathbb{K}$ is continuous

(ii) $- : \mathbb{K} \to \mathbb{K}$ ———

(iii) $\times : \mathbb{K}\times\mathbb{K} \to \mathbb{K}$ ———

(iv) $\cdot^{-1} : \mathbb{K}^* \to \mathbb{K}^*$ ———

Proof

(i) $|(x+y)-(x'+y')| \leq |x-x'| + |y-y'|$

(ii) $|-x-(-y)| = |x-y|$

(iii) $|xy - x'y'| \leq |x-x'||y| + |x'||y-y'|$

(iv) $|x^{-1} - y^{-1}| = \frac{1}{|x||y|}|x-y|$ □

Proposition 2

Let $|\cdot|_1$ and $|\cdot|_2$ be absolute values on $\mathbb{K}$. The following conditions are equivalent

(i) $|\cdot|_1$ and $|\cdot|_2$ are dependent

(ii) $\{x \in \mathbb{K} \mid |x|_1 < 1\} = \{x \in \mathbb{K} \mid |x|_2 < 1\}$

(iii) $\exists \lambda > 0$ such that $|x|_1 = |x|_2^{\lambda}$ for any $x \in \mathbb{K}$

(i) ⇒ (ii)

because $|x|_i < 1 \Leftrightarrow x^n \underset{n\to\infty}{\to} 0$ for the topology defined by $|\cdot|_i$;

(ii) ⇒ (iii)

if $|\ |_1$ is trivial then so is $|\cdot|_2$ and $|\cdot|_1 = |\cdot|_2$

otherwise none of them are trivial

Since $\forall x \in \mathbb{K}^*$, $|x|_1 > 1 \Leftrightarrow |x^{-1}|_1 < 1$

So $\{x \in \mathbb{K} \mid |x|_1 > 1\} = \{x \in \mathbb{K} \mid |x|_2 > 1\}$

and both are not empty

Let x_0 such that $|x_0| > 1$

Put $a = |x_0|_1$ and $b = |x_0|_2$

and put $\lambda = \dfrac{\log(b)}{\log(a)} > 0$.

Let $x \in \mathbb{K}$ $x \neq 0$.

Let $\alpha = \dfrac{\log |x|_1}{\log(a)}$

If $m, n \in \mathbb{Z}$, $n > 0$, $\alpha < \frac{m}{n}$

Then $|x_0^{\frac{m}{n}}|_1 > |x|_1$

this $\left|\dfrac{x_0^m}{x^n}\right|_1 > 1$

or $\left|\dfrac{x_0^m}{x^n}\right|_2 > 1$

we get $|x|_2 \leq |x_0|_2^{m/n}$

Since it is true for any m/n

$$|x|_2 \leq |x_0|_2^{\alpha}$$

Similarly $|x|_2 \geq |x_0|_2^{\alpha}$

and $|x|_2 = |x_0|_2^{\alpha} = |x_0|_1^{\lambda\alpha} = |x|_2^{\lambda}$.

(iii) ⇒ (i) the balls are the same. □

Définition:

A place of a field K is a topology on K defined by a nontrivial absolute value on K. We denote by $\mathcal{M}(K)$ the set of places of K.

If a place v of K is defined by an absolute value $|\cdot|$ any function of the form $x \mapsto |x|^\lambda$ with $\lambda > 0$ is called a representative of v

2 If v is defined by an archimedean absolute value, $|\cdot|^\lambda$ do not on absolute value for λ big enough (do not satisfy $|x+y|^\lambda \leq |x|^\lambda + |y|^\lambda$).

2 Ostrowski's theorem

Theorem

Let P be the set of prime numbers

Then

$$\begin{aligned} P \cup \{\infty\} &\longrightarrow \mathcal{M}(\mathbb{Q}) \\ v &\mapsto \text{topology defined by } |\cdot|_v \end{aligned}$$

is a bijection.

Proof:

- Injectivity:

For $p \in P$, v a place defined by an element of $P \cup \{\infty\}$, then

$p^n \xrightarrow[n \to +\infty]{} 0$ if and only if v is defined by $|\cdot|_p$

- Surjectivity:

Let $v \in \mathrm{Val}(\mathbb{Q})$ be defined by an absolute value $|\cdot|$.

$|-1|^2 = |1|^2 = |1| \Rightarrow |-1| = |1| = 1$.

1st case

$\mathbb{Z} \subset \{x \in \mathbb{Q} \mid |x| \leq 1\}$

If $\forall x \in \mathbb{Z}^*, |x| = 1$ then

$\forall x \in \mathbb{Q}^*, |x| = 1$ contradicts $|\cdot|$ not trivial.

We may choose $n \in \mathbb{N}$ such that $|n| < 1$

Write $n = \prod_{i=1}^{r} p_i^{\alpha_i}$

We may find $p \in P$ such that $|p| < 1$.

Let $n \in \mathbb{Z}$ such that $p \nmid n$.

By Bezout, we may find $(u_k, v_k) \subset \mathbb{Z}^2$ such that

$$u_k p^k + v_k n^k = 1$$

Thus

$$1 = |u_k p^k + v_k n^k|$$
$$\leq |u_k| |p|^k + |v_k| |n|^k$$

If $|n| < 1$, $|n|^k \xrightarrow[k \to +\infty]{} 0$ absurd!

Thus $|n| = 1$

Therefore, for $n \in \mathbb{Z}$,

$$|n| = |p|^{v_p(n)}$$

Thus for $x \in \mathbb{Q}$, $|x| = |p|^{v_p(x)}$

$$= p^{v_p(x) \frac{\ln(|p|)}{\ln(p)}}$$
$$= |x|_p^{\lambda}$$

where $\lambda = -\frac{\ln(|p|)}{\ln(p)}$

2nd case

There exists $n \in \mathbb{Z}$ such that $|n| > 1$.

One may assume $n > 0$ and, since $|1| = 1$,

$n > 1$.
Let $a, b \in \mathbb{N}$, $a > 1$ $b > 1$
Put $M_a = \max\{|0|, |1|, \dots, |a-1|\}$
Write b^n in the base a

$$b^n = \sum_{k=0}^{t} r_k a^k \quad \text{with } r_k \in \{0, \dots, a-1\}$$

$$t = \left[\frac{n \ln(b)}{\ln(a)}\right] \leq n \frac{\ln(b)}{\ln(a)}$$

$$(*) \quad |b|^n \leq M_a \frac{|a|^{t+1} - 1}{|a| - 1}$$

If $|a| < 1$ we get that $\{|m|^n, n \in \mathbb{N}\}$ bounded which contradicts $|m| > 1$
Therefore
$\forall a \in \mathbb{Z} - \{-1, 0, 1\}$ $|a| > 1$.
$(*)$ gives

$$\ln(|b|) \leq \frac{1}{n}\left(\ln(M_a) - \ln(|a|-1) + \ln(|a|^{t+1} - 1)\right)$$
$$\leq \frac{1}{n}\left(\ln(M_a) + \ln(|a|-1) + \ln(|a|) + \frac{\ln(b)}{\ln(a)} \ln(|a|)\right)$$

Thus $\dfrac{\ln(|b|)}{\ln(|a|)} \leq \dfrac{\ln(b)}{\ln(a)}$

By exchanging a and b, we get

$$\frac{\ln(|b|)}{\ln(|a|)} = \frac{\ln(b)}{\ln(a)}.$$

Put $\lambda = \dfrac{\ln(|m|)}{\ln(m)}$

for any $m \in \mathbb{N}$, we get $|m| = |m|_\infty^\lambda$
Therefore
$\forall x \in \mathbb{Q}$, $|x| = |x|_\infty^\lambda$. □

Convention.
From now on, we identify $P \cup \{\infty\}$ and $\mathrm{Val}(\mathbb{Q})$.

Corollary (Product formula on $\mathbb{Q}$).
$\forall x \in \mathbb{Q}^*, \prod_{v \in \mathrm{Val}(\mathbb{Q})} |x|_v = 1.$

Proof.
$$x = \epsilon \prod_{p \in P} p^{v_p(x)}, \quad \epsilon \in \{-1, 1\}$$
For $p \in P$, $|x|_p = p^{-v_p(x)}$
$$|x|_\infty = \prod_{p \in P} p^{v_p(x)}. \quad \square$$

Remark
- Let X be a compact connected Riemann surface. For $x \in X$, put
$$|f|_x = \exp(-v_x(f))$$
We get
$\forall f \in \mathbb{C}(X)^*, \prod_{x \in X} |f|_x = 1$
- Thus $\sum_{x \in X} v_x(f) = 0 \iff \prod_{v \in \mathrm{Val}(\mathbb{Q})} |x|_v = 1$

3) Completion

a) Construction

Definition
Let $\mathbb{K}$ be a field with a nontrivial absolute value $|\cdot|$; a Cauchy sequence in $\mathbb{K}$ is a sequence $(x_n)_{n \in \mathbb{N}}$ such that
$\forall \varepsilon \in \mathbb{R}_{>0}, \exists N \in \mathbb{N}, \forall p, q \in \mathbb{N}, p, q \geq N \Rightarrow |u_p - u_q| < \varepsilon$

$\mathbb{K}$ is said to be complete if any Cauchy sequence in $\mathbb{K}$ converges

Proposition

Let $\mathbb{K}$ be a field with a nontrivial absolute value $|\cdot|$ then there exists a field $\widehat{\mathbb{K}}$ equipped with an absolute value $|\cdot|$ and a morphism $\iota : \mathbb{K} \to \widehat{\mathbb{K}}$ such that

(i) $\forall x \in \mathbb{K}, \quad |\iota(x)| = |x|$

(ii) $\iota(\mathbb{K})$ is dense in $\widehat{\mathbb{K}}$

(iii) $\widehat{\mathbb{K}}$ is complete

Moreover if $\mathbb{K}'$ is a field with an absolute value $|\cdot|'$ and a morphism $\iota' : \mathbb{K} \to \mathbb{K}'$ which satisfies (i), (ii) & (iii) then there exists a unique isomorphism

$$\widehat{\mathbb{K}} \xrightarrow{\varphi} \mathbb{K}'$$

such that $|\cdot| = |\cdot|' \circ \varphi$ and $\iota' = \varphi \circ \iota$.

Proof

Existence : construction of $\mathbb{R}$.

- Let $(x_k)_{k \in \mathbb{N}}$ be a Cauchy sequence in $\mathbb{K}$ then $\{|x_k|, k \in \mathbb{N}\}$ is bounded.

Thus

$$A = \{\text{Cauchy sequences in } \mathbb{K}\}$$

is a subring of $\mathbb{K}^{\mathbb{N}}$.

and

$$I = \{\text{sequences converging to } 0 \text{ in } \mathbb{K}\}$$

is an ideal in A.

Let's consider the quotient ring

$$\widehat{\mathbb{K}} = A/I$$

- It is a $\mathbb{K}$ algebra for
$$\mathbb{1} : \mathbb{K} \longrightarrow \widetilde{\mathbb{K}}$$
$$x \longmapsto \overline{(x)}_{n\in\mathbb{N}}$$
$\mathbb{1}$ constant sequence.
which is injective
- Let $(x_n)_{n\in\mathbb{N}}$ be a Cauchy sequence in $\mathbb{K}$ which does not converge to 0.
(ie $\overline{(x_n)}_{n\in\mathbb{N}} \neq 0$)
and let $\varepsilon \in]0,1[$ be such that
$\forall m \in \mathbb{N}, \exists n \in \mathbb{N}, n \geq m$ and $|u_n| \geq \varepsilon$.
Let $N \in \mathbb{N}$ be such
$\forall p,q \in \mathbb{N}, \quad p,q \geq N \to |u_p - u_q| < \varepsilon/2$
then
$\forall n \in \mathbb{N}, \quad n \geq N \to |u_n| > \varepsilon/2$
Put
$$v_n = \begin{cases} 1 & \text{if } n < N \\ u_n & \text{if } n \geq N \end{cases}$$
Then
$\forall n \in \mathbb{N}, \quad |v_n| > \varepsilon/2$
From $\left|\frac{1}{v_p} - \frac{1}{v_q}\right| = \frac{|v_p - v_q|}{|v_p||v_q|} \leq \frac{4}{\varepsilon^2}|v_p - v_q|$
we get that $\left(\frac{1}{v_n}\right)_{n\in\mathbb{N}}$ is a cauchy sequence in $\mathbb{K}$
and $\frac{1}{v_n} u_n = 1$ for $n \geq N$.
Then $\overline{\left(\frac{1}{v_n}\right)}_{n\in\mathbb{N}} \cdot \overline{(u_n)}_{n\in\mathbb{N}} = \underline{1}$.
So $\widetilde{\mathbb{K}}$ is a field.
- If $(u_n)_{n\in\mathbb{N}}$ is a Cauchy sequence in $\mathbb{K}$
Then $(|u_n|)_{n\in\mathbb{N}}$ ——— in $\mathbb{R}$

Thus it converges, and we put

$$|\overline{(u_n)_{n\in\mathbb{N}}}| = \lim_{n\to+\infty} |u_n|.$$

we have

$$\forall x, y \in \widehat{\mathbb{K}}, \quad |x+y| \leq |x| + |y|$$

$$\forall x, y \in \widehat{\mathbb{K}}, \quad |xy| = |x| \cdot |y|$$

and $\forall x \in \widehat{\mathbb{K}} \quad |x| = 0 \Leftrightarrow x = 0$.

since it exactly means that the sequence converges to 0

and $|\cdot| \circ i = |\cdot|$. which proves (i)

- If $(x_n)_{n\in\mathbb{N}}$ is a Cauchy sequence in $\mathbb{K}$, then $(i(x_n))_{n\in\mathbb{N}}$ converges to $\overline{(x_n)_{n\in\mathbb{N}}}$

Thus we have (ii)

- Let $(u_n)_{n\in\mathbb{N}}$ be a Cauchy sequence in $\widehat{\mathbb{K}}$ for any $n \in \mathbb{N}$, by (ii) we may find $x_n \in \mathbb{K}$ such that

$$|i(x_n) - u_n| < \frac{1}{n+1}$$

Then $(x_n)_{n\in\mathbb{N}}$ is a Cauchy sequence in $\mathbb{K}$ and

$$u_n \xrightarrow[n\to+\infty]{} \overline{(x_n)_{n\in\mathbb{N}}} \quad \text{in } \widehat{\mathbb{K}}.$$

which proves (iii)

Uniqueness

- Let $x \in \widehat{\mathbb{K}}$; by (ii) x is the limit of $(i(x_n))_{n\in\mathbb{N}}$; $(x_n)_{n\in\mathbb{N}}$ is Cauchy thus $(i'(x_n))$ is Cauchy and we put

$$\varphi(x) = \lim_{n\to+\infty} i'(x_n).$$

φ is a morphism of fields which satisfy the conditions

- Since φ has to be continuous,

$i(K)$ is dense in $\widehat{K}$ and $\varphi \circ i = i'$;
φ is unique.

- Similarly we construct $\varphi' : K' \to \widehat{K}$
- Using unicity we get
$$\varphi \circ \varphi' = Id_{K'}, \quad \varphi' \circ \varphi = Id_{\widehat{K}}$$
and φ is an isomorphism. □

Remark

If $|\cdot|_2 = |\cdot|_1^\lambda$, then a sequence is Cauchy for $|\cdot|_1$ iff it is Cauchy for $|\cdot|_2$
So $\widehat{K}$ depends only on the place defined by the absolute value

Notation

For any $v \in Pl(K)$, K_v is the completion of K at v.

Examples

$\mathbb{R} = \mathbb{Q}_\infty$
For $p \in \mathbb{P}$, $\mathbb{Q}_p$: p-adic field

b) Norms

Definition

Let K be a field equiped with an absolute value $|.|$ and let E be a K-vector space
A norm on E is a map $\|\cdot\| : E \to \mathbb{R}_{\geq 0}$ such that
(i) $\forall x \in E$, $\|x\| = 0 \Leftrightarrow x = 0$
(ii) $\forall \lambda \in K$, $\forall x \in E$, $\|\lambda x\| = |\lambda| \, \|x\|$.

(iii) $\forall x, y \in E$, $\|x+y\| \leq \|x\| + \|y\|$

Norms $\|\cdot\|_1$ and $\|\cdot\|_2$ on E are <u>equivalent</u> if and only if there exists $C, C' \in \mathbb{R}_{>0}$ such that

$$\forall x \in E, \quad C\|x\| \leq \|x\|' \leq C'\|x\|$$

<u>Remark</u>

- $\mathbb{K}$ vector space equiped with a norm $\|\cdot\|$ has a structure of a metric space with the distance
$$d(x,y) = \|x-y\|$$
for $x, y \in E$. This defines a topology on E
- Equivalent norms define the some topology on E

<u>Theorem</u>

Let $\mathbb{K}$ be a complete field for an absolute value $|\cdot|$; Let E be a finite dimensional vector space on E then any two norms on E are equivalent and E is complete for any such norm.

<u>Remark</u>

Choose a basis $(e_1, \dots, e_d)$ of E then

$$\left\| \sum_{i=1}^{d} x_i e_i \right\|_0 = \max_{1 \leq i \leq d} |x_i|$$

defines a norm on E. Thus We get a topology on E which do not depends on the choice of the norm

(but only on the chosen place of $\mathbb{K}$)
This topology is said to be canonical.

Proof of the theorem

It is enough to prove that a norm $\|\cdot\|$ on E is equivalent to $\|\cdot\|_0$

Let
$$\left\| \sum_{i=1}^{d} x_i e_i \right\| \leq \sum_{i=1}^{d} |x_i| \, \|e_i\|$$
$$\leq \left(d \max_{1 \leq i \leq d} \|e_i\| \right) \left\| \sum_{i=1}^{d} x_i e_i \right\|_0 .$$

We proceed by induction on $\dim(E)$;
true if $\dim(E) = 0$
Assume that there exists no $c \in \mathbb{R}_{>0}$ such that
$$\forall x \in E, \quad \|x\| \geq c \|x\|_0$$
Then for any $n \in \mathbb{N}$ we may find
$$x_n \in E, \quad \|x_n\| < \frac{1}{n+1} \|x_n\|_0$$
We have $\|x_n\|_0 > 0$
We put $y_n = \dfrac{1}{\|x_n\|_0} x_n$

Then $y_n \xrightarrow[n \to +\infty]{} 0$ and $\|y_n\|_0 = 1$ for $n \in \mathbb{N}$.

Write $y_n = \sum_{i=1}^{d} y_{n,i} e_i$
the set
$$\{ |y_{n,i}| = 1, \ n \in \mathbb{N} \}$$
is infinite for some $i \in \{1, \dots, d\}$
By permuting $(e_1, \dots, e_d)$, we may assume
$$\{ |y_{n,d}| = 1, \ n \in \mathbb{N} \}$$
is infinite and choose
$\varphi : \mathbb{N} \to \mathbb{N}$ strictly increasing

so that $|y_{\varphi(n),d}| = 1$ for all $n \in \mathbb{N}$

Then put

$$z_n = \frac{1}{y_{\varphi(n),d}} y_{\varphi(n)} \quad \text{for } n \in \mathbb{N}$$

Then we may write

$$z_n = \left(\sum_{i=1}^{d-1} z_{n,i} e_i \right) + e_d$$

and

$$z_n \xrightarrow[n \to +\infty]{} 0.$$

We put

$$z'_n = \sum_{i=1}^{d-1} z_{n,i} e_i \qquad \|z'_p - z'_q\| = \|z_p - z_q\|$$

By induction hypothesis the sequence $(z'_n)_{n \in \mathbb{N}}$ converges in $E' = \sum_{i=1}^{d-1} \mathbb{K} e_i$

Both for $\|\cdot\|$ and $\|\cdot\|_0$

Thus $(z_{n,i})_{n \in \mathbb{N}}$ converges for $i \in \{1, \dots, d-1\}$

Let

$$a_i = \lim_{n \to +\infty} z_{n,i} \quad \text{for } i \in \{1, \dots, d-1\}$$

We get for $\|\cdot\|$

$$\lim_{n \to +\infty} z'_n = \sum_{i=1}^{d-1} a_i e_i$$

Thus

$$0 = \lim_{n \to +\infty} z_n = \lim_{n \to +\infty} z'_n + e_n = \left(\sum_{i=1}^{d-1} a_i e_i \right) + e_n$$

Which is absurd since $(e_1, \dots, e_d)$ is free.

It remains to check that E is complete

Since $\|\ \|$ is equivalent to $\|\cdot\|_0$

if $(x_n)_{n \in \mathbb{N}}$ is a Cauchy sequence in E

so is the sequences given by the i-th coordinate. Thus $(x_n)_{n \in \mathbb{N}}$ converges. □

C) Archimedean complete fields

Theorem (Ostrowski)
Let $\mathbb{K}$ be a complete field for an archimedean absolute value $|\cdot|$ then there exists an isomorphism

$$\varphi : \mathbb{K} \xrightarrow{\sim} \mathbb{R} \text{ or } \varphi : \mathbb{K} \to \mathbb{C}$$

and $\lambda \in \mathbb{R}_{>0}$ such that

$$|x| = |\varphi(x)|^{\lambda}$$

for $x \in \mathbb{K}$.

Lemma 1
Let $\mathbb{K}$ be an extension of $\mathbb{R}$ with an absolute value $|\cdot|$ such that

$$\forall x \in \mathbb{R}, \quad |\xi_{\mathbb{K}/\mathbb{R}}(x)| = |x|$$

then $\mathbb{K}/\mathbb{R}$ is algebraic

Proof.
Let $\xi \in \mathbb{C}$ and consider

$$f : \mathbb{C} \longrightarrow \mathbb{R}$$
$$\alpha \longmapsto |\xi^2 - (\alpha+\bar{\alpha})\xi + \alpha\bar{\alpha}|$$

$$|f(\alpha_1) - f(\alpha_2)| \leq |\xi^2 - (\alpha_1+\bar{\alpha}_1)\xi + \alpha_1\bar{\alpha}_1 - (\xi^2 - (\alpha_2+\bar{\alpha}_2)\xi + \alpha_2\bar{\alpha}_2)|$$
$$\leq |(\alpha_1+\bar{\alpha}_1) - (\alpha_2+\bar{\alpha}_2)|\,|\xi| + |\alpha_1\bar{\alpha}_1 - \alpha_2\bar{\alpha}_2|$$

(triangular inequality for $|\cdot|$)

f is continuous

and $f(\alpha) \geqslant |\alpha|^2 - |\xi|^2 - |\alpha+\bar{\alpha}|\,|\xi|$

$|\alpha| \to +\infty$, $+\infty$

Let $\alpha_0 \in \mathbb{C}$

Thus $\{\beta \in \mathbb{C} \mid f(\beta) \leq f(\alpha_0)\}$ is compact and there exists $\alpha_1 \in \mathbb{C}$ such that

$$f(\alpha_1) = \inf_{\beta \in \mathbb{C}} f(\beta).$$

$\mathcal{S} = \{\beta \in \mathbb{C} \mid f(\beta) = f(\alpha_1)\}$ is compact.
so there exists $\alpha_2 \in \mathcal{S}$
such that $|\alpha_2| = \sup_{\beta \in \mathcal{S}} |\beta|$

We want to prove that $f(\alpha_2) = 0$
Assume that $f(\alpha_2) > 0$ and choose $\varepsilon \in]0, f(\alpha_2)[$
Let $q = X^2 - (\alpha_2 + \bar{\alpha}_2) X + \alpha_2 \bar{\alpha}_2 + \varepsilon$.
$\Delta = (\alpha_2 + \bar{\alpha}_2)^2 - 4\alpha_2\bar{\alpha}_2 - \varepsilon = -|\alpha_2 - \bar{\alpha}_2|^2 - \varepsilon < 0$
Let $\alpha_3, \bar{\alpha}_3 \notin \mathbb{R}$ be the roots of q

$$\alpha_3 \bar{\alpha}_3 = \alpha_2 \bar{\alpha}_2 + \varepsilon > \alpha_2 \bar{\alpha}_2$$

Thus $|\alpha_3| > |\alpha_2|$ and $\alpha_3 \notin \mathcal{S}$
Let $n \in \mathbb{N} - \{0\}$, put

$$G_n(X) = \left[X^2 - (\alpha_2 + \bar{\alpha}_2) X + \alpha_2 \bar{\alpha}_2\right]^n - (-\varepsilon)^n \in \mathbb{R}[X]$$
$$= \prod_{i=1}^{n} (X - \beta_i) = \prod_{i=1}^{n} (X - \bar{\beta}_i)$$

$G_n(\alpha_3) = 0$, so we may assume that $\beta_1 = \alpha_3$

$$G_n(X)^2 = \prod_{i=1}^{n} \underbrace{(X^2 - (\beta_i + \bar{\beta}_i) X + \beta_i \bar{\beta}_i)}_{\in \mathbb{R}[X]}$$

$$|G_n(\xi)|^2 = \prod_{i=1}^{2n} f(\beta_i) \geq f(\alpha_3)\, f(\alpha_2)^{2n-1}$$

On the other hand

$$|G_n(\xi)| \leq f(\alpha_2)^n + \varepsilon^n$$

We get

$$f(\alpha_3)\, f(\alpha_2)^{2n-1} \leq \left(f(\alpha_2)^n + \varepsilon^n\right)^2$$

and $\dfrac{f(\alpha_3)}{f(\alpha_2)} \leq \left[1 + \left(\underbrace{\dfrac{\varepsilon}{f(\alpha_0)}}_{<1}\right)^n\right]^2 \xrightarrow[n \to +\infty]{} 1$

and $f(\alpha_3) = f(\alpha_2)$ thus $\alpha_3 \in \mathcal{S}$ ↯ contradiction

Therefore $f(\alpha_2)=0$ and $\xi^2-(\alpha_2+\bar{\alpha}_2)\xi+\alpha_2\bar{\alpha}_2=0$
Thus $\mathbb{K}/\mathbb{R}$ is algebraic. □

Lemma 2

An absolute value $|\cdot|$ on a field $\mathbb{K}$ is non-archimedean if and only if

$$\mathbb{Z}.1 \subset \{x\in\mathbb{K} \mid |x|\leq 1\}.$$

Proof

⇒) If $|\cdot|$ is non-archimedean

$$\forall n\in\mathbb{N},\ \begin{cases} |n+1| \leq \max(|n|,1) \\ |-n1| = |n1| \end{cases}$$

Thus by induction we get

$$\mathbb{Z}.1 \subset \{x\in\mathbb{K} \mid |x|\leq 1\}$$

⇐) Assume that $\forall n\in\mathbb{Z},\ |n|\leq 1$

Let $a, b\in\mathbb{K}$, we want to prove that $|a+b|\leq \max(|a|,|b|)$

But

$$|a+b|^n = |(a+b)^n| = \left|\sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}\right|$$

$$\leq \sum_{k=0}^{n} \left|\binom{n}{k}.1\right| |a|^k |b|^{n-k}$$

$$\leq \sum_{k=0}^{n} \max(|a|,|b|)^n$$

Therefore

$$|a+b| \leq (n+1)^{\frac{1}{n}} \max(|a|,|b|)$$

but $\frac{1}{n}\log(1+n) \underset{n\to+\infty}{\Rightarrow} 0$ so $(n+1)^{\frac{1}{n}} \underset{n\to+\infty}{\to} 1$

and

$$|a+b| \leq \max(|a|,|b|). \quad \square$$

Proof of the theorem

- Let $\mathbb{K}$ be complete for an archimedean absolute value $|\cdot|$. By lemma 2, there exists $n \in \mathbb{Z}$ such that $|n.1| > 1$
  In particular $|n^k.1| \xrightarrow[k\to+\infty]{} +\infty$
  and $\{|n.1|,\ n \in \mathbb{Z}\}$ is infinite
  Thus $\mathrm{char}(\mathbb{K}) = 0$ and $\mathbb{K}$ is a $\mathbb{Q}$ algebra
- $|\cdot| \circ \varphi_{\mathbb{K}/\mathbb{Q}}$ is an archimedean absolute value on $\mathbb{Q}$, and by the classification on $\mathbb{Q}$ there is $\lambda \in \mathbb{R}_+^*$ such that
  $$\forall x \in \mathbb{Q} \quad |\varphi_{\mathbb{K}/\mathbb{Q}}(x)| = |x|_\infty^\lambda$$
- Let $\mathbb{R}'$ be the closure of $\varphi_{\mathbb{K}/\mathbb{Q}}(\mathbb{Q})$ in $\mathbb{K}$.
  Let $x, y \in \mathbb{R}'$, choose $(x_n)_{n\in\mathbb{N}}, (y_n)_{n\in\mathbb{N}}$ in $\mathbb{Q}^{\mathbb{N}}$ such that $\varphi_{\mathbb{K}/\mathbb{Q}}(x_n) \xrightarrow[n\to+\infty]{} x$ and $\varphi_{\mathbb{K}/\mathbb{Q}}(y_n) \xrightarrow[n\to+\infty]{} y$

  Then $x+y = \lim_{n\to+\infty} (x_n + y_n) \in \mathbb{R}'$
  $xy = \lim_{n\to+\infty} (x_n y_n) \in \mathbb{R}'$
  Similarly $\forall x \in \mathbb{R}'^* = \mathbb{R}' - \{0\}$, $1/x \in \mathbb{R}'$
  $\mathbb{R}'$ is a field
  It is closed in $\mathbb{K}$, therefore it is complete.
- By the unicity statement for the completion, there exists a unique isomorphism
  $$\varphi : \mathbb{R} \to \mathbb{R}'$$
  such that
  $$\forall x \in \mathbb{Q}, \quad \varphi(x) = \varphi_{\mathbb{K}/\mathbb{Q}}(x)$$
  and $\forall x \in \mathbb{R}, \quad |\varphi(x)| = |x|^\lambda$.
- Thus $\mathbb{K}$ is an $\mathbb{R}$-algebra and by lemma 1
  $\mathbb{K}/\mathbb{R}$ is algebraic
  Since $\mathbb{C}$ is algebraic closed

There is a morphism of $\mathbb{R}$ algebras
$$\sigma : K \to \mathbb{C}$$
Since $[\mathbb{C} : \mathbb{R}] = 2$, $\sigma(K) = \mathbb{R}$ or $\sigma(K) = \mathbb{C}$
In the first case we are done
otherwise
$$|\cdot| \circ \sigma \quad \text{and} \quad |\cdot|^{1/\lambda}$$
are norms of the $\mathbb{R}$ algebra K
thus they define the same topology on K
therefore they are dependant.
So there is $\lambda' \in \mathbb{R}_{>0}$ such that
$$\forall x \in K \quad |x| = |\sigma(x)|^{\lambda'}$$
(In fact $\lambda' = \lambda$). □

d) Algebraic extensions of complete fields

Theorem 1

Let K be a complete field for a non-trivial absolute value $|\cdot|$
Let L be an algebraic extension of K
Then there exists a unique absolute values $|\cdot|'$ on L such that $|\cdot|' \circ \iota_{L/K} = |\cdot|$
If L/K is finite then L is complete and
$$\forall \alpha \in L, \quad |\alpha|' = |N_{L/K}(\alpha)|^{\frac{1}{[L:K]}}$$

Beginning of the proof.

