M601 - Algebraic Number Theory - Fall 2024

taught by Matthias Strauch, with notes by Thanic Nur Samin

Contents

Tuesday, 8/27/2024

Introduction and Motivation: Fermat's Last Theorem

THEOREM 0.1 (Wiles, Taylor-Wiles, 1995). Let x, y, z and n be positive integers and $n \geq 3$ then $x^n + y^n \neq z^n$

While the method of Taylor-Wiles has been refined and extended greatly since its inception, there is no proof of this theorem known which is of a substantially different nature.

THEOREM 0.2. Let $p \geq 3$ be a prime, $\zeta_p = e^{2\pi i/p} \in \mathbb{C}$, and suppose $R := \mathbb{Z}[\zeta_p] = \{\sum_{i=0}^{p-2} a_i \zeta_p^i \mid a_i \in \mathbb{Z}\}$ is a UFD. Then FLT is true for $n = p$ and consequently for any n divisible by p.

This is far easier to prove!
Sketch of Proof when $p \geq 5$ and $p \nmid xyz$:
Set $\zeta = \zeta_p$
Key idea 1: $x^p + y^p = \prod_{i=0}^{p-1}(x + \zeta^i y)$
Key observation 2 (HW1): for $0 \leq i < j \leq p - 1$, $x + \zeta^i y$ and $x + \zeta^j y$ are coprime in R
Now assume $x^p + y^p = z^p$. We want to obtain a contradiction.
Since R is a UFD, we see that $x + \zeta y = \epsilon \cdot \alpha^p$ for some unit ϵ and $\alpha \in R$
Taking complex conjugate, $x + \zeta^{-1} y = \bar{\epsilon}(\bar{\alpha})^p$
Key lemma 3: 1. $p = (\prod_{i=1}^{p-1} \frac{1-\zeta^i}{1-\zeta})(1 - \zeta)^{p-1}$
2. For all unit ϵ we can find unit ϵ_1 that is both unit and real and integer r so that $\epsilon = \epsilon_1 \cdot \zeta^r$
3. There exists integer c so that $\alpha^p \equiv c \pmod{p}$ which means $\alpha^p - c \in pR$
End of Proof: $\zeta^{-r}(x + \zeta y) = \zeta^{-r}\epsilon\alpha^p = \epsilon_1\alpha^p \equiv \epsilon_1 c \mod p$
Since $\epsilon_1 c$ is real, taking complex conjugates on both sides, we get,
$\zeta^r(x + \zeta^{-1}y) \equiv \epsilon_1 c \mod p$
So, their difference is 0 mod p
Therefore, $x + \zeta y + \zeta^{2r}x + \zeta^{2r-1}y \equiv 0 \pmod{p}$
Since R is a free $\mathbb{Z}$-module with basis $\{1, \zeta, \zeta^2, \ldots, \zeta^{p-2}\}$,
We have $p \mid x$ or $p \mid y$
So we have contradiction!
Remarks: 1. For the case $p \mid xyz$: Washington, Intro to Cyclotomic Fieldes, Ch 9.
2. In 1985, Adleman and Heath-Brown showed that the first case $p \nmid xyz$ of FLT is true for infinitely many primes
The proof of FLT being true just outlined requires R to be UFD. But it also works under the assumption that:
If I is an ideal of R and I^p is a principal ideal, then I is a principal ideal $(*)$
This is good, because UFD is a very strong assumption, and $(*)$ is significantly weaker.
$(*)$ is equivalent to saying: the class number $h_{\mathbb{Q}(\zeta_p)}$ is not divisible by p

THEOREM 0.3 (Kummer, 1847). i. FLT is true for exponent $n = p$ if $p \nmid h_{\mathbb{Q}(\zeta_p)}$ [the class number]
ii. $p \nmid h_{\mathbb{Q}(\zeta_p)} \iff p$ does not divide the numerator of the Bernoulli numbers $B_2, B_4, \ldots, B_{p-3}$
where $\frac{x}{e^x-1} = \sum_{k=0}^{\infty} B_k \frac{x^k}{k!}$

This would be very useful if we knew more about Bernoulli numbers.

DEFINITION. A prime p is called regular if $p \nmid h_{\mathbb{Q}(\zeta_p)}$

It is known that there are infinitely many irregular primes. So, we can't prove Fermat's Last Theorem with this approach for all primes.
It is not known whether there are infinitely many regular primes. If we assume Bernoulli numbers are random mod p then probability of none being divisible by p is $(1 - \frac{1}{p})^{\frac{p-3}{2}} \approx e^{-\frac{1}{2}} \approx 0.61$
So, Heuristically, 61% primes are regular.

The ring of integers $\mathcal{O}_K$

DEFINITION. i. A <u>number field</u> is a finite field extension of $\mathbb{Q}$.
Its elements are called <u>algebraic numbers</u>
ii. If $K/\mathbb{Q}$ is a number field, then $\alpha \in K$ is called an <u>algebraic integer</u> (or <u>integral over</u> $\mathbb{Z}$), if $\exists$ monic polynomial $f(x) \in \mathbb{Z}[x]$ such that $f(\alpha) = 0$
$\mathcal{O}_K = \{\alpha \in K \mid \alpha \text{ is integral over } \mathbb{Z}\} \subset K$

Example: 1. $K = \mathbb{Q}(\sqrt{-1}) \implies \mathcal{O}_K = \mathbb{Z}[\sqrt{-1}]$
2. $K = \mathbb{Q}(\sqrt{5}) \implies \mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$
Key questions: Is $\mathcal{O}_K$ a ring? Why are sums and products of algebraic integers algebraic?

DEFINITION. Let B be a ring (always commutative with 1), and $A \subset B$ a subring. Then $b \in B$ is called <u>integral over A</u> if there exists a monic polynomial $f(x) \in A[x]$ such that $f(b) = 0$.
Set of integral elements is called $\overline{A}$, the integral closure of A.
<u>Note that integral closure of A depends on B.</u>
B is called <u>integral over A</u> if $B = \overline{A}$. So every element $b \in B$ is integral over A.

PROPOSITION 1.1. Finitely many elements $b_1, \ldots, b_n \in B$ are all integral over A if and only if the subring $A[b_1, \ldots, b_n]$ of B of B ($\coloneqq$ the smallest subring of B containing A and $b_1, \ldots, b_n$) is a finitely generated (f.g.) A-module.

LEMMA 1.2. Let $S = (a_{ij})_{1 \le i, j \le r} \in M_r(B)$ be a matrix and let $S^* = (S^*_{ij})_{1 \le i, j \le r} \in M_r(B)$ be its <u>adjugate matrix</u>, ie $S^*_{ij} = (-1)^{i+j} \det(S_{ji})$ where S_{ji} is obtained from S by removing the j'th row and i'th column.
Then $S \cdot S^* = S^* \cdot S = \det(S)I$

PROOF. HW1 □

PROOF OF PROPOSITION 1.1. let $b \in \overline{A}$, $f \in A[x]$ monic, $f(b) = 0$ and $\deg f = n$
Let $g \in A[x]$ be any poly. Long division implies $g(x) = q(x)f(x) + r(x)$ with $\deg r \le n - 1$
So, $g(b) = q(b)f(b) + r(b) \in \sum_{i=0}^{n-1} A \cdot b^i$
So, $A[b] \subset \sum_{i=0}^{n-1} Ab^i \subset A[b]$ is a finitely generated A-module.
The case of several elements is proved by induction on n.
For the other direction, suppose $R \coloneqq A[b_1, \ldots, b_n]$ is a finitely generated A-module. We want to prove that $b_1, \ldots, b_n$ are integral over A.
Let $b \in R$ be any element.
$R = \sum_{j=1}^r Ac_j$ for some $c_1, \ldots, c_r \in R$
$\implies bc_j = \sum_{j=1}^r a_{ij}c_j$ with $a_{ij} \in A$ where $a_{ij} \in A$
This gives us a linear equation:
$$\underbrace{(bI_r - (a_{ij}))}_{=:S} \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_r \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$
So $S\vec{c} = \vec{0}$
So, $S^* S \vec{c} = \vec{0} \implies \det(S)I\vec{c} = \vec{0} \implies \det(S)c_j = 0$ for all j.
Therefore, $\det(S) = 0$
$\det S$ is of the form $b^r + Ab^{r-1} + \cdots = 0$
So, b is integral $/ A$

□

COROLLARY 1.3. $\overline{A}$ is a subring of B [meaning integral elements are closed under addition and product]

    PROOF. Suppose $b_1, b_2 \in \overline{A}$.
By 1.1, $A[b_1, b_2]$ is a f.g. A-module.
Thus, $A[b_1, b_2, b_1 \pm b_2, b_1 b_2]$ is a f.g. A-module.
Again, by 1.1, $b_1 \pm b_2, b_1 b_2$ are in $\overline{A}$ $\square$

So, $\mathcal{O}_K$ is a ring!

Thursday, 8/29/2024

Recap: Given <u>rings</u> $A \subset B$ we define the integral closure of A in B as

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

Corollary 1.3: $\overline{A}$ is a subring of B

PROPOSITION 1.4. If $A \subset B$ are subrings of C, then C is integral over A iff C is integral over B and B is integral over A.

    PROOF. HW (one direction is trivial). $\square$

<u>Remarks</u>: Let K be a number field [finite field extension of $\mathbb{Q}$]
i. $\mathcal{O}_K$ is a ring by 1.3
ii. $\{\alpha \in K \mid \alpha \text{ is integral over } \mathcal{O}_K\} = \mathcal{O}_K$ by 1.4

DEFINITION. An integral domain A with field of fractions $\text{Frac}(A) = K$ is called <u>integrally closed</u> if it is equal to its integral closure in K
Meaning $\{\alpha \in K \mid \alpha \text{ is integral over } A\} = A$

Counterexample: $\mathbb{Z}[\sqrt{5}] \subsetneq \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right] = \mathcal{O}_{\mathbb{Q}(\sqrt{5})}$ so $\mathbb{Z}[\sqrt{5}]$ is not integrally closed.
Examples: $\mathbb{Z}[i]$ is integrally closed since $\mathbb{Z}[i] = \mathcal{O}_{\mathbb{Q}(i)}$
Counterexample from geometry: $\mathbb{C}[x,y]/(x^3 - y^2)$ is an integral domain. Is it integrally closed?
No! Denote $\overline{y}$ to be the class of y in the quotient ring. Then $\frac{\overline{y}}{\overline{x}}$ is in the field of fractions of the quotient.
Now, $\left(\frac{\overline{y}}{\overline{x}}\right)^2 = (\overline{y})^2 / \overline{x}^2 = \overline{x}^3 / \overline{x}^3 = \overline{x}$
So, $\overline{y}/\overline{x}$ is the solution to $t^2 - \overline{x}$ so $\overline{y}/\overline{x}$ is integral over R but not in R
Morally, a ring not being integrally closed correspond to some singularity.
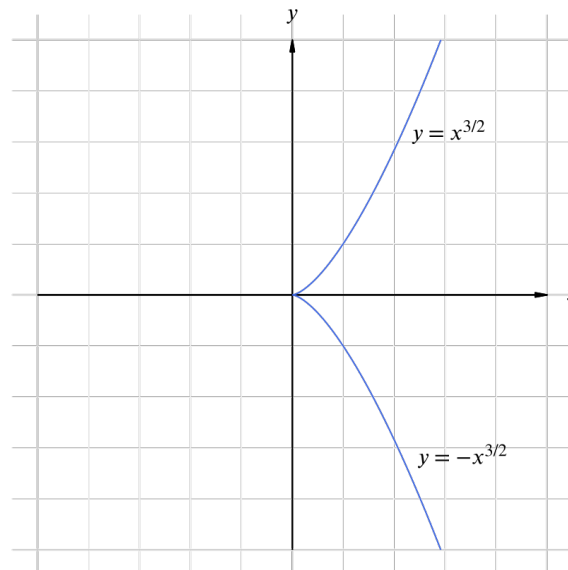
PROPOSITION 1.5. Let A be an integrally closed domain and $K = \text{Frac}(A)$. Let $\alpha \in \overline{K}$ (= algebraic closure of K. We can take the closure in any finite extension). We have $A \subset K \subset \overline{K}$. Consider $\alpha \in \overline{K}$.
Then, α is integral over A iff the minimal polynomial $p_\alpha(x) \in K[x]$ of α over K

Note that minimal polynomial often depends on base field. For example, $\sqrt[4]{2}$ has min poly $x^4 - 2$ over $\mathbb{Q}$ and $x^2 - \sqrt{2}$ over $\mathbb{Q}(\sqrt{2})$

PROOF. $\impliedby$ by definition.
$\implies$: we have α is integral.
So, we have monic $g(x) \in A[x]$ which is monic and $g(\alpha) = 0$.
Can we write $g(x) = h(x)p_\alpha(x)$ in $K[x]$?
Note that every root $\beta \in \overline{K}$ of $p_\alpha(x)$ is a root of g. So, all roots of $p_\alpha(x)$ are integral over A.
Note that coefficients of $p_\alpha(x)$ are generated by the roots of the polynomial. The coefficients are the elementary symmetric polynomials.
Thus, coefficients of p_α lie in $B \coloneqq \{\alpha \in \overline{K} \mid \alpha \text{ is integral over } A\}$
They also lie in K
So, the coefficients are integral over A and in K, hence in A.

$\square$

Proposition 1.5 can be used to find $\mathcal{O}_K$ for quadratic extension, $[K : \mathbb{Q}] = 2$ (HW)

Preliminaries from the theory of fields. In the following L/K will be a finite extension of fields.
L/K is called <u>simple</u> if $\exists \theta \in L$ such that $L = K(\theta)$
L/K is called <u>separable</u> if every $\alpha \in L$ has a separable minimal polynomial over K [separable polynomial meaning no double roots in any extension field.]
For example, in $K = \mathbb{F}_p(t)$ and $L = K(\sqrt[p]{t})$. Then $p_{\sqrt[p]{t}}(x) = x^p - t = (x - \sqrt[p]{t})^p$ so not separable

THEOREM 1.6 (Theorem of the Primitive Element). If L/K is a finite separable extension, it is simple.

DEFINITION. The <u>trace</u> $\text{Tr}_{L/K} : L \to K$ and norm $\text{N}_{L/K} : L \to K$ are defined by:
$\text{Tr}_{L/K}(x) = \text{Tr}(T_x)$
$N_{L/L}(x) = \det(T_x)$
Where $T_x : L \to L$ is defined by $T_x(y) = xy$ considered as an element of $\text{End}_K(L)$

If $n = [L : K]$ and $f_x(t) = \det(t \, \text{id}_L - T_x) = t^n + \alpha_1 t^{n-1} + \dots$
Then $Tr_{L/K}(x) = -\alpha$ and $N_{L/K}(x) = (-1)^n a_n$
Since $T_{x+y} = T_x + T_y$ and $T_{xy} = T_x \cdot T_y$ we have:
$\text{Tr}_{L/K}(x + y) = \text{Tr}(T_{x+y}) = \text{Tr}(T_x + T_y) = \text{Tr}(T_x) + \text{Tr}(T_y) = \text{Tr}_{L/K}(x) + \text{Tr}_{L/K}(y)$
$N_{L/K}(xy) = \det(T_{xy}) = \det(T_x T_y) = \det(T_x)\det(T_y) = N_{L/K}(x)N_{L/K}(y)$.
So, $\text{Tr}_{L/K} : L \to K$ is a homomorphism of vector spaces and $N_{L/K} : L^\times \to K^\times$ is a homomorphism of the (product) group.

DEFINITION. Fix an algebraic closure $\overline{L}$ of L. A <u>K-embedding</u> of L into E is a field homomorphism $\sigma : L \to \overline{L}$ so tat $\sigma(x) = x$ for all $x \in K$.
In other words, $\sigma : L \to \overline{L}$ so that σ is K-linear.
$\Sigma(L/K)$ is the set of all such embeddings.

Suppose L/K is simple and $L = K(\theta)$. Let $p_\theta(t) \in K[t]$ be the minimal polynomial of θ over K.
Then, the map from $\Sigma(L/K)$ to the set of roots of the minimal polynomial $\alpha \in \overline{L} \mid p_\theta(\alpha) = 0$ given by $\sigma \mapsto \sigma(\theta)$ is a bijection.
In particular if L/K separable, then: $|\Sigma(L/K)| = \deg(p_\theta) = [L : K]$.

LEMMA 1.7. Let L be finite and $K \subset M \subset L$ an intermediate field. Then the restriction map $\text{res} : \Sigma(L/K) \to \Sigma(M/K)$ given by $\text{res}(\sigma) = \sigma \mid_M$ is surjective.
Now suppose that $\Sigma(M/K) \to \Sigma(L/K)$, given by $\tau \mapsto \tilde{\tau}$, is any right inverse of res [meaning, $\tilde{\tau} \mid_M = \tau$]. Then, for each $\tau \in \Sigma(M/K)$, the map $\text{res}^{-1}(\tau) : \Sigma(L/K) \to \Sigma(\tilde{\tau}(L)/\tilde{\tau}(M))$ given by $\sigma \mapsto [\tilde{\tau}(y) \mapsto \sigma(y)]$ is bijective.[1]

---

[1]Here we consider $\overline{L}$ as an algebraic closure of $\tilde{\tau}(L) \subset L$.

Written by Thanic Nur Samin

PROOF. Lorenz, *Algebra*, Volume 1, chapter 7, section 1, Lemma. $\qquad\square$

PROPOSITION 1.8. Let L/K be finite separable and $x \in L$. Then,

    i) $f_x(t) = \det(t\,\mathrm{id}_L - T_x) = \prod_{\sigma \in \Sigma(L/K)}(t - \sigma(x))$

    ii) $\mathrm{Tr}_{L/K}(x) = \Sigma_{\sigma \in \Sigma(L/K)}\sigma(x)$

    iii) $N_{L/K}(x) = \prod_{\sigma \in \Sigma(L/K)}\sigma(x)$

    iv) If $K \subset M \subset L$, then $\mathrm{Tr}_{L/K} = \mathrm{Tr}_{M/K} \circ \mathrm{Tr}_{L/M}$ and $N_{L/K} = N_{M/K} \circ N_{L/M}$.

PROOF. Neukirch, ch I, 2.6 and 2.7 $\qquad\square$

DEFINITION. Let L/K be finite separable extension and $\alpha_1, \ldots, \alpha_n$ be basis of L as a K vector space.
Then the discriminant of $\alpha_1, \ldots, \alpha_n$ is defined by:
$d(\alpha_1, \ldots, \alpha_n) = \det(\sigma_i(\alpha_j))^2$ where $\Sigma(L/K) = \{\sigma_1, \ldots, \sigma_n\}$

Remark: $d(\alpha_1, \ldots, \alpha_n)$ does not depend on the ordering of $\alpha_1, \ldots, \alpha_n$ and not on the chosen ordering of the elements in $\Sigma(L/K)$
We now show that the $d(\alpha_1, \ldots, \alpha_n)$ is in K. Let S be the matrix.

$$d(\alpha_1, \ldots, \alpha_n) = \det(S)^2 = \det(S)\det(S^T) = \det(S^T S)$$

$$= \det\left[\left[\sum_k \sigma_k(\alpha_i)\sigma_k(\alpha_j)\right]_{ij}\right] = \det\left[\left[\sum_k \sigma_k(\alpha_i\alpha_j)\right]_{ij}\right]$$

$$= \det\left[(\mathrm{Tr}_{L/K}(\alpha_i\alpha_j))_{ij}\right]$$

Since the trace is in K, we see that the determinant must also be in K.

Tuesday, 9/3/2024

The Discriminant. Let L/K be a finite separable field extension, and $(\alpha_1, \ldots, \alpha_n)$ a basis of L/K. Then,

$$d(\alpha_1, \ldots, \alpha_n) = \det[(\sigma_i(\alpha_j))_{1 \leq i,j \leq n}]^2$$

Where $\Sigma(L/K) = \{\sigma_1, \ldots, \sigma_n\}$. Note that this is independent of order.
We have seen,

$$d(\alpha_1, \ldots, \alpha_n) = \det\left[(\mathrm{Tr}_{L/K}(\alpha_i\alpha_j))_{ij}\right] \in K$$

In fact this is an alternate definition.

PROPOSITION 1.9. Let L/K be any (possibly inseparable) finite field extension. Then the K-bilinear form

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

is non-degenrate if and only if L/K is separable. In this case, $d(\alpha_1, \ldots, \alpha_n) \neq 0$ for any basis $(\alpha_1, \ldots, \alpha_n)$ of L/K.

PROOF. Sketch $\Longleftarrow$: Let $L = K(\theta)$. It can be proven [HW2] that

$$d(1, \theta, \theta^2, \ldots, \theta^{n-1}) = \prod_{1 \leq i \neq j \leq n}(\theta_i - \theta_j)^2$$

where θ_i are the conjugates of θ in $\overline{L}$.
This finishes the proof. $\qquad\square$

Written by Thanic Nur Samin

General Setting: Let A be an integral domain, $K = \text{Frac}(A)$. Suppose L/K is a finite separable extension.

$B :=$ integral closure of A in L. Let C be the integral closure of A in $\overline{L}$.

Assume in the following that A is integrally closed.

Observation: If $x \in B \subset C$ then $\forall \sigma \in \Sigma(L/K), \sigma(x) \in C$.

Therefore, $\text{Tr}_{L/K}(x) = \Sigma_{\sigma \in \Sigma(L/K)}\sigma(x) \in C \cap K = A$ [since A is integrally closed.]

Similarly, $N_{L/K}(x) = \prod_{\sigma \in \Sigma(L/K)} \sigma(x) \in C \cap K = A$.

So, the norm and trace of elements of B are contained in A.

Remark: If $x \in B$, then $x \in B^\times \iff N_{L/K}(x) \in A^\times$

    PROOF. Suppose $xy = 1$ for some $y \in B \implies N_{L/K}(xy) = 1 \implies N_{L/K}(x)N_{L/K}(y) = 1$.

For the other direction, $N_{L/K}(x) = x \underbrace{\prod_{\sigma \neq \text{id}} \sigma(x)}_{b} = xb$. Note that $b \in C \cap L = B$.

Since the norm is a unit, there exists $a \in A \subset B$ such that $axb = 1$. Therefore, $x(ab) = 1 \implies x \in B^\times$.

    $\square$

LEMMA 1.10. Let $(\alpha_1, \ldots, \alpha_n)$ be a basis of L/K such that $\alpha_i \in B$. Then,

$$d(\alpha_1, \ldots, \alpha_n)B \subset A\alpha_1 + \cdots + A\alpha_n$$

    PROOF. By 1.9, we may assume L/K is separable. Write an arbitrary element $\alpha \in B$ as $\alpha = a_1\alpha_1 + \cdots + a_n\alpha_n$ with $a_i \in K$.

Then, $\text{Tr}(\alpha_i\alpha) = \sum_{j=1}^n \text{Tr}(\alpha_i\alpha_j)a_j = \begin{bmatrix} \text{Tr}(\alpha_i\alpha_1) & \cdots & \text{Tr}(\alpha_i\alpha_n) \end{bmatrix} \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix}$. Therefore,

$$\begin{bmatrix} \text{Tr}(\alpha_1\alpha) \\ \vdots \\ \text{Tr}(\alpha_n\alpha) \end{bmatrix} = \underbrace{[\overbrace{\text{Tr}(\alpha_i\alpha_j)}^{\in A}]_{1 \leq i,j \leq n}}_{S} \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix}$$

Multiplying on the left by S^* [the adjugate matrix of S],

$$S^*S \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} = S^* \begin{bmatrix} \text{Tr}(\alpha_1\alpha) \\ \vdots \\ \text{Tr}(\alpha_n\alpha) \end{bmatrix}$$

$$\underbrace{\det(S)}_{d(\alpha_1, \ldots, \alpha_n)} \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} = \underbrace{S^*}_{\text{all entries are in } A} \begin{bmatrix} \text{Tr}(\alpha_1\alpha) \\ \vdots \\ \text{Tr}(\alpha_n\alpha) \end{bmatrix} \in A^n$$

Therefore, $d(\alpha_1, \ldots, \alpha_n)\alpha = \underbrace{(d(\alpha_1, \cdots, \alpha_n)a_1)}_{\in A}\alpha_1 + \cdots + \underbrace{(d(\alpha_1, \cdots, \alpha_n)a_1)}_{\in A}\alpha_n$

    $\square$

Example: Let $K = \mathbb{Q}, L = \mathbb{Q}(\sqrt{5}), \alpha_1 = 1, \alpha_2 = \sqrt{5}$

Then $A = \mathbb{Z}, B = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ and $d(1, \sqrt{5}) = \det\begin{bmatrix} 1 & \sqrt{5} \\ 1 & -\sqrt{5} \end{bmatrix} = 20$

Then, $20 \cdot \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right] \subset \mathbb{Z} + \mathbb{Z}\sqrt{5} = \mathbb{Z}[\sqrt{5}]$

Remarks:

    1) $\forall \alpha \in L, \exists a \in A \setminus \{0\}$ such that $a\alpha \in B$.

        PROOF. Suppose minimal polynomial of α over K is $p_\alpha(x) = x^d + a_1 x^{d-1} + \cdots + a_d \in K[x] \implies \exists a \in A \setminus \{0\}$ such that $aa_i \in A, 1 \leq i \leq d$.

        Thus, $(ax)^d + \underbrace{a_1 a}_{\in A}(ax)^{d-1} + \cdots + \underbrace{(a^d a_d)}_{\in A}$.

        Thus, $a\alpha$ is integral. Therefore, $a\alpha \in B$ $\square$

2) $\text{span}_K(B) = L$

3) $\text{Frac}(B) = L$

DEFINITION. An n-tuple $(\omega_1, \cdots, \omega_n) \in B^n$ is called an <u>integral basis</u> of B over A if $B = \bigoplus_{i=1}^{n} A\omega_i$

<u>Remark</u>: If $(\omega_1, \ldots, \omega_n)$ is an integral basis of B over A, then it is a basis of L/K and hence $n = [L : K]$.

Note that integral basis is <u>not guaranteed</u> to exist.

PROPOSITION 1.11. If L/K is finite separable and A is a PID, then every finitely generated B-submodule $M \neq 0$ of L is a free A-module of rank $[L : K]$.

In particular, B has an integral basis over A. [Apply the proposition to $M = B$].

PROOF. Write $M = \sum_{i=1}^{s} B\alpha_i$ with $\alpha_i \in L^\times$. By the remark 1 above, we can find $a \in A \setminus \{0\}$ such that $a\alpha_i \in B$ for $1 \leq i \leq s$.

Therefore, $a \cdot M \subset B$. Since $aM \underset{ax \leftarrow x}{\cong} M$ [as A-module], we may assume $M \subset B$.

Therefore, $\alpha_1 B = \underset{\neq 0}{B\alpha_1} \subset M \subset B$. (1)

<u>Fact</u> (from M502): Let A be a PID. Then every submodule N of a finitely generated free A-module F is free, and $\text{rank}_A(N) \leq \text{rank}_A(F)$.

Applying the fact to (1), it suffices to show that B is free of rank n over A.

Choose a basis $(\alpha_1, \cdots, \alpha_n)$ of L/K with all $\alpha_i \in B$.

By 1.10, $d(\alpha_1, \ldots, \alpha_n)B \underset{(2)}{\subset} A\alpha_1 + \cdots + A\alpha_n \underset{(3)}{\subset} B$

Since $(\alpha_1, \cdots, \alpha_n)$ is a basis of L/K, $A\alpha_1 + \cdots + A\alpha_n$ is finitely generated free A-module of rank n.

(2) and fact together imply that $d(\alpha_1, \cdots, \alpha_n)B$ is free of rank $\leq n$ over A, and it is nonzero by 1.9.

But $B \to d(\alpha_1, \cdots, \alpha_n)B$, $x \mapsto d(\alpha_1, \cdots, \alpha_n)x$, is an isomorphism of A-modules.

(3) and fact together imply that B has rank $\geq n$.

Therefore, $\text{rank}_A(B) = n$.

$\square$

<u>Remark</u>: If $L = K(\alpha)$ and $p(x) = p_\alpha(x) \in K[x]$ is the minimal polynomial of α over K.

Let $\alpha = \alpha_1, \cdots, \alpha_n$ be the roots of p_α in $\overline{L}$, counted with multiplicity.

Then, $d(1, \alpha, \alpha^2, \cdots, \alpha^{n-1}) = \prod_{i<j}(\alpha_i - \alpha_j)^2 = \text{disc}(p_\alpha(x))$

Recall that $\text{disc}(p) = \text{resultant}(p, p')$.

DEFINITION. Let K be a number field and $n = [K : \mathbb{Q}]$.

1) If $0 \neq I \subseteq K$ is a finitely generated $\mathcal{O}_K$-module and $(\alpha_1, \cdots, \alpha_n)$ a basis of I as a $\mathbb{Z}$-module (exists by 1.11), then $d(I) := d(\alpha_1, \cdots, \alpha_n)$ is called the <u>discriminant</u> of I.

2) $d_K = d(\mathcal{O}_K)$ is called <u>the discriminant of K</u>.

<u>Remarks</u>:

1) $\mathbb{Z}$ is a PID $\overset{1.11}{\implies}$ every I as in (1) is indeed free of rank $n = [K : \mathbb{Q}]$ over $\mathbb{Z}$.

2) $d(I)$ doesn't depend on the choice of a basis. If $(\beta_1, \cdots, \beta_n)$ is another basis I over $\mathbb{Z}$, then we can find a matrix $M \in M_n(\mathbb{Z})$ such that $M \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} = \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_1 \end{bmatrix}$. Note that M must be invertible in $M_n(\mathbb{Z})$ since we can also express the elements of the first basis as linear combination of the elements of the second basis with integral coefficients. Therefore, $\det(M) \in \{\pm 1\}$.

Therefore, $\det(\beta_1, \cdots, \beta_n) = \det(M)^2 d(\alpha_1, \cdots, \alpha_n) = d(\alpha_1, \cdots, \alpha_n)$.

Thursday, 9/5/2024

<u>Example</u>: $K = \mathbb{Q}(i) \implies \mathcal{O}_K = \mathbb{Z} + \mathbb{Z}i \implies d_K = \det \begin{bmatrix} 1 & i \\ 1 & -i \end{bmatrix}^2 = -4$.

Note: $K = \mathbb{Q}(\sqrt{d_K})$. If $[K : \mathbb{Q}] = 2$ then $K = \mathbb{Q}(\sqrt{d_K})$ [Exercise]

Written by Thanic Nur Samin

PROPOSITION 1.12. Let $0 \neq I \subset J$ be finitely generated $\mathcal{O}_K$-submodules of K. Then,

$$d(I) = [J : I]^2 d(J)$$

PROOF. Let $I = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n$ and $J = \mathbb{Z}\beta_1 \oplus \cdots \oplus \mathbb{Z}\beta_n$. Then, there exists $M \subset M_n(\mathbb{Z})$ such that $M \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_n \end{bmatrix} = \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix}$.