1st case

If $|\cdot|$ is archimedean then K is isomorphic to $\mathbb{R}$ or $\mathbb{C}$ and the result is true.

2nd case:

o From now on, we assume that $|\cdot|$ is not archimedean, & the topology defined by $|\cdot|$

Then

$$A = \mathcal{O}_v = \{x \in \mathbb{K} \mid |x| \leq 1\}$$

is a subring of $\mathbb{K}$, and

$$\mathfrak{M}_v = \{x \in \mathbb{K} \mid |x| < 1\} \neq 1$$

is an ideal in $\mathcal{O}_{\mathbb{K}}$.

$$\mathbb{K} = \mathcal{O}_v \cup \mathcal{O}_v^{-1}$$

where $\mathcal{O}_{\mathbb{K}}^{-1} = \{\frac{1}{x},\ x \in \mathcal{O}_{\mathbb{K}} - \{0\}\}$.

and

$$\mathcal{O}_v^* = \mathcal{O}_v \cap \mathcal{O}_v^{-1} = \{x \in \mathbb{K} \mid |x| = 1\}.$$

By definition the projection map

$$\mathcal{O}_v^* \longrightarrow \mathcal{O}_v/\mathfrak{M}_v - \{0\} \text{ is surjective}$$

thus

$$\kappa_v = \mathcal{O}_v/\mathfrak{M}_v$$

is a field and $\mathfrak{M}_v$ is a maximal ideal of $\mathcal{O}_{\mathbb{K}}$

o We shall first consider the case where $\mathbb{L}/\mathbb{K}$ is finite

o Let B_0 be the integral closure of A in $\mathbb{L}$.

We want to find a maximal ideal $\mathfrak{M}$ of B_0 such that $\mathfrak{M} \cap \mathcal{O}_{\mathbb{K}} = \mathfrak{M}_v$

we need to prove that

$$B_0 \neq \mathfrak{M}_v B_0.$$

Lecture 9

Definition

A commutative ring A is called a local ring if it has a unique maximal ideal $\mathfrak{M}_A$.

Examples

- If A is a discrete valuation ring, A is a local ring, $\mathfrak{m}_A = \{x \in A \mid v(x) > 0\}$.
- Let $\mathfrak{p}$ be a prime ideal of ring A, $A_{(\mathfrak{p})}$ is local
- Let K be a complete field for a non trivial absolute value $|\cdot|$ then

$\mathcal{O}_K$ is a local ring

Proof

Let I be an ideal of $\mathcal{O}_K$, $I \subsetneq \mathfrak{m}_K$
then let $x \in I - \mathfrak{m}_K \subset \mathcal{O}_K - \mathfrak{m}_K = \mathcal{O}_K^*$
$1 = x^{-1} x \in I$
Thus $I = \mathcal{O}_K$. □

Theorem 2 (Nakayama's lemma)

Let A be a commutative ring and let $\mathfrak{a} \subset A$ be an ideal contained in any maximal ideal of A
Let M be a finitely generated A-module
If $\mathfrak{a} M = M$ then $M = \{0\}$.

Proof

Let $(e_1, \dots, e_s)$ be a generating family for M. We prove the result by induction on s.
If $s = 0$ then $M = \{0\}$.
Assume $s > 0$ and the result proven for $s-1$.
$e_s \in M = \mathfrak{a} M$ thus

$$e_s = \sum_{i=1}^{n} a_i x_i \quad \text{with } (a_1, \dots, a_n) \in \mathfrak{a}^n, \ (x_1, \dots, x_n) \in M^n$$

Writing $x_i = \sum_{j=1}^{s} \lambda_{ij} e_j$

we get $e_s = \sum_{j=1}^{s} \underbrace{\left(\sum_{i=1}^{n} b_i \lambda_{ij}\right)}_{a_j \in \mathfrak{a}} e_j$

Thus $(1 - a_s) e_s = \sum_{i=1}^{s-1} a_i e_i$

But, for any maximal ideal $\mathfrak{m}$ of A $a_s \in \mathfrak{m}$, thus $1 - a_s \notin \mathfrak{m}$ ie $(1-a_s) \notin \mathfrak{m}$

we get $A = (1-a_s)$ and $1 - a_s \in A^*$

$$e_s = \sum_{i=1}^{s-1} \frac{a_i}{1-a_s} e_i$$

and M is generated by $(e_1, \dots, e_{s-1})$

By induction we get that $M = \{0\}$ □

Corollary 1

Let A be a local ring and let M be a finitely generated A-module

If $M = \mathfrak{m}_A M$ then $M = \{0\}$

We apply Nakayama's lemma to the ideal $\mathfrak{m}_A$ which is the unique maximal ideal of A.

Corollary 2

Let A be an integral ring, $K = Fr(A)$, L be a finite extension of K and $\mathfrak{m}$ be a maximal ideal of A.

Let B be the integral closure of A in L

Then there exists a maximal ideal $\mathfrak{M}$ of B such that

$$\mathfrak{m} B \subset \mathfrak{M}$$

Proof By localizing we may assume $A = A_{(\mathfrak{p})}$
Assume that $B = \mathfrak{m} B$, then we may write

$$(*) \qquad 1 = \sum_{i=1}^{r} a_i b_i$$

with $r \in \mathbb{N}$, $a_1, \dots, a_r \in \mathfrak{m}$ and $b_1, \dots, b_r \in B$
Let $B_0 = A[b_1, \dots, b_r] \subset B$
Since $b_1, \dots, b_r$ are integral over A,
B_0 is a finitely generated A-module
By $(*)$, $B_0 = \mathfrak{m} B_0$
Absurd since $1 \neq 0$ in $\mathbb{L}$ and thus in B_0
So $B \neq \mathfrak{m} B$ and we may apply
Krull's theorem □

NB

$$\mathfrak{f}_{\mathbb{L}/\mathbb{K}}^{-1}(\mathfrak{M}) \cap A \supset \mathfrak{m}$$

$\mathfrak{M}$
1

Thus $\mathfrak{m} = \mathfrak{f}_{\mathbb{L}/\mathbb{K}}^{-1}(\mathfrak{M}) \cap A$.

Let me turn back to the proof of theorem 1

Lemma 1
There exists a subring B of $\mathbb{L}$ containing $\mathfrak{f}_{\mathbb{L}/\mathbb{K}}(G_v)$ such that
(i) $\mathfrak{m}_v B \neq B$
(ii) $\forall x \in \mathbb{L}$, $x \in B$ or $x^{-1} \in B$.

Proof
Let X be the set of subrings B

of $\mathcal{U}$ which satisfy (i). We have seen that $B_0 \in X$ (corollary 2)
X is ordered by the inclusion.
If Y is a totally ordered non empty subset of X then

$B' = \bigcup_{B \in Y} B$ is a subring of $\mathcal{U}$

and if $\mathfrak{M}' = \mathfrak{M} \cap B'$ then we may write

$(*)$ $1 = \sum_{i=1}^{n} a_i b_i$ as before

and there is $B \in Y$ such that $b_1, \dots, b_n \in B$

By $(*)$ $B = \mathfrak{M} \cap B$ obtained

Thus $B' \in X$.

By Zorn's lemma X has a maximal element B.

By corollary 2, B is integrally closed.

Let $\mathfrak{M}$ be a maximal ideal of B which contains $\mathfrak{M} \cap B$.

we have $B_{(\mathfrak{M})} \supset \mathfrak{M} \cdot B_{(\mathfrak{M})} \supset \mathfrak{M} \cap B_{(\mathfrak{M})}$

Thus $B = B_{(\mathfrak{M})}$ is local

Let $x \in \mathcal{U} - B$

By maximality of B

$$B[x] = \mathfrak{M} \cap B[x]$$

and thus $B[x] = \mathfrak{M} B[x]$

we may write

$$1 = \sum_{i=1}^{n} a_i x^i$$

with $a_1, \dots, a_n \in \mathfrak{M}$.

$1 - a_0 \in B^*$ since B is local

and $\left(\frac{1}{x}\right)^n + \sum_{i=2}^{n} \frac{a_i}{1-a_0} \left(\frac{1}{x}\right)^{n-i} = 0$

Thus $\frac{1}{x}$ is integral over B; we get $\frac{1}{x} \in B$. □

We now put

$$V_K = K^*/\mathcal{O}_K^* \quad \text{and} \quad V_L = L^*/B^*$$

The absolute value

$$|\cdot| : K \longrightarrow \mathbb{R}$$

induce an injective morphism of group

$$\nu : V_K \hookrightarrow \mathbb{R}_{>0}$$
$$\bar{x} \longmapsto |x|$$

and the structural morphism $\beta_{L/K}$ gives a morphism

$$\varphi : V_K \longrightarrow V_L .$$

Lemma 2

The relation on V_L defined by

$$\bar{a} \leq \bar{b} \iff aB \subset bB$$

is a total order compatible with the group law on V_L.

Proof.

- reflexive, transitive;
- $\bar{a} \leq \bar{b}$ & $\bar{b} \leq \bar{a}$ implies $bB = aB$

  that is $\begin{cases} b = ac, & \text{for } c \in B \\ a = bd & \text{for } d \in B \end{cases}$

  $cd = 1$ thus $\bar{a} = \bar{b}$
- $\forall a, b, c \in L$, $\bar{a} \leq \bar{b} \Rightarrow \bar{a}\,\bar{c} \leq \bar{b}\,\bar{c}$
- $a, b \in L$ $\frac{b}{a} \in B$ or $\frac{a}{b} \in B$

  thus $\bar{a} \geqslant \bar{b}$ or $\bar{b} \geqslant \bar{a}$. □

N.B.

ν induces an order $\leqslant$ on V_K such that $\bar{a} \leqslant \bar{b} \iff a\mathcal{O}_K \subset b\mathcal{O}_K$

$\Updownarrow$

$|a| \leq |b|$

Thus φ is increasing.

Lemma 3

$f_{L/K}^{-1}(B) = \mathcal{O}_L$ and φ is injective.

Proof.

If $x \in K$, $|x| > 1$, then $x^{-1} \in \mathfrak{m}_v$

Thus $f_{L/K}(x^{-1}) \in \mathfrak{m}_v B$ and $\mathfrak{m}_v B \cap B^* = \emptyset$

So $f_{L/K}(x) \notin B$.

If $f_{L/K}(a) = f_{L/K}(b)$

we have $f_{L/K}(a/b) \in B$ and $f_{L/K}(b/a) \in B$

Thus $\bar{a} = \bar{b}$. □

Lemma 4

$[V_L : \varphi(V_K)] < [L : K]$

Proof

Let $e_1, \dots, e_d \in L^*$ have distinct images in $V_L / \varphi(V_K)$.

Assume they are linear dependant on K.

ie

$$\sum_{i=1}^{d} a_i e_i = 0$$

with $a_1, \dots, a_d \in K$, $(a_1, \dots, a_d) \neq 0$.

We may assume (reducing d if necessary)

that $a_1 \neq 0, \dots, a_d \neq 0$.

By exchanging $e_1, \dots, e_d$ we may also assume

$$\overline{a_1 e_1} \geq \overline{a_2 e_2} \geq \dots \geq \overline{a_d e_d}$$

ie $a_{i+1} e_{i+1} \in a_i e_i B$

Thus $\sum_{i=2}^{n} a_i e_i \in a_2 e_2 B$.

$= -a_1 e_1$

$\overline{a_1 e_1} = \overline{a_2 e_2}$

contradicts the fact that e_1 and e_2 have different images in $V_\mu / \varphi(V_K)$

So $e_1, \dots, e_d$ are linearly independent over K

We get $\# V_\mu / \varphi(V_K) \leq d$.

End of the proof of Theorem 2

- Existence in the finite case

Since V_μ is totally ordered.

for any $n \in \mathbb{N}_{>0}$, $x \mapsto x^n$ is injective in V_μ. ($x > 0 \Rightarrow x^n > 0$).

Let $e = V_\mu / \varphi(V_K)$

we have

$$\begin{array}{ccccc} U^* & \longrightarrow & V_\mu & \xrightarrow{\times e} & \varphi(V_K) \\ \downarrow |\cdot|' & & \downarrow & \text{increasing injection} & \updownarrow \text{bijection} \\ \mathbb{R}_{>0} & \xleftarrow{x^{1/n}} & \mathbb{R}_{>0} & \xleftarrow{|\cdot|} & V_K \end{array}$$

If $|x|' \leq |y|'$ ie $\overline{x} \leq \overline{y}$ ie $x \in yB$

$x + y \in yB$ ie $\overline{x+y} \leq \overline{y}$

ie $|x+y|' \leq |y|'$

So $|x+y|' \leq \max(|x|', |y|')$.

And by construction

$\forall x \in K$, $|\varphi_{\mu|K}(x)|' = |x|$

- Unicity in the finite case.

$|\cdot|'$ and $|\cdot|''$ are norms on the K vector space μ

they define the same topology
thus they are dependant
Since they coincide on $\mathbb{Q}$ ($\mathbb{K}$)
and $|\cdot|$ is not trivial, they coincide.

- If $\mathbb{L}/\mathbb{K}$ is finite, $\mathbb{L}$ is complete.
- Construction and unicity in the algebraic case:

$$\mathbb{L} = \bigcup_{\substack{\mathbb{L}' \subset \mathbb{L} \\ \mathbb{L}'/\mathbb{K} \text{ finite}}} \mathbb{L}'$$

On any such $\mathbb{L}'$ $|\cdot|'$ is well defined and $|x|'$ does not depend on the choice of $\mathbb{L}' \subset \mathbb{L}$, $\mathbb{L}' \ni x$, $\mathbb{L}'/\mathbb{K}$ finite we get $|\cdot|' : \mathbb{L} \to \mathbb{R}$.

It remains to prove the formula.

- Let $\overline{\mathbb{K}}$ be an algebraic closure of $\mathbb{K}$ and $|\cdot|''$ the extension of $|\cdot|$ to $\overline{\mathbb{K}}$. By unicity

$$\forall \sigma \in \mathbb{L}/\mathbb{K}, \quad |x|' = |\sigma(x)|''$$

So

$$|x^{[\mathbb{L}:\mathbb{K}]}|' = \left| \left(\prod_{\sigma \in \Sigma_{\mathbb{L}/\mathbb{K}}} \sigma(x) \right)^{[\mathbb{L}:\mathbb{K}]_s} \right|''$$

$$= \left| \mathbb{Q}_{\mathbb{L}/\mathbb{K}} \left(N_{\mathbb{L}/\mathbb{K}}(x) \right) \right|''$$

$$= |N_{\mathbb{L}/\mathbb{K}}(x)| \quad \square$$

6) Completion for discrete valuations

Aim

Describe $|K_v$ when v is defined by $x \mapsto \alpha^{v(x)}$ where v is a surjective discrete valuation (eg $\mathbb{Q}_p$).

Definition

Let I be an ordered set. An *inverse system of sets relative to I* is a family of sets $(E_\alpha)_{\alpha \in I}$ equipped for each $(\alpha, \beta) \in I^2$ such that $\alpha \leq \beta$ with a map

$$f_{\alpha,\beta} : E_\beta \to E_\alpha$$

so that

(i) $\forall \alpha \in I$, $f_{\alpha,\alpha} = Id_{E_\alpha}$

(ii) $\forall \alpha, \beta, \gamma \in I$, $\alpha \leq \beta \leq \gamma \Rightarrow f_{\alpha,\gamma} = f_{\alpha,\beta} \circ f_{\beta,\gamma}$

The *inverse limit* of the system $(E_\alpha)_{\alpha \in I}$ is the set

$$\varprojlim_{\alpha \in I} E_\alpha = \left\{ (x_\alpha)_{\alpha \in I} \in \prod_{\alpha \in I} E_\alpha \;\middle|\; \forall \alpha, \beta \in I, \alpha \leq \beta \Rightarrow f_{\alpha,\beta}(x_\beta) = x_\alpha \right\}$$

We denote f_α the restriction of the projection p_α to $\varprojlim_{\alpha \in I} E_\alpha$

$$\forall \alpha, \beta \in I, \quad \alpha \leq \beta \Rightarrow f_\alpha = f_{\alpha,\beta} \circ f_\beta$$

Remark

We say that $(E_\alpha)_{\alpha \in I}$ is an inverse system of groups (resp. ring, module, topological space, ...) if each E_α is a group (resp ring, module, top. space, ...)

and the maps $f_{\alpha\beta}$ are morphism (resp. morphism, morphism, continuous, ...)
Then the inverse limit is a group (resp. ring, module, top. space (for the topology induced by the product topology).

Universal Property of the inverse limit

Let $(E_\alpha)_{\alpha \in I}$ be an inverse system
Let F be a set and for each $\alpha \in I$
Let $g_\alpha : F \to E_\alpha$ be a map so that

$$\forall \alpha, \beta \in I, \ \alpha \leq \beta \Rightarrow g_\alpha = f_{\alpha,\beta} \circ g_\beta$$

Then there exists a unique map

$$g : F \to \varprojlim_{\alpha \in I} E_\alpha$$

which satisfies

$$\forall i \in I, \quad g_\alpha = f_\alpha \circ g.$$

it is given by

$$g(f) = (g_\alpha(f))_{\alpha \in I}.$$

The proof is in the statement.

Notation

Let v be a surjective discrete valuation on a field $\mathbb{K}$, let $\alpha \in \mathbb{R}_{>1}$

$$|x|_v = \alpha^{-v(x)}$$

for $x \in \mathbb{K}$, we also denote by v the place of $\mathbb{K}$ defined by $|\cdot|_v$ (abuse of language) in that case,

$$\mathcal{O}_v = \{ x \in \mathbb{K} \mid v(x) \geq 0 \}$$

$\mathfrak{m}_v = \{ x \in K \mid v(x) > 0 \}$

We equip $\mathcal{O}_v / \mathfrak{m}_v^n$ with the discrete topology and for $m, n \in \mathbb{N}$ with $m \leq n$ we define

$$\pi_{m,n} : \mathcal{O}_v / \mathfrak{m}_v^n \longrightarrow \mathcal{O}_v / \mathfrak{m}_v^m$$

as the quotient map. This defines a inverse system of topological rings relative to $\mathbb{N}$

Let $\widehat{K}_v$ be the completion of K for v, $|\cdot|_w$ be the extension of $|\cdot|_v$ to $\widehat{K}$ and

$$\mathcal{O}_w = \{ x \in \widehat{K} \mid |x|_w \leq 1 \}$$
$$\mathfrak{m}_w = \{ x \in \widehat{K} \mid |x|_w < 1 \} \qquad \hat{\pi}_n : \mathcal{O}_w \to \mathcal{O}_w / \mathfrak{m}_w^n$$

Theorem

a) $\mathcal{O}_w$ is the closure of $j(\mathcal{O}_v)$ in $\widehat{K}$

b) The natural morphism of $\mathcal{O}_w$ algebras

$$\varphi_n : \mathcal{O}_w / \mathfrak{m}_w^n \longrightarrow \mathcal{O}_w / \mathfrak{m}_w^n$$

is an isomorphism and the induced map $\varphi_n^{-1} \circ \pi_n : \mathcal{O}_w \to \mathcal{O}_v / \mathfrak{m}_v^n$ give an isomorphism of topological rings

$$\mathcal{O}_w \longrightarrow \varprojlim_n \mathcal{O}_v / \mathfrak{m}_v^n$$

Proof

a) Let $x \in \mathcal{O}_w$ and let $(x_n)_{n \in \mathbb{N}}$ a sequence in K such that $j_{\widehat{K}/K}(x_n) \xrightarrow[n \to +\infty]{} x$

Then $(|x_n|_v)_{n\in\mathbb{N}}$ converges in $\mathbb{R}$ to $|x|_v \leq 1$

But

$$\forall x \in \mathbb{K},\ |x| \in \{0\} \cup \alpha^{\mathbb{Z}}$$

There is $N \in \mathbb{N}$ such that

$$\forall n \in \mathbb{N},\ n \geq N \Rightarrow |x_n|_v < \alpha$$

So $n \geq N \Rightarrow x_n \in \mathcal{O}_v$

So $\mathcal{O}_w \subset \overline{\jmath_{\mathbb{K}/\mathbb{K}}(\mathcal{O}_v)}$ since $\mathcal{O}_w$ is closed

and $\jmath_{\mathbb{K}/\mathbb{K}}(\mathcal{O}_v) \subset \mathcal{O}_w$, $\mathcal{O}_w = \overline{\jmath_{\mathbb{K}/\mathbb{K}}(\mathcal{O}_v)}$

b) • Let $x \in \mathcal{O}_v$ if $\jmath_{\mathbb{K}/\mathbb{K}}(x) \in \mathfrak{M}_w^n$

then $|\jmath_{\mathbb{K}/\mathbb{K}}(x)|_w \leq \alpha^{-n}$

and $|x|_v \leq \alpha^{-n}$ and $x \in \mathfrak{m}_v^n$

Therefore

$\jmath_n$ is injective

• Let $n \in \mathbb{N}$

Take $x \in \mathcal{O}_w$ let $(x_n)_{n\in\mathbb{N}}$

be a sequence in $\mathcal{O}_v$ converging to x

There is $N \in \mathbb{N}$ such that

$$\forall m \in \mathbb{N},\ m \geq N \Rightarrow |x - \jmath_{\mathbb{K}/\mathbb{K}}(x_n)|_w < \alpha^{-n}$$

so

$$x - \jmath_{\mathbb{K}/\mathbb{K}}(x_N) \in \mathfrak{M}_w^n$$

and

$$\jmath_n(\overline{x_N}) = \overline{x}$$

So $\jmath_n$ is surjective.

• We get a morphism of rings

$$\varphi : \mathcal{O}_w \longrightarrow \varprojlim_n \mathcal{O}_v/\mathfrak{M}_v^n$$

• Let $x \in \mathcal{O}_w$

If $\varphi(x) = 0$

then $\forall n$ $\jmath_n^{-1} \circ \pi_n(x) = 0$

then $\forall n$ $x \in \mathfrak{m}_w^n$

then $\forall n \in \mathbb{N} \quad |x|_w \leq \alpha^{-n}$
then $|x|_w = 0$ and $x = 0$
Thus φ is injective.

- Let $x = (x_n)_{n\in\mathbb{N}} \in \varprojlim_n G_v / \mathfrak{M}_v^n$

for any $n \in \mathbb{N}$ let $y_n \in G_v$ be a representative of x_n
for any $p, q \in \mathbb{N}$ with $p \leq q$
we have

$$\pi_{p,q}(x_q) = x_p .$$

Thus

$$y_q - y_p \in \mathfrak{M}_v^p$$

and $$|y_q - y_p|_v \leq \alpha^{-\min(p,q)} \qquad (*)$$

so $(y_n)_{n\in\mathbb{N}}$ is a Cauchy sequence
as is its image in $\widehat{K}$
Let $y = \lim_{n\to+\infty} g_{\widehat{K}/K}(y_n)$

By $(*)$

$$|y - g_{\widehat{K}/K}(y_p)|_w \leq \alpha^{-p}$$

ie

$$g_n^{-1} \circ \pi_n(y) = \overline{y_p} = x_p$$

So $\varphi(y) = x$ and φ is surjective.

- We still have to show that φ is an homeomorphism.
Let $n \in \mathbb{N}$, $x \in G_v / \mathfrak{M}_v^n$
Let $y = g_{\widehat{K}/K}(x)$

Then $g_n^{-1} \circ \pi_n(\{x\}) = y + \mathfrak{M}_w^n$
$= \{z \in G_w \mid |y - z|_w < \alpha^{-n+1}\}$
is open in G_w

So φ is continuous.
We only have to show that φ is open that is sends open subsets of $\mathcal{O}_w$ to open subsets

Let U be open in $\mathcal{O}_w$, $U \neq \emptyset$
Let $y \in U \cap \varphi_{H/K}(\mathcal{O}_v)$ ($\mathcal{O}_v$ is dense in $\mathcal{O}_w$)
There is $m \in \mathbb{N}$ such that

$$\{ z \in \mathcal{O}_w \mid |z-y|_w < \alpha^{-m+1} \} \subset U$$

ie $y + \mathfrak{m}_w^m \subset U$ $\quad y = \varphi_{H/K}(x)$.

Let $z = (\overline{z}_n)_{n \in \mathbb{N}} \in \varprojlim_{n \in \mathbb{N}} \mathcal{O}_v/\mathfrak{m}_v^n$

Δ $z \in \varphi(y + \mathfrak{m}_w^m)$
iff $y - \lim_{n \to +\infty} \varphi_{H/K}(z_n) \in \mathfrak{m}_w^m$

iff $\lim_{n \to +\infty} |x - z_n|_v \leq \alpha^{-m}$

Remember $|z_p - z_q|_v \leq \alpha^{-\min(p,q)}$
We get
Δ iff $|x - z_m|_v \leq \alpha^{-m}$
ie $\overline{z}_m = \overline{x}$ in $\mathcal{O}_v/\mathfrak{m}_v^m$

if $\mathrm{pr}_m : \varprojlim_{n \in \mathbb{N}} \mathcal{O}_v/\mathfrak{m}_v^n \to \mathcal{O}_v/\mathfrak{m}_v^m$
is the m-th projection

$$\varphi(y + \mathfrak{m}_w^m) = \mathrm{pr}_m^{-1}(\mathrm{pr}_m(\overline{x})).$$

But pr_m is continuous so it is open in $\varprojlim_{n \in \mathbb{N}} \mathcal{O}_v/\mathfrak{m}_v^n$.

Corollary

K is locally compact if and only if $\mathcal{O}_v / \mathfrak{m}_v$ is finite.

Then $\mathcal{O}_w$ is compact.

Proof

$\Leftarrow$ $\mathfrak{m}_v^n / \mathfrak{m}_v^{n+1}$ is a $\mathcal{O}_v / \mathfrak{m}_v$ vector space of dimension one. ($\mathcal{O}_v$ is a Dedekind ring). Thus $\mathcal{O}_v / \mathfrak{m}_v^k$ is finite

A finite set is compact for the discrete topology

By ~~Tychonov's~~ theorem,

$$\prod_{n \in \mathbb{N}} \mathcal{O}_v / \mathfrak{m}_v^n \text{ is compact}$$

$\cup$ closed

$$\varprojlim_n \mathcal{O}_v / \mathfrak{m}_v^n$$

So it is compact and $\mathcal{O}_w$ is compact

$\therefore$ $\mathfrak{m}_w^n = \{ x \in \mathcal{O}_w \mid |x|_w \leq \alpha^{-n} \} \subset \mathcal{O}_w$ closed

is compact.

$y + \mathfrak{m}_w^n$ is compact for any $y \in K_w$

But any neighbourhood of y contains such a set

$\Rightarrow$ Let $\pi \in K_w$ be such that $|\pi|_w = \alpha^{-1}$

Let K be a compact neighbourhood of 0, there is $n \in \mathbb{N}$ such that

$\mathfrak{m}_w^n \subset K$

compact $\quad \pi^n \mathcal{O}_w \subset \mathfrak{m}_w^n$

So $\mathcal{O}_w$ is compact

So $\underbrace{\varphi_n^{-1} \circ \pi_n}_{\text{continuous}} (\mathcal{O}_w) = \mathcal{O}_v / \mathfrak{m}_v^n$

is compact and discrete, it is finite □

Example

p a prime number

$\mathbb{Z}_p$ closure of $\mathbb{Z}$ in $\mathbb{Q}_p$.

$\mathbb{Z}_p \simeq \varprojlim_{n \in \mathbb{N}} \mathbb{Z}/p^n\mathbb{Z}$

$\mathbb{Q}_p = \mathrm{Fr}(\mathbb{Z}_p)$ is locally compact, $\mathbb{Z}_p$ is compact.

$\mathrm{char}(\mathbb{Z}_p) = 0$!