Then, $d(I) = d(\alpha_1, \cdots, \alpha_n) = \det(M)^2 d(\beta_1, \cdots, \beta_n) = \det(M)^2 d(J)$.

To finish the proof, note that $J/I \cong \mathbb{Z}^n / M(\mathbb{Z}^n) \cong \mathbb{Z}/(m_1) \oplus \cdots \oplus \mathbb{Z}/(m_n) \implies |m_1 \cdots m_n| = |\det(M)| = [J : I]$.

$\square$

COROLLARY 1.13. If $0 \neq I \subset \mathcal{O}_K$ is an ideal and $d(I)$ is square-free, then $I = \mathcal{O}_K$. If $\theta \in \mathcal{O}_K$ and $K = \mathbb{Q}(\theta)$, then $d(1, \theta, \theta^2, \cdots, \theta^{n-1})$ is square-free, then $\mathbb{Z}[\theta] = \mathcal{O}_K$.

PROOF. $d(I)$ is square free.

$1.12 \implies d(I) = [\mathcal{O}_K : I]^2 d(\mathcal{O}_K)$, which is only possible when $[\mathcal{O}_K : I] = 1$.

Suppose $\mathcal{O}_K = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n$ and $M \in M_n(\mathbb{Z})$ such that $M \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} = \begin{bmatrix} 1 \\ \vdots \\ \theta^{n-1} \end{bmatrix}$.

It follows that $d(1, \theta, \cdots, \theta^{n-1}) = \det(M)^2 d(\alpha_1, \cdots, \alpha_n)$, implying $\det(M)^2 = 1 \implies \det(M) = \pm 1$.

Therefore $\begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} = M^{-1} \begin{bmatrix} 1 \\ \vdots \\ \theta^{n-1} \end{bmatrix} \implies \mathbb{Z}[\theta] = \mathcal{O}_K$. $\square$

CHAPTER 2

Ideals

Suppose K is a number field, and $\mathcal{O} = \mathcal{O}_K$.

DEFINITION. An element $\alpha \in \mathcal{O} \setminus \{0\}$ is called <u>irreducible</u> if α is not a unit $[\alpha \notin \mathcal{O}^\times]$ and whenever $\alpha = \beta\gamma$ with $\beta, \gamma \in \mathcal{O}$ then either $\beta \in \mathcal{O}^\times$ or $\gamma \in \mathcal{O}^\times$

This is not the same as the definition of a prime element. In general, irreducible elements may not be prime elements (which are those non-zero elements which generate prime ideals).
<u>Observation</u>: Every $0 \neq \alpha \in \mathcal{O} \setminus \mathcal{O}^\times$ can be expressed as a product of irreducible elements.

PROOF. If α is irreducible, there's nothing to do.
If it is not irreducible, then $\alpha = \beta\gamma$ with β, γ both non-units.
Using the remark before 1.10, $|N_{K/\mathbb{Q}}(\beta)| > 1$ and $|N_{K/\mathbb{Q}}(\gamma)| > 1$.
Moreover, $|N_{K/\mathbb{Q}}(\alpha)| > |N_{K/\mathbb{Q}}(\beta)|, |N_{K/\mathbb{Q}}(\gamma)|$.
By applying <u>strong induction</u> on $|N_{K/\mathbb{Q}}(\alpha)|$, we see that β and γ can be written as products of irreducibles. Thus, α can be written as a product of irreducibles. $\square$

Example: $K = \mathbb{Q}(\sqrt{-5}), \mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. Here,

$$21 = 3 \cdot 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$$

HW2: $3, 7, 1 + 2\sqrt{-5}, 1 - 2\sqrt{-5}$ are all irreducibles and are pairwise non-associates.
$\implies$ factorization into irreducibles is <u>not</u> unique.
[This is equivalent to the fact that not every irreducible element is a prime element.]
<u>Conclusion</u>: $\mathcal{O}_K$ is not a UFD in general!

THEOREM 2.1. The ring $\mathcal{O}_K$ is noetherian, integrally closed and every non-zero prime ideal is maximal $[\iff$ Krull dimension of $\mathcal{O}_K$ is 1$]$.

PROOF. $\mathcal{O}_K$ is noetherian: if $0 \neq I \subset \mathcal{O}_K$ is an ideal $\overset{1.11}{\implies}$ I is a finitely generated as a $\mathbb{Z}$-module $\implies I$ is finitely generated as an $\mathcal{O}_K$-module.
$\underline{\mathcal{O}_K \text{ is integrally closed}}$: remark after 1.4.
<u>Non-zero prime ideals are maximal</u>: Suppose $0 \neq P \subset \mathcal{O}_K$ is a non-zero prime ideal.
$\overset{1.12}{\implies} [\mathcal{O}_K : P]$ is finite. In fact, $d(P) = [\mathcal{O}_K : P]^2 d(\mathcal{O}_K)$.
Hence, $\mathcal{O}_K/P$ is a finite integral domain. But finite integral domains are fields.
Thus, $\mathcal{O}_K/P$ is a field, and thus P is maximal.

$\square$

This gives us the inspiration to define Dedekind domain.

DEFINITION. An integral domain A is called <u>Dedekind domain</u> if:
1) A is noetherian.
2) A is integrally closed.
3) Every non-zero prime ideal P of A is maximal.

By Theorem 2.1, $\mathcal{O}_K$ is a <u>Dedekind domain</u>.
Moreover, we have:
1) $k[x]$ when k is a field is a Dedekind domain.
2) $\mathbb{C}[x, y]/(y^2 - x^3)$ is <u>not</u> a Dedekind domain. It fails the integrally closed condition, as we saw earlier.

From now on, $\mathcal{O}$ denotes a Dedekind domain.

DEFINITION. $\mathrm{Id}(\mathcal{O}) =$ set of ideals of $\mathcal{O}$.
$\mathrm{Id}^{\times}(\mathcal{O}) = \mathrm{Id}(\mathcal{O}) \setminus \{(0)\}$.
$\mathrm{Max}(\mathcal{O}) =$ set of maximal ideals of $\mathcal{O}$.

LEMMA 2.2. $\forall I \in \mathrm{Id}^{\times}(\mathcal{O})$, there exists primes $P_1, \cdots, P_r \in \mathrm{Max}(\mathcal{O})$ such that $P_1 \cdots P_r \subset I$.

PROOF. Suppose $X = \{J \in \mathrm{Id}^{\times}(\mathcal{O}) \mid J$ does not contain a product of maximal ideals$\}$
Note that X does not contain $\mathcal{O} = (1)$ since it X contains all the prime ideals.
Goal: We want to show that $X = \varnothing$. Suppose X is non-empty. Since $\mathcal{O}$ is noetherian, we cannot have infinite ascending chains.
Using the fact that X is partially ordered by $\subset$, X contains maximal elements. Let $I \in X$ be a maximal element.
Since $I \in X$, I is not a prime. Which means, we can find $x, y \notin I$ such that $xy \in I$.
Set $I_1 := (x) + I$ and $I_2 := (y) + I$.
Then, I_1 and I_2 contain I. Since I is maximal, $I_1, I_2 \notin X$.
This means we can find $P_1, \cdots, P_m$ and $Q_1, \cdots, Q_{m'}$ such that $\prod_{i=1}^{m} P_i \subset I_1$ and $\prod_{j=1}^{m'} Q_j \subset I_2$.
Then, $\prod_i P_i \prod_j Q_j \subset I_1 I_2 = ((x) + I)((y) + I)$, since $xy \in I$ we have $I_1 I_2 \subset I$.
$\square$

LEMMA 2.3. Suppose $P \in \mathrm{Max}(\mathcal{O})$ and $P^{-1} = \left\{ x \in \underset{=\mathrm{Frac}(\mathcal{O})}{K} \mid xP \subset \mathcal{O} \right\}$ [this is an $\mathcal{O}$-submodule of K, containing $\mathcal{O}$]
Then, $\forall I \in \mathrm{Id}^{\times}(\mathcal{O}), IP^{-1} \supsetneq I$.

PROOF. Step 1: We sow $P^{-1} \supsetneq \mathcal{O}$. Suppose $c \in P \setminus \{0\}$.
$2.2 \implies \exists P_1, \cdots, P_r \in \mathrm{Max}(\mathcal{O})$ such that $P_1 \cdots P_r \subset (c) = c \cdot \mathcal{O} \subset P$
Assume that r is minimal with this property.
Recall that, if ideal product $IJ \subset P$ then $I \subset P$ or $J \subset P$.
Therefore, there exists i such that $P_i \subset P$. Since P_i is also a maximal ideal, $P_i = P$.
This means the chain of subsets are all equalities. By reordering the prime ideals, we may assume $i = 1$.
Since r is minimal, $P_2 P_3 \cdots P_r \not\subset (c)$.
This implies there exists $b \in P_2, \cdots, P_r \setminus (c)$ such that $\underset{\in K}{\frac{b}{c}} \notin \mathcal{O}$. However,

$$\frac{b}{c} \cdot P = \frac{b}{c} \subset P_1 \subset \frac{1}{c} P_2 \cdots P_r P_1 \subset \frac{1}{c}(c) = \mathcal{O}$$

Therefore, $\frac{b}{c} \in P^{-1} \setminus \mathcal{O} \implies P^{-1} \supsetneq \mathcal{O}$.
Step 2: We'll show: $IP^{-1} \supsetneq I$ where $I \neq (0)$.
Write $I = \sum_{i=1}^{m} \mathcal{O}\alpha_i$ where $\alpha_i \neq 0$.
Suppose $IP^{-1} = I \implies$ if $x \in P^{-1}$, then $x\alpha_i = \sum_{j=1}^{m} a_{ij}\alpha_j$.

Set $A := [x\partial_{ij} - a_{ij}]_{1 \le i,j \le m}$. Then, $A \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}$. Multiplying on the left by A^* we see that,

$$\det(A) \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix} \implies \forall i, \det(A)\alpha_i = 0 \implies \det(A) = 0$$

Since $\det(A)$ is a monic polynomial, we deduce that x is integral over $\mathcal{O}$, which means $x \in \mathcal{O}$.
Therefore, $P^{-1} \subset \mathcal{O}$. This is a contradiction.
Therefore, $IP^{-1} \supsetneq I$.
$\square$

THEOREM 2.4 (Unique Factorization in Dedekind Domain). Every $I \in \mathrm{Id}^{\times}(\mathcal{O})$ can be written as:

$$I = P_1 P_2 \cdots P_r$$

with $P_1, \cdots, P_r \in \mathrm{Max}(\mathcal{O})$, and this factorization is unique upto ordering.

Written by Thanic Nur Samin

Tuesday, 9/10/2024

PROOF. Step 1, Existence:

Let $X = \{J \in \text{Id}^\times(\mathcal{O}) \mid J \text{ does not have a factorization into prime ideals}\}$. We want to show that $X = \varnothing$.

Assume $X \neq \varnothing$. $\mathcal{O}$ is a dedekind domain, and thus it is noetherian. Therefore, X has a maximal element I.

$I \neq \mathcal{O}$ [since $\mathcal{O} \notin X$].

Thus, there is a maximal ideal P containing I.

Since $I \in X$, $I \neq P$. Therefore, $P \supsetneq I$.

By lemma 2.3, $IP^{-1} \supsetneq I$.

Again, by lemma 2.3, $P^{-1}P \supsetneq P$, $P^{-1}P$ is an ideal $\subsetneq \mathcal{O}$. Therefore, by the maximality of P, we see that $P^{-1}P = \mathcal{O}$.

Now, suppose $\mathcal{O} = IP^{-1}$. Multiplying both sides by $P = IP^{-1}P = I$, which is a contradiction.

Thus, $I \subsetneq IP^{-1} \subsetneq \mathcal{O}$.

Now, since I is a maximal element of X, $IP^{-1} \notin X$.

Thus, we can find maximal ideals $P_1, \cdots, P_r$ so that $IP^{-1} = P_1 \cdots P_r$.

Multiplying both sides by P, we see that,

$I = IP^{-1}P = P_1 \cdots P_r P$ which is a contradiction.

Thus, X must be empty. This shows existence.

Uniqueness: HW.

$\square$

THEOREM 2.5 (Chinese Remainder Theorem). Let $I_1, \cdots, I_r$ be ideals of a ring R which are pairwise co-prime [i.e. $I_i + I_j = R \quad \forall i \neq j$]. Then,

    i) $I_1 \cdots I_r = \bigcap_{j=1}^{r} I_j$

    ii) The canonical map $R / \bigcap_{j=1}^{r} I_j \to \prod_{j=1}^{r} R/I_j$ sending $a + \bigcap_{j=1}^{r} I_j \mapsto (a + I_j)_{j=1}^{r}$ is a ring isomorphism.

PROOF. Neukirch 3.6, Atiyah-MacDonald $\square$

DEFINITION. Let $\mathcal{O}$ be a Dedekind domain, and $K = \text{Frac}(\mathcal{O})$. Then, a <u>fractional ideal</u> of K is a non-zero finitely generated $\mathcal{O}$-submodule of K.

For any $a \in K^\times$, we call $a \cdot \mathcal{O}$ a <u>principal fractional ideal</u>.

The non-zero ideals of $\mathcal{O}$ are called <u>integral ideals</u>.

We denote by $\mathcal{J}_K$ the set of fractional ideals of K, and by $\mathcal{P}_K$ the set of principal fractional ideals.

EXAMPLE. $\frac{1}{2}\mathbb{Z}$ is a fractional ideal for $\mathcal{O} = \mathbb{Z}$.

<u>Observation</u>: Let $I \subset K$ be a non-zero $\mathcal{O}$-submodule.

Then I is fractional of $K \iff \exists c \in \mathcal{O} \setminus \{0\}$ such that $c \cdot I \subset \mathcal{O}$.

PROOF. If it is a fractional ideal of K, it is finitely generated as an $\mathcal{O}$-module. Suppose it is generated by $\frac{a_1}{s_1}, \ldots, \frac{a_r}{s_r}$ for nonzero $s_1, \cdots, s_r \in \mathcal{O}$. We can set $c = s_1 \cdots s_r$ which gives us $c \cdot I = 0$.

For the other direction, suppose $c \cdot I \subsetneq \mathcal{O}$. Since $\mathcal{O}$ is noetherian, it is finitely generated as an $\mathcal{O}$-module.

Therefore, $I = \frac{1}{c}(cI)$ is also finitely generated as an $\mathcal{O}$-module. Thus, I satisfies all the conditions of being a fractional ideal, and thus is a fractional ideal by definition.

$\square$

PROPOSITION 2.6 (Definition of Ideal Group). The fractional ideals of K form an abelian group w.r.t. multiplication, which is called the <u>ideal group</u> of K.

The identity element is $(1) = \mathcal{O}$.

Inverse is given by $I^{-1} = \{x \in K \mid xI \subsetneq \mathcal{O}\}$

PROOF. First we prove that the product of two fractional ideals are fractional ideals.

$I, J \subset \mathcal{J}_K \implies cI \subset \mathcal{O}, dJ \subset \mathcal{O}$. Therefore, $(cd)IJ = (cI)(dJ) \subset \mathcal{O}$. Therefore, $IJ \subset \mathcal{J}_K$.

Commutatitivty and associativity follows from $\mathcal{O}$ itself being a commutative ring.

We need to prove the existence of inverses. Idea: $(P_1 \cdots P_r)^{-1} = P_1^{-1} \cdots P_r^{-1}$

Given $I \subset \mathcal{J}_K, \exists c \in \mathcal{O} \setminus \{0\}$ such that $cI \subseteq \mathcal{O}$.

We can factor cI into primes. Thus, $cI = P_1 \cdots P_r$.

For any $J \in \mathcal{J}_K$, we define $\overline{J} = \{x \in K \mid xJ \subseteq \mathcal{O}\}$.

Note that, if $d \in J \setminus \{0\}$, we have $d\overline{J} \subseteq \mathcal{O}$.

Furthermore, $d\overline{J}$ is finitely generatd implies $\overline{J} = \frac{1}{d} = \frac{1}{d}(d\overline{J})$ is finitely generated as a $\mathcal{O}$-module.

Thus, $\overline{J} \in \mathcal{J}_K$.

Going back to I, we see that $(c)\overline{P_1} \cdots \overline{P_r} I = \overline{P_1} \cdots \overline{P_r}(cI) = (\overline{P_1}P_1) \cdots (\overline{P_r}P_r) = \mathcal{O} \cdots \mathcal{O} = \mathcal{O}$.

Thus, $\forall J \in \mathcal{J}_K, \exists J^{-1} \in \mathcal{J}_K$ such that $J^{-1} \cdot J = J \cdot J^{-1} = \mathcal{O}$.

$\square$

COROLLARY 2.7. Every $I \in \mathcal{J}_K$ has a factorization:

$$I = P_1^{e_1} \cdots P_r^{e_r}$$

where $P_1, \cdots, P_r$ are pairwise distinct prime/maximal ideals and $e_1, \cdots, e_r$ are uniquely determiend integers.

As usual, if $e < 0$ then $J^e := (J^{-1})^{-e}$ for any $J \in \mathcal{J}_K$.

PROOF. Choose $c \in \mathcal{O} \setminus \{0\}$ so that $cI \subset \mathcal{O} \implies cI = P_1^{a_1} \cdots P_r^{a_r}$ with $a_i \geq 0$.

Also write $c\mathcal{O} = P_1^{b_1} \cdots P_r^{b_r}$ with $b_i \geq 0$.

Exponent of 0 are allowed to make sure the primes are the same.

Therefore, $I = (c)^{-1}(cI) = P_1^{a_1 - b_1} \cdots P_r^{a_r - b_r}$

Uniqueness is HW.

$\square$

Note that, in the group of (fractional) ideals, the principal ideals form a subgroup.

DEFINITION. The ideal class group of K is defined as $\mathcal{J}_K / \mathcal{P}_K$ and denoted by Cl_K. We call $h_K = |\mathrm{Cl}_K|$ the class number of K.

We have the exact sequences:

$$1 \to \mathcal{P}_K \to \mathcal{J}_K \to \mathrm{Cl}_K \to 1$$

$$1 \to \mathcal{O}^\times \to \underset{c}{K^\times} \underset{\mapsto}{\to} \underset{c\mathcal{O}}{\mathcal{P}_K} \to 1$$

Remark: $\mathcal{O}$ is a PID $\iff \mathrm{Cl}_K = \{1\}$

PROOF. Suppose I is a fractional ideal. Then, cI is an ideal for some c. Since $\mathcal{O}$ is a PID, we see that cI is a principal ideal, so $cI = (d)$. Therefore, $I = \frac{d}{c}\mathcal{O}$. Thus, $\mathcal{J}_K = \mathcal{P}_K \implies \mathrm{Cl}_K = \{1\}$. For the other direction, suppose $\mathrm{Cl}_K = \{1\}$. Then, $\mathcal{J}_K = \mathcal{P}_K$. Given $I \in \mathrm{Id}^\times(\mathcal{O})$ there exists $c \in K^\times$ such that $I = c\mathcal{O}$. Since $c \in I$ we see that I is a principal ideal. $\square$

Note that Cl_K being trivial is also equivalent to $\mathcal{O}$ being a UFD.

The main results of the first part of the course are: if K is a number field,

- The finiteness of the class number
- Dirichlet's Theorem on Units.
    $\mathcal{O}_K^\times \cong \mathbb{Z}^{r+s-1} \oplus \{\text{roots of unity in } K\}$
    Where r is the number of real embeddings
    $r = |\{K \hookrightarrow \mathbb{R}\}|$.
    And $2s$ is the number of complex embeddings which do not factor through $\mathbb{R}$
    $2s = |\{K \underset{\mathbb{Q}}{\hookrightarrow} \mathbb{C} \text{ does not factor through } \mathbb{R}\}|$.

Decomposition of primes in $\mathcal{O}_K$. c.f. Neuker, ch I

Here, K = number field, $\mathcal{O} = \mathcal{O}_K, n = [K : \mathbb{Q}]$.

DEFINITION. Given a prime number $p \in \mathbb{Z}_{>0}$ we write $p \cdot \mathcal{O}_K = P_1^{e_1} \cdots P_r^{e_r}$ $(*)$ with pairwise distinct maximal ideals P_i. p is called:

   i) unramified (in K) if $e_1 = \cdots = e_r = 1$.
   ii) ramified (in K) if $\exists 1 \leq i \leq r : e_i > 1$.

    iii) <u>completely split</u> (<u>totally split</u>, <u>totally demomposed</u>) if it is unramified and $r = n$.

    iv) <u>inert</u> if $r = 1, e_1 = 1$.

EXAMPLE. Suppose $K = \mathbb{Q}(i)$, then $\mathcal{O}_K = \mathbb{Z}[i]$ and $2 \cdot \mathbb{Z}[i] = (1 + i)^2$ so 2 ramified.

If $p \equiv 1 \pmod 4$ then $p\mathbb{Z}[i] = P_1 P_2$ with $P_1 \neq P_2$ maximal ideals, so p is completely split [and also unramified].

If $p \equiv 3 \pmod 4$ then $p\mathbb{Z}[i]$ is a maximal ideal, therefore p is inert.

<u>Fundamental Questions</u>: Given K, how can we characterize

$$\mathrm{Spl}_K = \{p \in \mathbb{Z}_{>0} \text{ is prime } \mid p \text{ is totally split in } K\}\,?$$

In $\mathbb{Q}(i)$ we have a rule: $p \equiv 1 \pmod 4$ if and only if p is totally split. For quadratic extensions we have similar rules. More generally, if the Galois closure of K over $\mathbb{Q}$ has an abelian Galois group over $\mathbb{Q}$, then Spl_K can be described using congruence conditions.

If the Galois group of (the normal closure of) K over $\mathbb{Q}$ is not abelian, one can sometimes use modular forms or Maass forms to describe Spl_K. In general, the *Langlands Program* predicts that one can use automorphic representations to describe Spl_K.

Thursday, 9/12/2024

Recall that,

$$\mathrm{Spl}_K = \{p \in \mathbb{Z}_{>0} \mid p \text{ is totally split in } K\}$$

EXAMPLE. $\mathrm{Spl}_{\mathbb{Q}(\sqrt{-3})} = \{p \text{ prime } \mid p \equiv 1 \pmod 3\}$

$\mathrm{Spl}_{\mathbb{Q}(\sqrt[3]{2})} = \{p \text{ prime } \mid \exists x, y \in \mathbb{Z} \times \mathbb{Z} : p = x^2 + 27y^2\}$

We can write:

$$p\mathcal{O}_K = P_1^{e_1} \cdots P_r^{e_r} \text{ with pairwise distinct } P_i \in \mathrm{Max}(\mathcal{O}_K), e_i > 0 \quad (*)$$

<u>Question</u>: How does one find a decomposition $(*)$?

DEFINITION (Conductor). Let $\theta \in \mathcal{O} = \mathcal{O}_K$ such that $K = \mathbb{Q}(\theta)$. Then,

$$C = \{\alpha \in \mathcal{O} \mid \alpha \mathcal{O} \subset \mathbb{Z}[\theta]\}$$

C is called the <u>conductor</u> of $\mathbb{Z}[\theta]$.

This is an ideal in $\mathcal{O}$.

<u>Note</u>: 1.10 implies, $d(1, \theta, \cdots, \theta^{n-1}) \cdot \mathcal{O} \subset \mathbb{Z} + \mathbb{Z}\theta + \cdots + \mathbb{Z}\theta^{n-1} = \mathbb{Z}[\theta]$ where $n = [K : \mathbb{Q}]$. Thus, $d(1, \theta, \cdots, \theta^{n-1}) \in C \implies C \neq 0$

<u>Note</u>: $Q \in \mathrm{Max}(\mathbb{Z}[\theta])$ so that Q is not invertible in $\mathbb{Z}[\theta] \iff C \subset Q$. C is the largest ideal of $\mathcal{O}_K$ such that: if $Q \in \mathrm{Max}(\mathbb{Z}[\theta])$ is not invertible in $\mathbb{Z}[\theta] \iff C \subset Q$.

DEFINITION (Norm of an Ideal). If $I \in \mathrm{Id}^{\times}(\mathcal{O})$ then $N(I) = [\mathcal{O} : I]$ is called the <u>norm</u> of I [finite by 1.12].

LEMMA 2.8. For $I, J \in \mathrm{Id}^{\times}(\mathcal{O})$, $N(I \cdot J) = N(I)N(J)$.

    PROOF. Write $I = P_1^{e_1} \cdots P_r^{e_r}$ by 2.4. By 2.5, $\mathcal{O}/I \cong \prod_{i=1}^{r} \mathcal{O}/P_i^{e_i} \implies N(I) = \prod_{i=1}^{r} N(P_i^{e_i})$.

So, the norm is multiplicative in distinct prime factors.

It suffices to show that for non-zero prime ideals P, we have $N(P^e) = N(P)^e$.

We consider the following filtration of P^e:

$$P^e \subset P^{e-1} \subset P^{e-2} \subset \cdots \subset P \subset \mathcal{O}$$

$$\implies |\mathcal{O}/P^e| = \prod_{i=0}^{e-1} |P^i/P^{i+1}|$$

With $P^0 = \mathcal{O}$.

<u>Claim</u>: Since $\mathcal{O}/P$ is a vector space, P^i/P^{i+1} is a vector space. Then, $\dim_{\mathcal{O}/P} P^i/P^{i+1} = 1$

<u>Proof of Claim</u>: Homework 4.

From the claims, we deduce that $N(P^e) = N(P)^e$. $\square$

                               Written by Thanic Nur Samin

THEOREM 2.9 (Dedekind). Let $\theta \in \mathcal{O}_K$ be such that $K = \mathbb{Q}(\theta)$ and $\mu_\theta(x) \in \mathbb{Z}[x]$ be the minimal polynomial of θ over $\mathbb{Q}$.
Let p be a prime such that $p \cdot \mathcal{O} + C = \mathcal{O}$ where C is the conductor of $\mathbb{Z}[\theta]$. [p is relatively prime to the conductor. This is always true for $\mathbb{Z}[\theta] = \mathcal{O}$] [This condition only excludes at most finitely many primes].
Let $\mu \mod p \in \mathbb{Z}[x]/p\mathbb{Z}[x] = \mathbb{F}_p(x)$. Since $\mathbb{F}_p[x]$ is a UFD, we can write,

$$\overline{\mu} = \overline{\mu}_1^{e_1} \cdots \overline{\mu}_r^{e_r}$$

where $\overline{\mu}_1, \cdots, \overline{\mu}_r$ are pairwise distinct monic irreduible polynomials over $\mathbb{F}_p[x]$.
Let $\mu_i(x) \in \mathbb{Z}[x]$ be any polynomial such that $\mu_i \mod p = \overline{\mu}_i$
Then, $P_i := (p, \mu_i(\theta)) \in \text{Max}(\mathcal{O})$ for $1 \leq i \leq r$ and $p\mathcal{O} = P_e^{e_1} \cdots P_r^{e_r}$

Note that, $p\mathcal{O} + C = \mathcal{O}$ implies $\mathbb{Z}[\theta]/p\mathbb{Z}[\theta] \cong \mathcal{O}/p\mathcal{O}$.

PROOF. <u>Claim:</u> $p\mathbb{Z} + (C \cap \mathbb{Z}) = \mathbb{Z}$
<u>Proof of Claim:</u> If not, since $p\mathbb{Z}$ is a maximal ideal, we have $C \cap \mathbb{Z} \subseteq p\mathbb{Z}$. Also, $C \cap \mathbb{Z}$ is non-empty since the discriminant is in it.
Therefore, $\mathbb{Z}/(C \cap \mathbb{Z}) \rightarrowtail \mathbb{Z}/p\mathbb{Z}$ [surjectve]
Thus, $p \mid N(\mathbb{Z} \cap C) = [\mathbb{Z} : C \cap \mathbb{Z}]$.
On the other hand, $\mathbb{Z}/(\mathbb{Z} \cap C) \hookrightarrow \mathcal{O}/C$.
Therefore, $p \mid [\mathcal{O} : C] = N(C)$.
Write $C = Q_1^{f_1} \cdots Q_s^{f_s}$ prime factorization.
$2.8 \implies N(C) = \prod_{j=1}^s N(Q_j)^{f_j} \implies \exists 1 \leq j \leq s : P \mid N(Q_j) = |\mathcal{O}/Q_j|$.
Therefore, $p = \text{char}(\mathcal{O}/Q_j) \implies p \cdot 1_{\mathcal{O}/\mathcal{O}_j} = 0 \implies p \in Q_j$.
But then, since $C \subset Q_j$, $p \cdot \mathcal{O} + C \subset p \cdot \mathcal{O} + Q_j \subset Q_j$, which is a contradiction. This proves the claim.
Therefore, $p\mathbb{Z} + (\mathbb{Z} \cap C) = \mathbb{Z}$.
Recall that $C = \{\alpha \in \mathcal{O} \mid \alpha \cdot \mathcal{O} \subset \mathbb{Z}[\theta]\} \subset \mathbb{Z}[\theta]$.

$$\implies \mathcal{O} = p\mathcal{O} + C \subseteq p\mathcal{O} + \mathbb{Z}[\theta] \subseteq \mathcal{O}$$

$\implies \mathcal{O} = p\mathcal{O} + \mathbb{Z}[\theta]$
$\implies \mathbb{Z}[\theta]/p\mathbb{Z}[\theta] \rightarrowtail \mathcal{O}/p\mathcal{O}$ is a surjection (1). Furthermore,
$\mathbb{Z}[\theta] \cap p\mathcal{O} \underset{\text{claim}}{=} (\mathbb{Z}[\theta] \cap p\mathcal{O})(p\mathbb{Z} + (\mathbb{Z} \cap C)) \subseteq p\mathbb{Z}[\theta] + p\mathcal{O}(\mathbb{Z} \cap C) \subseteq p\mathbb{Z}[\theta] + p\mathcal{O} \cdot C \subseteq p\mathbb{Z}[\theta]$
<u>Upshot:</u> $\mathbb{Z}[\theta]/p\mathbb{Z}[\theta] \overset{\cong}{\to} \mathcal{O}/p\mathcal{O}$ is an isomorphism. (2)
This gives us an isomorphism of rings:

$$\mathbb{F}_p[x]/(\overline{\mu}(x)) \overset{\cong}{\to} \mathbb{Z}[\theta]/p\mathbb{Z}[\theta] \overset{\cong}{\to} \mathcal{O}/p\mathcal{O}$$

First isomorphism is given by $f(x) + (\overline{\mu}(x)) \mapsto f(\theta) + p\mathbb{Z}[\theta]$
Let φ be the map from $\mathbb{F}_p[x]/(\overline{\mu}(x)) \to \mathcal{O}/p\mathcal{P}$.
Chinese remainder theorem gives us:

$$\mathbb{F}_p[x]/(\overline{\mu}(x)) = \prod_{i=1}^r \mathbb{F}_p[x]/(\overline{\mu_i}(x)^{e_i})$$

Then, the prime ideals of $\mathcal{O}/p\mathcal{P}$ are precisely $\varphi(\overline{\mu}_i(x)) = \underset{=\overline{\mathcal{P}}_i}{\mu_i(\theta) + p\mathcal{O}} \in \mathcal{O}/p\mathcal{O} \leftarrowtail \mathcal{O}$.