Theorem ("Reminder")

Any locally compact commutative group admits a Haar measure [that is a measure on the σ-algebra generated by compact subsets such that

(i) $\mu(a+U) = \mu(U)$

(ii) $\mu(E) = \inf\{\mu(U),\ E \subset U,\ U \text{ open and Borel}\}$

(iii) $\mu(E) = \sup\{\mu(K),\ K \subset E,\ K \text{ compact}\}$

(iv) $\mu(K) < +\infty$ for K compact]

and it is unique up to multiplication by a scalar.

Definition

If $\mathrm{Card}\, k_v$ is finite, dx_v is the unique Haar measure on k_v such that

$$dx_v(\mathcal{O}_v) = 1.$$

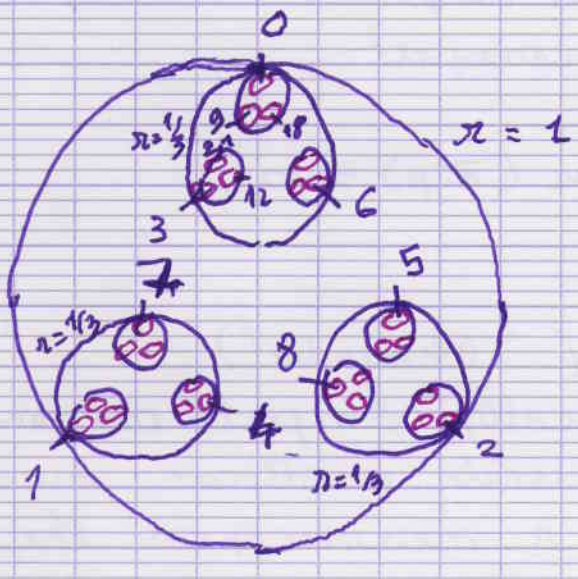
(2) In $\mathbb{K}$ the balls
$B(y,r) = \{z \in \mathbb{K} \mid |y-z|_v < r\}$
are open and closed !

That finishes the paragraph about completions

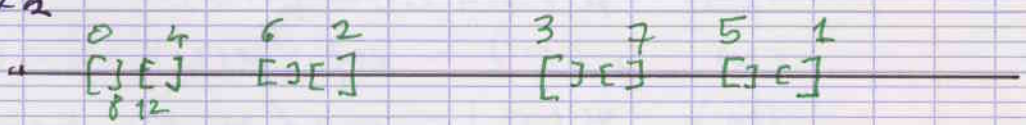
Lecture 10

Two pictures

$\mathbb{Z}_3$



$\mathbb{Z}_2$



Exercise

a) Let $\mathbb{K}$ be a complete field for a non-archimedean absolute value $|.|$. Show that a series $\sum_{n \in \mathbb{N}} \alpha_n$ converges in $\mathbb{K}$ if and only if

$$\alpha_n \xrightarrow[n \to +\infty]{} 0$$

b) Prove that any $a \in \mathbb{Z}_p$ can uniquely be written as

$$\sum_{n \in \mathbb{N}} \alpha_n p^n \text{ with } \alpha_n \in \{0, \dots, p-1\} \text{ for } n \in \mathbb{N}$$

c) Let
$$\mathcal{D} = \{ \alpha \in \mathbb{R} \mid \exists\, (\alpha_n)_{n\in\mathbb{N}} \in \{0,2\}^{\mathbb{N}},\ \alpha = \sum_{n\in\mathbb{N}} \alpha_n 3^{-(n+1)} \}$$
be the dyadic set of Cantor
Prove that
$$\mathbb{Z}_2 \longrightarrow \mathcal{D}$$
$$\sum_{n\in\mathbb{N}} \alpha_n 2^n \mapsto \sum_{n\in\mathbb{N}} 2\alpha_n 3^{-(n+1)}$$
is a homeomorphism

Lecture 16 d) Is $\mathbb{Z}_p$ homeomorphic to $\mathcal{D}$?

4) Restriction and extension of absolute values

Terminology

Let $\mathbb{L}/\mathbb{K}$ be a field extension

a) If $|\cdot|$ is an absolute value on $\mathbb{L}$, $|\cdot|_{\mathbb{L}/\mathbb{K}} = |\cdot| \circ i_{\mathbb{L}/\mathbb{K}}$ is called the restriction of $|\cdot|$ to $\mathbb{K}$.

b) If $|\cdot|$ is an absolute value on $\mathbb{K}$ and $|\cdot|'$ an absolute value on $\mathbb{L}$ we say that $|\cdot|'$ is an extension of $|\cdot|$ to $\mathbb{L}$ iff $|\cdot|$ is the restriction of $|\cdot|'$ to $\mathbb{K}$.

Proposition 1

Let $\mathbb{L}/\mathbb{K}$ be an algebraic extension and let $|\cdot|$ be an absolute value on $\mathbb{L}$

a) $|\cdot|$ is trivial iff $|\cdot|_{\mathbb{L}/\mathbb{K}}$ is trivial

b) $|\cdot|$ is non-archimedean iff $|\cdot|_{\mathbb{L}/\mathbb{K}}$ is.

Remarks

(i) The fact $|\cdot|_{\mathbb{L}/\mathbb{K}}$ is an absolute value follows from the definitions.

(ii) $\Leftarrow$ in a) and $\Rightarrow$ in b) is a consequence of the definitions

Proof

b) If $|\cdot|_{|K}$ is non archimedean
then $\mathbb{Z}.1_K \subset \{x \in |K \mid |S_{L/K}(x)| \leq 1\}$
and $\mathbb{Z}.1_L \subset \{x \in L \mid |x| \leq 1\}$
So $|\cdot|$ is non archimedean

a) Assume that $|\cdot|_{|K}$ is trivial
then it is non-archimedean
and therefore $|\cdot|$ is non-archimedean.
Let $\xi \in L$, write $\mu_\xi^K = X^d + \sum_{i=0}^{d-1} a_i X^i$
Since $|\cdot|_{|K}$ is trivial

$$|a_i| \leq 1 \text{ for } i \in \{0, \dots, d-1\}$$

So

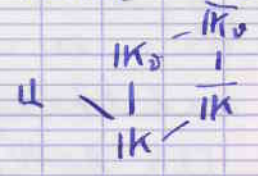
$$|\xi|^d \leq \max(1, |\xi|^{d-1})$$

we get $|\xi| \leq 1$ for $\xi \in L$
If $\xi \neq 0$ $|\xi| \leq 1$ and $|\xi^{-1}| \leq 1$ give $|\xi| = 1$.
So $|\cdot|$ is trivial. □

From now on.

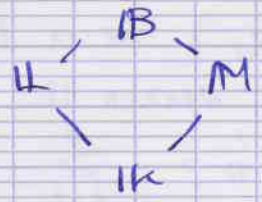
L/K is a finite extension of fields
and $|\cdot|_K$ is a non trivial absolute value on K,
$v \in \mathcal{P}\ell(K)$ is the corresponding place, K_v the completion
Then let $\overline{K_v}$ be an algebraic closure of K_v
We denote by $|\cdot|_{K_v}$ the continuous extension
of $|\cdot|_K$ to K_v
and by $|\cdot| = |\cdot|_{\overline{K_v}}$ the unique extension
of $|\cdot|_{K_v}$ to $\overline{K_v}$ (there exists a unique
such extension by last time's theorem).
Let $\overline{K}$ be the relative algebraic closure

of K in $\overline{K}_v$; it is an algebraic closure of K.
We identify a field with its image in its completion



Notation

If we have extensions of fields



We write

$$L.M = \xi_{B/L}(L)\,\xi_{B/M}(M) = K(\xi_{B/L}(L) \cup \xi_{B/M}(M)) \subset B$$

Proposition 2

Let $|\cdot|_L$ be an extension of $|\cdot|_K$ to L
We denote by $w \in Pl(L)$ the corresponding place (and write $w|v$ to say that the topology on K is the one induced by w).
Let K'_v be the closure of $\xi_{L_w/K}(K)$ in L_w
then

(i) There is a unique isomorphism of K-extensions

$$\varphi : K_v \to K'_v$$

such that $|\cdot|_{L_w} \circ \varphi = |\cdot|_{K_v}$
(we may seen L_w as a K_v-algebra)

(ii) $L_w = L.K_v$

in particular L_w/K_v is finite.

Definition

$N_w = N_{w/v} = [L_w : K_v]$ is called the local degree of w/v

Example

If v is archimedean, $N_w \in \{1, 2\}$.

Proof of proposition 2

(i) $\mathbb{K}'_v$ is closed in $\mathbb{L}_w$ and therefore complete

(i) follows from the unicity of the completion of $\mathbb{K}$ for v

(ii) Let $(e_1, \dots, e_d)$ be a basis of the $\mathbb{K}$-vector space $\mathbb{L}$.

Then $\mathbb{L}\,\mathbb{K}'_v = \sum_{i=1}^{d} \mathbb{K}'_v e_i$ is a $\mathbb{K}'_v$-vector space of finite dimension

Therefore it is complet and thus closed in $\mathbb{L}_w$

Since $\mathbb{L}$ is dense in $\mathbb{L}_w$, $\mathbb{L}_w \subset \mathbb{L}\,\mathbb{K}'_v$ □

Remark

For any $\sigma \in \Sigma_{\mathbb{L}/\mathbb{K}}$, $|\cdot|_{\overline{\mathbb{K}}_v} \circ \sigma$

defines an absolute value on $\mathbb{L}$ which extends $|\cdot|_{\mathbb{K}}$.

Theorem

a) Any extension of $|\cdot|_{\mathbb{K}}$ to $\mathbb{L}$ is of the form

$$|\cdot|_{\overline{\mathbb{K}}_v} \circ \sigma$$

for some $\sigma \in \Sigma_{\mathbb{L}/\mathbb{K}}$

b) Let $\sigma, \sigma' \in \Sigma_{\mathbb{L}/\mathbb{K}}$

then

$$|\cdot|_{\overline{\mathbb{K}}_v} \circ \sigma = |\cdot|_{\overline{\mathbb{K}}_v} \circ \sigma'$$

iff there exist $\tau \in \mathrm{Aut}_{\mathbb{K}_v}(\overline{\mathbb{K}}_v)$ such that

$$\sigma' = \tau \circ \sigma$$

Proof.

a) Let $|\cdot|_{\mathbb{L}}$ be an extension of $|\cdot|_v$ to $\mathbb{L}$ and let w be the corresponding place of $\mathbb{L}$. We have seen that $\mathbb{L}_w$ is a finite extension of $\mathbb{K}_v$ so that $|\cdot|_{\mathbb{L}_w}$ extends $|\cdot|_{\mathbb{K}_v}$.

Let $\sigma \in \Sigma_{\mathbb{L}_w/\mathbb{K}_v}$.

Then $|\cdot|_{\overline{\mathbb{K}}_v} \circ \tilde{\sigma}$ extends $|\cdot|_{\mathbb{K}_v}$.

By unicity of the extension of $|\cdot|_{\mathbb{K}_v}$ to $\mathbb{L}_w$,

$$|\cdot|_{\mathbb{L}_w} = |\cdot|_{\overline{\mathbb{K}}_v} \circ \tilde{\sigma}$$

But $\sigma = \tilde{\sigma}_{|\mathbb{L}}$ we get $|\cdot|_{\mathbb{L}} = |\cdot|_{\overline{\mathbb{K}}_v} \circ \sigma$.

b) Let w be the place of $\mathbb{L}$ defined by $|\cdot|_{\overline{\mathbb{K}}_v} \circ \sigma = |\cdot|_{\overline{\mathbb{K}}_v} \circ \sigma'$

The morphisms

$$\sigma, \sigma' : \mathbb{L} \to \overline{\mathbb{K}}_v$$

are continuous.

Let $\mathbb{L}^n \subset \overline{\mathbb{K}}$ be the normal closure of $\mathbb{L}/\mathbb{K}$

We have $\sigma(\mathbb{L}) \subset \mathbb{L}^n$ and $\sigma(\mathbb{L}') \subset \mathbb{L}^n$ and $\mathbb{L}^n/\mathbb{K}$ is finite.

Indeed let $\alpha_1, \dots, \alpha_r \in \mathbb{L}$ such that

$$\mathbb{L} = \mathbb{K}(\alpha_1, \dots, \alpha_r)$$

Then $\mathbb{L}^n = \mathbb{K}\left(\{\beta \in \overline{\mathbb{K}} \mid \exists i \in \{1, \dots, r\}, M_{\alpha_i}^{\mathbb{K}}(\beta) = 0\}\right)$

because this extension $\nearrow$ is normal over $\mathbb{K}$ and contains $\sigma(\mathbb{L})$ for any $\sigma \in \Sigma_{\mathbb{L}/\mathbb{K}}$.

We get that $\mathbb{L}^n \mathbb{K}_v \subset \overline{\mathbb{K}}_v$ is a finite extension of $\mathbb{K}_v$ and therefore complete.

So $\sigma, \sigma' : \mathbb{L} \to \mathbb{L}^n \mathbb{K}_v$ extend uniquely

to morphisms of $\mathbb{K}_v$ algebras

$$\tilde{\sigma}, \tilde{\sigma}' : \mathbb{L}_w \longrightarrow \mathbb{L}^n \mathbb{K}_v \subset \overline{\mathbb{K}_v}$$

ie $\tilde{\sigma}, \tilde{\sigma}' \in \Sigma_{\mathbb{L}_w / \mathbb{K}_v}$

Using the extension of morphisms, there is $\tau \in Aut_{\mathbb{K}_v}(\overline{\mathbb{K}_v})$ such that

$$\tilde{\sigma}' = \tilde{\sigma} \circ \tau$$

Restricting to $\mathbb{L}$ we get

$$\sigma' = \sigma \circ \tau . \qquad \square$$

Proposition

We assume moreover that $\mathbb{L}/\mathbb{K}$ is a finite separable extension then

a) $[\mathbb{L} : \mathbb{K}] = \sum_{w|v} N_w$

b) $N_{\mathbb{L}/\mathbb{K}}(\alpha) = \prod_{w|v} N_{\mathbb{L}_w/\mathbb{K}_v}(\alpha)$ for $\alpha \in \mathbb{L}$

c) $Tr_{\mathbb{L}/\mathbb{K}}(\alpha) = \sum_{w|v} Tr_{\mathbb{L}_w/\mathbb{K}_v}(\alpha)$ for $\alpha \in \mathbb{L}$

Proof

- If $w|v$, $\mathbb{L}_w = \mathbb{L}\mathbb{K}_v$.
  Thus if $\mathbb{L} = \mathbb{K}(\alpha)$,
  $\mathbb{L}_w = \mathbb{K}_v(\alpha)$
  and $\mu_\alpha^{\mathbb{K}_v} \mid \mu_\alpha^{\mathbb{K}}$ is separable
  Therefore $\mathbb{L}_w / \mathbb{K}_v$ is separable
- a) By the proof of the theorem

$$\Sigma_{\mathbb{L}/\mathbb{K}} \xrightarrow{1:1} \coprod_{w|v} \Sigma_{\mathbb{L}_w/\mathbb{K}_v}$$

$$\sigma \longmapsto \tilde{\sigma}$$

$$\sigma_{|\mathbb{L}} \longleftarrow \tilde{\sigma}$$

is a bijection

So

$$[L:K] = \#\Sigma_{L/K} = \sum_{w|v} \#\Sigma_{L_w/K_v} = \sum_{w|v} N_w$$

b) From this bijection, we also get

$$\mathcal{S}_{\bar{K}/K}(N_{L/K}(\alpha)) = \prod_{\sigma \in \Sigma_{L/K}} \sigma(\alpha)$$

$$= \prod_{w|v} \prod_{\sigma \in \Sigma_{L_w/K_v}} \sigma(\alpha)$$

$$= \prod_{w|v} \mathcal{S}_{\bar{K}_v/K_v}(N_{L_w/K_v}(\alpha)).$$

c) Similarly

$$Tr_{L/K}(\alpha) = \sum_{\sigma \in \Sigma_{L/K}} \sigma(\alpha) = \sum_{w|v} \sum_{\sigma \in \Sigma_{L_w/K_v}} \sigma(\alpha)$$

$$= \sum_{w|v} Tr_{L_w/K_v}(\alpha). \square$$

5 Applications to Dedekind rings

Remarks

(i) Let $\sigma : K \to \mathbb{R}$ be a morphism of fields and L/K a finite extension. The relative algebraic closure $\bar{K}$ of $\sigma(K)$ in $\mathbb{C}$ is an algebraic closure of K; and $|\cdot| \circ \sigma$ defines an absolute value and a place v on K.

$$N_{\mathbb{C}} = \#\{w|v,\ N_w = 2\} = \frac{1}{2}\#\{\sigma \in \Sigma_{L/K} \mid \sigma(L) \not\subset \mathbb{R}\}$$

$$|\cdot| \circ \sigma \longleftrightarrow \sigma \neq \bar{\sigma} : z \mapsto \overline{\sigma(z)}$$

$$N_{\mathbb{R}} = \#\{w|v,\ N_w = 1\}$$

and $[L:K] = 2N_{\mathbb{C}} + N_{\mathbb{R}}$.

(ii) A a Dedekind ring $K = Fr(A)$
L/K a finite extension of fields
B the integral closure of A in L.
$p \in Pl(A)$ $q \in Pl(B)$, $q \mid p$.
we have the corresponding
surjective discrete valuations
$v_p : K \to \mathbb{Z} \cup \{+\infty\}$ $v_q : L \to \mathbb{Z} \cup \{+\infty\}$
and (see a remark for an alternate description of the ramification)

(*) $\forall x \in K$, $v_q(s_{L/K}(x)) = e_{q/p} v_p(x)$

$$\begin{array}{ccc} K & \xrightarrow{v_p} & \mathbb{Z} \cup \{+\infty\} \\ \downarrow s_{L/K} & & \downarrow \times e_{L/p} \\ L & \xrightarrow[v_L]{} & \mathbb{Z} \cup \{+\infty\} \end{array}$$

v_p, v_L defines a (non-archimedean) place v of K, w of L

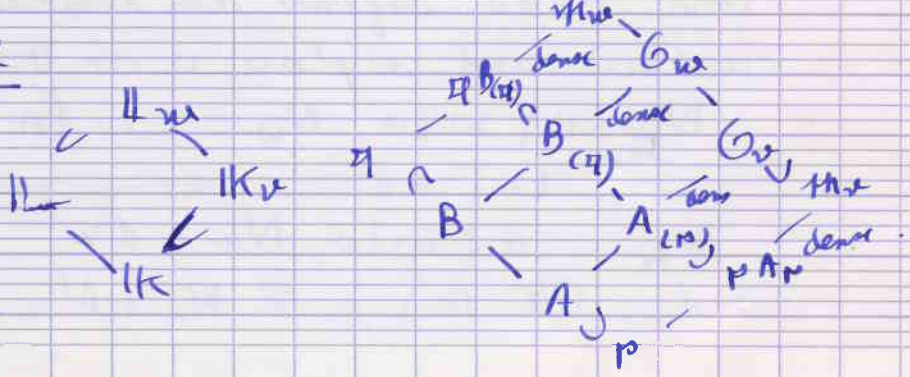
$|\cdot|_v = \alpha^{-v_p(x)}$ (for $\alpha > 1$.)

$|\cdot|_w = \alpha^{-v_q(x)}$ extends $|\cdot|_v^{e_{q/p}}$
$|\cdot|'_w = |\cdot|_w^{1/e_{q/p}}$ ——— $|\cdot|_v$

Formula

$$N_{w/v} = e_{q/p} f_{q/p}$$

Proof



Lemma 1

$$A/\mathfrak{p} \xrightarrow{\sim} A_{(\mathfrak{p})}/\mathfrak{p}A_{(\mathfrak{p})} \xrightarrow{\sim} \mathcal{O}_v/\mathfrak{M}_v$$

(and $B/\mathfrak{q} \xrightarrow{\sim} B_{(\mathfrak{q})}/\mathfrak{q}B_{(\mathfrak{q})} \xrightarrow{\sim} \mathcal{O}_w/\mathfrak{M}_w$)

Proof

- The first isomorphism has already been seen.
- $A \xrightarrow{\pi} A_{(\mathfrak{p})} \xrightarrow{\text{canonical}} A_{(\mathfrak{p})}/\mathfrak{p}A_{(\mathfrak{p})}$ is continuous for $|\cdot|_{\mathfrak{p}}$
(Indeed, $|x-y|_{\mathfrak{p}} < 1 \Leftrightarrow \pi(x) = \pi(y)$).
and $A_{(\mathfrak{p})}$ is dense in $\mathcal{O}_v$
so π extends to $\mathcal{O}_v \xrightarrow{\tilde{\pi}} A_{(\mathfrak{p})}/\mathfrak{p}A_{(\mathfrak{p})}$

$$\begin{array}{ccc} A_{(\mathfrak{p})} & \longrightarrow & A_{(\mathfrak{p})}/\mathfrak{p}A_{(\mathfrak{p})} \\ \downarrow & \overset{\tilde{\pi}}{\nearrow} & \downarrow \overset{\tilde{\pi}}{\wr} \\ \mathcal{O}_v & \longrightarrow & \mathcal{O}_v/\mathfrak{M}_v \end{array}$$

the map is 1:1.

Remark

we get $f_{\mathfrak{M}_w/\mathfrak{M}_v} = f_{\mathfrak{N}/\mathfrak{p}}$

Lemma 2

$\mathcal{O}_w$ is the integral closure of $\mathcal{O}_v$ in $\mathbb{L}_w$.

Proof

Let $\overline{\mathbb{K}_v}$ be an algebraic closure of $\mathbb{K}_v$ and $|\cdot|_{\overline{\mathbb{K}_v}}$ the unique extension of $|\cdot|_v$ to $\overline{\mathbb{K}_v}$
$\forall \sigma \in \Sigma_{\mathbb{L}_w/\mathbb{K}_v}$, $|\cdot|_{\overline{\mathbb{K}_v}} \circ \sigma = |\cdot|_w$
Thanks to the unicity of extension

So if $\alpha \in \mathcal{O}_w$ $\sigma(\alpha) \in \{\beta \in \overline{K_v} \mid |\beta|_{\overline{K}} \leq 1\}$
Σ_w
$P_\alpha^{K_v} = \prod_{\sigma \in \Sigma_{L_w/K_v}} (X - \sigma(\alpha)) \in \mathcal{O}_{\overline{K}_v}[X] \cap K_v[X]$
$\mathcal{O}_{\overline{K}}$
$\mathcal{O}_v[X]$

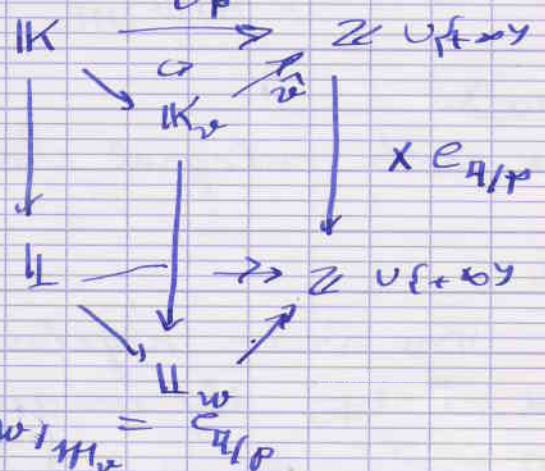
So α is integral over $\mathcal{O}_v$

Conversely, remember that
$$|\alpha|'_w = \left| N_{L_w/K_v}(\alpha) \right|^{1/N_w}$$

So if α is integral over $\mathcal{O}_v$
$|\alpha|'_w \leq 1$. □

Proof of the formula

$v_p : K^* \to \mathbb{Z}$
continuous extends to
$\hat{v} \quad K_v^* \to \mathbb{Z}$
which is the surjective discrete valuation associated to $\mathcal{O}_v$.
We do the same for $v_q : L^* \to \mathbb{Z}$
and get



So $e_{w/v} = e_{q/p}$

The formula

$$[L:K] = \sum_{q|p} e_{q/p} f_{q/p}$$

applied to L_w / K_v gives

$$N_w = e_{m_w/m_v} f_{m_w/m_v} = e_{q/p} f_{q/p}$$

since $P(\mathcal{O}_w) = \{m_w\}$, $P(\mathcal{O}_v) = \{m_v\}$ ∎

Remark The trick of the proof is:

- If you localize you get

$$B\left[S_{L/K}(A-\{p\})^{-1}\right] \quad \#P(-) = \#\{q \mid q|p\}$$

$\uparrow$

$A_{(p)}$ local $\quad \#P(A_{(p)}) = 1$

- If you localize and complete you get

$\mathcal{O}_w$ local $\#P(\mathcal{O}_w) = 1$

$|$

$\mathcal{O}_v$ local $\#P(\mathcal{O}_v) = 1$

V Number fields

1) Product formula

Definition

Let K be a number field

Let $w \in Pl(K)$ and let v be the induced place of $\mathbb{Q}$

(Remember: $Pl(\mathbb{Q}) = P \cup \{\infty\}$)

The normalized absolute (primes) value for w on K_w is defined by

$$|x|_w = |N_{K_w/\mathbb{Q}_v}(x)|_v^{\frac{1}{[K:\mathbb{Q}]}}$$

Remark (i) absolute value by the (sum of complete fields) $[K_w:\mathbb{Q}_v]$

(ii) $\forall x \in \mathbb{Q} \quad |x|_w = |x|_v^{[K:\mathbb{Q}]}$

($|\cdot|_w$ is not an extension of $|\cdot|_v$)

Theorem (Product formula)

$$\forall x \in K^*, \quad \prod_{w \in Pl(K)} |x|_w = 1$$

Proof

$$\prod_{w \in Pl(K)} |x|_w = \prod_{v \in Pl(\mathbb{Q})} \prod_{w \mid v} |x|_w$$

$$= \prod_{v \in Pl(\mathbb{Q})} \prod_{w \mid v} |N_{K_w/\mathbb{Q}_v}(x)|_v^{\frac{1}{[K:\mathbb{Q}]}}$$

$$= \prod_{v \in Pl(\mathbb{Q})} \left| \prod_{w \mid v} N_{K_w/\mathbb{Q}_v}(x) \right|_v^{\frac{1}{[K:\mathbb{Q}]}}$$

$$= \left(\prod_{v \in Pl(\mathbb{Q})} |N_{K/\mathbb{Q}}(x)| \right)^{\frac{1}{[K:\mathbb{Q}]}}$$

$$= 1 . \quad \square$$

Remark

If X is a compact connected Riemann surface, $f \in \mathbb{C}(X)^*$ and $\pi : X \to \mathbb{P}^1$ induces $\pi^* : \mathbb{C}(T) \to \mathbb{C}(X)$ then a similar argument leads to

$$\sum_{x \in X} v_x(f) = \sum_{t \in \mathbb{P}^1} \sum_{\pi(x) = t} v_x(f)$$

$$= \sum_{t \in \mathbb{P}^1} v_t\left(N_{\mathbb{C}(X)/\mathbb{C}(t)}(f)\right) = 0$$

$\square$

2) Norm of an ideal

Definition

Let A be a commutative ring and $\mathfrak{a}$ be an ideal of A such that $A/\mathfrak{a}$ is finite, then

$$N(\mathfrak{a}) = \#\, A/\mathfrak{a}.$$

Property

Let K be a number field, and $\mathcal{O}_K$ be the ring of integers in K, then.

(i) for any ideal $\mathfrak{a}$ of $\mathcal{O}_K$, $\mathcal{O}_K/\mathfrak{a}$ is finite and

$$N(\mathfrak{a}) = \prod_{\mathfrak{P} \in P(\mathcal{O}_\mathfrak{a})} N(\mathfrak{P})^{v_\mathfrak{P}(\mathfrak{a})} = \prod_{p \in P} \prod_{\mathfrak{P}/p} p^{f_{\mathfrak{P}/p}\, v_\mathfrak{P}(\mathfrak{a})}$$

(ii) $\forall x \in \mathcal{O}_K$, $N((x)) = |N_{K/\mathbb{Q}}(x)|$.

Proof.

(i) $\mathcal{O}_K/\mathfrak{a} \xrightarrow{\sim} \prod_{\mathfrak{P} \in P(\mathcal{O}_K)} \mathcal{O}_K/\mathfrak{P}^{v_\mathfrak{P}(\mathfrak{a})}$

finite of order $\#(\mathcal{O}_K/\mathfrak{P})^{v_\mathfrak{P}(\mathfrak{a})}$

$= \#\, \mathbb{F}_p^{\,f_{\mathfrak{P}/p}\, v_\mathfrak{P}(\mathfrak{a})}$

(ii)

$$|p|_p = \left| p^{\frac{[K_p : \mathbb{Q}_p]}{[K:\mathbb{Q}]}} \right|_p = p^{-e_{\mathfrak{P}/p} f_{\mathfrak{P}/p}/[K:\mathbb{Q}]} = p^{-v_\mathfrak{P}(p)\, f_{\mathfrak{P}/p}/[K:\mathbb{Q}]}$$

We get for $x \in K$

$$|x|_\mathfrak{P} = p^{-v_\mathfrak{P}(x)\, f_{\mathfrak{P}/p}/[K:\mathbb{Q}]}$$

So By (i)

$$N(x) = \prod_{p \in P} \prod_{\mathfrak{p} \mid p} |x|_{\mathfrak{p}}^{-[K:\mathbb{Q}]}$$

$$= \prod_{p \in P} \left| \prod_{\mathfrak{p} \mid p} N_{K_{\mathfrak{p}}/\mathbb{Q}_p}(x) \right|_p^{-\frac{[K:\mathbb{Q}]}{[K:\mathbb{Q}]}}$$

$$= \prod_{p \in P} |N_{K/\mathbb{Q}}(x)|_p^{-1}$$

Product formula

$$= |N_{K/\mathbb{Q}}(x)|.$$

3) Lattices in $\mathbb{R}^n$. (Reminders and complements)

Definition.