Therefore, prime ideals of $\mathcal{O}$ containing $\mathcal{O}$ are precisely the ideals $\mathcal{P}_i := (\mu_i(\theta), p)$. Also,

$$\bigcap_{i=1}^r (\overline{\mu_i}(x)^{e_i}) \overset{CRT}{=} (0_{\mathbb{F}_p[x]/(\overline{\mu}(x))})$$

$$\implies \bigcap_{i=1}^r \overline{\mathcal{P}_i^{e_i}} = (0_{\mathcal{O}/p\mathcal{O}}) \implies \prod_{i=1}^r \mathcal{P}_i^{e_i} \subset p\mathcal{O}$$

If $n = [K : \mathbb{Q}]$ then $p^n = \underset{[\underset{\oplus_1^n \mathbb{Z}\alpha_i}{\mathcal{O}} : \underset{\oplus_1^n p\mathbb{Z}\alpha_i}{p\mathcal{O}}]}{N}(p\mathcal{O}) \leq \prod_{i=1}^r (P_i^{e_i}) = \prod N(P_i)^{e_i} = \prod [\mathcal{O} : P_i]^{e_i} = p^{\deg(\mu)} =$

p^n.

Therefore, $p^n = \prod_{i=1}^{r} N(P_i^{e_i}) \implies \boxed{\prod_{i=1}^{r} P_i^{e_i} = p\mathcal{O}}$

$\square$

EXAMPLE. Let $K = \mathbb{Q}(\sqrt{D})$ for $D \in \mathbb{Z} \setminus \{0,1\}, D$ square-free, <u>and</u> $D \equiv 1 \pmod 4 \underset{HW}{\implies} \mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right]$.

Recall that minimal polyonomial of $\frac{1+\sqrt{D}}{2}$ is given by:

$$\mu(x) = x^2 - x - \frac{1-D}{4}$$

If $p \neq 2$ then $\mu(x) \pmod p$ is equivalent to the factorization of $4\mu(x) \pmod p$.

$$4\mu(x) = 4x^2 - 4x + (1 - D) = (2x - 1)^2 - D$$

It splits into two distinct factors of degree 1 if and only if D is a quadratic residue $\pmod p$.
This gives us the cases:
$p \mid D$ then $y^2 - D \equiv y^2 \pmod p$ and therefore p <u>ramifies</u> in K
D is not a square $\pmod p$ then $y^2 - D$ is irreducible $\pmod p$ and therefore p is inert in K.
D is a square $\pmod p$ then $y^2 - D$ has two distinct roots and therefore p is totally split in K.
For which primes p is D a square?
Answer: We use <u>Quadratic Reciprocity</u>. This gives us,

$$\mathrm{Spl}_{\mathbb{Q}(\sqrt{D})} \doteq \left\{p \text{ prime } \mid p \nmid D \text{ and the Jacobi symbol } \left(\frac{p}{D}\right) = 1\right\}$$

$\doteq$ means "up to at most finitely many exceptions".
If $D = q$ a prime number, then we have,

$$\left(\frac{q}{p}\right) = \left(\frac{p}{l}\right)(-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

Since in our case $p \equiv 1 \pmod 4$ we have,

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$$

If $D = \prod_{i=1}^{r} q_i$ we have,

$$\left(\frac{p}{D}\right) = \prod_{i=1}^{r}\left(\frac{p}{q_i}\right)$$

<u>Consequence</u>: There exists finitely many congruence classes $\bar{a}_1, .., \bar{a}_s \in \mathbb{Z}/D\mathbb{Z}$ such that,

$$p \in \mathrm{Spl}_K \iff \exists 1 \leq i \leq s : p \equiv a_i \pmod D$$

Tuesday, 9/17/2024

$D \equiv 1 \pmod 4, K = \mathbb{Q}(\sqrt{D})$ implies:

$$\mathrm{Spl}_K = \left\{p \text{ prime } \mid p \nmid D \text{ and } \left(\frac{p}{D}\right) = 1\right\}.$$

If $D \equiv 2, 3 \pmod 4$ then there s a similar description of Spl_K in terms of congruences mod $4D$.

COROLLARY 2.10. For a number field K there are only finitely many primes p which <u>ramify</u> in K.

PROOF. Suppose $K = \mathbb{Q}(\theta)$ so that $\theta \in \mathcal{O}_K$. Set C to be the conductor of $\mathbb{Z}[\theta]$.
<u>Note</u>: Only finitely many primes p <u>do not satisfy</u> $p\mathcal{O}_K + C = \mathcal{O}_K$.
If p has this property $[p\mathcal{O}_K + C = \mathcal{O}_K]$ then p ramifies in $\mathcal{O}_K$ if and only if the minimal polynomial of θ: $\mu_{\theta,\mathbb{Q}}(x) \pmod p$ has prime factors in $\mathbb{F}_p(x)$ with multiplicity > 1 [by theorem 2.9, Dedekind-Kummer]
$\iff \mu_\theta(x) \pmod p$ has multiple roots
$\iff \mathrm{disc}(\mu_\theta(x) \pmod p) \in \mathbb{F}_p$ vanishes

$\Longleftrightarrow \text{disc}(\mu_\theta)$ is divisible by p. [since discriminant of μ_θ is a polynomial in coefficients]
Since μ_θ is separable, $\text{disc}(\mu_\theta) \neq 0$ and so only finitely many primes p divide $\text{disc}(\mu_\theta)$. $\square$

Consequences of proof of 2.10: If $\mathcal{O}_K = \mathbb{Z}[\theta]$ then the primes that ramify in K are exactly those that divide $\text{disc}(\mu_\theta) = d(1, \theta, \cdots, \theta^{n-1}) = d_K$.

EXAMPLE (Splitting primes in cyclotomic fields). Suppose $K = \mathbb{Q}(\zeta_n)$. Then, $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$. [Will be proved later].
Minimal polynomial $\mu_{\zeta_n}(x) = \Phi_n(x) = n$'th cylotomic polynomial. Fix a prime p. Then,

$$p \in \text{Spl}_K \underset{2.9}{\Longleftrightarrow} \Phi_n(x) \pmod{p} \text{ has } d = \phi(n) \text{ distinct roots in } \mathbb{F}_p \text{ [HW]}$$

$$\underset{\substack{n \not\equiv 2 \\ (\text{mod } 4)}}{\Longleftrightarrow} x^n - 1 \text{ has } n \text{ distinct roots in } \mathbb{F}_p$$

$$\Longleftrightarrow \mathbb{F}_p^\times \text{ has a subgroup of order } n$$

$$\Longleftrightarrow n \mid p - 1 \Longleftrightarrow p \equiv 1 \pmod{n}$$

So, we have the theorem:
If $n \not\equiv 2 \pmod 4$ then $\text{Spl}_{\mathbb{Q}(\zeta_n)} = \{p \text{ prime } \mid p \equiv 1 \pmod{n}\}$

COROLLARY 2.11. Let K, L be number fields which are Galois over $\mathbb{Q}$ and $M = K.L$ [composite extension, smallest subfield of algebraic extension containing both] Then,

$$\text{Spl}_M \doteq \text{Spl}_K \cap \text{Spl}_L$$

[up to finitely many exceptions]

EXAMPLE.
$$\text{Spl}_{\mathbb{Q}(\sqrt{2}+\sqrt{3})} = \text{Spl}_{\mathbb{Q}(\sqrt{2})} \cap \text{Spl}_{\mathbb{Q}(\sqrt{3})}$$
To find $\text{Spl}_{\mathbb{Q}(\sqrt{2})}$ and $\text{Spl}_{\mathbb{Q}(\sqrt{3})}$ we need the Quadratic Reciprocity Law.

The Quadratic Reciprocity Law (QRL):.

DEFINITION (Legendre Symbol). Let p be an odd prime. The Legendre symbol is defined by:

$$\left(\frac{\cdot}{p}\right) : \mathbb{F}_p^\times \to \{1, -1\}$$

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a = b^2 \text{ for some } b \in \mathbb{F}_p^\times; \\ -1, & \text{if otherwise} \end{cases}$$

We also define for $a \in \mathbb{Z} \setminus p\mathbb{Z} : \left(\frac{a}{p}\right) := \left(\frac{a \ (\text{mod } p)}{p}\right)$

Euler proved that,

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$$

In particular,

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

DEFINITION (Gauss Sum). Suppose $\epsilon_p = \sum_{a \in \mathbb{F}_p^\times} \left(\frac{a}{p}\right) \zeta_p^a$ where ζ_p is a primitive p'th root of unity.

This is called the Gauss Sum.

Then we have the following lemma:

LEMMA 2.12.
$$\epsilon_p^2 = \left(\frac{-1}{p}\right) p = (-1)^{\frac{p-1}{2}} p$$

PROOF. HW 5. □

Note: $|\epsilon_p|_{\mathbb{C}} = \sqrt{p}$ [by 2.12].

THEOREM 2.13 (Quadratic Reciprocity Law / QRL). For two distinct odd primes p and l we have:

$$\left(\frac{p}{l}\right)\left(\frac{l}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{l-1}{2}}$$

Moreover, $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ and $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

PROOF. Set $\zeta = \zeta_p$, and the Gauss sum $\epsilon = \epsilon_p$
For all $x, y \in \mathbb{Z}[\zeta]$ we have:

$$(x+y)^l \equiv x^l + y^l \pmod{l\mathbb{Z}[\zeta]}$$

Therefore, using the fact $\left(\frac{\cdot}{p}\right)$ is a homomorphism,

$$\epsilon^l \equiv \sum_{a \neq 0}\left(\frac{a}{l}\right)^l \zeta^{al} = \sum_{a \neq 0}\left(\frac{a}{l}\right)\zeta^{al} \underset{b=al}{=} \sum_{b \neq 0}\left(\frac{bl^{-1}}{p}\right)\zeta^b = \left(\frac{l^{-1}}{p}\right)\epsilon = \left(\frac{l}{p}\right)\epsilon \pmod{l\mathbb{Z}[\zeta]} \quad (1)$$

$$\implies \epsilon^{l+1} = \epsilon^l \epsilon \overset{(1)}{\equiv} \left(\frac{l}{p}\right)\underbrace{\epsilon \cdot \epsilon}_{\epsilon^2} \overset{2.2}{=} \left(\frac{l}{p}\right)\left(\frac{-1}{p}\right)p \pmod{l\mathbb{Z}[\zeta]} \quad (2)$$

But also:

$$\epsilon^{l+1} = (\epsilon^2)^{\frac{l+1}{2}} \overset{2.12}{=} \left(\left(\frac{-1}{p}\right)p\right)^{\frac{l+1}{2}} = \left(\left(\frac{-1}{p}\right)p\right)^{\frac{l-1}{2}+1} = \left(\frac{-1}{p}\right)^{\frac{l-1}{2}} p^{\frac{l-1}{2}}\left(\frac{-1}{p}\right)p$$

$$\overset{\text{Euler}}{\equiv} (-1)^{\frac{p-1}{2}\frac{l-1}{2}}\left(\frac{p}{l}\right)\left(\frac{-1}{p}\right) \pmod{l\mathbb{Z}[\zeta]} \quad (3)$$

Combining 2 and 3 we get:

$$\left(\frac{l}{p}\right)\left(\frac{-1}{p}\right)p \equiv (-1)^{\frac{p-1}{2}\frac{l-1}{2}}\left(\frac{p}{l}\right)\left(\frac{-1}{p}\right)p \pmod{l\mathbb{Z}[\zeta]}$$

Cancelling,

$$\left(\frac{l}{p}\right) \equiv (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{l}\right) \pmod{l\mathbb{Z}[\zeta]} \overset{l>2}{\implies} \text{Statement}$$

□

COROLLARY 2.14. Let $D \in \mathbb{Z} \setminus \{0, 1\}$ be square free and $K = \mathbb{Q}(\sqrt{D})$. Let d_K be the discriminant of K. Then there exists a group homomorphismism:

$$\chi : (\mathbb{Z}/d_k\mathbb{Z})^\times \to \{-1, 1\} \text{ s.t.}$$

$$\text{Spl}_K = \{p \text{ prime } \mid p \nmid d_K \text{ and } \chi(p \pmod{d_K}) = 1\}$$

CHAPTER 3

Lattices

DEFINITION. Let V be an n-dimensional $\mathbb{R}$-vector space. A subgroup $\Gamma \subset V$ is called a <u>lattice</u> if:
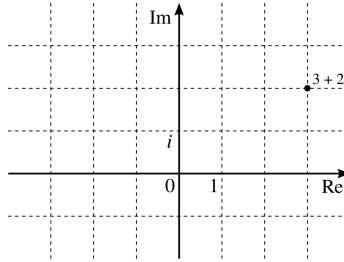
$$\Gamma = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_m$$

where $(v_1, \cdots, v_m)$ is a linearly independent set of vectors. $(v_1, \cdots, v_m)$ is called a <u>basis</u> for Γ. Γ is called <u>complete</u> if $m = \dim V$. The set

$$\Phi = \left\{ \sum_{i=1}^{m} x_i v_i \mid \forall 1 \leq i \leq m : x_i \in [0, 1) \right\}$$

is called the <u>fundamental mesh</u> associated to the basis $(v_1, \cdots, v_m)$

EXAMPLE. Suppose $V = \mathbb{C} = \mathbb{R} \cdot 1 \oplus \mathbb{R}i$. Then, $\mathbb{Z} = \mathbb{Z} + \mathbb{Z}i$ is a lattice.

PROPOSITION 3.1. A subgroup Γ of V [a finite dimensional $\mathbb{R}$-vector space] is a lattice $\iff$ it is <u>discrete</u> [i.e. $\exists$ open neighborhood U of 0_V in V so that $U \cap \Gamma = \{0\}$]

PROOF. $\implies$: If it is a lattice, we can write $\Gamma = \mathbb{Z}v_1 + \cdots \mathbb{Z}v_m$ where $(v_1, \cdots, v_m)$ is part of a basis $(v_1, \cdots, v_n)$ with $n = \dim_{\mathbb{R}} V$. Then,

$$U = \left\{ \sum_{i=1}^{n} x_i v_i \mid x_i \in \left(-\frac{1}{2}, \frac{1}{2} \right) \right\}$$

is open in V and $U \cap \Gamma = \{0\}$. Thus, Γ must be discrete.

Thursday, 9/19/2024

$\impliedby$: Assume Γ is descrete.
<u>Claim</u>: Γ is closed.
<u>Proof of Claim</u>: Fix a norm $\|\cdot\|$ on V. Assume Γ is not closed.
Then, for $v_0 \in V \setminus \Gamma$ we can find a sequence $(\gamma_i)_{i \geq 1}$ in Γ such that $\gamma_i \neq \gamma_{i+1}$ and $\lim_{i \to \infty} \gamma_i = v_0$.
Thus, $0 < \|\gamma_{i+1} - \gamma_i\| \to 0$ as $i \to \infty$.
Thus, in any neighborhood of 0, there are infinitely many distinct elements in Γ. Then Γ is not discrete. This is a contradiction.
Therefore, Γ is closed.
Now we resume the main proof.
Set $U = \operatorname{Span}_{\mathbb{R}} \Gamma \subset$ and set $m := \dim_{\mathbb{R}}(U)$ Let $v_1, \cdots, v_m$ be a basis of U contained in Γ.
$\Phi_0 = $ <u>fundamental mesh</u> associated to this basis.
Set $\Gamma_0 := \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_m \leq \Gamma$.
<u>Claim</u>: $[\Gamma : \Gamma_0] < \infty$.
<u>Proof of Claim</u>: Given $\gamma \in \Gamma$ write $\gamma = \mu(\gamma) + \gamma_0(\gamma)$ where $\gamma_0(\gamma) \in \Gamma_0$ and $\mu(\gamma) \in \Phi_0$.
Note that $\mu(\gamma) \in \Gamma$. Hence $S = \{\mu(\gamma) \mid \gamma \in \Gamma\} \subseteq \Gamma \cap \overline{\Phi}_0$.