- A lattice in a real vector space E is a subgroup generated by a basis of E
- Let E be a euclidean vector space of finite dimension over $\mathbb{R}$. and let Λ be a lattice in E. Let $(e_1, \dots, e_d)$ be an orthonormal basis of E and $(b_1, \dots, b_d)$ be a basis of E which generates Λ; then

$$\left| \det_{(e_1, \dots, e_d)} (b_1, \dots, b_d) \right|$$

do not depend on the choice of the basis and is called the « covolume » of the lattice.

$$\operatorname{covol}(\Lambda) = \left| \det_{(e_1, \dots, e_d)} (b_1, \dots, b_d) \right|$$

$$= \operatorname{vol}(E/\Lambda).$$

for the measure induced by the euclidean volume in E.

Proof

$(e'_1, \dots, e'_d)$ BON of E

$(f'_1, \dots, f'_d)$ basis of Λ.

$Mat_f^{f'} \in Gl_n(\mathbb{Z})$, $|\det(Mat_f^{f'})| = 1$

$Mat_e^{e'} \in G_n(\mathbb{R})$, $|\det(Mat_e^{e'})| = 1$. □

Notation In Arakelov theory, one may ax.

$\widehat{deg}(E, \Lambda) = -\log(\text{covol}(E))$.

Theorem (Minkowski)

Let Λ be a lattice in E and S be an integrable set of E such that

$\text{Vol}(S) > \text{covol}(\Lambda)$

Then there exists $x, y \in S$ such that

$x - y \in \Lambda - \{0\}$

Proof

Equip E/Λ of the induced topology and measure. (so that if $K \subset E$ is integrable and $\pi : E \to E/\Lambda$ is injective on K

$\text{Vol}(\pi(K)) = \text{Vol}(K)$.)

Hence $\text{Vol}(\pi(S)) \leq \text{Vol}(E/\Lambda) = \text{covol}(\Lambda)$

$\pi_{|S}$ is not injective. □.

Corollary

Let Λ be a lattice in E and $S \subset E$ be integrable and such that

(i) S is convex and $S = -S$,

(ii) either a) $\mathrm{Vol}(S) > 2^d \operatorname{covol}(\Lambda)$
or b) $\mathrm{Vol}(S) = 2^d \operatorname{covol}(\Lambda)$ and S is compact.

Then
$$S \cap \Lambda \neq \{0\}$$

Proof
(a) Take $S' = \frac{1}{2} S$ we
In case a) we find by the theorem
$x, y \in S'$ such that $x - y \in \Lambda - \{0\}$
$x - y \in S$.

(b) by (a) for $(1 + \frac{1}{n+1}) S$
find:
$$x_n \in \Lambda - \{0\} \cap (1 + \tfrac{1}{n+1}) S$$
extract $(x_{\varphi(n)})_{n \in \mathbb{N}}$ convergent in $2S$

$\Lambda \cap 2S$ compact, discrete
therefore finite
$(x_{\varphi(n)})_{n \in \mathbb{N}}$ is ultimately stationnary
and its limit belongs to $\Lambda \cap S$. □

Proposition
Let Γ be a lattice in E and
Let Γ' be a subgroup of Γ of finite index
Then Γ' is a lattice in E and
$$\operatorname{covol}(\Gamma') = [\Gamma : \Gamma'] \operatorname{covol}(\Gamma)$$

Proof
By the "théorème de la base adaptée"
there exists a basis $(e_1, \dots, e_d)$ of Γ

and $\lambda_1, \dots, \lambda_r \in \mathbb{Z}$ with $\lambda_1 | \lambda_2 | \dots | \lambda_r$ $r \leq d$ such that

$$(\lambda_1 e_1, \dots, \lambda_r e_r)$$

is a basis of Γ'. Since $[\Gamma : \Gamma']$ is finite $r = d$ and Γ' is a lattice of E

$$\det_{ONB}(\lambda_1 e_1, \dots, \lambda_d e_d) = \prod_{i=1}^{d} \lambda_i \cdot \det_{ONB}(e_1, \dots, e_d).$$

Lecture 11 ☐

proof ⊢

4] The ring of integers as a lattice.

Remark (technical convention)

Let $\mathbb{K}$ be a number field and let $w \in \mathrm{Pl}(\mathbb{K})$ be an archimedean place, $w | \infty$ such that $[\mathbb{K}_w : \mathbb{R}] = 2$.

The field $\mathbb{K}_w$ is isomorphic to $\mathbb{C}$ but this isomorphism is not canonical. (There is no way to choose a canonical isomorphism from $\mathbb{K}_w$ to $\mathbb{C}$)

There is a natural morphism of $\mathbb{R}$-algebra

$$\varphi : \mathbb{K}_w \longrightarrow \mathbb{C}^{\Sigma_{\mathbb{K}_w/\mathbb{R}}}$$
$$x \longmapsto (\sigma(x))_{\sigma \in \Sigma_{\mathbb{K}_w/\mathbb{R}}}$$

cardinal 2.

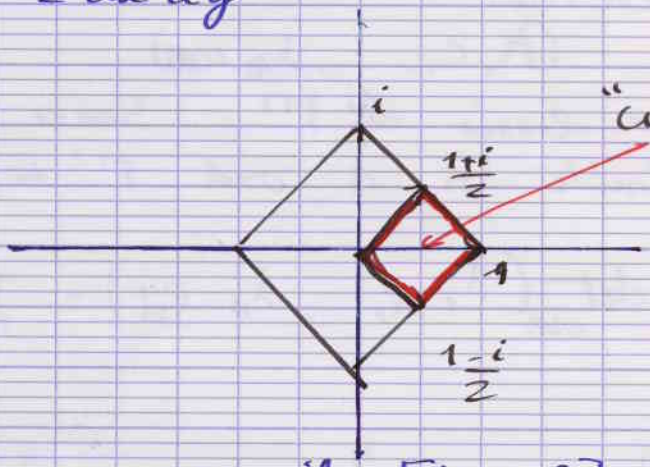
φ is a euclidean space for $\|\cdot\| : (z_\sigma)_\sigma \longmapsto \sqrt{\sum_{\sigma \in \Sigma_{\mathbb{K}_w/\mathbb{R}}} |z_\sigma|^2}$ $\|\varphi(z)\| = \sqrt{2}\,|z|$

If $i \in \mathbb{K}_w$ satisfies $i^2 = -1$

$$\left\| \varphi\left(\frac{1+i}{2}\right) \right\| = \left\| \left(\frac{1+i}{2}, \frac{1-i}{2}\right) \right\| = 1$$

So an orthonormal basis for $\mathbb{K}_w$ is $\left(\frac{1+i}{2}, \frac{1-i}{2}\right)$

The corresponding Haar measure on $\mathbb{K}_w = \mathbb{R}$ or $\mathbb{R}i$ is $2\,dx\,dy$



From now on if $[\mathbb{K}_w : \mathbb{R}] = 2$ it is equipped with this particular euclidean structure.

Definition

- Let $\mathbb{K}$ be a number field, the morphism of rings

$$\begin{aligned} \ell_\infty : \mathbb{K} &\longrightarrow \prod_{w|\infty} \mathbb{K}_w \\ x &\longmapsto (\ell_{\mathbb{K}_w/\mathbb{K}}(x)) \end{aligned}$$

is called **the canonical embedding of $\mathbb{K}$**

- $r_1 = \#\{w \mid v \mid [\mathbb{K}_w : \mathbb{R}] = 1\}$, $r_2 = \#\{w \mid v \mid [\mathbb{K}_w : \mathbb{R}] = 2\}$

Theorem

Let $\alpha \in \mathcal{I}(\mathcal{O}_\mathbb{K})$; $\ell_\infty(\alpha)$ is a lattice in $\prod_{w|\infty} \mathbb{K}_w$ of covolume

$$\operatorname{covol}(\ell_\infty(\alpha)) = N(\alpha)\,|d_\mathbb{K}|^{1/2}$$

p. 195

2 With the naïve euclidean structure on $\prod_{w|v} \mathbb{K}_w$, given by

$$\| (z_w)_{w|\alpha} \|^2 = \sum_{w|\alpha} |z_w|^2$$

we would get

$$\mathrm{covol}\left(\varphi_{\mathbb{Z}}(\mathcal{O}_K)\right) = \boxed{2^{-r_2}} |d_K|^{1/2} N(\alpha)$$

(See eg SAMUEL's book)

Remark

$N_w = [K_w : \mathbb{R}]$, so $[K : \mathbb{Q}] = \sum_{w|v} N_w$ implies

$$[K : \mathbb{Q}] = r_1 + 2r_2$$

So

$$\dim_{\mathbb{R}} \prod_{w|v} K_w = [K : \mathbb{Q}]$$

Lemma

σ_K is a free $\mathbb{Z}$-module of rank $n = [K : \mathbb{Q}]$ and if $\Sigma_{K/\mathbb{Q}} = \{\sigma_1, \dots, \sigma_n\}$ and $(e_1, \dots, e_n)$ a basis of $\mathcal{O}_K$ as a $\mathbb{Z}$-module, then

$$|D_{K/\mathbb{Q}}(\alpha)| = |\det(\sigma_i(e_j))_{1 \le i,j \le n}|^2$$

Proof

Remember the more general setting (5th lecture)

Let A be a Dedekind ring, $K = \mathrm{Fr}(A)$

L/K be a separable extension of degree n

B be the integral closure of A in L

Let $(e_1, \dots, e_d)$ be a basis of L as a K-vector space

Write $\Sigma_{L/K} = \{\sigma_1, \dots, \sigma_n\}$

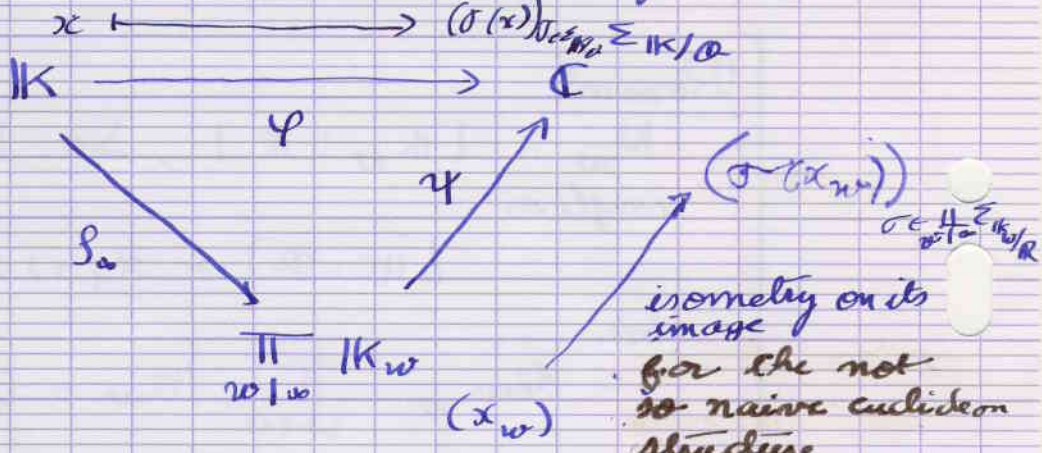
$$\det\left(\mathrm{Tr}_{L/K}(e_i e_j)_{1 \le i,j \le n}\right) = |\det(\sigma_i(e_j))_{1 \le i,j \le n}|^2$$

and if $\alpha \in S(B)$ is a free A-module with basis $(e_1, \dots, e_n)$

$$D_{L/K}(b) = \left(\det\left(\mathrm{Tr}_{L/K}(e_i e_j)\right)_{1\le i,j\le n}\right) \square$$

Proof of the theorem

- We have a commutative diagram



where we identify $\prod_{w|v} \Sigma_{K_w/\mathbb{R}}$ with $\Sigma_{K/\mathbb{Q}}$

$$\sigma \longmapsto \sigma_{|K}$$

$\mathbb{C}^{\Sigma_K}$ is equipped with the hermitian structure

$$\|(z_\sigma)\|^2 = \sum_{\sigma \in \Sigma_K} |z_\sigma|^2 \qquad (*)$$

for which the usual basis is orthonormal.

If $(e_1, \dots, e_n)$ is an orthonormal basis for the not so naive euclidean structure $(\psi(e_1), \dots, \psi(e_n))$ is orthonormal for the above hermitian structure;

- Let $\Lambda = \jmath_\infty(\mathcal{O}_K)$

Let $e_1, \dots, e_n$ be a basis of $\mathcal{O}_K$ as a $\mathbb{Z}$-module

$$|d_K| = \left|\det\left(\sigma_i(e_j)\right)_{1\le i,j\le n}\right|^2 \neq 0$$

and

$$(\varphi(e_1), \dots, \varphi(e_n))$$

is free in the $\mathbb{C}$-vector space $\mathbb{C}^{\Sigma_{K/\mathbb{Q}}}$

Then $(\xi_\infty(e_1), \dots, \xi_\infty(e_n))$ is free in the $\mathbb{R}$-vector space $\prod_{w\mid\infty} K_w$

and

$$\begin{aligned}\mathrm{covol}(\Lambda) &= \left|\det_{ONB}\left(\xi_\infty(e_1), \dots, \xi_\infty(e_n)\right)\right| \\ &= \left|\det\left(\sigma_i(e_j)\right)_{1\le i,j\le n}\right| \\ &= |d_K|^{1/2}.\end{aligned}$$

If $\alpha \in \mathcal{I}(\mathcal{O}_K)$ let $c \in \mathcal{O}_K - \{0\}$ such that $c\alpha$ is an ideal in $\mathcal{O}_K$

writing $c^{-1} = \frac{b}{m}$ with $b \in \mathcal{O}_K$ and $m \in \mathbb{N}_{>0}$,

we get $m\alpha \subset c\,b\,\mathcal{O}_K \subset \mathcal{O}_K$

$$\begin{aligned}\mathrm{covol}(\xi_\infty(m\alpha)) &= \mathrm{covol}(m\,\xi_\infty(\alpha)) \\ &= m^n \mathrm{covol}(\xi_\infty(\alpha)) \\ \| & \\ [\mathcal{O}_K : m\alpha]\,\mathrm{covol}(\xi_\infty(\mathcal{O}_K)) & \\ \| & \\ N(m\alpha)\,|d_K|^{1/2} & \\ \| & \\ m^n N(\alpha)\,|d_K|^{1/2} & .\end{aligned}$$

□

Remark 5) $\left(\prod_{w\mid\infty} K_w\right) \otimes_{\mathbb{R}} \mathbb{C} \xrightarrow{\sim} \mathbb{C}^{\Sigma_{K/\mathbb{Q}}}$ as $\mathbb{C}$-algebras

The group of ideal classes.

Theorem (Dirichlet)

Let K be a number field; the ideal class group

$$\mathcal{Cl}(\mathcal{O}_K) = \mathcal{I}(\mathcal{O}_K)/\mathcal{H}(A)$$

is finite

Its cardinal is often denoted by h_K

Proposition 1

Let K be a number field,

$n = [K : \mathbb{Q}]$, $r_1 = \#\{w \mid \infty \mid [K_w : \mathbb{R}] = 1\}$

... $r_2 = $ ——————— $2-$

Let $\alpha \in \mathcal{I}(\mathcal{O}_K)$. Then there is $x \in \alpha$ such that

$$|N_{K/\mathbb{Q}}(x)| \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} |d|^{1/2} N(\alpha)$$

Proof

For $t \in \mathbb{R}_{\geq 0}$ we consider

$$B_t = \left\{(x_w) \in \prod_{w \mid \infty} K_w \;\middle|\; \sum_{w \mid \infty} [K_w : \mathbb{R}] \, |x_w| \leq t\right\}$$

B_t is compact, convex, $-B_t = B_t$.

To apply the corollary of Minkowski's theorem we need to compute its volume for the not so naïve Haar measure.

If $[K_w : \mathbb{R}] = 2$ we use $2\,dx\,dy = 2\,r\,dr\,d\theta$.

Thus

$$\mathrm{Vol}(B_t) = (4\pi)^{r_2} \times 2^{r_1} \int_{\substack{r_w \geq 0 \\ \sum N_w r_w \leq t}} \prod_w r_w^{N_w - 1} \prod_w dr_w$$

But $\displaystyle\int_{0 \leq r \leq t} f(r)\, r\, dr = \int_{\substack{0 \leq x \\ 0 \leq y \\ x+y \leq t}} f(x+y)\, dx\, dy$

$$\mathrm{Vol}(B_t) = (4\pi)^{r_2} 2^{r_1} \frac{1}{4^{r_2}} \underbrace{\int_{\sum_{i=1}^{n} x_i \leq t} dx_1 \cdots dx_n}_{\substack{\text{Volume} \\ \text{of a simplex}}} \quad \frac{t^n}{n!}$$

(By induction on n).

$$\mathrm{Vol}(B_\epsilon) \geq 2^n \mathrm{covol}(S_\infty(\mathfrak{a}))$$

iff $$\pi^{r_2} 2^{r_1} \frac{\epsilon^n}{n!} \geq 2^n N(\mathfrak{a}) |d_K|^{1/2}$$

that is $$\epsilon^n \geq 2^{n-r_1} \pi^{-r_2} n! |d_K|^{1/2} N(\mathfrak{a})$$

For such a ϵ, by the corollary to Minkowski's theorem there is $x \in \mathfrak{a} - \{0\} \cap B_\epsilon$

$$|N_{K/\mathbb{Q}}(x)| = \prod_{w|\infty} |N_{K_w/\mathbb{R}}(x)|$$
$$= \prod_{w|v} |\xi_{K_w/\mathbb{R}}(x)|^{N_w}$$

Since log is concave

$$\frac{\sum_{w|v} N_w \log |\xi_{K_w/K}(x)|}{n} \leq \log\left(\frac{1}{n}\sum_{w|v} N_w |\xi_{K_w/K}(x)|\right)$$

thus ($\exp^n$ is increasing)

$$|N_{K/\mathbb{Q}}(x)| \leq \left(\sum_{w|v} N_w |\xi_{K_w/K}(x)|\right)^n \times \frac{1}{n^n}$$

and $$|N_{K/\mathbb{Q}}(x)| \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} |d_K|^{1/2} N(\mathfrak{a}). \square$$

Corollary 1 (to proposition 1)

Any class of ideals in $Cl(\mathcal{O}_K)$ contains an ideal $\mathfrak{b}$ of $\mathcal{O}_K$ such that

$$N(\mathfrak{b}) \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} |d|^{1/2}$$

Proof

Take any $\mathfrak{a}$ in the given class of ideals. Let $x \in \mathfrak{a}^{-1}$ be such that

$$N(x) \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} |d_K|^{1/2} N(\mathfrak{a})^{-1}$$

$$x\, \mathcal{O}_{\mathbb{K}} \subset \mathfrak{a}^{-1}$$

gives $x\mathfrak{a} \subset \mathcal{O}_{\mathbb{K}}$.

and $N(x\mathfrak{a}) \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} |d_{\mathbb{K}}|^{1/2}$. □

Proof of Dirichlet's theorem

By the previous corollary, we only have to prove that for any $n \in \mathbb{N}_{>0}$

$$\#\{\mathfrak{b} \text{ ideal of } \mathcal{O}_{\mathbb{K}} \mid N(\mathfrak{b}) = n\}$$

is finite

But if $\#(\mathcal{O}_{\mathbb{K}}/\mathfrak{b}) = n$

then $n \cdot 1 = 0$ in $\mathcal{O}_{\mathbb{K}}/\mathfrak{b}$

So $n \in \mathfrak{b}$

and $\mathfrak{b} \mid n$.

Using the decomposition of ideals as product of prime ideals,

There is a finite number of such ideals (if $n = \prod_{\mathfrak{p} \in \mathcal{P}(\mathcal{O}_{\mathbb{K}})} \mathfrak{p}^{v_{\mathfrak{p}}(n)}$,

it is given by $\prod_{\mathfrak{p}} (v_{\mathfrak{p}}(n)+1)$) □

Corollary 2 to proposition 1.

With notations as in proposition 1.

If $\mathbb{K} = \mathbb{Q}$, $|d_{\mathbb{K}}| \geq \frac{\pi}{3}\left(\frac{3\pi}{4}\right)^{n-1}$

in particular there exists $C \in \mathbb{R}$ such that

$$\frac{[\mathbb{K}:\mathbb{Q}]}{\log |d_{\mathbb{K}}|} < C$$

for any number field $\mathbb{K}$.

In other words, $d_{\mathbb{K}}$ grows exponentially with the degree.

Proof

Apply corollary 1 to any class

$$1 \leq N(\mathfrak{b}) \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} |d|^{1/2}$$

So

$$|d_k| \geqslant \underbrace{\left(\frac{\pi}{4}\right)^{2r_2}}_{\leq 1} \frac{n^{2n}}{(n!)^2} \geqslant \underbrace{\left(\frac{\pi}{4}\right)^n \frac{n^{2n}}{(n!)^2}}_{a_n}$$

and $2r_2 \leq n$

$$a_2 = \frac{\pi^2}{4^2} \frac{2^4}{2^2} = \frac{\pi^2}{4}$$

$$\frac{a_{n+4}}{a_n} = \frac{\pi}{4}\left(1 + \frac{1}{n}\right)^{2n} \geqslant \frac{3\pi}{4}$$

So $|d_{IK}| \geqslant \frac{\pi^2}{4}\left(\frac{3\pi}{4}\right)^{n-2}$ □

Theorem 2 (Hermite–Minkowski)

For any number field $IK \neq \mathbb{Q}$, $d_{IK/\mathbb{Q}} \neq 1$

Proof

By corollary 2, $|d_{IK}| \geqslant \frac{\pi^2}{4} > 1$. □

Remark

In particular the set of ramified primes p is not empty.

Theorem 3 (Hermite)

Up to isomorphism, there is a finite number of number fields with a given discriminant.

Proof

By corollary 2 $n = [IK : \mathbb{Q}]$ is bounded,

So it is enough to prove that there is a finite number of number fields $\mathbb{K} \subset \bar{\mathbb{Q}}$ with a given n, r_1, r_2, and $d_{\mathbb{K}}$.

Pick $w_0 | \infty$ such that N_{w_0} is minimal.

a) if $N_{w_0} = 1$

$$\mathcal{B} = \left\{ (z_w)_w \in \prod_{w | \infty} \mathbb{K}_w \;\middle|\; \begin{cases} |z_w| \leq \frac{1}{2} \text{ for } w \neq w_0 \\ |z_{w_0}| \leq 2^n \left(\frac{\pi}{2}\right)^{-r_2} |d_{\mathbb{K}}|^{\frac{1}{2}} \end{cases} \right\}$$

$$\mathrm{Vol}(\mathcal{B}) = \left(2\frac{\pi}{4}\right)^{r_2} \times 1^{r_1} \times 2^n \left(\frac{\pi}{2}\right)^{-r_2} |d_{\mathbb{K}}|^{\frac{1}{2}} = 2^n |d_{\mathbb{K}}|^{1/2}$$

b) if $N_{w_0} \neq 1$

$$\mathcal{B} = \left\{ (z_w)_w \in \prod_{w | \infty} \mathbb{K}_w \;\middle|\; \begin{cases} |z_w| \leq \frac{1}{2} \text{ for } w \neq w_0 \\ |z_{w_0} + \bar{z}_{w_0}| \leq \frac{1}{2} \\ |z_{w_0} - \bar{z}_{w_0}| \leq 2\pi \left(\frac{1}{2}\right)^{-r_2} |d_{\mathbb{K}}|^{\frac{1}{2}} \end{cases} \right\}$$

$$\mathrm{Vol}(\mathcal{B}) = 2^n |d_{\mathbb{K}}|^{1/2} \times \frac{2}{\pi} \times 2\frac{1}{4} \times \pi$$

In any case

$$\mathrm{Vol}(\mathcal{B}) = 2^n |d_{\mathbb{K}}|^{1/2} = 2^n \, \mathrm{covol}(\sigma_\infty(\mathcal{O}_{\mathbb{K}}))$$

So There is $x \in \mathcal{O}_{\mathbb{K}}$ such that $\sigma_\infty(x) \in \mathcal{B}$.

From

$$1 \leq |N_{\mathbb{K}/\mathbb{Q}}(x)| = \prod_{w | \infty} |\sigma_{\mathbb{K}_w/\mathbb{K}}(x)|^{N_w}$$

It follows that

$$|\sigma_{\mathbb{K}_{w_0}/\mathbb{K}}(x)| > 1.$$

And in case b, $f_{K_w/K}(x) \notin \mathbb{R}$.

Choose $\sigma \in \Sigma_{K/\mathbb{Q}}$ such that $|.|_w = |\sigma(.)|^{\frac{N_w}{[K:\mathbb{Q}]}}$

we get

$$\forall \sigma' \in \Sigma_{K/\mathbb{Q}},\ \sigma' \neq \sigma \Rightarrow \sigma'(x) \neq \sigma(x).$$

But all the fibers of the reduction map

$$\text{rés} : \Sigma_{K/\mathbb{Q}} \longrightarrow \Sigma_{\mathbb{Q}(x)/\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}$$

$$\sigma \longmapsto \sigma_{|\mathbb{Q}(x)} \longmapsto \sigma(x)$$

have the same cardinal,

So this map is injective

And

$$[K : \mathbb{Q}] = [\mathbb{Q}(x) : \mathbb{Q}]$$

In other words

$$K = \mathbb{Q}(x).$$

But the coefficients of $P_x^{\mathbb{Q}} = X_x^{\mathbb{Q}}$ are (up to sign) symmetric polynomials in $(\sigma(x))_{\sigma \in \Sigma_{K/\mathbb{Q}}}$ and belong to $\mathbb{Z}$.

Therefore they are bounded integers

The number of possible $P_x^{\mathbb{Q}}$ (and therefore of possible x in $\overline{\mathbb{Q}}$) is finite. □

6) The theorem of units

Notation

For any field K, let $\mu_\infty(K)$ be the group of roots of unity in K.

P. 206

Theorem (Dirichlet)

Let K be a number field,
let n, r_1, r_2 be defined as in §5
Put $r = r_1 + r_2 - 1$
Then

$$G_K^* \text{ is isomorphic to } W_\infty(K) \times \mathbb{Z}^r$$

Plan of the proof

The proof will be very similar to the problem 1 in the first exam (about Pell's equation).

Step 1 Construct a morphism

$$\log \quad G_K^* \longrightarrow \prod_{v|\infty} \mathbb{R}$$

Step 2

Show that $\ker(\log) = W_\infty(K)$

Step 3

Show that $\operatorname{Im}(\log)$ is discrete in $\prod_{v|\infty} \mathbb{R}$

Step 4

Show that $\operatorname{Im}(\log) \subset \underbrace{\left\{(x_v) \in \prod_{v|\infty} \mathbb{R} \;\middle|\; \sum_{v|\infty} N_v x_v = 0\right\}}_{E}$

Step 5 (most difficult!)

Show that for any $f \in E^* - \{0\}$ dual space there is $u \in G_K^*$ such that $f(u) \neq 0$
(Which implies that $\operatorname{Im}(\log)$ generates E)

Step 1

$$\log : \mathbb{G}_{\mathbb{K}}^{\mathbb{A}} \longrightarrow \prod_{w \mid \infty} \mathbb{R}$$

$$x \longmapsto \left(\log |x|_{\mathbb{K}_w/\mathbb{K}} (x) | \right)_{w \mid \infty}$$

it is a morphism of groups.

Lemma

Let $t \in \mathbb{R}$ the set

$$\{ x \in \mathbb{G}_{\mathbb{K}}^{*} \mid \log(x) \in \prod_{w \mid \infty} [-t, t] \}$$

is finite

Proof

This condition is equivalent to

$$\forall \sigma \in \Sigma_{\mathbb{K}}, \quad e^{-t} \leq |\sigma(x)| \leq e^{t}$$

But this implies that the coefficients of

$$\chi_x^{\mathbb{Q}} \in \mathbb{Z}[T]$$

are bounded. So there are a finite number of possible $\chi_x^{\mathbb{Q}}$, and therefor a finite number of possible x in $\mathbb{K}$. □

Step 2

By the lemma any $z \in \ker(\log)$ has a finite order, and belongs to $W_\infty(\mathbb{K})$

Conversely, $W_\infty(\mathbb{K}) \subset \mathbb{G}_{\mathbb{K}}^{*}$

and $W_\infty(\mathbb{K}) \subset \ker(\log)$

Step 3

follows from the lemma.

Step 4

For any $x \in G_K^x$ and any $p \in P(G_K)$

$v_p(x) = 0 \quad (x \notin p)$

Therefore $|x|_p = 1$

So By the product formula

$$\prod_{w|\infty} |\mathcal{S}_{K_w/K}(x)|^{N_w} = 1$$

and $\mathrm{Im}(\log) \subset E$, $\dim_{\mathbb{R}} E = r$.

Step 5

we choose an order on $\{w|\infty\}$ so that $w \mapsto N_w$ is increasing

$$\prod_{w|v} \mathbb{R} = \mathbb{R}^{r+1}$$

Write $f \in E = \{0\} \cup \mathbb{R}$

$$f(y_1, \dots, y_{r+1}) = \sum_{i=1}^{r} c_i y_i$$

(The projection $E \to \mathbb{R}^r$ is an isomorphism)

$$(y_1, \dots, y_{r+1}) \mapsto (y_1, \dots, y_r)$$

Proposition

Let $x \in G_K$; then

$$x \in G_K^x \Leftrightarrow |N_{K/\mathbb{Q}}(x)| = 1$$

p. 203 ↕

Proof

$\Rightarrow$) If $x, y \in G_K$ satisfy $xy = 1$,

$N_{K/\mathbb{Q}}(x) N_{K/\mathbb{Q}}(y) = 1$

and $N_{K/\mathbb{Q}}(x) \in \mathbb{Z}^\times = \{-1, 1\}$.