As Γ is closed and $\overline{\Phi_0}$ is compact, $\Gamma \cap \overline{\Phi_0}$ is closed in a compact set and hence compact. But it is also discrete (as Γ is discrete), so it is finite. Therefore, S must also be finite.
Thus, $[\Gamma : \Gamma_0]$ is finite.
Now, set $q := [\Gamma : \Gamma_0]$.
Then, $q\Gamma \subset \gamma_0$. Therefore,

$$\Gamma \subset \frac{1}{q}\Gamma_0 = \mathbb{Z}\left(\frac{1}{q}v_1\right) \oplus \cdots \oplus \mathbb{Z}\left(\frac{1}{q}v_m\right)$$

Thus, Γ is contained in a finitely generated abelian group of rank m which is generated by an $\mathbb{R}$-linearly independent set of vectors. This implies that Γ itself is generated by an $\mathbb{R}$-linearly independent set of vectors.
Thus Γ is a lattice.

$\square$

PROPOSITION 3.2 (Complete Lattices). A lattice $\Gamma \subset V$ is complete $\iff$ there exists a bounded [with respect to a fixed but arbitrary norm] set $M \subset V$ so that $V = \bigcup_{\gamma \in \Gamma} \gamma + M$.

PROOF. $\implies$: If $\Gamma = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_n$ is a complete lattice where $(v_1, \cdots, v_n)$ is a basis of V then we can take for M the fundamental mesh associated to this basis.
$\impliedby$: Fix a norm $\|\cdot\|$ in V and suppose there exists a bounded set M such that $V = \bigcup_{\gamma \in \Gamma}(\gamma + M)$.
Set $V_0 = \mathrm{Span}_{\mathbb{R}}(\Gamma)$. For $v \in V$ and $j \in \mathbb{Z}_{>0}$ we can choose $\gamma_j \in \Gamma$ and $m_j \in M$ such that:

$$j \cdot v \in V = \gamma_j + v_j$$

$$\implies v = \underbrace{\frac{1}{j}\gamma_j}_{\in V_0} + \underbrace{\frac{1}{j}m_j}_{\|\frac{1}{j}m_j\| \to 0}$$

Then, $V_0 \ni \frac{1}{j}\gamma_j \to v$ and since V_0 is closed in V, $v \in V_0$. Therefore, $V_0 = V$ and Γ contains a basis in V. $\square$

Now suppose $\langle \cdot, \cdot \rangle : V \times V \to \mathbb{R}$ is an inner product, in which case we have the associated norm:

$$\|v\| = \sqrt{\langle v, v \rangle}$$

Let $\varepsilon_1, \cdots, \varepsilon_n$ be an ONB [orthonormal basis of $(V, \langle \cdot, \cdot \rangle)$].
Then, we have an isometry

$$\iota : (V, \langle \cdot, \cdot \rangle) \to (\mathbb{R}^n, \langle \cdot, \cdot \rangle_{st})$$

where $\langle \cdot, \cdot \rangle_{st}$ is the standard inner product. Then,

$$\iota\left(\sum_{j=1}^n x_j \varepsilon_j\right) = \sum_{j=1}^n x_j e_j$$

Then $\forall v, w \in V, \langle \iota(v), \iota(w) \rangle_{st} = \langle v, w \rangle$
We use ι to transfar the Lebesgue measure on $\mathbb{R}^n$ to V:

$$\mathrm{vol}_{\langle,\rangle}(\underbrace{M}_{\subset V}) = \mathrm{vol}_{\mathrm{Leb}}(\iota(M))$$

Then, the volume of the fundamental w.r.t. any orthonormal basis $\varepsilon_1, \cdots, \varepsilon_n$ mesh is:

$$\mathrm{vol}_{\langle,\rangle}(\Phi) = \mathrm{vol}_{\mathrm{Leb}}(\iota(\Phi)) = \mathrm{vol}_{\mathrm{Leb}}([0,1)^n) = 1$$

More generally: if $\underline{v} = (v_1, \cdots, v_n)$ is any basis of V and A is the change-of-basis matrix from $\varepsilon_1, \cdots, \varepsilon_n$:

$$A = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix} \iff v_j = \sum_{i=1}^n a_{ij}\varepsilon_i$$

Written by Thanic Nur Samin

Then, if $\Phi_{\underline{v}} = \{\sum x_i v_i \mid x_i \in [0,1)\}$ is the fundamental mesh associated to $\underline{v}$ we have:

$$\boxed{\mathrm{vol}_{\langle,\rangle} = |\det A|}$$

Notation: If $\Gamma \subset V$ is a complete lattice with fundamental mesh Φ [for some basis of Γ] we set

$$\mathrm{vol}_{\langle,\rangle}(\Gamma) := \mathrm{vol}_{\langle,\rangle}(\Phi)$$

and it does not depend on the basis of Γ, since the transformation matrix has determinant ± 1.

DEFINITION (Centrally Symmetric Set, Convex Set). A subset $X \subset V$ is called <u>centrally symmetric</u> if $\forall v \in X$, $-v \in X$.
It is called <u>convex</u> if $\forall t \in [0,1]$ and $\forall v, w \in X$, $tv + (1-t)w \in X$. Meaning, all points in the <u>line</u> between v and w are in X.

THEOREM 3.3 (Lattice Point Theorem). Let $\Gamma \subset (V, \langle \cdot, \cdot \rangle)$ be a complete lattice and $X \subset V$ a centrally symmetric and convex measurable subset. Then if $\mathrm{vol}_{\langle,\rangle}(X) > 2^n \mathrm{vol}(\Gamma)$ where $n = \dim_{\mathbb{R}}(V)$ then,

$$X \cap (\Gamma \setminus \{0\}) \neq \varnothing$$

Meaning X must contain a non-zero lattice point.

EXAMPLE. Suppose $V = \mathbb{R}^2$ with the standard inner product, and $\Gamma = \mathbb{Z} \oplus \mathbb{Z}$. Take $X = (-1,1) \times (-1,1)$ So $\mathrm{vol}(X) = 4$. It does not contain any non-zero lattice point, but that is not a contradiction since $\mathrm{vol}(X)$ is not strictly bigger than 4.
If we take any convex symmetric set even a little bit bigger, we must have one lattice point.

PROOF. Suppose $\gamma_1, \gamma_2 \in \Gamma, \gamma_1 \neq \gamma_2$ and $\left(\gamma_1 + \frac{1}{2}X\right) \cap \left(\gamma_2 + \frac{1}{2}X\right) \neq \varnothing$

Then, $\exists x, y \in X$ such that $\gamma_1 + \frac{1}{2}x = \gamma_2 + \frac{1}{2}y \implies \underbrace{\gamma_1 - \gamma_2}_{\Gamma \setminus \{0\}} = \underbrace{\frac{1}{2}y + \frac{1}{2}(-x)}_{\in X}$ so we're done.

Now, we use contradiction. Assume that the intersection is empty. Then, for any distinct $\gamma_1, \gamma_2 \in \Gamma$ we must have $\left(\gamma_1 + \frac{1}{2}X\right) \cap \left(\gamma_2 + \frac{1}{2}X\right) = \varnothing$.
Note that $\gamma + \frac{1}{2}X$ is measurable. All these are distinct.
Let Φ be a fundamental mesh for Γ. Then,

$$\mathrm{vol}(\Phi) \geq \sum_{\gamma \in \Gamma} \mathrm{vol}\left(\left(\gamma + \frac{1}{2}X\right) \cap \Phi\right)$$

Note that,

$$\left(\left(\gamma + \frac{1}{2}X\right) \cap \Phi\right) - \gamma = (\Phi - \gamma) \cap \frac{1}{2}X$$

Therefore,

$$\mathrm{vol}(\Phi) \geq \sum_{\gamma \in \Gamma} \mathrm{vol}\left((\Phi - \gamma) \cap \frac{1}{2}X\right)$$

Furthermore,

$$\mathrm{vol}\left(\frac{1}{2}X\right) = \sum_{\gamma \in \Gamma} \mathrm{vol}\left((\Phi - \gamma) \cap \frac{1}{2}X\right) \leq \mathrm{vol}(\Phi) = \mathrm{vol}(\Gamma)$$

$$\implies \frac{1}{2^n} \mathrm{vol}(X) \leq \mathrm{vol}(\Gamma)$$

$$\implies \mathrm{vol}(X) \leq 2^n \mathrm{vol}(\Gamma)$$

Which contradicts our assumption. So we're done.

$\square$

Geometry of Numbers

Goal: We want to find find an embedding $j : K \hookrightarrow K_{\mathbb{R}}$, a $\mathbb{Q}$-linear map where $K_{\mathbb{R}}$ is a certain inner product space such that $\forall I \in \mathrm{Id}^{\times}(\mathcal{O}_K)$, $j(I)$ is a complete lattice in $K_{\mathbb{R}}$.

EXAMPLE. Suppose $K = \mathbb{Q}(\sqrt{-1})$. Then $K_{\mathbb{R}} = \mathbb{C} = \mathbb{R} \oplus \mathbb{R}i$, the embedding j is the obvious map and $j(\mathbb{Z}[i]) = \mathbb{Z} \oplus \mathbb{Z}i$ is a complete lattice.

Set $\Sigma_K = \{\sigma : K \hookrightarrow \mathbb{C} \mid \sigma$ is a field homomorphism$\}$.
If $K = \mathbb{Q}(\theta)$ and $\mu_{\theta,\mathbb{Q}}(x) = \prod_{i=1}^{n}(x - \theta_i)$ where $\theta_i \in \mathbb{C}$ then the map $\Sigma_K \to \{\theta_1, \cdots, \theta_n\}, \sigma \mapsto \sigma(\theta)$ is bijective.
We call $\tau \in \Sigma_K$ <u>real</u> (respectively <u>complex</u>) if $\tau(K) \subset \mathbb{R}$ (respectively $\tau(K) \not\subset \mathbb{R}$).

Tuesday, 9/24/2024

Suppose $\Sigma_K = \{\tau : K \to \mathbb{C}\}$, $\begin{cases} \tau \text{ real,} & \iff \tau \subset \mathbb{R}; \\ \tau \text{ complex,} & \iff \tau(K) \not\subset \mathbb{R} \end{cases}$
$K = \mathbb{Q}(\theta)$ and $\theta_1, \cdots, \theta_n \in \mathbb{C}$ are conjugates of θ [=roots of minimal polynomial of $\theta/\mathbb{Q}$].

$$\Sigma_K \underset{\text{bijection}}{\to} \{\theta_1, \cdots, \theta_n\}, \tau \to \tau(\theta)$$

Let $\rho_1, \cdots, \rho_r : K \hookrightarrow \mathbb{R}$ real embeddings and $\sigma_1, \cdots, \sigma_s, \overline{\sigma}_1, \cdots, \overline{\sigma}_s : K \implies \mathbb{C}$ complex embeddings $[\overline{\sigma}(\alpha) = \overline{\sigma(\alpha)}]$
Then $n = [K : \mathbb{Q}] = r + 2s$
$K_{\mathbb{C}} := \mathbb{C}^{\Sigma_K} = $ set of maps $\Sigma_K \to \mathbb{C} = \{(z_\tau)_{\tau \in \Sigma_K} \mid z_\tau \in \mathbb{C}\}$
$K_{\mathbb{R}} = \{(x_1, \cdots, x_r, z_1, \cdots, z_s, \overline{z}_1, \cdots, \overline{z}_s) \in K_{\mathbb{C}} \mid \forall 1 \le i \le r : x_i \in \mathbb{R}, \forall 1 \le j \le s : z_j \in \mathbb{C}\}$
$x_i \leftrightarrow x_{e_i}, z_j \leftrightarrow z_{\sigma_j}, \overline{z}_j \leftrightarrow z_{\overline{\sigma}_j}$
$\dim_{\mathbb{R}} K_{\mathbb{R}} = r + 2s = n$
Let $\langle, \rangle$ be the restriction of the standard inner product $\langle, \rangle_{K_{\mathbb{C}}}$ on $K_{\mathbb{C}}$ to $K_{\mathbb{R}}$

$$\langle (z_\tau)_\tau, (w_\tau)_\tau \rangle_{K_{\mathbb{C}}} = \sum_{\tau \in \Sigma_K} z_\tau \overline{w}_\tau$$

$$\left\langle \begin{bmatrix} x_1 \\ \vdots \\ x_r \\ z_1 \\ \vdots \\ z_s \\ \overline{z}_1 \\ \vdots \\ \overline{z}_s \end{bmatrix}, \begin{bmatrix} x'_1 \\ \vdots \\ x'_r \\ z'_1 \\ \vdots \\ z'_s \\ \overline{z}'_1 \\ \vdots \\ \overline{z}'_s \end{bmatrix} \right\rangle = \sum_{i=1}^{r} x_i x'_i + \sum_{j=1}^{s}[z_j \overline{z}'_j + \overline{z}_j \overline{\overline{z}'_j}] = \sum_{i=1}^{r} x_i x'_i + \sum_{j=1}^{s} 2\,\mathrm{Re}(z_j z'_j) \in \mathbb{R}$$

Define $j : K \hookrightarrow K_{\mathbb{R}}, j(\alpha) = (\tau(\alpha))_{\tau \in \Sigma_K} \in K_{\mathbb{R}}$ because $\overline{\sigma}(\alpha) = \overline{\sigma(\alpha)}$
Define Orthonormal Basis of $K_{\mathbb{R}}$ by:

$$\varepsilon_k = (0, \cdots, 0, \underbrace{1}_{k\text{'th spot}}, 0, \cdots, 0), 1 \le j \le r$$

$$\varepsilon_{r+k} = \frac{1}{\sqrt{2}}(\underbrace{0,\cdots,0}_{r},0,\cdots,\underbrace{1}_{r+k},0,\cdots,0,\underbrace{1}_{r+s+k},0,\cdots,0), 1 \leq k \leq s$$

$$\varepsilon_{r+k} = \frac{1}{\sqrt{2}}(\underbrace{0,\cdots,0}_{r},0,\cdots,\underbrace{i}_{r+k},0,\cdots,0,\underbrace{-i}_{r+s+k},0,\cdots,0), 1 \leq k \leq s$$

Now, $\mathrm{vol}_{\langle\cdot,\cdot\rangle}$(fundamental mesh associated to $(\varepsilon_1,\cdots,\varepsilon_n)) = 1$

PROPOSITION 4.1. For any ideal $I \in \mathrm{Id}^{\times}(\mathcal{O}_K)$ th set $j(I)$ is a <u>complete lattice</u> in $K_{\mathbb{R}}$ with $\mathrm{vol}_{\langle\cdot,\cdot\rangle}(j(I)) = \sqrt{|d_K|}\cdot N(I)$

PROOF. We can write $I = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n$ where $n = [K:\mathbb{Q}]$. Consider the matrix:

$$A = \begin{bmatrix} \vdots & \vdots & \vdots & \vdots \\ j(\alpha_1) & j(\alpha_2) & \cdots & j(\alpha_n) \\ \vdots & \vdots & \vdots & \vdots \end{bmatrix} \in M_n(\mathbb{C})$$

$$= \begin{bmatrix} \rho_1(\alpha_1) & & \rho_1(\alpha_n) \\ \vdots & & \vdots \\ \rho_r(\alpha_1) & & \rho_r(\alpha_n) \\ \sigma_1(\alpha_1) & & \sigma_1(\alpha_n) \\ \vdots & \cdots & \vdots \\ \sigma_s(\alpha_1) & & \sigma_s(\alpha_n) \\ \overline{\sigma}_1(\alpha_1) & & \overline{\sigma}_1(\alpha_n) \\ \vdots & & \vdots \\ \overline{\sigma}_s(\alpha_1) & & \overline{\sigma}_s(\alpha_n) \end{bmatrix}$$

$$\implies \det(A)^2 = \det\left(\underbrace{(\tau_i(\alpha_j))}_{\in \overline{K}}\right)^2 = d(\alpha_1,\cdots,\alpha_n)$$

Where $\Sigma_K = \{\tau_1,\cdots,\tau_n\}$
Proposition 1.12 $\implies d(\alpha_1,\cdots,\alpha_n) = d_K N(I)^2$ (1).
Proposition 1.9 $\implies d(\alpha_1,\cdots,\alpha_n) \neq 0 \implies (j(\alpha_1),\cdots,j(\alpha_n))$ is a linearly independent set of vectors, hence a basis.
$\implies j(I) = \mathbb{Z}j(\alpha_1) + \cdots \mathbb{Z}j(\alpha_n)$ is a complete lattice in $K_{\mathbb{R}}$.

$$B = \begin{bmatrix} \langle j(\alpha_1),\varepsilon_1\rangle & & \langle j(\alpha_n),\varepsilon_1\rangle \\ \vdots & \cdots & \vdots \\ \langle j(\alpha_1),\varepsilon_n\rangle & & \langle j(\alpha_n),\varepsilon_n\rangle \end{bmatrix} \in M_n(\mathbb{R})$$

B is the change-of-basis matrix from the orthonormal basis $(\varepsilon_1,\cdots,\varepsilon_n)$ to $(j(\alpha_1),\cdots,j(\alpha_n))$
$\implies \mathrm{vol}_{\langle,\rangle}(j(I)) = |\det B|$ (2)
By the definition of $\langle,\rangle_{K_{\mathbb{R}}}$ we have: $B^T B = (\langle j(\alpha_i),j(\alpha_j)\rangle) = A^T\overline{A}$ (3)
Thus, we have

$$\sqrt{|d_K|}N(I) \overset{1}{=} |\det A|_{\mathbb{C}} \overset{3}{=} |\det B|_{\mathbb{C}} \overset{2}{=} \mathrm{vol}_{\langle,\rangle}(j(I))$$

$\square$

LEMMA 4.2. The map $f : K_{\mathbb{R}} \to \mathbb{R}^n$ given by

$$(\underbrace{x_1,\cdots,x_r}_{\in\mathbb{R}},\underbrace{z_1,\cdots,z_s}_{\in\mathbb{C}},\overline{z}_1,\cdots,\overline{z}_s) \mapsto (x_1,\cdots,x_r,\mathrm{Re}(z_1),\cdots,\mathrm{Re}(z_s),\mathrm{Im}(z_1),\cdots,\mathrm{Im}(z_s))$$

Is an isometry of $\mathbb{R}$-vector spaces and for any measurable $X \subset K_{\mathbb{R}}$ we have:

$$\mathrm{vol}_{\langle\cdot,\cdot\rangle}(X) = 2^s \mathrm{vol}_{\mathrm{Leb}}(f(X))$$

PROOF. Let $(\varepsilon_1, \cdots, \varepsilon_n)$ be the orthonormal basis of $K_{\mathbb{R}}$ as defined above and

$$\iota : K_{\mathbb{R}} \to \mathbb{R}^n, \iota(\nu) = \begin{bmatrix} \langle \nu, \varepsilon_1 \rangle \\ \vdots \\ \langle \nu, \varepsilon_n \rangle \end{bmatrix}$$

Then $\mathrm{vol}_{\langle \cdot, \cdot \rangle}(X) := \mathrm{vol}_{\mathrm{Leb}}(\iota(X)) = \mathrm{vol}_{\mathrm{Leb}}((\iota \circ f^{-1})(f(X))) - |\det(\iota \circ f^{-1})| \mathrm{vol}_{\mathrm{Leb}}(f(X))$
Now,

$$(\iota \circ f^{-1})(e_i) = \begin{cases} e_i, & \text{if } 1 \le i \le r; \\ \sqrt{2}e_i, & \text{if } r+1 \le i \le n \end{cases}$$

This is an exercise.
Also, $|\det(\iota \circ f^{-1})| = (\sqrt{2})^{2s} = 2^s$. $\qquad\square$

THEOREM 4.3. Let $I \in \mathrm{Id}^\times(\mathcal{O}_K)$ and let $(c_\tau)_{\tau \in \Sigma_\tau}$ be positive real numbers such that $c_{\bar\tau} = c_\tau$ for all $\tau \in \Sigma_K$. Suppose:

$$\prod_{\tau \in \Sigma_K} c_\tau > \left(\frac{2}{\pi} \right)^s \sqrt{|d_K|} N(I)$$

Then, $\exists \alpha \in I \setminus \{0\}$ such that $\forall \tau \in \Sigma_K : |\tau(\alpha)|_{\mathbb{C}} < c_\tau$

PROOF. $X = \{(z_\tau)_\tau \in K_{\mathbb{R}} \mid \forall \tau \in \Sigma_K : |z_\tau| < c_\tau\}$
Note that $0 \in X$ trivially. Also, if $v \in X$ then $-v \in X$. Thus X must be centrally symmetric.
Also, $\forall t \in [0, 1]$ we have: $|tz_\tau + (1-t)z'_\tau| \le t|z_\tau| + (1-t)|z'_\tau| < c_\tau$ when $|z_\tau|, |z'_\tau| < c_\tau$ so X is conve.
Now,

$$\mathrm{vol}_{\langle,\rangle}(X) \overset{4.2}{=} 2^s \mathrm{vol}_{\mathrm{Leb}}(f(X)) = 2^s \prod_{\tau \text{ real}} (2c_\tau) \prod_{\substack{\tau \text{ complex} \\ \text{modulo complex conjugation}}} \pi c_\tau^2$$

$$= 2^s \cdot 2^r \cdot \pi^s \prod_{\tau \in \Sigma_K} c_\tau \underset{\text{by assumption}}{>} 2^{r+s} \pi^s \left(\frac{2}{s} \right)^s \sqrt{|d_K|} N(I) = 2^n \sqrt{|d_K|} N(I) \overset{4.1}{=} 2^n \mathrm{vol}_{\langle,\rangle}(j(I))$$

Lattice Point Theorem implies $\exists \alpha \in I \setminus \{0\} : j(\alpha) \in X$. Thus it must also satisfies the inequality. $\qquad\square$

LEMMA 4.4. For all $t > 0$ the set $X_t = \{(z_\tau)_\tau \in K_{\mathbb{R}} \mid \Sigma_{\tau \in \Sigma_K} |z_\tau| < t\}$. This set is centrally symmetric and convex, and

$$\mathrm{vol}_{\langle,\rangle}(X_t) = 2^n \left(\frac{\pi}{4} \right)^s \frac{t^n}{n!}$$

PROOF. HW5 $\qquad\square$

The following claim is instrumental in proving the finiteness of the class number.

THEOREM 4.5. $\forall I \in \mathrm{Id}\,\dot{\mathcal{O}}_K, \exists \alpha \in I \setminus \{0\}$ such that $|N_{K/\mathbb{Q}}(\alpha)| \le M_K \cdot N(I)$ where

$$M_K = \frac{n!}{n^n} \left(\frac{4}{\pi} \right)^s \sqrt{|d_K|}$$

is called the <u>Minkowski Constant</u>.

PROOF. Let $\epsilon > 0$ and set $t = t_\epsilon = n \sqrt[n]{M_K N(I) + \epsilon}$
Then, applying Lemma 4.4 we see that:

$$\mathrm{vol}_{\langle,\rangle}(X_t) \overset{4.4}{=} 2^n \left(\frac{\pi}{4} \right)^s \frac{t^n}{n!} = 2^n \left(\frac{\pi}{4} \right)^s \frac{n^n}{n!} (M_K N(I) + \epsilon)$$

$$> 2^n \left(\frac{\pi}{4} \right)^s \frac{n^n}{n!} \frac{n!}{n^n} \left(\frac{4}{\pi} \right)^s \sqrt{|d_K|} N(I) \overset{4.1}{=} 2^n \mathrm{vol}_{\langle,\rangle}(j(I))$$

Lattice Point Theorem $\implies \exists \alpha \in I \setminus \{0\} : j(\alpha) \in X_t$ therefore $\sum |\tau(\alpha)| < t$

Using the AM-GM inequality,

$$\sqrt[n]{\prod_{i=1}^{n} c_i} \leq \frac{1}{n} \sum_{i=1}^{n} c_i$$

$$\implies |N(\alpha)| = \prod_{\tau} |\tau(\alpha)| \leq \frac{t^n}{n!} = M_K N(I) + \epsilon$$

Choose ϵ to be small enough so that $\lfloor M_K N(I) + \epsilon \rfloor = \lfloor M_K N(I) \rfloor$

Thus, we have $|N_{K/\mathbb{Q}}(\alpha)| \leq M_K N(I)$. $\qquad\qquad\qquad\square$

CHAPTER 5

The Class Number

Thursday, 9/26/2024

Suppose K is a number field, $\mathcal{O} = \mathcal{O}_K$ and $n = [K : \mathbb{Q}]$. Suppose $\mathcal{J}_K$ is the group of fractional ideals.

Suppose $I \in \mathcal{J}_K$. Choose $\alpha \in \mathcal{O} \setminus \{0\}$ such that $\alpha I \subset \mathcal{O}$.

DEFINITION. Norm of the fractional ideal I is given by:

$$N(I) \coloneqq \frac{N(\alpha I)}{N(\alpha \cdot \mathcal{O})}$$

Lemma 2.8 implies it is well defined.

This gives us a homomorphism $\mathcal{J}_K \to \mathbb{Q}^\times$.

LEMMA 5.1. $\forall \alpha \in K^\times : |N_{K/\mathbb{Q}}(\alpha)| = N(\alpha \cdot \mathcal{O})$.

PROOF. HW 4 problem 6 for $\alpha \in \mathcal{O} \setminus \{0\}$, from which the general case follows by the multiplicativity of the norm function. $\square$

THEOREM 5.2. Let M_K be the Minkowski constant. Then any class $I \cdot \mathcal{P}_K$ [$\mathcal{P}_K$ is the subgroup of principal fractional ideals] contains an ideal $I_1 \in \mathrm{Id}^\times(\mathcal{O})$ such that $N(I_1) \leq M_K$.

PROOF. Let I be a fractional ideal and $\alpha \in I \setminus \{0\}$. Set $J \coloneqq \alpha I^{-1}$ where $I^{-1} = \{\beta \in K \mid \beta \cdot I \subset \mathcal{O}\}$.

Theorem 4.5 implies $\exists \beta \in J \setminus \{0\}$ such that $|N(\beta)| \leq M_K N(J)$ (1).

Now set $I_1 \coloneqq \beta J^{-1} = \beta \alpha^{-1} I \in I \cdot \mathcal{P}_K$.

Then, $N(I_1) = N(\beta \cdot \mathcal{O}) N(J^{-1}) \overset{5.1}{=} |N_{K/\mathbb{Q}}(\beta)| N(J)^{-1} \overset{(1)}{\leq} M_K$. $\square$

THEOREM 5.3 (Definition and Finiteness of the Class Number). The idea class group $\mathrm{Cl}_K \coloneqq \mathcal{J}_K/\mathcal{P}_K$ is finite. Its cardinality $h_K = |\mathrm{Cl}_K|$ is called the <u>class number</u> of K.

PROOF. Theorem 5.2 $\implies$ it suffices to show $|\{I \in \mathrm{Id}^\times(\mathcal{O}) \mid N(I) \leq M_K\}| < \infty$.

Write $I \in \mathrm{Id}^\times(\mathcal{O})$ as $I = P_1^{e_1} \cdots P_r^{e_r} \overset{2.8}{\implies} N(I) = N(P_1)^{e_1} \cdots N(P_r)^{e_r} = q_1^{e_1} \cdots q_r^{e_r}$ where $q_i = N(P_i) = p_i^{f_i}$ for some prime $p_i \in \mathbb{Z}$.

Therefore, it suffices to show that $|\{P \in \mathrm{Max}(\mathcal{O}) \mid p \mid N(P)\}| < \infty$ for any given prime p.

Note that, $p \mid N(P) \iff \mathrm{char}(\mathcal{O}/P) = p \iff p \in P \iff p \cdot \mathcal{O} \subset P \overset{HW4,P2}{\iff} P$ is one of the prime ideals of $\mathcal{O}$ in the factorization of $p\mathcal{O}$.

This prives that $|\{P \in \mathrm{Max}(\mathcal{O}) \mid p \mid N(P)\}| < \infty$ $\square$

<u>Remarks</u>:

1) Proof of 5.3 shows that for any $x \geq 0$: $\pi_K(x) = |\{P \in \mathrm{Max}(\mathcal{O}) \mid N(P) \leq x\}|$ is well defined.

The <u>Prime Number Theorem</u> for K says that:

$$\pi_K(x) \sim \frac{x}{\log x}$$

In other words:

$$\lim_{x \to \infty} \frac{\pi_K(x)}{x/\log x} = 1$$

This was proved first by Hadamard, De la Vallée-Poisson

2) For <u>imaginary quadratic number fields</u> $K = \mathbb{Q}(\sqrt{-D}), D > 0$ square-free it is known that the only such K for which $h_K = 1$ are given by: $D = 1, 2, 3, 7, 11, 19, 43, 67, 163$. This was proved by A. Baker, H. Stark (1969), Heegner (1950s).

COROLLARY 5.4. Cl_K is generated by the classes $P \cdot \mathcal{P}_K$ with prime ideals $P \in \mathrm{Max}(\mathcal{O})$ such that $N(P) \leq M_K$.