$\Leftarrow$) If $|N_{K/\mathbb{Q}}(x)| = 1$, then
$x_x^{\mathbb{Q}} = X^n + a_{n-1}X^{n-1} + \cdots + a_0$
with $a_0 \in \{-1, 1\}$
and
$$x \cdot (-a_0) \cdot (\underbrace{X^{n-1} + a_{n-1}X^{n-2} + \cdots + a_1}_{\in \mathcal{O}_K}) = (a_0)^2 = 1$$
So $x \in \mathcal{O}_K^\times$. $\square$

Proof of the theorem (continued)
Let $\alpha \in \mathbb{R}$ be such that $\alpha \geq 2^n \left(\frac{1}{2\pi}\right)^{r_2} |d_K|^{1/2}$
For $\underline{\lambda} = (\lambda_1, \dots, \lambda_n) \in \mathbb{R}_{>0}^n$
Take $\lambda_{n+1} \in \mathbb{R}_{>0}$ such that
$$\prod_{i=1}^{r_1+r_2} \lambda_i^{N_{w_i}} = \alpha.$$
and define

$$\mathcal{B}_{\underline{\lambda}} = \left\{ (z_w)_w \in \prod_{w \mid \infty} K_w \;\middle|\; \forall i,\ |z_{w_i}| \leq \lambda_i \right\}$$

$\mathcal{B}_{\underline{\lambda}}$ is compact $\mathrm{Vol}(\mathcal{B}_{\underline{\lambda}}) \geq 2^n |d_K|^{1/2}$
So there exists $x_{\underline{\lambda}} \in \mathcal{O}_K$ such that $\delta_\infty(x_{\underline{\lambda}}) \in \mathcal{B}_{\underline{\lambda}}$.
We have
$$(*) \qquad 1 \leq |N_{K/\mathbb{Q}}(x_{\underline{\lambda}})| = \prod_{w \mid \infty} |\delta_{K_w/K}(x)|^{N_w} \leq \alpha.$$
If w_i corresponds to $|\sigma(\cdot)|$ for $\sigma \in \Sigma_{K/\mathbb{Q}}$
write $\lambda_\sigma = \lambda_i$.
We get
$$|\sigma(x_{\underline{\lambda}})| \leq \lambda_\sigma \quad \text{for } \sigma \in \Sigma_{K/\mathbb{Q}}$$
and $(*)$
$$|\sigma(x)| \geq \lambda_\sigma \alpha^{-1}$$
So
$$0 \leq \log(\lambda_\sigma) - \log|\sigma(x_{\underline{\lambda}})| \leq \log(\alpha).$$

$$(*) \qquad \left| f\left(\log(x_{\underline{\lambda}})\right) - \sum_{i=1}^{n} c_i \lambda_i \right| \leq \underbrace{\sum_{i=1}^{n} |c_i|}_{\epsilon} \log(\alpha).$$

Put $\beta = C \log \alpha$.
For any $h \in \mathbb{N}_{>0}$, choose $\lambda(h) = (\lambda_1, \dots, \lambda_r)$ such that

$$\sum_{i=1}^{r} c_i \log \lambda_i = 2\beta h.$$

and put $x_h = x_{\lambda(h)}$.
By (*) $\quad |f(-\underline{\log}(x_h)) - 2\beta h| < \beta$
Thus

$$\cdot\, h \mapsto f(\underline{\log}(x_h)) \text{ is injective.}$$

But

$$\forall h \in \mathbb{N}_{>0}, \quad N(G_K x_h) = N(x_h) \leq \alpha$$

And we have seen that the set of ideals $\mathfrak{a}$ of G_K such that $N(\mathfrak{a}) \leq t$ is finite for any $t \in \mathbb{R}_{>0}$
So there exists $h < h'$ such that

$$G_K x_h = G_K x_{h'}$$

and there is $u \in G_K^\times$ such that

$$x_{h'} = u x_h.$$

But

$$f(\underline{\log} u) = f(\underline{\log} x_{h'}) - f(\underline{\log} x_h) \neq 0$$

o We have proven that

Im($\underline{\log}$) generates E as an $\mathbb{R}$-vector space. Voilà

p. 193

Theorem
Let E be a finite dimensional euclidean vector space, let $\Lambda \subset E$ be a subgroup then Λ is a lattice if and only if
(i) Λ is discrete in E
and (ii) Λ generates E as an $\mathbb{R}$-vector space.

Proof ($\Leftarrow$)

- extract from Λ a basis $(e_1, \dots, e_d)$ of E.
  $B = \sum_{i=1}^{d} [0,1]\, e_i \subset E$ $\quad B' = \sum_{i=1}^{d} [0,1[\, e_i$
  is compact
  $\therefore B \cap \Lambda$ is compact and discrete
  thus finite.
  and $B' \cap \Lambda \to \Lambda / \sum_{i=1}^{d} \mathbb{Z} e_i$
  is a bijection.
  So $\Lambda / \sum_{i=1}^{d} \mathbb{Z} e_i$ is a finite group

- Therefore Λ is a finitely generated torsion free $\mathbb{Z}$-module
  so it is a free $\mathbb{Z}$-module of rank $n \geq d$
- But since $\Lambda / \sum_{i=1}^{d} \mathbb{Z} e_i$ is finite, $n = d$.
- Let $b_1, \dots, b_d$ be a basis of Λ.
  the $\mathbb{R}$-vector space
  generated by $b_1, \dots, b_d$ contains
  $e_1, \dots, e_d$, and is equal to E

$\Rightarrow$). Let $e_1, \dots, e_d$ be a basis of E
which generates Λ.
Let $f_1, \dots, f_d$ be an orthonormal basis of E
and let $u : E \to E$ be the
endomorphism which maps f_i to e_i
for any $\lambda \in \Lambda - \{0\}$

$$\|u^{-1}(\lambda)\| \leq |||u^{-1}||| \, \|\lambda\|$$

so $\|\lambda\| \geq |||u^{-1}|||^{-1} \, \|u^{-1}(\lambda)\| \geq |||u^{-1}|||^{-1}$
($u^{-1}(\lambda) \in \sum_{i=1}^{d} \mathbb{Z} f_i$)

$$\forall x, y \in \Lambda, \; x \neq y \Rightarrow \|x - y\| \geq |||u^{-1}|||^{-1}$$

[So Λ satisfies (i). ☐]

Conclusion : Structure of K^*

$$1 \to \mathcal{O}_K^* \to K^* \xrightarrow{(v_p)_{p \in P(\mathcal{O}_K)}} \bigoplus_{\mathfrak{p} \in P(\mathcal{O}_K)} \mathbb{Z} \to \underbrace{Cl(\mathcal{O}_K)}_{\text{finite}} \to 0$$

and

$$1 \to \underbrace{\mu_\infty(K)}_{\text{finite}} \to \mathcal{O}_K^* \to \mathbb{Z}^{r} \to 0$$

Lecture 12

Remark

There is no finite extension of $\mathbb{C}(T)$ which is everywhere unramified :

Indeed let S be a connected Riemann surface and $f : S \to \mathbb{P}^1(\mathbb{C})$ a non constant map such that there are no branch points Then

$f : S \to \mathbb{P}^1(\mathbb{C})$ is a cover
Riemann sphere

Theorem (Topology, admitted)

Let X be a topological space which is

(i) path-connected.

(ii) simply connected

then any cover $f : Y \to X$ with Y connected is a homeomorphism

VI Local to Global

1) Global and local fields

Terminology

A **global field** is a finite extension of $\mathbb{Q}$ (number field) or a finite extension of $\mathbb{F}_p(T)$ for p a prime number.

A **local field** is a completion of a global field. (eg p-adic field)

2) Global to local

For any scheme V over a commutative ring A (that is V equipped with a structural morphism $V \to \mathrm{Spec}(A)$) and any commutative A-algebra B, we define the **set of B-points of V** as

$$V(B) = \mathrm{Hom}_{\mathrm{Spec}(A)}(\mathrm{Spec}(B), V)$$

(ie $\mathrm{Spec}(B) \to V$ commutes).

$$\mathrm{Spec}(B) \to V \to \mathrm{Spec}(A)$$

Example

If $V = \mathrm{Spec}(A[x_1, \dots, x_n]/(f_1, \dots, f_k))$ then there is a bijection:

$$V(B) \longrightarrow \{(x_1, \dots, x_n) \in B^n \mid \forall i\ f_i(x_1, \dots, x_n) = 0\}$$

$$f : \mathrm{Spec}(B) \to V \longmapsto (f^\#(X_1), \dots, f^\#(X_n))$$

$$f^\# : A[X_1, \dots, X_n]/(f_1, \dots, f_k) \to B$$

In particular: If V is defined over a field $\mathbb{K}$, for any $\mathbb{K}$-extension L we get a "push-forward map"

$$f_{L/\mathbb{K}*} : \mathcal{V}(\mathbb{K}) \longrightarrow \mathcal{V}(L)$$
$$(x : \mathrm{Spec}(\mathbb{K}) \to V) \longmapsto (\mathrm{Spec}(L) \xrightarrow{f_{L/\mathbb{K}}} \mathrm{Spec}(\mathbb{K}) \xrightarrow{x} V)$$

Conclusion

For any scheme V over a global field $\mathbb{K}$ there is a map (called the canonical map)

$$V(\mathbb{K}) \longrightarrow \prod_{v \in Pl(\mathbb{K})} V(\mathbb{K}_v) \quad \text{(taken in the complete)}$$
$$P \longmapsto \left(f_{\mathbb{K}_v/\mathbb{K}*}(P)\right)_{v \in Pl(\mathbb{K})}$$

Question

What can we say about the image?

Let us start with the simplest example: $\mathbb{H}^1_{\mathbb{K}} = \mathrm{Spec}(\mathbb{K}[T])$

3) Adele ring

Let $\mathbb{K}$ be a number field (big!)

We consider

$$\mathbb{K} \longrightarrow \prod_{v \in Pl(\mathbb{K})} \mathbb{K}_v$$

Remark 1

Let $x \in \mathbb{K}^*$

$\{ p \in P(\mathcal{O}_{\mathbb{K}}) \mid v_p(x) \neq 0 \}$ is finite, therefore

$\{ v \in Pl(\mathbb{K}) \mid |x|_v \neq 1 \}$ is finite.

$\forall x \in \mathbb{K}$, $\{ v \in Pl(\mathbb{K}) \mid |x|_v > 1 \}$ is finite

Definition

$$\mathbb{A}_K = \left\{ (x_v) \in \prod_{v \in \mathrm{Pl}(K)} K_v \;\middle|\; \forall v \in \mathrm{Pl}(K),\ |x_v| > 1 \text{ fini} \right\}$$

is a subring of $\prod_{v \in \mathrm{Pl}(K)} K_v$ which is called the *Adele ring* of K

The map

$$K \longrightarrow \prod_{v \in \mathrm{Pl}(K)} K_v$$
$$x \longmapsto (\varphi_{K_v/K}(x))$$

induce a map

$$\varphi_{\mathbb{A}_K/K} : K \longrightarrow \mathbb{A}_K$$

which is said to be *canonical*

Remark

We may also describe the Adele ring as

$$\mathbb{A}_K = \bigcup_{\substack{S \subset \mathrm{Pl}(K) \\ \text{finie} \\ \{v \mid \infty\} \subset S}} \prod_{v \notin S} \mathcal{O}_v \times \prod_{v \in S} K_v$$

where $\mathcal{O}_v = \{ x \in K_v \mid |x|_v \leq 1 \}$

Structure :

- **Topology**

For $S \subset \mathrm{Pl}(K)$ finite,

$$\prod_{v \notin S} \mathcal{O}_v \times \prod_{v \in S} K_v$$

is given the product topology

The topology on $\mathbb{A}_K$ is the one generated by the open sets in all

$$\prod_{v \in S} \mathcal{O}_v \times \prod_{v \in S} K_v \text{ for } S \subset \mathrm{Pl}(K) \text{ finie}$$

$\mathbb{A}_K$ is locally compact (by Tychonov's theorem)

- Haar measure

$\prod_{v \in Pl(\mathbb{K})} dx_v$ defines a Haar measure on $\mathbb{T}_{\mathbb{K}}$

Theorem

a) The image of $\mathbb{K}$ is discrete in $\mathbb{T}_{\mathbb{K}}$

b) $\mathbb{T}_{\mathbb{K}} / \mathbb{K}$ is a compact space

c) $\mathrm{Vol}(\mathbb{T}_{\mathbb{K}} / \mathbb{K}) = |d_{\mathbb{K}}|^{1/2}$

Proof -

Let $d = [\mathbb{K} : \mathbb{Q}]$ and let $(e_1, \dots, e_d)$ be a basis of $\mathcal{O}_{\mathbb{K}}$ in $\prod_{v|\infty} \mathbb{K}_v$.

Lemma

The set

$$\mathcal{B} = \left(\sum_{i=1}^{d} [0,1[\, e_i \right) \times \prod_{\mathfrak{p} \in P(\mathcal{O}_{\mathbb{K}})} \mathcal{O}_{v_{\mathfrak{p}}}$$

is a fundamental domain for $\mathbb{K}$ in $\mathbb{T}_{\mathbb{K}}$; in other words any $\xi \in \mathbb{T}_{\mathbb{K}}$ may be written in a unique way as

$$\xi = b + x$$

with $b \in \mathcal{B}$ and $x \in \mathbb{K}$.

Proof -

Existence

Write $\xi = (\xi_v)_{v \in Pl(\mathbb{K})}$

and consider

$$x \in \mathfrak{a} = \prod_{\mathfrak{p} \in P(\mathcal{O}_{\mathbb{K}})} \mathfrak{p}^{-v_{\mathfrak{p}}(\xi_{v_{\mathfrak{p}}})} \quad \text{ideal of } \mathcal{O}_{\mathbb{K}}$$

$x \neq 0$ $\quad |\xi_{v_{\mathfrak{p}}}|_{v_{\mathfrak{p}}} \geq 1$

$x\xi = (x\xi_v)_{v \in P(\mathbb{K})}$
satisfies
$\forall\, p \in P(\mathcal{O}_{\mathbb{K}}) \quad v_p(x\xi_{v_p}) \geq 0$
That is $x\xi_{v_p} \in \mathcal{O}_v$
But

$$\mathcal{O}_{\mathbb{K}}/x\mathcal{O}_{\mathbb{K}} \xrightarrow{\sim} \prod_p \mathcal{O}_{\mathbb{K}}/p^{v_p(x)}$$

$$\xrightarrow{\sim} \prod_p \mathcal{O}_{v_p}/p^{v_p(x)}\mathcal{O}_{v_p}$$

Choose $y \in \mathcal{O}_{\mathbb{K}}$ such that
$(y - x\xi_{v_p}) \in p^{v_p(x)}\mathcal{O}_{v_p}$
for $p \nmid x$.
We get that
$\xi_{v_p} - f_{\mathbb{K}/\mathbb{K}}(y/x) \in \mathcal{O}_{v_p}$ for any $p \in P(\mathcal{O}_{\mathbb{K}})$
and
$\xi - f_{\mathbb{K}\otimes\mathbb{K}/\mathbb{K}}(y/x) \in \prod_{v\mid\infty} \mathbb{K}_v \times \prod_{v\nmid\infty} \mathcal{O}_v$.

Choose $u \in \mathcal{O}_{\mathbb{K}}$ such that
$(\xi_v)_{v\mid\infty} - f_{\infty}(y/x) - u) \in \sum_{i=1}^{d} [0,1[\, e_i$
(in the bases $(e_1, \dots, e_d)$ of the $\mathbb{R}$ vector space $\prod_{v\mid\infty} \mathbb{K}_v$, let $(y_1, \dots, y_d)$ be the coordinates of $(\xi_v)_{v\mid\infty} - f_{\infty}(y/x)$ and take
$u = \sum_{i=1}^{d} \lfloor y_i \rfloor e_i$)

Take $c = y/x + u$

Unicity
If $b + c = b' + c'$, $b, b' \in \mathcal{O}$, $c, c' \in \mathbb{K}$

Then $\xi_{\mathbb{A}_K/K}(c-c') \in \prod_{v|\infty} K_v \times \prod_{v\nmid\infty} \mathcal{O}_v$

in particular

$\forall\, p \in P(\mathcal{O}_K) \quad v_p(c-c') \geq 0$

so $c-c' \in \mathcal{O}_K$.

$\xi_v(c_i-c') \in \bigoplus_{i=1}^{d} \mathbb{Z} e_i$

but

$-(b_v - b'_v)_{v|\infty} \in \sum_{i=1}^{d}]-1,1[\, e_i$

$\xi_\infty(c-c') \in \bigoplus_{i=1}^{d} \mathbb{Z} e_i$

Therefor

$c = c'$ and $b = b'$. □

Proof of the theorem

a) $\sum_{i=1}^{d}]-\frac{1}{2},\frac{1}{2}[\, e_i \times \prod_{v\nmid\infty} \mathcal{O}_v \cap \xi_{\mathbb{A}_K/K}(K) = \{0\}$.

b) $\sum_{i=1}^{d} [0,1]\, e_i \times \prod_{v|\infty} \mathcal{O}_v \twoheadrightarrow \mathbb{A}_K/K$

compact

c) $\mathrm{Vol}(\mathbb{A}_K/K) = \mathrm{Vol}\left(\left(\prod_{v|\infty} K_v\right)/\xi_\infty(K)\right) \times \prod_{v\nmid\infty} \mathrm{Vol}(\mathcal{O}_v)$

$= |d_K|^{1/2}$, $\prod_{v\nmid\infty} = 1$

□

4] Idèles group

$\mathbb{G}_m = \mathrm{Spec}\, K[T,T^{-1}] \cdot \mathrm{Spec}\, K[U,V]/(UV-1)$

For any commutative $\mathbb{K}$-algebra A,

$$\mathbb{G}_m(A) = \mathrm{Mor}_{\mathrm{Spec}(\mathbb{K})}(\mathrm{Spec}(A), \mathbb{G}_m)$$

$$\Leftrightarrow \{(u,v) \in A^2 \mid uv = 1\}$$

$$\Leftrightarrow A^*$$

Definition

$\mathbb{A}_{\mathbb{K}}^* = \mathbb{G}_m(\mathbb{A}_{\mathbb{K}})$ is called the *group of Idèles*

Remark

By the product formula

$$\xi_{\mathbb{A}_{\mathbb{K}}/\mathbb{K}}(\mathbb{K}^*) \subset \underbrace{\{(\xi_v)_{v \in \mathrm{Pl}(\mathbb{K})} \in \mathbb{A}_{\mathbb{K}}^* \mid \prod_{v \in \mathrm{Pl}(\mathbb{K})} |\xi_v|_v = 1\}}_{\mathbb{G}_m(\mathbb{A}_{\mathbb{K}})^1}$$

Theorem

a] $\mathbb{K}^*$ is discrete in $\mathbb{G}_m(\mathbb{A}_{\mathbb{K}})^1$

b] $\mathbb{G}_m(\mathbb{A}_{\mathbb{K}})^1 / \mathbb{K}^*$ is compact

Proof

- Define

$$\mathrm{Log} : \mathbb{A}_{\mathbb{K}}^* \longrightarrow \prod_{v \mid \infty} \mathbb{R}$$

$$(\xi_v)_{v \in \mathrm{Pl}(\mathbb{K})} \longrightarrow \prod_{v \mid \infty} |\xi|_v$$

and

$$\tau : \mathbb{G}_m(\mathbb{A}_{\mathbb{K}})^1 \longrightarrow \mathcal{S}(G_{\mathbb{K}}) \text{ surjective } (\xi_{v_{\mathfrak{p}}})_{v_{\mathfrak{p}}}$$

$$(\xi_v)_{v \in \mathrm{Pl}(\mathbb{K})} \longmapsto \prod_{\mathfrak{p} \in \mathcal{P}(G_{\mathbb{K}})} \mathfrak{p}$$

- Consider a basis $(f_1, \dots, f_r)$ of $\mathrm{Log}(\mathcal{O}_{\mathbb{K}}^*)$ in $E \subset \prod_{v \mid \infty} \mathbb{R}$

$$E : \sum_{v \mid \infty} N_v x_v = 0.$$

- Choose $a_1, \dots, a_Q$ representative in $\mathcal{Y}(\mathcal{O}_{\mathbb{K}})$ of the elements of $\mathcal{CL}(\mathcal{O}_{\mathbb{K}})$.
  $\xi_1, \dots, \xi_Q \in \mathbb{G}_m(\mathbb{A}_{\mathbb{K}})^1$
  Such that $\tau(\xi_i) = a_i$

- We have
  $$\mathbb{G}_m(\mathbb{A}_{\mathbb{K}})^1 \cap \mathrm{Ker}(\tau) = \left\{ \left(\frac{\xi}{v}\right) \in \prod_{v|\infty} |\mathbb{K}_v| \prod_{v} |\xi_v|^{N_v} = 1 \right\} \times \prod_{v \nmid \infty} \mathcal{O}_v^*$$
  $$\underline{\mathrm{Log}}\left(\mathbb{G}_m(\mathbb{A}_{\mathbb{K}})^1 \cap \mathrm{Ker}(\tau)\right) \subset E.$$

  We define in $\mathbb{G}_m(\mathbb{A}_{\mathbb{K}})^1$
  $$\mathcal{B}_0 = \underline{\mathrm{Log}}^{-1}\left(\sum_{i=1}^{r} [0,1[\, f_i\right) \cap \mathrm{Ker}(\tau)$$
  and
  $$\mathcal{B} = \bigcup_{i=1}^{Q} \xi_i \cdot \mathcal{B}_0$$

Lemma

The set $\mathcal{B}$ is a fundamental domain for $\mathbb{K}^*$ in $\mathbb{G}_m(\mathbb{A}_{\mathbb{K}})^1$ modulo $\mu_\infty(\mathbb{K})$
($x\mathcal{B} = x'\mathcal{B} \Leftrightarrow x\mathcal{B} \cap x'\mathcal{B} \neq \emptyset \Leftrightarrow x'/x \in \mu_\infty(\mathbb{K})$)

Proof — *Existence*

Take $\xi \in \mathbb{G}_m(\mathbb{A}_{\mathbb{K}})^1$.
There is a (unique) i such that
$\tau(\xi \xi_i^{-1}) \in \mathcal{CL}(\mathcal{O}_{\mathbb{K}})$
ie we may choose $x \in \mathbb{K}^*$
such that
$$\tau(\xi\, \xi_i^{-1}) = (x)$$
ie $\xi\, \xi_i^{-1}\, x^{-1} \in \mathrm{Ker}(\tau)$
$\underline{\mathrm{Log}}(\xi\, \xi_i^{-1}\, x^{-1}) \in E$

we write it a

$$\underline{\log}\left(\xi \xi_i^{-1} x^{-1}\right) = \underline{\log}(u) + b$$

where

$$b \in \sum_{i=1}^{r}]0,1[\, \beta_i$$

Then $\xi (xu)^{-1} \in \xi_i \mathcal{B}_0$.

Unicity

$x, x' \in \mathbb{K}^*$, $i, j \in \{1, \dots, h\}$, $\xi, \xi' \in \mathcal{B}_0$

so that

$$\xi \xi_i x = \xi' \xi_j x'$$

$$\overline{\tau(\xi_i)} = \overline{\tau(\xi_j)} \text{ in } \mathcal{Cl}(\mathcal{O}_{\mathbb{K}})$$

So $i = j$ and

$$\xi x = \xi' x'$$

$\forall \mathfrak{p} \in \mathcal{O}_{\mathbb{K}}$ $\quad v_{\mathfrak{p}}(x) = v_{\mathfrak{p}}(x')$

So $x/x' \in \mathcal{O}_{\mathbb{K}}^*$

But $\underline{\log}(x/x') \in \sum_{i=1}^{r}]-1,1[\, \beta_i$

So

$$\underline{\log}(x/x') = 0$$

$$x/x' \in \mu_\infty(\mathbb{K}). \quad \square$$

End of the proof

a) $\underbrace{\underline{\log}^{-1}\left(\sum_{i=1}^{r}]-\tfrac{1}{2}, \tfrac{1}{2}[\, \beta_i\right) \cap \ker(\tau) \cap \mathbb{K}^*}_{\text{open in } \mathcal{G}_m(\mathbb{K}^*)} = \underbrace{\mu_\infty(\mathbb{K})}_{\text{finite}}$

b) $k_0 = \left\{ \underline{x} \in \prod_{v \mid \infty} \mathbb{K}_v \;\middle|\; \underline{\log}(\underline{x}) \in \sum_{i=1}^{r} [0,1]\, \beta_i \right\}$

is closed and bounded in the $r+1$ vector space $\prod_{v \mid \infty} \mathbb{K}_v$ therefor compact

$K_\infty \times \prod_{v \neq \infty}{}' G_v$ is compact

$G_k - \Pi_v$ closed in G_v

and surjects onto

$G_m(\mathbb{A}_K)^1 / \mathbb{K}^*$. □

5) Weak approximation.

Definition

One says that a variety V / K satisfies weak approximation if and only if for any $S \subset \Omega(K)$ finite $V(K)$ is dense in $\prod_{v \in S} V(K_v)$

Exercise

Show that $\mathbb{H}^1_K$ and G_m satisfy Weak approximation

Definition (This is weaker than weak approximation)

One says that V / K satisfies Hasse principle if and only if

$$\prod_{v \in \Omega(K)} V(K_v) \neq \emptyset \Rightarrow V(K) \neq \emptyset$$

To go further

J.P. Serre : Cours d'arithmétique; (PUF)

Theorem (Hasse)

Any quadric / $\mathbb{Q}$ satisfies the Hasse principle.

VII Heights

1) Definition

Notation

For any field k

$\mathbb{P}^n(k) = \{$vector subspaces of dimension 1 in $k^{n+1}\}$

$k^{n+1} - \{0\} \longrightarrow \mathbb{P}^n(k)$ surjective

$(x_0, \dots, x_n) \longmapsto (x_0 : \dots : x_n) = k(x_0, \dots, x_n)$

$(x_0 : \dots : x_n) = (y_0 : \dots : y_n) \Leftrightarrow \exists \lambda \in k^*, y_i = \lambda x_i$ for $i = 0, \dots, n$

Definition

Let k be a number field, and let $n \in \mathbb{N}$

The usual normalized exponential height function on $\mathbb{P}^n(k)$ is

$$H_n : \mathbb{P}^n(k) \longrightarrow \mathbb{R}$$

defined by

$$H_n(x_0 : \dots : x_n) = \prod_{v \in Pl(k)} \max_{0 \le i \le n} |x_i|_v .$$

Remark

This is well defined:

if $(x_0 : \dots : x_n) = (y_0 : \dots : y_n)$

then $(y_0, \dots, y_n) = \lambda (x_0, \dots, x_n)$ for $\lambda \in k^*$

$$\prod_{v \in Pl(k)} \max_i |y_i|_v = \prod_{v \in Pl(k)} \max_i |\lambda x_i|_v$$

$$= \underbrace{\left(\prod_{v \in Pl(k)} |\lambda|_v \right)}_{= 1 \text{ by the product formula}} \prod_{v \in Pl(k)} \max_i |x_i|_v$$

Example

If $k = \mathbb{Q}$

Terminology

$(x_0, \dots, x_n) \in \mathbb{Z}^{n+1}$ is said to be primitive iff $\gcd(x_0, \dots, x_n) = 1$

Claim

Let $P \in \mathbb{P}^n(\mathbb{Q})$ there exists up to multiplication by -1 a unique primitive element $(x_0, \dots, x_n) \in \mathbb{Z}^{n+1}$ such that

$$P = (x_0 : \dots : x_n)$$

Proof

- Multiplying by the product of the denominators of coordinates we get that

$$P = (y_0 : \dots : y_n)$$

with $(y_0, \dots, y_n) \in \mathbb{Z}^{n+1} - \{0\}$ and divide by the gcd.

- if $(x_0, \dots, x_n)$, $(y_0, \dots, y_n)$ are primitive and $(x_0 : \dots : x_n) = (y_0 : \dots : y_n)$ then $(y_0, \dots, y_n) = \lambda (x_0, \dots, x_n)$ $\lambda = \frac{p}{q}$ and $\gcd(y_0, \dots, y_n) = 1 = \gcd(x_0, \dots, x_n)$ gives $p \mid 1$ and $q \mid 1$ so $\lambda \in \{-1, 1\}$. □

Formula

If $(x_0, \dots, x_n) \in \mathbb{Z}^{n+1}$ is primitive

$$H_n(x_0 : \dots : x_n) = \max_{0 \le i \le n} |x_i|$$

Proof

Since $(x_0, \dots, x_n)$ is primitive for any prime p

$$\min_i v_p(x_i) = 0$$

so $\max_i |x_i|_p = 1$ $\square$

In particular for any $B \in \mathbb{R}$

$$\{ P \in \mathbb{P}^n(\bar{\mathbb{Q}}) \mid H_n(P) \leq B \}$$

is finite

Notation

If $P = (x_0 : \dots : x_n) \in \mathbb{P}^n(\bar{\mathbb{Q}})$, $x_i \neq 0$

$\mathbb{Q}(x_0/x_i, \dots, x_n/x_i)$ does not depend on the choice of i such that $x_i \neq 0$

$$d(P) = [\mathbb{Q}(x_0/x_i, \dots, x_n/x_i) : \mathbb{Q}].$$

Lemma

Let $\mathbb{L}/\mathbb{K}$ be number fields

Let $g_{\mathbb{L}/\mathbb{K}} : \mathbb{P}^n(\mathbb{K}) \to \mathbb{P}^n(\mathbb{L})$

$$(x_0 : \dots : x_n) \mapsto (g_{\mathbb{L}/\mathbb{K}}(x_0) : \dots : g_{\mathbb{L}/\mathbb{K}}(x_n))$$

Then

$$\forall P \in \mathbb{P}^n(\mathbb{K}) \quad H_n(g_{\mathbb{L}/\mathbb{K}}(P)) = H_n(P)$$

Proof

$$H_n(g_{\mathbb{L}/\mathbb{K}}(P)) = \prod_{w \in Pl(\mathbb{L})} \max_i |g_{\mathbb{L}/\mathbb{K}}(x_i)|_w$$

$$= \prod_{v \in Pl(\mathbb{K})} \left(\prod_{w|v} \max_i |g_{\mathbb{L}/\mathbb{K}}(x_i)|_w \right)$$

$$= \prod_{v \in Pl(K)} \prod_{w|v} \max_i \left| N_{L_w/Q_{K_v}}(\xi_{K,i}(x)) \right|_v^{\frac{1}{[L:K]}}$$

Lemma

If $M/L/K$ are field extensions, finite

$\forall x \in M$, $N_{M/K}(x) = N_{L/K}(N_{M/L}(x))$

Proof

$$N_{M/K}(x) = \prod_{\tau \in \Sigma_{M/K}} \tau(x)$$

(K is a L-algebra for σ)

$$= \prod_{\sigma \in \Sigma_{L/K}} \prod_{\substack{\tau \in \Sigma_{M/K} \\ \tau \circ \delta_{L/K} = \sigma}} \tau(x)$$

$$= \prod_{\sigma \in \Sigma_{L/K}} \sigma(N_{M/L}(x))$$

$$= N_{L/K}(N_{M/L}(x)) \quad \square$$

Proof (continued)

if $w \mid v \mid u$

$\wedge \quad \wedge \quad \wedge$

$Pl(L) \quad Pl(K) \quad Pl(Q)$

$$|N_{L_w/Q_u}(x)|_u^{\frac{1}{[L:Q]}}$$

$$= |N_{K_v/Q_u}(N_{L_w/K_v}(x))|_u^{\frac{1}{[L:K][K:Q]}}$$

$$= |N_{L_w/K_v}(x)|_v^{\frac{1}{[L:K]}}.$$

$$H_n(\underset{\in \mathbb{K}}{P}(P)) = \prod_{v \in \mathcal{P}\ell(\mathbb{K})} \prod_{w|v} \max_i |x_i|_v^{\frac{N_{w|v}}{[\mathbb{L}:\mathbb{K}]}}$$

$$= \prod_{v \in \mathcal{P}\ell(\mathbb{K})} \left(\max_i |x_i|_v\right)^{\frac{\sum N_{w|v}}{[\mathbb{L}:\mathbb{K}]}} = 1 \quad \square$$

2| Northcott theorem.

Theorem (Northcott)

Let $d \in \mathbb{N}_{>0}$, $B \in \mathbb{R}$

$\{ P \in \mathbb{P}^n(\overline{\mathbb{Q}}) \mid d(P) \leq d \text{ and } H_n(P) \leq B \}$

is finite.

Proof

$d = 1$ already seen.

$d \geq 2$ we want to construct

1| $\varphi : (\mathbb{P}^n)^d \longrightarrow \mathbb{P}^N$

inducing

$$\bar{\varphi} : (\mathbb{P}^n)^d / \mathfrak{S}_d \hookrightarrow \mathbb{P}^N$$

- Consider polynomial in $\mathbb{K}[X_{i,j}, 0 \leq i \leq n, 1 \leq j \leq d]$

of the forme

$$\prod_{i=0}^{n} \sigma_{\alpha_i}(X_{i,1}^{\alpha_i}, \dots, X_{i,d}^{\alpha_i})$$

where $\alpha_0 + \dots + \alpha_n = d$. $0 \leq \alpha_i \leq d$.

- they are homogeneous of degree d in each set of variable

$$(X_{0,j}, \dots, X_{n,j})$$

and symmetric in $(X_{i,1}, \dots, X_{id})$.

- Let $N+1$ be the cardinal of this set of polynomials, we get

$$\bar{\varphi} : (\mathbb{P}^n)^d / \mathfrak{S}_d \hookrightarrow \mathbb{P}^N$$

as wanted.

2] Take $(x_0, \dots, x_n) \in \mathbb{K}^{n+1} - \{0\}$
such that $[\mathbb{K} : \mathbb{Q}] = d$.
and consider $\{\sigma_1, \dots, \sigma_d\} = \Sigma_{\mathbb{K}/\mathbb{Q}}$

$$(\sigma_i(x_0) : \cdots : \sigma_i(x_n))_{1 \le i \le d} \in (\mathbb{P}^n(\bar{\mathbb{Q}})^d / \mathfrak{S}_d)^{Gal(\bar{\mathbb{Q}}/\mathbb{Q})}$$

$$\downarrow \qquad\qquad \downarrow$$

$$P \in \mathbb{P}^N(\bar{\mathbb{Q}})^{Gal(\bar{\mathbb{Q}}/\mathbb{Q})}$$

But

$$\mathbb{P}^N(\bar{\mathbb{Q}})^{Gal(\bar{\mathbb{Q}}/\mathbb{Q})} = \mathbb{P}^N(\mathbb{Q})$$

$$\left(x_i/x_j \in (\bar{\mathbb{Q}})^{Gal(\bar{\mathbb{Q}}/\mathbb{Q})} \in \mathbb{Q} \right)$$

So $P \in \mathbb{P}^N(\mathbb{Q})$ and depends only on $(x_0 : \cdots : x_n) \in \mathbb{P}^n(\mathbb{K})$
We get a map ψ

$$\{(x_0 : \cdots : x_n) \in \mathbb{P}^N(\bar{\mathbb{Q}}) \mid \deg(x_0 : \cdots : x_n) = d\}$$

$$\psi \downarrow$$

$$\mathbb{P}^N(\mathbb{Q})$$

3] The fibers of ψ have at most $d!$ elements
$\left((\mathbb{P}^n)^d(\bar{\mathbb{Q}}) / \mathfrak{S}_d \hookrightarrow \mathbb{P}^N(\bar{\mathbb{Q}}) \right)$

4] There exists $C > 0$ and $\alpha \in \mathbb{N}_{>0}$

$$H_N(\psi(P)) \le C \, H_n(P)^\alpha$$

$$\left| \prod_{i=0}^{n} \sigma_{j_i}(x_{i,1}^{\alpha_1} \cdots x_{i,d}^{\alpha_n}) \right|_v$$

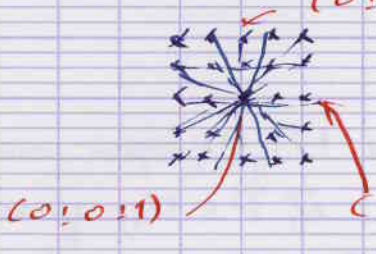
$$\le \left| 2^{\delta} \right|_v \prod_{i=0}^{n} \max_{0 \le i \le n} (x_{i,j})^{\alpha_i} \le |2^d|_v \, H_n(P)^{d^{n+1}} \quad \square$$

To go further :

* J. P. Serre lectures on the Mordell-Weil theorem.
* E. P. : Points de hauteur bornée et géométrie des variétés (Seminaire Bourbaki, exposé 891) on my web page.

3] A few pictures

a] $\mathbb{P}^n(\mathbb{Q})$



$$\{(x,y)\in\mathbb{Q}^2 \mid \begin{cases} |x|\leq 1 \\ |y|\leq 1 \\ H_2(x:y:1)\leq 1600 \end{cases}\}$$

b] $\mathbb{P}^1(\mathbb{Q}(i\sqrt{5}))$

$$\{(x,y)\in\mathbb{Q}^2 \mid \begin{cases} |x|\leq 1 \\ |y|\leq 1/\sqrt{5} \\ H_1(x+iy\sqrt{5}:1)\leq \end{cases}\}$$

two colors : $\mathcal{O}_{\mathbb{Q}(i\sqrt{5})}$ is not principal.

Let $P=(x:y)\in\mathbb{P}^1(\mathbb{Q}(i\sqrt{5}))$

The class in $Cl(\mathcal{O}_{\mathbb{Q}(i\sqrt{5})})$ of the fractional ideal generated by $\{x,y\}$ does not depend on the choice of the homogeneous coordinates, but only on P

We get a map

$$d: \mathbb{P}^1(\mathbb{Q}(i\sqrt{5})) \to \underbrace{Cl(\mathcal{O}_{\mathbb{Q}(i\sqrt{5})})}_{\text{cardinal 2}}$$

Schanuel has proven that

$$\#\{P \in \mathbb{P}^1(\mathbb{Q}(i\sqrt{5})) \mid H_1(P) \leq B \text{ and } d(P) = 4\}$$
$$\sim_{B \to +\infty}$$
$$\#\{P \in \mathbb{P}^1(\mathbb{Q}(i\sqrt{5})) \mid H_1(P) \leq B \text{ and } d(P) = 2\}$$

3) Châtelet surfaces

$S(\mathbb{R})$ two real connected components

$S : Y^2 + Z^2 = X^3 - X$

two colors

$S(\mathbb{Q}_2) = U_1 \amalg U_2$; U_1, U_2 open and closed

the color is red if $P \in U_1$, green if $P \in U_2$

all the red points are on the same connected component on $S(\mathbb{R})$

$S(\mathbb{R}) = V_1 \amalg V_2$; V_1, V_2 open and closed $\neq \emptyset$

So

$$S(\mathbb{Q}_2) \times S(\mathbb{R}) = U_1 \times V_1 \amalg U_1 \times V_2 \amalg U_2 \times V_1 \amalg V_1 \times V_2$$

We have

$$S(\mathbb{Q}) \subset U_1 \times V_1 \amalg V_1 \times V_2$$

and $S(\mathbb{Q})$ is not dense in $S(\mathbb{Q}_2) \times S(\mathbb{R})$

S does not satisfy weak approximation.

Wednesday September 18, 2013

Algebraic Number Theory

Problem

Principality for ring of integers in quadratic extensions

In this problem, $\mathbf{N}$ denotes the set of nonnegative integers, $\mathbf{Z}$ the ring of integers, and $\mathbf{C}$ the field of complex numbers. If p is a prime number, $\mathbf{F}_p$ denotes the field $\mathbf{Z}/p\mathbf{Z}$. We denote by i an element of $\mathbf{C}$ such that $\mathrm{i}^2 = -1$.

Les S be a commutative ring. We denote by $\mathscr{M}_n(S)$ the S-algebra of square $n \times n$ matrices and by $\mathrm{GL}_n(S)$ the group of invertible elements in $\mathscr{M}_n(S)$. We denote by ${}^tM$ the transpose of a matrix M. For any M in $\mathscr{M}_n(\mathbf{C})$, M^* is the adjoint matrix of M (that is the conjugate of ${}^tM$).

We say that a real symmetric or complex hermitian matrix is positive definite if the corresponding form is.

Part I

Ring of Integers

Let $D \geqslant 1$ be a squarefree positive integer (that is D is not divisible by the square of a prime number). We put $\mathbf{K} = \mathbf{Q}(\mathrm{i}\sqrt{D}) \subset \mathbf{C}$.

1. Prove that $(1, \mathrm{i}\sqrt{D})$ is a basis of the $\mathbf{Q}$-vector space $\mathbf{K}$. For $x, y \in \mathbf{Q}$, compute $N_{\mathbf{K}/\mathbf{Q}}(x + y\mathrm{i}\sqrt{D})$ and $\mathrm{Tr}_{\mathbf{K}/\mathbf{Q}}(x + y\mathrm{i}\sqrt{D})$.

2. Let $x, y \in \mathbf{Q}$. Prove that if $x + y\mathrm{i}\sqrt{D} \in \mathscr{O}_{\mathbf{K}}$, then $2x \in \mathbf{Z}$ and $x + y \in \mathbf{Z}$.

3. When does $\frac{1+\mathrm{i}\sqrt{D}}{2}$ belong to $\mathscr{O}_{\mathbf{K}}$?

4. We put

$$\omega_D = \begin{cases} \mathrm{i}\sqrt{D} \text{ if } D \equiv 1 \text{ or } 2 \pmod 4, \\ \frac{1+\mathrm{i}\sqrt{D}}{2} \text{ otherwise.} \end{cases}$$

Give a basis of the free $\mathbf{Z}$-module $\mathscr{O}_{\mathbf{K}}$.

5. Compute the discriminant $d_{\mathbf{K}}$.

Part II

Technical lemmata

Let p be an odd prime number.

1. (a) Let u, v, and w be nonzero elements in $\mathbf{F}_p$. Prove that the equation

$$ux^2 + vy^2 = w$$

has a solution in $\mathbf{F}_p$ (you may consider the cardinal of the image of the map $y \mapsto w - vy^2$).

(b) Let $n > 1$ be an integer such that $4n - 1$ is not divisible by p. Prove that there exist $a, b \in \mathbf{Z}$ and $m \geqslant 1$ such that

$$a^2 + ab + nb^2 + 1 = mp$$

2. Assume that either $p = 8k + 1$ or $p = 8k + 3$ and let $\mathbf{K}$ be the splitting field of $X^4 + 1$ over $\mathbf{F}_p$. Let b be a root of $X^4 + 1$ in $\mathbf{K}$. We put $x = b - b^{-1}$

(a) Prove that $x^2 = -2$ and $x^p = x$. Does x come from $\mathbf{F}_p$?

(b) Prove that there exist integers a and m such that

$$2a^2 + 1 = (2m - 1)p$$

and prove that the matrix

$$\begin{pmatrix} p & a & 0 \\ a & m & 1 \\ 0 & 1 & 2 \end{pmatrix}$$

is a positive definite symmetric matrix with determinant 1. Find (a, m) for $p = 17$.

Part III

Euclidean rings of integers

We use the notations D and ω_D of part I.

1. Let p be a prime number which is not a factor of D. Prove that there exist relative integers a, b and n such that the matrix

$$\begin{pmatrix} p & a + b\omega_D \\ a + b\overline{\omega}_D & m \end{pmatrix}$$

is a definite positive hermitian matrix with determinant 1.

2. We consider the complex plane as a euclidean plane and put $A = 0$, $B = 1$ and $C = \omega_D$. Let T be the convex hull of the points A, B and C. Denotes by R the radius of the circumcircle of the triangle T.

(a) Prove that for any M in T, one has

$$\inf(MA, MB, MC) \leqslant R$$

(b) We put

$$k = \sup_{z \in \mathbf{C}} \left(\inf_{u \in \mathscr{O}_\mathbf{K}} |z-u|^2 \right).$$

Prove that

$$k = \sup_{M \in T} (\inf(MA^2, MB^2, MC^2)).$$

(c) Prove that

$$k = \begin{cases} \frac{D+1}{4} \text{ if } D \equiv 1 \text{ or } 2 \pmod 4, \\ \frac{(D+1)^2}{16D} \text{ otherwise.} \end{cases}$$

(d) Let $\alpha, \beta \in \mathscr{O}_\mathbf{K}$. Assume that $\beta \neq 0$. Show that there exists $\gamma \in \mathscr{O}_\mathbf{K}$ such that

$$|\alpha - \gamma\beta|^2 \leqslant k|\beta|^2$$

Prove that $\mathscr{O}_\mathbf{K}$ is an euclidean ring if $D \in \{1, 2, 3, 7, 11\}$.

Part IV

Hermitian matrices of the form B^*B

In this part $\mathbf{K}$ is either the field $\mathbf{Q}$ or of the form $\mathbf{Q}(\mathrm{i}\sqrt{D})$ with $D \in \{1, 2, 3, 7, 11\}$. The constant k is $1/4$ if $\mathbf{K} = \mathbf{Q}$ and is the constant defined in question III.2.(c) otherwise.

Two hermitian matrices A and B in $\mathscr{M}_n(\mathscr{O}_\mathbf{K})$ are said to be congruent if there exists $U \in \mathrm{GL}(\mathscr{O}_\mathbf{K})$ such that $A = UBU^*$. Equivalence classes for this relation are called congruence classes.

1. Compare $\det(A)$ and $\det(B)$ for congruent hermitian matrices A and B.

2. (a) Let A be a hermitian positive definite matrix in $\mathscr{M}_n(\mathscr{O}_\mathbf{K})$. Prove that there exist an integer $m(A) > 0$ and an element z of $\mathscr{O}_\mathbf{K}^n$ with coprime coordinates such that we have the equality

$$m(A) = \inf_{x \in \mathscr{O}_\mathbf{K}^n - \{0\}} xAx^* = zAz^*.$$

(b) Compare $m(A)$ and $m(B)$ when A and B are congruent hermitian positive definite matrices.

(c) Find $m(A)$ for $\mathbf{K} = \mathbf{Q}$ and $A = \left(\begin{smallmatrix} 2 & 7 \\ 7 & 25 \end{smallmatrix}\right)$.

3. In this question, we denote by A a hermitian positive definite matrix in $\mathscr{M}_2(\mathscr{O}_\mathbf{K})$ and by z an element in $\mathscr{O}_\mathbf{K}^2$ such that $m(A) = zAz^*$.

(a) Prove that there exists a matrix $U \in \mathrm{GL}_2(\mathscr{O}_\mathbf{K})$, the first column of which is ${}^t z$. Prove that there exist a hermitian matrix $B = (b_{i,j})_{1 \leqslant i,j \leqslant 2}$, congruent to A and such that $b_{1,1} = m(A)$.

(b) Prove that there exists $s \in \mathscr{O}_{\mathbf{K}}$ such that

$$|b_{1,1}s + b_{1,2}| \leqslant k^{1/2} b_{1,1}.$$

Prove that there exists a hermitian matrix $C = \left(\begin{smallmatrix} a & b \\ \overline{b} & c \end{smallmatrix}\right)$ which is congruent to A and which satisfies the following two conditions

(i) $a = m(A) = m(C)$;

(ii) $k^{-1/2}|b| \leqslant a \leqslant c$.

(c) Let $A \in \mathscr{M}_2(\mathscr{O}_{\mathbf{K}})$ be a hermitian positive definite matrix of determinant d. Prove that

$$m(A) \leqslant (1-k)^{-1/2} d^{1/2}.$$

(d) Prove that the set of congruence classes of hermitian positive definite matrices in $\mathscr{M}_2(\mathscr{O}_{\mathbf{K}})$ with determinant d is finite.

(e) We assume that $d = 1$ and that $\mathbf{K} = \mathbf{Q}$ or $\mathbf{K} = \mathbf{Q}(\mathrm{i}\sqrt{D})$ for some $D \in \{1, 3, 7\}$. Prove that $m(A) = 1$ and that there exists $B \in \mathrm{GL}_2(\mathscr{O}_{\mathbf{K}})$ such that $A = B^* B$.

(f) Prove the following statements :

(i) Any prime number is the sum of four squares ;

(ii) For any prime number p, there exists $a, b, c, d \in \mathbf{Z}$ such that

$$p = a^2 + ab + b^2 + c^2 + cd + d^2;$$

(iii) For any prime number p, there exists $a, b, c, d \in \mathbf{Z}$ such that

$$p = a^2 + ab + 2b^2 + c^2 + cd + 2d^2.$$

(g) Using Hamilton quaternion algebra, prove that any nonnegative integer is the sum of four squares.

4. (a) Let $f : \mathbf{Z}^n \to \mathbf{Z}$ be a surjective morphism of groups and let $x \in \mathbf{Z}^n$ be such that $f(x) = 1$. Prove that $\mathbf{Z}^n$ is the direct sum of $\mathrm{Ker}(f)$ and $\mathbf{Z}x$.

(b) Let $x = (x_1, \ldots, x_n) \in \mathbf{Z}^n$. Prove that the following statements are equivalent :

(i) The vector x is the first vector of a basis of $\mathbf{Z}^n$;

(ii) There exists $(a_1, \ldots, a_n) \in \mathbf{Z}^n$ such that $\sum_{i=1}^n a_i x_i = 1$;

(iii) There exists a surjective morphism of groups $f : \mathbf{Z}^n \to \mathbf{Z}$ such that $f(x) = 1$.

5. Let $A \in \mathscr{M}_n(\mathbf{Z})$ be a symmetric definite positive matrix. Prove that there exists a matrix $B = (b_{i,j})_{1 \leqslant i,j \leqslant n}$ which is congruent to A and such that $b_{1,1} = m(A)$.

6. Let $A = (a_{i,j})_{1 \leqslant i,j \leqslant n} \in \mathscr{M}_n(\mathbf{Z})$ be a symmetric definite positive matrix such that $m(A) = a_{1,1}$. Let $\boldsymbol{x} = (x_1, \ldots, x_n) \in \mathbf{Z}^n$ and let $U = (u_{i,j})_{1 \leqslant i,j \leqslant n}$ be defined by

$$u_{i,j} = \begin{cases} a_{i,j} a_{1,1}^{-1} \text{ if } i = 1 \text{ and } j > 1, \\ 1 \text{ if } i = j, \\ 0 \text{ otherwise.} \end{cases}$$

Put $\boldsymbol{z} = (x_2, \ldots, x_n)$ and $\boldsymbol{y} = {}^t(U^t x)$.

(a) Prove that there exists a symmetric definite positive matrix $B \in \mathscr{M}_{n-1}(\mathbf{Z})$ such that

$$\boldsymbol{x} A \, {}^t\boldsymbol{x} = a_{1,1} y_1^2 + a_{1,1}^{-1} \boldsymbol{z} B \, {}^t\boldsymbol{z},$$

$$A = {}^tU \begin{pmatrix} a_{1,1} & 0 \\ 0 & a_{1,1}^{-1} B \end{pmatrix} U.$$

Compute $\det(B)$.

(b) Prove that $m(A) \leqslant \left(\frac{4}{3}\right)^{\frac{n-1}{2}} (\det(A))^{1/n}$ (Choose $\boldsymbol{x}$ so that $y_1 \leqslant 1/2$ and $\boldsymbol{z} B \, {}^t\boldsymbol{z} = m(B)$).

7. (a) We assume that $n \leqslant 5$ and that $A \in \mathscr{M}_n(\mathbf{Z})$ is a symmetric definite positive matrix with determinant 1. Prove that $m(A) = 1$ and that there exists $B \in \mathscr{M}_n(\mathbf{Z})$ such that $A = {}^tBB$.

(b) prove that any prime number of the form $8n + 1$ or $8n + 3$ is the sum of three squares.

Part V

Principal rings of integers

Two matrices A and B in $\mathscr{M}_n(\mathbf{Z})$ are said to be similar if there exists $Q \in \mathrm{GL}_n(\mathbf{Z})$ such that $A = QBQ^{-1}$. The equivalence classes for this relation are called similitude classes.

Let $\theta \in \mathbf{C}$ be integral over $\mathbf{Z}$. Let P be the minimal polynomial of θ over $\mathbf{Q}$ and let $n = \deg(P)$. We say that two ideals I and J of $\mathbf{Z}[\theta]$ are equivalent if there exist non-zero elements a and b in $\mathbf{Z}[\theta]$ such that $aI = bJ$. Let $A \in \mathscr{M}_n(\mathbf{Z})$ be such that $P(A) = 0$.

1. Prove that any non-zero ideal in $\mathbf{Z}[\theta]$ is a free $\mathbf{Z}$-module of rank n.

2. (a) Prove that there exists $\boldsymbol{x} = (x_1, \ldots, x_n) \in \mathbf{Z}[\theta]^n - \{0\}$ such that $A\,{}^t\boldsymbol{x} = \theta\,{}^t\boldsymbol{x}$.

(b) Prove that $\mathbf{Z}x_1 + \ldots \mathbf{Z}x_n$ is an ideal in $\mathbf{Z}[\theta]$ the equivalence class of which does not depend on the choosen $\boldsymbol{x}$. Let I_A denotes this equivalence class.

(c) For any $Q \in \mathrm{GL}_n(\mathbf{Z})$, prove that $I_A = I_{QAQ^{-1}}$.

3. Let $J = \mathbf{Z}y_1 + \cdots + \mathbf{Z}y_n$ be an ideal of $\mathbf{Z}[\theta]$ and let $\boldsymbol{y} = (y_1, \ldots, y_n)$. Prove that there exists $B \in \mathscr{M}_n(\mathbf{Z})$ such that $B\,{}^t\boldsymbol{y} = \theta\,{}^t\boldsymbol{y}$ and $P(B) = 0$.

4. Prove that there exists a bijection between the similitude classes of matrices $A \in \mathscr{M}_n(\mathbf{Z})$ such that $P(A) = 0$ and the equivalence classes of ideals in $\mathbf{Z}[\theta]$.

5. Prove that the following statements are equivalent :

(i) $\mathbf{Z}[\theta]$ is a principal ring ;

(ii) There exists a unique similitude class of matrices $A \in \mathscr{M}_n(\mathbf{Z})$ such that $P(A) = 0$.

Part VI

The case of quadratic extensions

We use the notations of part I.

1. We assume that $D \equiv 1$ or $2 \pmod 4$ let

$$A(\alpha, \beta, \gamma) = \begin{pmatrix} -\alpha & \beta \\ \gamma & \alpha \end{pmatrix}$$

be a matrix in $\mathscr{M}_2(\mathbf{Z})$ with characteristic polynomial $X^2 + D$, Using $\alpha = 0$ or $\alpha = 1$, prove that $\mathscr{O}_{\mathbf{K}}$ is principal if and only if $D \in \{1, 2\}$.

2. Assume that $D \equiv 3 \pmod 4$ and put $K = (D+1)/4$. Let $A \in \mathscr{M}_2(\mathbf{Z})$ be a matrix with characteristic polynomial $P(X) = X^2 - X + K$.

(a) Let $B = \left(\begin{smallmatrix} -a & -b \\ c & a+1 \end{smallmatrix}\right)$ be a matrix similar to A with $|a|$ minimal. Compute PAP^{-1} when P is of the form

$$\left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right) \quad \left(\begin{smallmatrix} 1 & 0 \\ n & 1 \end{smallmatrix}\right) \quad \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \quad \text{or} \quad \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$$

and prove that we may assume that

$$a \geqslant 0, \quad c \geqslant 2a+1, \quad b \geqslant 2a+1, \quad \text{and} \quad 3(a^2+a)+1 \leqslant K$$

(b) Let $\alpha, \beta, \gamma \in \mathbf{N}$ satisfy

$$0 \leqslant \alpha < K-1, \quad 1 < \beta \leqslant \gamma, \quad \text{and} \quad \beta\gamma = K + \alpha^2 + \alpha$$

Prove that for any $(x, y) \in \mathbf{Z}^2 - \{0\}$, we have

$$\beta x^2 + \gamma y^2 + (2\alpha + 1)xy > y^2.$$

Prove that the matrices

$$A = \begin{pmatrix} 0 & -K \\ 1 & 1 \end{pmatrix} \quad \text{and} \quad A = \begin{pmatrix} -\alpha & -\gamma \\ \beta & \alpha + 1 \end{pmatrix}$$

are not similar.

(c) We assume that $\mathscr{O}_{\mathbf{K}}$ is a principal ring. Prove that $K = 1$ or that $K + a^2 + a$ is a prime number for any integer a such that $0 \leqslant a < K - 1$.

(d) Conversely assume that $K = 1$ or that $K + a^2 + a$ is a prime number for any integer a such that $0 \leqslant a < K - 1$. Prove that $\mathscr{O}_{\mathbf{K}}$ is principal.

(e) Assume $D \leqslant 200$. Prove that $\mathscr{O}_{\mathbf{K}}$ is principal if and only if $D = 3, 7, 11, 19, 43, 67, 163$.

(f)* *Small project : write a computer program to find any other value of* $D \leqslant 10^6$ *for which* $\mathscr{O}_{\mathbf{K}}$ *is principal.*

3. We assume that $D \in \{\, 19, 43, 67, 163 \,\}$. we assume that $\mathscr{O}_{\mathbf{K}}$ is an euclidean ring for some euclidean function $\varphi : \mathscr{O}_{\mathbf{K}} - \{0\} \to \mathbf{N}$. Let $a \in \mathscr{O}_{\mathbf{K}} - \{0\}$ be a non-invertible element such that $\varphi(a)$ is minimal.

(a) Prove that $\mathscr{O}_{\mathbf{K}}/a\mathscr{O}_{\mathbf{K}}$ is isomorphic to $\mathbf{F}_2$ or $\mathbf{F}_3$.

(b) Prove that for $D \in \{\, 19, 43, 67, 163 \,\}$, $\mathscr{O}_{\mathbf{K}}$ is principal but not euclidean.

Wednesday October 23, 2013

Algebraic Number Theory

Problem

Van der Waerden's theorem

The aim of this problem is to prove that, among the polynomials of degree n with integral coefficients in the interval $[-N, N]$, the proportion of those for which the corresponding Galois group is the symmetric group $\mathfrak{S}_n$ goes to 1 as the bound N goes to infinity.

In this problem, we denote by $\overline{K}$ an algebraic closure of a field $\mathbf{K}$. For any separable polynomial P in $\mathbf{K}[X]$, the set of roots of P in $\overline{\mathbf{K}}$ is denoted by $\mathscr{E}_P$ and $\mathbf{K}_P = \mathbf{K}(\mathscr{E}_P) \subset \overline{\mathbf{K}}$. The Galois group associated to P is then the Galois group $\mathscr{G}_P$ of the Galois extension $\mathbf{K}_P/\mathbf{K}$. For any set X, $\mathfrak{S}_X$ is the group of permutations of X. Remember that the action of $\mathscr{G}_P$ on $\mathscr{E}_P$ induces an embedding of $\mathscr{G}_P$ into $\mathfrak{S}_{\mathscr{E}_P}$ We also put $\mathbf{N}_{>0} = \mathbf{N} - \{0\}$. If $q \neq 1$ is a power of a prime number, we denote by $\mathbf{F}_q$ a field of cardinal q, so that if p is a prime number $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$.

Part I

Irreductible polynomials on finite fields

Let p be a prime number and let $q \neq 1$ be some power of p. We denote by $a_n(q)$ the number of irreducible polynomials of degree n in $\mathbf{F}_q[T]$ and by $b_n(q)$ the number of irreducible polynomials of degree n in $\mathbf{F}_q[T]$ with leading coefficient 1.

1. Prove that $q^n = \sum_{d|n} d\, b_d(q)$. (Hint : Consider $X^{q^n} - X$ over $\mathbf{F}_{q^n}$ and then find its decomposition in irreducible factors over $\mathbf{F}_q$).

2. We define the *Moebius map* $\mu : \mathbf{N}_{>0} \to \{-1, 0, 1\}$ by the fact it is *multiplicative* :

$$\forall a, b \in \mathbf{N}_{>0}, \quad \gcd(a, b) = 1 \Longrightarrow \mu(ab) = \mu(a)\mu(b)$$

and for any prime number ℓ and any $k \in \mathbf{N}$,

$$\mu(\ell^k) = \begin{cases} 1 \text{ if } k = 0, \\ -1 \text{ if } k = 1, \\ 0 \text{ otherwise.} \end{cases}$$

We also put $\psi(n) = \sum_{d|n} \mu(d)$ for any $n \in \mathbf{N}_{>0}$.

(a) Prove that ψ is also multiplicative.

(b) Compute $\psi(\ell^k)$ for ℓ prime and $k \in \mathbf{N}$, and then $\psi(n)$ for any $n \in \mathbf{N}_{>0}$.

(c) Let f, g be maps from $\mathbf{N}_{>0}$ to $\mathbf{Z}$. Prove that if

$$\forall n \in \mathbf{N}_{>0}, \quad f(n) = \sum_{d|n} g(d)$$

then

$$\forall n \in \mathbf{N}_{>0}, \quad g(n) = \sum_{d|n} \mu(d) f(n/d).$$

3. Prove that

$$b_n(q) = \frac{1}{n} \sum_{d|n} \mu(d) q^{n/d}.$$

4. Prove that

$$a_n(q) \geqslant \frac{q^n(q-2)}{n}.$$

(Hint : Use the value of $\sum_{m<n} q^m$ to find a lower bound for $nb_n(q)$). Deduce from the previous relation that $a_n(q) \geqslant q^{n+1}/(3n)$ when $q > 2$.

Part II

Reduction modulo p of Galois groups

Let p be a prime number. For any number field $\mathbf{K}$, we denote by $\mathscr{O}_{\mathbf{K},(p)}$ the integral closure of $\mathbf{Z}_{(p)}$ in $\mathbf{K}$.

1. Prove that the maximal ideal of $\mathbf{Z}_{(p)}$ is generated by p.

2. We assume that $\mathbf{K}/\mathbf{Q}$ is a Galois extension. Let $\mathfrak{p}$ be a prime ideal of $\mathscr{O}_{\mathbf{K}}$ such that $\mathfrak{p}|p$. We put $q = N(\mathfrak{p}) = \sharp(\mathscr{O}_{\mathbf{K}}/\mathfrak{p})$. We define

$$D_{\mathfrak{p}} = \{\, \sigma \in \mathrm{Gal}(\mathbf{K}/\mathbf{Q}) \mid \sigma(\mathfrak{p}) = \mathfrak{p} \,\}.$$

(a) Let $\sigma \in D_{\mathfrak{p}}$. Prove that the ring automorphism of $\mathscr{O}_{\mathbf{K}}$ defined by σ defines an element $\sigma_{\mathfrak{p}}$ in $\mathrm{Gal}((\mathscr{O}_{\mathbf{K}}/\mathfrak{p})/\mathbf{F}_p)$. Prove that $r_{\mathfrak{p}} : \sigma \mapsto \sigma_{\mathfrak{p}}$ is a morphism of groups.

(b) Prove that $r_{\mathfrak{p}}$ is surjective. (Hint : consider the field $\mathbf{L} = \mathbf{K}^{D_{\mathfrak{p}}}$ and choose $\theta \in \mathscr{O}_{\mathbf{K}}^*$ the image of which in $\mathscr{O}_{\mathbf{K}}/\mathfrak{p}$ is a generator of that $\mathbf{F}_p$-extension, then consider the roots in $\mathbf{K}$ of the minimal polynomial of θ over $\mathbf{L}$).

(c) We assume that there exists $P \in \mathbf{Z}[T]$ such that reduction $\overline{P}$ of P in $\mathbf{F}_p[T]$ is separable and such that $\mathbf{K} = \mathbf{Q}_P$. Prove that $r_{\mathfrak{p}}$ is also injective.

3. Let $P \in \mathbf{Z}[T]$ be such that the reduction $\overline{P}$ of P in $\mathbf{F}_p[T]$ is separable. Choosing $\mathfrak{p}$, and using $r_{\mathfrak{p}}^{-1}$, we get a morphism $\mathscr{G}_{\overline{P}} \to \mathscr{G}_P$.

(a) Prove that we may choose a bijection from $\mathscr{E}_P$ to $\mathscr{E}_{\overline{P}}$ so that the diagram

$$\begin{array}{ccc} \mathscr{G}_{\overline{P}} & \longrightarrow & \mathscr{G}_P \\ \downarrow & & \downarrow \\ \mathfrak{S}_{\mathscr{E}_{\overline{P}}} & \longrightarrow & \mathfrak{S}_{\mathscr{E}_P} \end{array}$$

commutes.

(b) Let $\overline{P} = f_1 \dots f_r$ be the decomposition of $\overline{P}$ in irreducible factors. Prove that the image of $\mathscr{G}_P$ in $\mathfrak{S}_{\mathscr{E}_P}$ contains the product $\sigma_1 \dots \sigma_r$ of cycles σ_i of order $\deg(f_i)$ with disjoint supports.

Part III

Dedekind's criterion

1. We put $P = X^5 - X - 1$. For a prime number p, we denote by $\overline{P}_p$ the reduction of P modulo p.

(a) Decompose $\overline{P}_2$ in a product of irreducible polynomials.

(b) Prove that $\overline{P}_3$ is irreducible.

(c) Describe the Galois groupe $\mathscr{G}_P$. Can $P = 0$ be solved using radicals ?

2. Let $n > 2$ be an integer. Let σ_2, σ_{n-1} and σ_n be cycles in $\mathfrak{S}_n$ of order respectively 2, $n-1$ and n. Prove that $\{\sigma_2, \sigma_{n-1}, \sigma_n\}$ generates $\mathfrak{S}_n$.

3. Let $n > 2$ be an integer. Let $P \in \mathbf{Z}[X]$ be a polynomial of degree n and p_1, p_2, and p_3 be distinct prime numbers which do not divide the leading coefficient of P, Let P_1 (resp. P_2, P_3) be the reductions of P modulo p_1 (resp. p_2, p_3). We assume that P_1, P_2 and P_3 are separable, that P_1 is the product of a polynomial of degree 1 by an irreducible polynomial of degree $n-1$, that P_2 is the product of polynomial of degree 2 by irreducible polynomials of odd degree and that P_3 is irreducible.

(a) Prove that P is irreducible.

(b) Prove that $\mathscr{G}_P$ is isomorphic to the permutation group $\mathfrak{S}_n$.

Part IV

Van der Waerden's theorem

Let $n > 2$ be an integer. For any $N \in \mathbf{N}_{>0}$, we denote by $L_{n,N}$ the set of polynomials in $\mathbf{Z}[X]$ of degree n with coefficients in the interval $[-N, N]$ and by $N_{n,N}$ the set of separable $P \in L_{n,N}$ such that $\mathscr{G}_P$ is isomorphic to $\mathfrak{S}_n$. We want to prove that $\sharp N_{n,N}/\sharp L_{n,N}$ goes to 1 as N goes to infinity.

1. Compute $\sharp L_{n,N}$.

2. Let $m \geqslant 2$ be an integer and let $f \in \mathbf{Z}/m\mathbf{Z}[X]$ be a polynomial of degree n. Prove that the cardinal of the set of polynomials P in $L_{n,N}$ the reduction modulo m of which is f is bigger than

$$\left\lfloor \frac{2N}{m} \right\rfloor^{n+1}$$

where $\left\lfloor \frac{2N}{m} \right\rfloor$ is biggest integer less than $2N/m$.

3. Let p be an odd prime number.

(a) Prove that the number of $f \in \mathbf{F}_p[X]$ of degree n which may be written as a product $f_1 f_2$ of irreducible polynomials with $\deg(f_1) = 1$ is bigger than $p^{n+1}/(3n)$.

(b) If n is odd, prove that the number of $f \in \mathbf{F}_p[X]$ of degree n which may be written as a product $f_1 f_2$ of irreducible polynomials with $\deg(f_1) = 2$ is bigger than $p^{n+1}/(18n)$.

(c) If n is even, prove that the number of $f \in \mathbf{F}_p[X]$ of degree n which may be written as a product $f_1 f_2 f_3$ of irreducible polynomials with $\deg(f_1) = 2$, $\deg(f_2) = 1$ and f_2 not proportional to f_3 is bigger than $p^{n+1}/(18n)$ (Hint : Handle the case $n = 4$ as a particular case).

4. Let $p_1, \ldots, p_r$ be odd prime numbers and $M = p_1 \ldots p_r$. Let $k \in \mathbf{R}$ be such that $0 < k < 1/(18n)$. Prove that are at least

$$(1 - 3(1-k)^r) M^{n+1}$$

polynomials $f \in (\mathbf{Z}/M\mathbf{Z})[X]$ such that if $P \in \mathbf{Z}[X]$ reduces to f modulo M then P is irreducible and $\mathscr{G}_P$ is isomorphic to $\mathfrak{S}_n$.

5. Prove Van der Waerden's theorem.

Wednesday December 11, 2013

Algebraic Number Theory

Problem

Topology of varieties over complete fields

In this problem, $\mathbf{K}$ denotes a complete field for a nontrivial absolute value $|\cdot|$. If $|\cdot|$ is non archimedean, then $\mathfrak{O}$ denotes the ring

$$\mathfrak{O} = \{\, x \in \mathbf{K} \mid |x| \leqslant 1 \,\}$$

and $\mathfrak{m}$ the ideal

$$\mathfrak{m} = \{\, x \in \mathbf{K} \mid |x| < 1 \,\}.$$

Part I

Hensel's lemma

1. Let $f \in \mathfrak{O}[X]$ be such that $f' \neq 0$ and let S be the set of roots of f'. we define $g : \mathbf{K} - S \to \mathbf{K}$ by $x \mapsto x - f(x)/f'(x)$. We define

$$\mathscr{D} = \{\, x \in \mathfrak{O} \mid |f(x)| < |f'(x)|^2 \,\}$$

We fix $\alpha \in \mathscr{D}$.

(a) Prove that for any $x \in \mathfrak{O}$, we have $X^2 | f(x+X) - f(x) - Xf'(x)$ and $X | f'(x+X) - f'(x)$ in $\mathfrak{O}[X]$.

(b) Prove that for any $x \in \mathscr{D}$, one has $|f'(g(x))| = |f'(x)|$ and

$$\frac{|f(g(x))|}{|f'(g(x))^2|} \leqslant \left(\frac{|f(x)|}{|f'(x)^2|} \right)^2.$$

Prove the inclusion $g(\mathscr{D}) \subset \mathscr{D}$.

We define a sequence $(\alpha_n)_{n \in \mathbf{N}}$ of elements of $\mathscr{D}$ by the conditions $\alpha_0 = \alpha$ and $\alpha_{n+1} = g(\alpha_n)$ for $n \in \mathbf{N}$.

(c) We put $\lambda = |f(\alpha)|/|f'(\alpha)^2| < 1$. Prove that $|\alpha_{n+1} - \alpha_n| \leqslant \lambda^{2^n}$ and that the sequence $(\alpha_n)_{n \in \mathbf{N}}$ converges in $\mathfrak{O}$ to a root β of f.

(d) Prove that $|\alpha - \beta| \leqslant |f(\alpha)|/|f'(\alpha)|$

(e) Let $\beta' \neq \beta$ be another root of f. Prove that $|\beta' - \beta| \geqslant |f'(\alpha)|$.

2. Let p be a prime number and let $f \in \mathbf{Z}[X]$. let $n \in \mathbf{N}_{>0}$ and let $\alpha \in \mathbf{Z}$ be such that $f(\alpha) \equiv 0 \pmod{p^{2n+1}}$ and $f'(\alpha)$ is not divisible by p^{n+1}. Prove

that there exists a *unique* root β of f in the p-adic ring $\mathbf{Z}_p$ such that $\beta \equiv \alpha \pmod{p^{n+1}}$.

Part II

Theorem of implicit functions

From now on we assume that $\mathbf{K}$ is *locally compact*. For any integer $n \in \mathbf{N}$, the vector space $\mathbf{K}^n$ is equipped with the product topology. Let $f \in \mathbf{K}[X_1, \ldots, X_n]$. We define

$$V(f) = \{\, \boldsymbol{x} \in \mathbf{K}^n \mid f(\boldsymbol{x}) = 0 \,\}.$$

We remind you that $V(f)$ is said to be smooth at $\boldsymbol{x} \in V(f)$ if and only if it satisfies the following condition

$$d_{\boldsymbol{x}} f = \sum_{i=1}^{n} \frac{\partial f}{\partial X_i}(\boldsymbol{x}) dX_i \neq 0.$$

From now on, we assume that $V(f)$ is smooth at $\boldsymbol{x} = (x_1, \ldots, x_n) \in V(f)$.

1. Prove that there exist $i \in \{1, \ldots, n\}$ and a neighbourhood W of $\boldsymbol{x}$ in $\mathbf{K}^n$ such that $\frac{\partial f}{\partial X_i}(\boldsymbol{y}) \neq 0$ for any $\boldsymbol{y} \in W$.

We denote by $\pi : V(f) \to \mathbf{K}^{n-1}$ the projection mapping $(y_1, \ldots, y_n)$ onto $(y_1, \ldots, y_{i-1}, y_{i+1}, \ldots, y_n)$.

2. If $\mathbf{K}$ is archimedean, what does the theorem of implicit functions say about π in a neighbourhood of $\boldsymbol{x}$ in $V(f)$?

We now assume that $\mathbf{K}$ is non-archimedean. Let $\varpi \in \mathbf{K}$ be such that $|\varpi| < 1$.

3. Prove that there is integers a and b such that

$$g(X_1, \ldots X_n) = \varpi^a f(x_1 + X_1, \ldots x_n + X_n)$$

satisfies

(i) $g \in \mathfrak{O}[X_1, \ldots, X_n]$;

(ii) $|g(\boldsymbol{y})| < \left|\frac{\partial g}{\partial X_i}(\boldsymbol{y})\right|^2$ for all $\boldsymbol{y} \in (\varpi^b)^n$.

(Look for a to satisfy (i) and then adjust b).

4. (a) Let $V(g) = \{\, \boldsymbol{y} \in \mathbf{K}^n \mid g(\boldsymbol{y}) = 0 \,\}$. Prove that π restricted to $V(g) \cap (\varpi^b)^n$ is surjective.

(b) Prove that there is a compact neighbourhood K of 0 such that the restriction of π to $V(g) \cap K$ defines a homeomorphism.

(c) Prove that there is a neighbourhood K' of $\boldsymbol{x}$ such that π restricted to $V(f) \cap K'$ defines a homeomorphism.

Épreuve du Mercredi 6 novembre 2013

Théorie algébrique des nombres

Durée : 3 heures

La clarté, la concision et la précision des réponses données seront des facteurs importants d'appréciation des copies. On justifiera chaque réponse donnée.

Problème 1

Extensions quadratiques réelles

Soit $D \in \mathbf{N} - \{0, 1\}$ un entier sans facteur carré (autrement dit, D n'est pas divisible par le carré d'un nombre premier). On pose $\mathbf{K} = \mathbf{Q}(\sqrt{D}) \subset \mathbf{R}$.

Partie I

Anneau des entiers

1. (a) Démontrer que l'extension $\mathbf{K}/\mathbf{Q}$ est galoisienne. Donner une base du $\mathbf{Q}$-espace vectoriel $\mathbf{K}$ et décrire le groupe de Galois $\mathrm{Gal}(\mathbf{K}/\mathbf{Q})$.

(b) Déterminer $\mathrm{Tr}_{\mathbf{K}/\mathbf{Q}}(x + y\sqrt{D})$ et $N_{\mathbf{K}/\mathbf{Q}}(x + y\sqrt{D})$ pour $x, y \in \mathbf{Q}$.

2. On pose

$$\omega_D = \begin{cases} \frac{1+\sqrt{D}}{2} \text{ si } D \equiv 1 \text{ modulo } 4, \\ \sqrt{D} \text{ sinon.} \end{cases}$$

Démontrer que l'anneau des entiers de $\mathbf{K}$ est donné par

$$\mathscr{O}_{\mathbf{K}} = \mathbf{Z} + \mathbf{Z}\omega_D.$$

Partie II

Unités

1. Soit $z \in \mathscr{O}_{\mathbf{K}}$. Prouver que z est inversible dans $\mathscr{O}_{\mathbf{K}}$ si et seulement si $N_{\mathbf{K}/\mathbf{Q}}(z) \in \{-1, 1\}$.

On définit

$$\begin{array}{rccc} \varphi : & \mathscr{O}_{\mathbf{K}}^* & \longrightarrow & \mathbf{R} \\ & z & \longmapsto & \log|z|. \end{array}$$

2. (a) Prouver que φ est un morphisme de groupes.

T.S.V.P

(b) Déterminer le noyau de φ.

(c) Démontrer que pour tout nombre réel B, l'ensemble

$$\{\, z \in \mathscr{O}_{\mathbf{K}}^* \mid\ |\varphi(z)| \leqslant B \,\}$$

est fini (on pourra écrire $z = x + y\sqrt{D}$ avec $x, y \in \mathbf{Z}\frac{1}{2}$, écrire $N_{\mathbf{K}/\mathbf{Q}}(z)$ comme un produit et chercher une majoration de $|x|$).

(d) Démontrer que le groupe $\mathrm{Im}(\varphi)$ est engendré par l'un de ses éléments.

Partie III

Équation de Pell

1. On note $\lfloor x \rfloor$ la partie entière d'un nombre réel x et $\{x\} = x - \lfloor x \rfloor \in [0, 1[$ sa partie fractionnaire.

(a) Soient $\xi \in \mathbf{R}$ et N un entier strictement positif. Prouver qu'il existe des entiers j et k tels que $0 \leqslant j < k \leqslant N$ et $|\{k\xi\} - \{j\xi\}| < 1/N$ (on pourra éventuellement considérer l'application sur $\{0, \ldots, N\}$ définie par $k \mapsto \lfloor N\{k\xi\} \rfloor$).

(b) En déduire que pour tout $\xi \in \mathbf{R}$ et tout entier strictement positif N, il existe des entiers $p, q \in \mathbf{Z}$ avec $0 < q \leqslant N$ tels que $\mathrm{pgcd}(p, q) = 1$ et

$$\left| \xi - \frac{p}{q} \right| < \frac{1}{Nq}.$$

2. Soit $\xi \in \mathbf{R} - \mathbf{Q}$. Prouver qu'il existe une infinité de $(p, q) \in \mathbf{Z} \times (\mathbf{Z} - \{0\})$ tels que

$$\mathrm{pgcd}(p, q) = 1 \quad \text{et} \quad \left| \frac{p}{q} - \xi \right| < \frac{1}{q^2}.$$

3. (a) En appliquant la question précédente à $\sqrt{D}$, prouver que si $M = 1 + 2\sqrt{D}$, l'ensemble

$$\{\, (x, y) \in \mathbf{Z}^2 \mid\ |x^2 - Dy^2| \leqslant M, \mathrm{pgcd}(x, y) = 1 \,\}$$

est infini.

(b) Prouver qu'il existe $m, x_0, y_0 \in \mathbf{Z}$ avec $m \neq 0$ tels que l'ensemble des couples $(x, y) \in \mathbf{Z}^2$ vérifiant les conditions $\mathrm{pgcd}(x, y) = 1$, $x > 0$, $y > 0$, $x^2 - Dy^2 = m$, $x \equiv x_0\ (m)$ et $y \equiv y_0\ (m)$ soit infini.

(c) En déduire qu'il existe des entiers $x_1, y_1, x_2, y_2 \in \mathbf{Z}$ tels que $\mathrm{pgcd}(x_1, y_1) = \mathrm{pgcd}(x_2, y_2) = 1$, $x_1 \neq x_2$, $x_1 \neq -x_2$, $x_1 \equiv x_2\ (m)$, $y_1 \equiv y_2\ (m)$ et

$$x_1^2 - Dy_1^2 = x_2^2 - Dy_2^2 = m.$$

(d) En considérant $(x_1 + y_1\sqrt{D})(x_2 - y_2\sqrt{D})$, prouver qu'il existe $z \in \mathscr{O}_{\mathbf{K}}^*$ tel que $z \in \mathbf{Z} + \mathbf{Z}\sqrt{D}$ et $z \notin \{-1, 1\}$.

4. (a) Démontrer que l'équation

$$x^2 - Dy^2 = 1$$

a une infinité de solutions dans $\mathbf{Z}^2$.

(b) Démontrer qu'il existe $(x_0, y_0) \in \mathbf{Z}^2$ avec $x_0^2 - Dy_0^2 = 1$ tel que, pour toute solution $(x, y) \in \mathbf{Z}^2$ de l'équation $x^2 - Dy^2 = 1$, il existe $\varepsilon \in \{-1, 1\}$ et $m \in \mathbf{Z}$ tels que

$$x + y\sqrt{D} = \varepsilon(x_0 + y_0\sqrt{D})^m.$$

Problème 2

Une extension cyclotomique

Soit p un nombre premier impair. On pose $\zeta = e^{\frac{2\pi i}{p}}$ et $\mathbf{K} = \mathbf{Q}(\zeta)$. On rappelle que l'extension $\mathbf{K}/\mathbf{Q}$ est galoisienne de degré $p-1$ et que $(\mathbf{Z}/p\mathbf{Z})^*$ est isomorphe au groupe de Galois $\mathrm{Gal}(\mathbf{K}/\mathbf{Q})$. On note $\varpi = \zeta - 1$.

1. Déterminer le polynôme minimal de ζ sur $\mathbf{Q}$.

2. (a) Démontrer que $\mathbf{Z}[\zeta] \subset \mathscr{O}_{\mathbf{K}}$ et que $\mathbf{Z}[\zeta]^* \subset \mathscr{O}_{\mathbf{K}}^*$.

(b) Démontrer que $(1, \zeta, \ldots, \zeta^{p-2})$ est une base du $\mathbf{Z}$-module $\mathbf{Z}[\zeta]$.

(c) Démontrer que $(1, \varpi, \ldots, \varpi^{p-2})$ est une base du $\mathbf{Z}$-module $\mathbf{Z}[\zeta]$ (on pourra considérer la matrice de changement de base).

(d) Démontrer que $\mathbf{Z}[\zeta]$ est stable sous l'action de $\mathrm{Gal}(\mathbf{K}/\mathbf{Q})$.

(e) Calculer $\mathrm{Tr}_{\mathbf{K}/\mathbf{Q}}(\sum_{i=0}^{p-2} a_i\zeta^i)$ pour $(a_0, \ldots, a_{p-2}) \in \mathbf{Q}^{p-1}$.

3. (a) Démontrer que $\boldsymbol{\mu}_{\varpi}^{\mathbf{Q}}(X) = \boldsymbol{\mu}_{\zeta}^{\mathbf{Q}}(X + 1)$.

(b) Calculer $N_{\mathbf{K}/\mathbf{Q}}(\varpi)$.

(c) Démontrer que, pour $i \in \{1, \ldots, p-1\}$, ϖ divise $\zeta^i - 1$ dans $\mathbf{Z}[\zeta]$ et calculer $N_{\mathbf{K}/\mathbf{Q}}(\frac{\zeta^i - 1}{\zeta - 1})$.

(d) En déduire que pour tout $\sigma \in \mathrm{Gal}(\mathbf{K}/\mathbf{Q})$, $\sigma(\varpi)/\varpi \in \mathbf{Z}[\zeta]^*$.

(e) Démontrer qu'il existe $u \in \mathbf{Z}[\zeta]^*$ tel que $p = u\varpi^{p-1}$.

(f) Soit $n \in \mathbf{Z}$. Démontrer que ϖ divise n dans $\mathscr{O}_{\mathbf{K}}$ si seulement si n est un multiple de p (on pourra utiliser la norme).

(g) Démontrer que l'injection canonique $\mathbf{Z} \to \mathbf{Z}[\zeta]$ induit un isomorphisme d'anneaux

$$\mathbf{Z}/p\mathbf{Z} \longrightarrow \mathbf{Z}[\zeta]/\varpi\mathbf{Z}[\zeta].$$

(On pourra utiliser la question **2.(c)**). Que peut-on en déduire concernant l'idéal (ϖ) de $\mathbf{Z}[\zeta]$?

4. Soit $x \in \mathscr{O}_{\mathbf{K}}$ et soit $(a_0, \ldots, a_{p-2}) \in \mathbf{Q}^{p-1}$ tels que $x = \sum_{i=0}^{p-2} a_i\zeta^i$.

(a) Calculer $\mathrm{Tr}_{\mathbf{K}/\mathbf{Q}}((1-\zeta)x)$.

(b) Démontrer que $pa_0 \in \mathbf{Z}$.

(c) Démontrer que $pa_i \in \mathbf{Z}$ pour $i \in \{1, \ldots, p-2\}$.

(d) Démontrer qu'il existe $(b_0, \ldots, b_{p-2}) \in \mathbf{Z}^{p-1}$ tel que

$$px = \sum_{i=0}^{p-2} b_i \varpi^{p-2}.$$

(e) Démontrer que p divise b_0.

5. Démontrer que $\mathscr{O}_{\mathbf{K}} = \mathbf{Z}[\zeta]$.

6. Quel est le degré de ramification de (ϖ) au-dessus de $\mathbf{Z}$?

Exam, Wednesday, november 6 2013

Algebraic number theory

Duration : 3 hours

Any answer has to be justified. The concision, clarity and precision of the proofs are taken into account during the grading.

Problem 1

Real quadratic extensions

Let $D \in \mathbf{N} - \{0,1\}$ be a squarefree integer (that is D is not divisible by the square of a prime number). Let $\mathbf{K} = \mathbf{Q}(\sqrt{D}) \subset \mathbf{R}$.

Part I

Ring of integers

1. (a) Prove that the extension $\mathbf{K}/\mathbf{Q}$ is Galois. Give a basis of the $\mathbf{Q}$-vector space $\mathbf{K}$ and describe explicitely the Galois group $\mathrm{Gal}(\mathbf{K}/\mathbf{Q})$.

(b) Compute $\mathrm{Tr}_{\mathbf{K}/\mathbf{Q}}(x + y\sqrt{D})$ et $N_{\mathbf{K}/\mathbf{Q}}(x + y\sqrt{D})$ for $x, y \in \mathbf{Q}$.

2. Let

$$\omega_D = \begin{cases} \frac{1+\sqrt{D}}{2} \text{ if } D \equiv 1 \text{ modulo } 4, \\ \sqrt{D} \text{ otherwise.} \end{cases}$$

Prove that the ring of integers of $\mathbf{K}$ is given by

$$\mathscr{O}_{\mathbf{K}} = \mathbf{Z} + \mathbf{Z}\omega_D.$$

Part II

Units

1. Let $z \in \mathscr{O}_{\mathbf{K}}$. Prove that z is invertible in $\mathscr{O}_{\mathbf{K}}$ if and only if $N_{\mathbf{K}/\mathbf{Q}}(z) \in \{-1, 1\}$.

We define

$$\begin{array}{rccc} \varphi : & \mathscr{O}_{\mathbf{K}}^* & \longrightarrow & \mathbf{R} \\ & z & \longmapsto & \log|z|. \end{array}$$

2. (a) Prove that φ is a homomorphism of groups.

(b) What is the kernel of φ ?

(c) Prove that for any real number B, the set

$$\{\, z \in \mathscr{O}_{\mathbf{K}}^{*} \mid \ |\varphi(z)| \leqslant B \,\}$$

is finite (one may write $z = x + y\sqrt{D}$ with $x, y \in \mathbf{Z}\frac{1}{2}$, then write $N_{\mathbf{K}/\mathbf{Q}}(z)$ as a product and find an upper bound for $|x|$).

(d) Prove that the group $\mathrm{Im}(\varphi)$ is generated by one of its elements.

Part III

Pell Equation

1. For any $x \in \mathbf{R}$, let $\lfloor x \rfloor \in \mathbf{Z}$ be the biggest integer less or equal to x, and $\{x\} = x - \lfloor x \rfloor \in [0, 1[$.

(a) Let $\xi \in \mathbf{R}$ and let N be a strictly positive integer. Prove that there exist integers j and k such that $0 \leqslant j < k \leqslant N$ and $|\{k\xi\} - \{j\xi\}| < 1/N$ (one may consider the map on $\{0, \ldots, N\}$ defined by $k \mapsto \lfloor N\{k\xi\} \rfloor$).

(b) Prove that for any $\xi \in \mathbf{R}$ and any strictly positive integer N, there exist integers $p, q \in \mathbf{Z}$ with $0 < q \leqslant N$ such that $\mathrm{pgcd}(p, q) = 1$ and

$$\left| \xi - \frac{p}{q} \right| < \frac{1}{Nq}.$$

2. Let $\xi \in \mathbf{R}\text{—}\mathbf{Q}$. Prove that there exist infinitely many $(p, q) \in \mathbf{Z} \times (\mathbf{Z}\text{—}\{0\})$ such that

$$\mathrm{pgcd}(p, q) = 1 \quad \text{et} \quad \left| \frac{p}{q} - \xi \right| < \frac{1}{q^2}.$$

3. (a) Apply to $\sqrt{D}$, prove that if $M = 1 + 2\sqrt{D}$, the set

$$\{\, (x, y) \in \mathbf{Z}^2 \mid \ |x^2 - Dy^2| \leqslant M, \mathrm{pgcd}(x, y) = 1 \,\}$$

is infinite.

(b) Prove that there exist $m, x_0, y_0 \in \mathbf{Z}$ with $m \neq 0$ such that the set of $(x, y) \in \mathbf{Z}^2$ which satisfy the conditions $\mathrm{pgcd}(x, y) = 1$, $x > 0$, $y > 0$, $x^2 - Dy^2 = m$, $x \equiv x_0 \ (m)$ et $y \equiv y_0 \ (m)$ is infinite.

(c) Prove that there exist integers $x_1, y_1, x_2, y_2 \in \mathbf{Z}$ such that $\mathrm{pgcd}(x_1, y_1) = \mathrm{pgcd}(x_2, y_2) = 1$, $x_1 \neq x_2$, $x_1 \neq -x_2$, $x_1 \equiv x_2 \ (m)$, $y_1 \equiv y_2 \ (m)$ and

$$x_1^2 - Dy_1^2 = x_2^2 - Dy_2^2 = m.$$

(d) Consider the product $(x_1 + y_1\sqrt{D})(x_2 - y_2\sqrt{D})$, and prove that there exists $z \in \mathscr{O}_{\mathbf{K}}^{*}$ such that $z \in \mathbf{Z} + \mathbf{Z}\sqrt{D}$ and $z \notin \{-1, 1\}$.

4. (a) Prove that the equation

$$x^2 - Dy^2 = 1$$

has infinitely many solutions in $\mathbf{Z}^2$.

(b) Prove that there exists $(x_0, y_0) \in \mathbf{Z}^2$ with $x_0^2 - Dy_0^2 = 1$ so that, for any solution $(x, y) \in \mathbf{Z}^2$ of the equation $x^2 - Dy^2 = 1$, there exist $\varepsilon \in \{-1, 1\}$ and $m \in \mathbf{Z}$ such that

$$x + y\sqrt{D} = \varepsilon(x_0 + y_0\sqrt{D})^m.$$

Problem 2

A cyclotomic extension

Let p be an odd prime number. We put $\zeta = e^{\frac{2\pi i}{p}}$ and $\mathbf{K} = \mathbf{Q}(\zeta)$. We remind you that $\mathbf{K}/\mathbf{Q}$ is a Galois extension of degree $p-1$ and that $(\mathbf{Z}/p\mathbf{Z})^*$ is isomorphic to the Galois group $\mathrm{Gal}(\mathbf{K}/\mathbf{Q})$. Let $\varpi = \zeta - 1$.

1. Find the minimal polynomial of ζ over $\mathbf{Q}$.

2. (a) Prove that $\mathbf{Z}[\zeta] \subset \mathscr{O}_{\mathbf{K}}$ and that $\mathbf{Z}[\zeta]^* \subset \mathscr{O}_{\mathbf{K}}^*$.

(b) Prove that $(1, \zeta, \ldots, \zeta^{p-2})$ is a basis of the $\mathbf{Z}$-module $\mathbf{Z}[\zeta]$.

(c) Prove that $(1, \varpi, \ldots, \varpi^{p-2})$ is a basis of the $\mathbf{Z}$-module $\mathbf{Z}[\zeta]$ (you may consider the matrix for the change of bases).

(d) Prove that $\mathbf{Z}[\zeta]$ is stable under the action of $\mathrm{Gal}(\mathbf{K}/\mathbf{Q})$.

(e) Compute $\mathrm{Tr}_{\mathbf{K}/\mathbf{Q}}(\sum_{i=0}^{p-2} a_i\zeta^i)$ for $(a_0, \ldots, a_{p-2}) \in \mathbf{Q}^{p-1}$.

3. (a) Prove that $\boldsymbol{\mu}_{\varpi}^{\mathbf{Q}}(X) = \boldsymbol{\mu}_{\zeta}^{\mathbf{Q}}(X+1)$.

(b) Compute $N_{\mathbf{K}/\mathbf{Q}}(\varpi)$.

(c) Prove that, for $i \in \{1, \ldots, p-1\}$, ϖ divides $\zeta^i - 1$ in $\mathbf{Z}[\zeta]$ and compute $N_{\mathbf{K}/\mathbf{Q}}(\frac{\zeta^i - 1}{\zeta - 1})$.

(d) Prove that for any $\sigma \in \mathrm{Gal}(\mathbf{K}/\mathbf{Q})$, $\sigma(\varpi)/\varpi \in \mathbf{Z}[\zeta]^*$.

(e) Prove that there exists $u \in \mathbf{Z}[\zeta]^*$ such that $p = u\varpi^{p-1}$.

(f) Let $n \in \mathbf{Z}$. Prove that ϖ divides n in $\mathscr{O}_{\mathbf{K}}$ if and only if n is a multiple of p (you may use the norm map).

(g) Prove that the canonical injective morphism $\mathbf{Z} \to \mathbf{Z}[\zeta]$ induces an isomorphism of rings

$$\mathbf{Z}/p\mathbf{Z} \longrightarrow \mathbf{Z}[\zeta]/\varpi\mathbf{Z}[\zeta].$$

(You may use question **2.(c)**). What can we deduce from that about the ideal (ϖ) of $\mathbf{Z}[\zeta]$?

4. Let $x \in \mathscr{O}_{\mathbf{K}}$ and let $(a_0, \ldots, a_{p-2}) \in \mathbf{Q}^{p-1}$ be such that $x = \sum_{i=0}^{p-2} a_i \zeta^i$.

(a) Compute $\mathrm{Tr}_{\mathbf{K}/\mathbf{Q}}((1-\zeta)x)$.

(b) Prove that $pa_0 \in \mathbf{Z}$.

(c) Prove that $pa_i \in \mathbf{Z}$ for $i \in \{1, \ldots, p-2\}$.

(d) Prove that there exists $(b_0, \ldots, b_{p-2}) \in \mathbf{Z}^{p-1}$ such that

$$px = \sum_{i=0}^{p-2} b_i \varpi^{p-2}.$$

(e) Prove that p divides b_0.

5. Prove that $\mathscr{O}_{\mathbf{K}} = \mathbf{Z}[\zeta]$.

6. What is the ramification index of (ϖ) over $\mathbf{Z}$?

Answers to the exam of Wednesday, november 6 2013
Algebraic number theory

Problem 1

Part I

1. (a) As $\mathrm{Char}(\mathbf{Q}) = 0$, the extension $\mathbf{K}/\mathbf{Q}$ is separable and, since it is a splitting field for $X^2 - D$, it is normal and therefore Galois.

Since $D > 1$ is squarefree, it is not a square in $\mathbf{Z}$. As $\mathbf{Z}$ is integrally closed, D is not a square in $\mathbf{Q}$. Therefore the family $(1, \sqrt{D})$ is free and, since $[\mathbf{K} : \mathbf{Q}] = 2$, is a basis of $\mathbf{K}$ over $\mathbf{Q}$.

The Galois group $\mathrm{Gal}(\mathbf{K}/\mathbf{Q})$ has cardinal 2. Let σ be its nontrivial element. We have $\sigma(\sqrt{D}) \in \{\sqrt{D}, -\sqrt{D}\}$ and $\sigma(\sqrt{D}) \neq \sqrt{D}$, since $\sigma \neq \mathrm{Id}_{\mathbf{K}}$. Therefore $\sigma(x + y\sqrt{D}) = x - y\sqrt{D}$ for $x, y \in \mathbf{Q}$.

(b) We have

$$\mathrm{Tr}_{\mathbf{K}/\mathbf{Q}}(x + y\sqrt{D}) = x + y\sqrt{D} + \sigma(x + y\sqrt{D}) = 2x,$$

and

$$N_{\mathbf{K}/\mathbf{Q}}(x + y\sqrt{D}) = (x + y\sqrt{D})(x - y\sqrt{D}) = x^2 - y^2 D$$

for $x, y \in \mathbf{Q}$.

2. Since $\sqrt{D}$ is integral over $\mathbf{Z}$, we have the inclusion $\mathbf{Z} + \mathbf{Z}\sqrt{D} \subset \mathscr{O}_{\mathbf{K}}$.

Let $z = x + y\sqrt{D} \in \mathscr{O}_{\mathbf{K}}$ with $x, y \in \mathbf{Q}$. Then $2x \in \mathbf{Z}$. Write $y = p/q$ with $\gcd(p, q) = 1$ and $q > 0$.

Assume that $x = k + 1/2$ with $k \in \mathbf{Z}$. Using $x^2 - Dy^2 \in \mathbf{Z}$, we get that $1/4 - Dy^2 \in \mathbf{Z}$ and $4q^2 | q^2 - 4Dp^2$. This implies that $4 | q^2$ and $q^2 | 4Dp^2$. Therefore $2 | q | 2$ and $q = 2$.

If $x \in \mathbf{Z}$, then, from $q^2 | Dp^2$, it follows that $q = 1$ and $y \in \mathbf{Z}$.

Therefore $z \in \mathbf{Z} + \mathbf{Z}\sqrt{D}$ or $z - \frac{1+\sqrt{D}}{2} \in \mathbf{Z} + \mathbf{Z}\sqrt{D}$. This proves that the group $\mathscr{O}_{\mathbf{K}}/(\mathbf{Z} + \mathbf{Z}\sqrt{D})$ has order either 1 or 2, and that the later case occurs only if $\frac{1+\sqrt{D}}{2} \in \mathscr{O}_{\mathbf{K}}$, which is equivalent to $N_{\mathbf{K}/\mathbf{Q}}(1 + \sqrt{D}) = (1 - D)/4 \in \mathbf{Z}$, that is $4 | D - 1$. In all cases, we get $\mathscr{O}_{\mathbf{K}} = \mathbf{Z} + \mathbf{Z}\omega_D$.

Part II

1. If $z, z' \in \mathscr{O}_{\mathbf{K}}$ satisfy $zz' = 1$, then $N_{\mathbf{K}/\mathbf{Q}}(z)N_{\mathbf{K}/\mathbf{Q}}(z') = 1$, $N_{\mathbf{K}/\mathbf{Q}}(z)$ is invertible in $\mathbf{Z}$ and therefore $N_{\mathbf{K}/\mathbf{Q}}(z) \in \{-1, 1\}$. Conversely, if $N_{\mathbf{K}/\mathbf{Q}}(z)^2 = 1$, then $z \times (z\sigma(z)^2) = 1$ and z is invertible in $\mathscr{O}_{\mathbf{K}}$.

2. (a) The formulae

$$\varphi(zz') = \log(|zz'|) = \log(|z|) + \log(|z'|) = \varphi(z) + \varphi(z')$$

for $z, z' \in \mathscr{O}_{\mathbf{K}}^*$ prove that φ is a morphism of groups.

(b) We have $\mathbf{K} \subset \mathbf{R}$. Let $z \in \mathscr{O}_{\mathbf{K}}^*$. We have $\varphi(z) = 0$ if and only if $|z| = 1$, that is $z \in \{-1, 1\}$. So $\mathrm{Ker}(\varphi) = \{-1, 1\}$

(c) Let $z = x + y\sqrt{D} \in \mathscr{O}_{\mathbf{K}}^*$ with $x, y \in \mathbf{Q}$. By question I.2, $x, y \in \mathbf{Z}\frac{1}{2}$. Since $z \in \mathscr{O}_{\mathbf{K}}^*$, $(x + y\sqrt{D})(x - y\sqrt{D}) = 1$. Thus

$$|x - y\sqrt{D}| = \frac{1}{|x + y\sqrt{D}|}$$

La condition $|\varphi(z)| \leqslant B$, which is equivalent to

$$\exp(-B) \leqslant |z| \leqslant \exp(B) \tag{1}$$

implies

$$exp(-B) \leqslant |x - \sqrt{D}| \leqslant \exp(B)$$

and therefore $|x| \leqslant \exp(B)$. There is only a finite number of possible values for x and using (1) for y. The set

$$\{\, z \in \mathscr{O}_{\mathbf{K}}^* \mid |\varphi(z)| \leqslant B \,\}$$

is finite.

(d) The result is true if $\mathrm{Im}(\varphi) = \{0\}$. Otherwise let $\alpha \in \mathrm{Im}(\varphi) - \{0\}$. Since $\mathrm{Im}(\varphi)$ is a subgroup of $\mathbf{R}$, $|\alpha|$ belongs to $\mathrm{Im}(\varphi)$ and by the previous question the intersection $\mathrm{Im}(\varphi) \cap]0, |\alpha|]$ is finite and not empty. Thus $\mathrm{Im}(\varphi) \cap \mathbf{R}_{>0}$ has a smallest element α_0. Let $\beta \in \mathrm{Im}(\varphi)$, we may write

$$\beta = \left\lfloor \frac{\beta}{\alpha_0} \right\rfloor + \left\{ \frac{\beta}{\alpha_0} \right\} \alpha_0.$$

We get $\left\{ \frac{\beta}{\alpha_0} \right\} \alpha_0 \in [0, \alpha_0[\cap \mathrm{Im}(\varphi)$. This element is equal to 0 so $\beta \in \mathbf{Z}\alpha_0$. (One could also directly use the fact that a discrete subgroup of $\mathbf{R}$ is generated by one of its elements).

Part III

1. (a) The map $k \mapsto \lfloor N\{k\xi\}\rfloor$ takes its values in $\{0,\dots,N-1\}$. Since $\mathrm{Card}\{0,\dots N\} > \mathrm{Card}\{0,\dots,N-1\}$, this map is not injective, and there exists $0 \leqslant j < k \leqslant N$ and $m \in \{0,\dots,N-1\}$ such that

$$m \leqslant N\{j\xi\} < m+1 \qquad \text{and} \qquad m \leqslant N\{k\xi\} < m+1$$

Therefore $-1 < N(\{j\xi\} - \{k\xi\}) < 1$ and $|\{j\xi\} - \{k\xi\}| < 1/N$.

(b) With the notations of **(a)**, we put $m = \lfloor j\xi\rfloor$ and $n = \lfloor k\xi\rfloor$ then

$$|j\xi - m - k\xi + n| < 1/N$$

and, since $j < k$

$$\left|\xi - \frac{n-m}{k-j}\right| < \frac{1}{N(k-j)}.$$

We put $p = (n-m)/\gcd(m-n, k-j)$ and $q = (k-j)/\gcd(m-n,k-j) \leqslant N$. we have $\gcd(p,q) = 1$ and $|\xi - \frac{p}{q}| < \frac{1}{Nq}$.

2. Let us assume that there is a finite number of such (p,q). By question **1.(b)**, there exist such a pair, so we can choose $p, q \in \mathbf{Z}$, $q > 0$, $\gcd(p,q) = 1$ and $|\xi - p/q|$ minimal. Since $\xi \notin \mathbf{Q}$, this difference is not zero. Let $N > 1/|\xi - p/q|$. By **1.(b)**, we can find p', q' with $q' > 0$, $\gcd(p',q') = 1$ and $\left|\xi - \frac{p'}{q'}\right| < \frac{1}{Nq'}$. But $\frac{1}{Nq'} \leqslant \frac{1}{q'^2}$ and $\frac{1}{Nq'} < \left|\xi - \frac{p}{q}\right|$ and we get a contradiction.

3. (a) If $\left|\frac{p}{q} - \sqrt{D}\right| \leqslant \frac{1}{q^2}$, then $|p - q\sqrt{D}| \leqslant \frac{1}{q}$, which implies

$$|p^2 - q^2 D| \leqslant \left|\frac{p}{q} + \sqrt{D}\right| \leqslant \left|\frac{p}{q}\right| + \sqrt{D} \leqslant 2\sqrt{D} + \left|\frac{p}{q} - \sqrt{D}\right| \leqslant 2\sqrt{D} + 1.$$

the result then follows from question **2**.

(b) The only solution in $\mathbf{Z}^2$ of the equation $x^2 - y^2 D = 0$ is $(0,0)$, and

$$\{\,(x,y) \in \mathbf{Z}^2 |\, |x^2 - Dy^2| \leqslant M, \gcd(x,y) = 1\,\} = \bigcup_{m=-\lfloor M\rfloor}^{\lfloor M\rfloor} \{\,(x,y) \in \mathbf{Z}^2 |\, x^2 - Dy^2 = m, \gcd(x,y) = 1\,\}.$$

So there exists $m \neq 0$ such that $\{\,(x,y) \in \mathbf{Z}^2 |\, |x^2 - Dy^2| = m, \gcd(x,y) = 1\,\}$ is infinite. Taking into account the cases where $x = 0$ or $y = 0$, the cardinal of this set is less or equal to

$$4\,\mathrm{Card}(\{\,(x,y) \in \mathbf{Z}^2_{>0} |\, x^2 - Dy^2 = m, \gcd(x,y) = 1\,\}) + 2.$$

Therefore the cardinal of this last set is infinite as well. But we may describe it as

$$\bigcup_{(a,b)\in(\mathbf{Z}/m\mathbf{Z})^2} \{\,(x,y) \in \mathbf{Z}^2_{>0} \mid x^2 - Dy^2 = m,\ \gcd(x,y) = 1,\ x \equiv a\,(m) \text{ and } y \equiv b\,(m)\,\}$$

and one of these sets has to be infinite.

(c) Since an infinite set has two distinct elements, we may choose distinct elements (x_1, y_1) and (x_2, y_2) in the set of question **(b)**. They satisfy the requested conditions.

(d) Write

$$(x_1 + y_1\sqrt{D})(x_2 - y_2\sqrt{D}) = (x_1x_2 - y_1y_2D) + (x_2y_1 - x_1y_2)\sqrt{D}$$

in $\mathbf{Z} + \mathbf{Z}\sqrt{D}$. But $x_1x_2 - y_1y_2D \equiv x_1^2 - y_1^2D \equiv 0\ (m)$ and $x_2y_1 - x_1y_2 \equiv 0\ (m)$. Therefore $(x_1 + y_1\sqrt{D})(x_2 - y_2\sqrt{D}) = mz$ for some $z \in \mathbf{Z} + \mathbf{Z}\sqrt{D}$. We have $m^2 N_{\mathbf{K/Q}}(z) = N_{\mathbf{K/Q}}(mz) = N_{\mathbf{K/Q}}(x_1 + y_1\sqrt{D})N_{\mathbf{K/Q}}(x_2 - y_2\sqrt{D}) = m^2$. This $N_{\mathbf{K/Q}}(z) = 1$ and z is invertible in $\mathscr{O}_{\mathbf{K}}^*$. Since $\gcd(x_1, y_1) = \gcd(x_2, y_2) = 1$, $x_1y_2 - x_2y_1 = 0$ would imply $x_1|x_2|x_1$ which is not possible since $x_1 \neq x_2$ and $x_1 \neq -x_2$. Therefore $z \notin \{-1, 1\}$.

4. (a) Let N be the restriction of $N_{\mathbf{K/Q}}$ to $\mathbf{K}^*$. There is a bijection from the set of solutions to $\mathrm{Ker}(N) \cap (\mathbf{Z} + \mathbf{Z}\sqrt{D})$. Since $\sigma(\mathbf{Z} + \mathbf{Z}\sqrt{D}) \subset \mathbf{Z} + \mathbf{Z}\sqrt{D}$ and the inverse of an element $z \in \mathrm{Ker}(N)$ is $\sigma(z)$, $\mathrm{Ker}(N) \cap (\mathbf{Z} + \mathbf{Z}\sqrt{D})$ is a subgroup of $\mathscr{O}_{\mathbf{K}}^*$. By **3.(d)**, we may choose $z \in (\mathbf{Z} + \sqrt{D}\mathbf{Z}) \cap \mathscr{O}_{\mathbf{K}}^*$ with $\varphi(z) \neq 0$. For any $n \in \mathbf{N}_{>0}$, $z^{2n} \in \mathrm{Ker}(N) \cap (\mathbf{Z} + \mathbf{Z}\sqrt{D})$ and $\varphi(z^{2n}) = 2n\varphi(z)$. So the map $n \mapsto \varphi(z^{2n})$ is injective and the equation has infinitely many solutions.

(b) As in question **II.2.(d)**, $\varphi(\mathrm{Ker}(N) \cap (\mathbf{Z} + \mathbf{Z}\sqrt{D}))$ is generated by one of its elements, let say $\varphi(x_0 + y_0\sqrt{D})$ with $x_0, y_0 \in \mathbf{Z}$ and $x_0^2 - Dy_0^2 = 1$. The pair (x_0, y_0) satisfy the wanted condition, by the description of $\mathrm{Ker}(\varphi)$.

Problem 2

1. The polynomial $\Phi_p = \sum_{i=0}^{p-1} X^i = \frac{X^p - 1}{X - 1}$ is of degree $p - 1$ and vanishes at ζ. Since we are supposed to know that $\mathbf{Q}[\zeta]/\mathbf{Q}$ has degree $p-1$, Φ_p is the minimal polynomial of ζ. (In fact, this should go the other way around : Φ_p is the p-th cyclotomic polynomial, it is irreducible, therefore Φ_p is the minimal polynomial of ζ and $[\mathbf{K} : \mathbf{Q}] = p - 1$.)

2. (a) Since $\zeta \in \mathscr{O}_{\mathbf{K}}$, $\mathbf{Z}[\zeta] \subset \mathscr{O}_{\mathbf{K}}$.

(b) By the euclidean division of polynomials, $1, \overline{X}, \ldots, \overline{X}^{p-2}$ is a basis of $\mathbf{Z}[X]/(X^p - 1)$ which is isomorphic to $\mathbf{Z}[\zeta]$ therefore, $1, \zeta, \ldots, \zeta^{p-2}$ is a basis of $\mathbf{Z}[\zeta]$.

(c) We have

$$\varpi^k = \sum_{i=0}^{k} \binom{k}{i} (-\zeta)^i$$

Thus the matrix of the coordinates of $(1, \ldots, \varpi^{p-2})$ has integral coefficients and is triangular with 1 or -1 on the diagonal. Therefore it is invertible in $\mathscr{M}_n(\mathbf{Z})$ and $(1, \varpi, \ldots, \varpi^{p-2})$ is a basis of $\mathbf{Z}[\zeta]$.

(d) For any $\sigma \in \mathrm{Gal}(\mathbf{K}/\mathbf{Q})$, $\sigma(\zeta) \in \{1, \ldots, \zeta^{p-1}\}$. Therefore $\sigma(\mathbf{Z}[\zeta]) \subset \mathbf{Z}[\zeta]$.

(e) We have the relation

$$\mathrm{Tr}_{\mathbf{K}/\mathbf{Q}}\left(\sum_{i=0}^{p-2} a_i \zeta^i\right) = \sum_{i=0}^{p-2} a_i \,\mathrm{Tr}_{\mathbf{K}/\mathbf{Q}}(\zeta^i).$$

But $\mathrm{Tr}_{\mathbf{K}/\mathbf{Q}}(1) = [\mathbf{K} : \mathbf{Q}] = p-1$ and if $1 \leqslant i \leqslant p-1$,

$$\mathrm{Tr}_{\mathbf{K}/\mathbf{Q}}(\zeta^i) = \sum_{\sigma \in \mathrm{Gal}(\mathbf{K}/\mathbf{Q})} (\sigma(\zeta^i)) = \sum_{j=1}^{p-1} \zeta^j = -1.$$

So

$$\mathrm{Tr}_{\mathbf{K}/\mathbf{Q}}\left(\sum_{i=0}^{p-2} a_i \zeta^i\right) = (p-1)a_0 - \sum_{i=1}^{p-2} a_i.$$

3. (a) Since the morphism of $\mathbf{Q}$-algebra from $\mathbf{Q}[X]$ to $\mathbf{Q}[X]$ which maps X to $X+1$ is an isomorphism, $\Phi_p(X+1)$ is irreducible. It vanishes at ϖ, therefore $\boldsymbol{\mu}_{\varpi}^{\mathbf{Q}}(X) = \Phi_p(X+1)$.

(b) Since $\deg(\Phi_p(X+1)) = p-1$, $\Phi_p(X+1)$ is the characteristic polynomial of ϖ. Since $p-1$ is even, its constant term, namely p is the norm $N_{\mathbf{K}/\mathbf{Q}}(\varpi)$.

(c) We have

$$\frac{\zeta^i - 1}{\zeta - 1} = \sum_{j=0}^{i-1} \zeta^j \in \mathbf{Z}[\zeta],$$

and

$$N_{\mathbf{K}/\mathbf{Q}}\left(\frac{\zeta^i - 1}{\zeta - 1}\right) = \frac{\prod_{\sigma \in \mathrm{Gal}(\mathbf{K}/\mathbf{Q})} \sigma(\zeta^i - 1)}{\prod_{\sigma \in \mathrm{Gal}(\mathbf{K}/\mathbf{Q})} \sigma(\zeta - 1)} = \frac{\prod_{k=1}^{p-1}(\zeta^k - 1)}{\prod_{k=1}^{p-1}(\zeta^k - 1)} = 1.$$

(d) As in problem 1, we show that $z \in \mathscr{O}_{\mathbf{K}}$ belongs to $\mathscr{O}_{\mathbf{K}}^*$ if and only if $|N_{\mathbf{K}/\mathbf{Q}}(x)| = 1$. Since $\sigma(\varpi) = \zeta^i - 1$ for some $i \in \{1, \ldots, p-1$, the result follows from **(c)**.

(e) Using **(d)**, there exists $u \in \mathscr{O}_{\mathbf{K}}^*$ such that

$$p = N_{\mathbf{K}/\mathbf{Q}}(\varpi) = \prod_{\sigma \in \mathrm{Gal}(\mathbf{K}/\mathbf{Q})} \sigma(\varpi) = u\varpi^{p-1}.$$

(f) By **(e)**, if $p|n$ then $\varpi|n$ in $\mathscr{O}_{\mathbf{K}}$. Conversely, If $\varpi|n$ in $\mathscr{O}_{\mathbf{K}}$, then $N_{\mathbf{K}/\mathbf{Q}}(\varpi)|N_{\mathbf{K}/\mathbf{Q}}(n)$, that is $p|n^{p-1}$ and therefore $p|n$.

(g) We have just proven that the kernel of the unique morphism of rings $\mathbf{Z} \to \mathbf{Z}[\zeta]/\varpi\mathbf{Z}[\zeta]$ is $p\mathbf{Z}$. So we get an injection φ from $\mathbf{Z}/p\mathbf{Z}$ to $\mathbf{Z} \to \mathbf{Z}[\zeta]/\varpi\mathbf{Z}[\zeta]$. By the question **2.(c)**, the map $\mathbf{Z} \to \mathbf{Z}[\zeta]/\varpi\mathbf{Z}[\zeta]$ is surjective. Therefore φ is an isomorphism and the ideal $\varpi\mathbf{Z}[\zeta]$ is maximal.

4. (a) Using **2.(e)**,

$$\mathrm{Tr}_{\mathbf{K/Q}}((1-\zeta)x) = \mathrm{Tr}_{\mathbf{K/Q}}\left(\sum_{i=0}^{p-2} a_i(\zeta^i - \zeta^{i+1})\right) = (p-1)a_0 + a_0 + \sum_{i=1}^{p-2}(a_i - a_i) = pa_0.$$

(b) From $(1-\zeta)x \in \mathscr{O}_{\mathbf{K}}$ we get $pa_0 = \mathrm{Tr}_{\mathbf{K/Q}}((1-\zeta)x) \in \mathbf{Z}$.

(c) We apply the last question to $x_1 = \zeta^{p-1}(x - a_0)$ to get $pa_1 \in \mathbf{Z}$. An induction using $x_{i+1} = \zeta^{p-1}(x_i - a_i)$ then proves that $pa_i \in \mathbf{Z}$ for all $i \in \{1, \ldots, p-2\}$.

(d) It follows from last question that $px \in \mathbf{Z}[\zeta]$. Then we apply **2.(c)**.

(e) By **(d)**, $\varpi | b_0$ and by **3.(f)**, $p | b_0$.

5. From **4.(d)** and **(e)**, we get that $\varpi^2 | \varpi b_1$ and therefore $p | b_1$. Similarly, we get $p|b_2$,...,$p|b_{p-2}$. Therefore $x \in \mathbf{Z}[\varpi] = \mathbf{Z}[\zeta]$.

6. We have seen that $p\mathscr{O}_{\mathbf{K}} = (\varpi)^{p-1}$ thus the ramification index of (ϖ) in $\mathbf{K/Q}$ is $p-1$.