PROOF. Let $C_1 = I_1 \mathcal{P}_K, \cdots C_h = I_h \mathcal{P}_K$ be the elements of $\mathrm{Cl}_K, h = h_K$ with ideals $I_j \in \mathrm{Id}^{\times}(\mathcal{O})$ such that $N(I_j) \leq M_K$ by 5.2. Suppose, for each j,

$$I_j = P_{j,1}^{e_{j,1}} \cdots P_{j,r_j}^{e_{j,r_j}} \text{ where each } P_{j,k} \text{ is a prime ideal.}$$

$$\implies N(P_{j,k}) \leq M_K$$

In the subgroup of Cl_K generated by all the classes of $P_{j,k}, 1 \leq j \leq h, 1 \leq k \leq r_j$ we have the classes of $I_1, \cdots, I_h$. Hence that subgroup is the whole group. $\qquad \square$

EXAMPLE. $K = \mathbb{Q}(\sqrt{-17}) \overset{-17 \equiv 3 \pmod 4}{\implies} d_K = -68 \implies M_K = \frac{2!}{2^2}\left(\frac{4}{\pi}\right)\sqrt{|d_K|} = \frac{2}{\pi}\sqrt{68} < 6$
So, $M_K \leq 5$.
Note that $\mathcal{O}_K = \mathbb{Z}[\theta]$ where $\theta = \sqrt{-17}$ so $\mu(x) = x^2 + 17$.
By corollary 5.3 we need to check the prime factorization of $p \cdot \mathcal{O}_K$ with $p \leq 5$. So we need to check $2, 3, 5$
$\mu \mod 2 = (x-1)^2 \overset{2.9}{\implies} 2 \cdot \mathcal{O}_K = (2, \sqrt{-17}-1)^2$. Writing $\omega = \sqrt{-17}-1$ we see that $2 \cdot \mathcal{O}_K = (2, \omega)^2$ where $(2, \omega)$ is a prime.
$\mu \mod 3 = x^2 - 1 = (x+1)(x-1) \overset{2.9}{\implies} 3 \cdot \mathcal{O}_K = (3, \sqrt{-17}-1)(3, \sqrt{-17}+1) = (3, \omega)(3, \overline{\omega})$.
$\mu \mod 5 = x^2 + 2$ and since -2 is not a quadratic residue we see that $5 \cdot \mathcal{O}_K$ is a prime ideal.
<u>Note</u>: There does not exist $P \in \mathrm{Max}(\mathcal{O}_K)$ so that $N(P) = 4$ since that would imply $2 \in \mathcal{P} \implies P = (2, \omega)$ and $N((2, \omega)) = 2$.
It follows that Cl_K is generated by $(2, \omega)$ and $(3, \omega)$:

$$\mathrm{Cl}_K = \langle (2, \omega), (3, \omega) \rangle$$

<u>Claim</u>: $(2, \omega)(3, \omega)^2 = (\omega)$
Proof of Claim is in HW 6.
<u>Note</u>: $(2, \omega)$ is <u>not</u> principal $\implies \mathrm{ord}(\underbrace{[2, \omega]}_{\text{class in } \mathrm{Cl}_K}) = 2$.

Claim implies $\mathrm{ord}([3, \omega]) = 4$ since $[2, \omega] + 2[3, \omega] = 0_{\mathrm{Cl}_K}$. Therefore,

$$\mathrm{Cl}_K \underset{a \cdot [3, \omega] \ \hookleftarrow \ a + 4\mathbb{Z}}{\cong \mathbb{Z}/4\mathbb{Z}}$$

Dirichlet's Theorem on Units

We have:

$$j : K \hookrightarrow K_{\mathbb{R}}, j(\alpha) = (\tau(\alpha))_{\tau \in \Sigma_K} = (\underbrace{\rho_1(\alpha), \cdots, \rho_r(\alpha)}_{\text{real embeddings}}, \sigma_1(\alpha), \cdots, \sigma_s(\alpha), \overline{\sigma}_1(\alpha), \cdots, \overline{\sigma}_s(\alpha))$$

$$K_{\mathbb{R}}^{\times} = \{(z_\tau)_{\tau \in \Sigma_K, z_{\overline{\sigma}} = \overline{z_\sigma}} \mid \forall \tau \in \Sigma_K : z_\tau \neq 0\}$$

It is a multiplicative group w.r.t. componentwise multiplication.

Define $l : K_{\mathbb{R}}^{\times} \to \mathbb{R}^{r+s}$ so that:

$$\ell((x_1, \cdots, x_r, z_1, \cdots, z_s, \overline{z}_1, \cdots, \overline{z}_s)) = (\log|x_1|, \cdots, \log|x_r|, 2\log|z_1|, \cdots, 2\log|z_s|)$$

Suppose $\mathrm{Tr} : \mathbb{R}^{r+s} \to \mathbb{R}$ given by $\mathrm{Tr}(x_1, \cdots, x_r, y_1, \cdots, y_s) = \sum_{i=1}^{r} x_i + \sum_{j=1}^{s} y_j$.

Set $\lambda := l \circ j|_{K^{\times}} : K^{\times} \underset{j}{\hookrightarrow} K_{\mathbb{R}}^{\times} \underset{l}{\to} \mathbb{R}^{r+s}$ is a group homomorphism.

$\varepsilon \in \mathcal{O}_K^{\times} \implies |N_{K/\mathbb{Q}}(\varepsilon)| = 1 \iff \prod_{\tau \text{ real}} |\tau(\varepsilon)| \prod_{\{\tau \text{ complex}\}/(\text{conjugation})} |\tau(\varepsilon)|^2 = 1$

$\underset{\text{apply log}}{\implies} \mathrm{Tr}(\lambda(\varepsilon)) = \mathrm{Tr}(\ell(j(\varepsilon))) = 0.$

Thus, $\lambda(\varepsilon) \in \ker(\mathrm{Tr}) =: H$ which is the trace zero hyperplane. $\dim_{\mathbb{R}}(H) = r + s - 1$.

Set $\Gamma = \lambda(\mathcal{O}_K^{\times}) \subset H$. This is a complete lattice in H, which we will prove later.

Denote by μ_K the group of roots of unity in K. μ_K is finite.

THEOREM 6.1. We have the following exact sequence:

$$1 \to \mu_K \to \mathcal{O}_K^{\times} \overset{\lambda}{\to} \Gamma \to 0$$

Tuesday, 10/1/2024

PROOF. $\zeta \in \mu_K, \zeta^m = 1 \implies |\tau(\zeta)|^m = 1 \implies |\tau(\zeta)| = 1 \implies \lambda(\zeta) = 0.$

Conversely: set $U = \ker(\lambda|_{\mathcal{O}_K^{\times}})$.

$\varepsilon \in U \implies \forall \tau \in \Sigma_K : |\tau(\varepsilon)| = 1 \to \exists$ compact $C \subset K_{\mathbb{R}}$ such that $j(U) \subset C \cap j(\mathcal{O}_K)$.

$j(\mathcal{O})_K$ is a lattice in $K_{\mathbb{R}} \implies |C \cap j(K_{\mathbb{R}})| < \infty \implies |j(U)| < \infty \underset{j \text{ injective}}{\implies} |U| < \infty \implies U \subset \mu_K.$ $\square$

LEMMA 6.2. For all $a \in \mathbb{Z}_{\geq 0}$ the set $\{\alpha \in \mathcal{O}_K \mid N_{K/\mathbb{Q}}(\alpha) = \pm a\}/\mathcal{O}_K^{\times}$ is finite.

PROOF. If $a = 0$ then $\alpha = 0$, if $a = 1$ then α is a unit. These cases are trivial.

<u>Claim</u>: $\forall \beta \in \mathcal{O}_K : |\{\alpha \in \beta + a\mathcal{O}_K \mid N(\alpha) = \pm a\}/ \sim| \leq 1$ where $\alpha \sim \alpha' \iff \alpha \in \alpha' \cdot \mathcal{O}_K^{\times}$.

<u>Proof</u>: Suppose $N(\alpha) = \pm\alpha$ and $\alpha' = \beta + a\gamma$ is another such element ($N(\alpha') = \pm a$) for some $\gamma \in \mathcal{O}_K$. Write $\alpha = \beta + a\gamma$. Then,

$$\frac{\alpha}{\alpha'} = \frac{\beta + a\gamma}{\alpha'} = \frac{\beta + a\gamma' + a(\gamma - \gamma')}{\alpha'} = 1 + \frac{a}{\alpha'}(\gamma - \gamma')$$

Since $K \ni \frac{a}{\alpha'} = \pm\frac{N(\alpha')}{\alpha'} = \pm\frac{1}{\alpha'}\prod_\tau \in \Sigma_K \tau(\alpha') = \pm\prod_{\substack{\tau \in \Sigma_K \\ \tau \neq \mathrm{id}}} \tau(\alpha') \in \mathcal{O}_K$

Thus, $\frac{\alpha}{\alpha'} \in \mathcal{O}_K$.

Similarly, $\frac{\alpha'}{\alpha} \in \mathcal{O}_K$.

Therefore, $\frac{\alpha}{\alpha'} \in \mathcal{O}_K^{\times}$. This finishes the claim.

<u>Note</u>:

$$\{\alpha \in \mathcal{O}_K \mid N(\alpha) = \pm a\}/\mathcal{O}_K^\times \longrightarrow (\mathcal{O}_K/a\mathcal{O}_K)/\mathcal{O}_K^\times$$
$$\alpha \cdot \mathcal{O}_K^\times \longmapsto (\alpha + a\mathcal{O}_K) \cdot \mathcal{O}_K^\times$$

<u>Claim</u> $\implies$ the image is finite.

$\square$

THEOREM 6.3. The group $\Gamma = \lambda(\mathcal{O}_K^\times)$ is a complete lattice in $H = \ker(\mathrm{Tr})$ [the trace zero hyperplane].

PROOF. Step 1: We want to show that Γ is a discrete subgroup of H.
For $c > 0$, set $Q := [-c,c]^{r+s} \subset \mathbb{R}^{r+s}$ "hypercube". It suffices to show that $|\Gamma \cap Q| < \infty$.
<u>Note</u>: $l^{-1}(Q) = \left\{ (z_\tau)_\tau \in K_\mathbb{R}^\times \mid \begin{smallmatrix} e^{-c} \le |z_\tau| \le e^c \text{ for real } \tau \\ e^{-\frac{c}{2}} \le |z_\tau| \le e^{-\frac{c}{2}} \text{ for complex } \tau \end{smallmatrix} \right\}$ is a compact subset of $K_\mathbb{R}$.
Thus, $|l^{-1}(Q) \cap j(\mathcal{O}_K)| < \infty$ since $j(\mathcal{O}_K)$ is a lattice in $K_\mathbb{R}$.
$\implies |l^{-1}(Q) \cap j(\mathcal{O}_K^\times)| < \infty$
$\implies |Q \cap \Gamma| = |\ell(\ell^{-1}(Q) \cap j(\mathcal{O}_K^\times))| < \infty$
Since $\gamma(\varepsilon) = (l \circ j)(\varepsilon)$.
$\implies \Gamma$ is a discrete subgroup of $\mathbb{R}^{r+s}$ and also of $H \overset{3.1}{\implies} \Gamma$ is a lattice in H.
Step 2: We want to show that Γ is complete.
Proposition 3.2 $\implies$ it suffices to show that $\exists$ bounded subset $M \subset H : H = \bigcup_{\gamma \in \Gamma} \gamma + M$.
Put $S = \{(z_\tau)_\tau \in K_\mathbb{R}^\times \mid \prod_\tau |z_\tau| = 1\} = l^{-1}(H)$ [the norm-1 hypersurface].

We will construct $T \subset S$ such that $\ell(T)$ is bounded in H and $\boxed{S = \bigcup_{\varepsilon \in \mathcal{O}_K^\times} j(\varepsilon)T \quad (1)}$ and then take

$M = \ell(T)$.
$\forall \tau \in \Sigma_K$ choose $c_\tau \in \mathbb{R}_{>0}$ such that $c_{\overline{\tau}} = c_\tau$ and $C := \prod c_\tau > \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}$.
Consider $X = \{(z_\tau)_\tau \in K_\mathbb{R} \mid \forall \tau : |z_\tau|_\mathbb{C} < c_\tau\} \subset K_\mathbb{R}$.
For $y = (y_\tau)_\tau \in S \implies yX = \{(z_\tau)_\tau \mid \forall \tau : |z_\tau| < c_{\tau'}\}$ where $\boxed{c_\tau' = |y_\tau|c_\tau}$.
Write $z_\tau = y_\tau w_\tau$.
We have $c_{\overline{\tau}}' c_\tau'$ and $\prod_\tau c_\tau' = \prod_\tau |y_\tau| \prod_\tau c_\tau = C$ as before.
Theorem 4.3 $\implies \exists \alpha \in \mathcal{O}_K \setminus \{0\} : \forall \tau : |\tau(\alpha)| < c_\tau' (\iff j(\alpha) \in yX)$ (2).
Lemma 6.2 $\implies \exists \alpha_1, \cdots, \alpha_m \in \mathcal{O}_K \setminus \{0\}$ such that $\forall \beta \in \mathcal{O}_K : 0 < |N(\beta)| \le C \implies \beta$ is associated to one of $\alpha_1, \cdots, \alpha_m$.
<u>Claim</u>: $T := S \cap \left(\bigcup_{i=1}^m j(\alpha_i)^{-1}X\right)$ satisfies (1).
<u>Proof of Claim</u>: X is bounded in $K_\mathbb{R} \implies \bigcup_{i=1}^m j(\alpha_i)^{-1}X$ is bonded in $K_\mathbb{R} \implies \exists \delta > 0$ such that

$$S \cap \bigcup_{i=1}^m j(\alpha_i)^{-1}X \subset \{(z_\tau)_\tau \in K_\mathbb{R} \mid \forall \tau : \delta \le |z_\tau| \le \delta^{-1}\}$$

We get the lower bound since $\prod |z_\tau| = 1$ on S.

$$\implies \ell\left(S \cap \bigcup_{i=1}^m j(\alpha_i)^{-1}X\right) \text{ is bounded in } H$$

Let $y \in S$ be arbitrary. Then, by (2), $\exists \alpha \in \mathcal{O}_K \setminus \{0\}$ so that $j(\alpha) \in yX \implies y \in j(\alpha)^{-1}X$.
Moreover, $|N(\alpha)| = \prod_\tau |\tau(\alpha)| < \prod_\tau c_\tau' = \underbrace{\prod_\tau |y_\tau|}_{=1} \prod_\tau c_\tau = C$

$\implies 1 \le i \le m$ such that $\alpha = \varepsilon\alpha_i$ for some $\varepsilon \in \mathcal{O}_K^\times$
Hence, $y \in S \cap j(\alpha^{-1})X = S \cap j(\varepsilon)^{-1}j(\alpha_i)^{-1}X = j(\varepsilon)^{-1}\left(j(\varepsilon)S \cap j(\alpha_i)^{-1}X\right) = j(\varepsilon^{-1})(S \cap J(\alpha_i)^{-1}X) \subset j(\varepsilon^{-1}) \cdot \left(S \cap \bigcup_{i=1}^m j(\alpha_i)^{-1}X\right)$
If we define $T := S \cap \bigcup_{i=1}^m j(\alpha_i)^{-1}X$, then

$$S = \bigcup_{\varepsilon \in \mathcal{O}_K^\times} j(\varepsilon)T$$

This implies (1).

$\square$

THEOREM 6.4 (Dirichlet's Theorem on Units). $\mathcal{O}_K^\times$ is the direct product of μ_K (= group of roots of unity in K) and a free abelian group of rank $r + s - 1$. Meaning, $\mathcal{O}_K^\times \cong \mu_K \times \mathbb{Z}^{r+s-1}$.
In other words, $\mathcal{O}_K^\times/\mu_K \cong \mathbb{Z}^{r+s-1}$.

PROOF. 6.1 $\implies 1 \to \mu_K \to \mathcal{O}_K^\times \to \Gamma = \lambda(\mathcal{O}_K^\times) \to 0$ is exact.
6.2 $\implies \Gamma$ is a complete lattice in $H \cong \mathbb{R}^{r+s-1} \implies \Gamma \cong \mathbb{Z}^{r+s-1}$.
Hence the sequence above splits and $\mathcal{O}_K^\times \cong \mu_K \times \Gamma$. $\qquad\square$

Note: There's no canonical way to express $\mathcal{O}_K^\times$ as the direct product.
Remark: Equip $\mathbb{R}^{r+s}$ with the standard inner product $\langle \cdot, \cdot \rangle$ and let $\langle \cdot, \cdot \rangle_H$ be the restriction of $\langle \cdot, \cdot \rangle$ to H.
Then, $(H, \langle \cdot, \cdot \rangle_H)$ is an inner product space. Hence, the concept of volume is available!
Natural Question: What is the volume $\text{vol}_{\langle \cdot, \cdot \rangle_H}(\Gamma)$? Recall that $\Gamma = \lambda(\mathcal{O}_K)^\times$.

Thursday, 10/3/2024

Recall that $\mathcal{O}_K^\times \cong \mu_K \times$ (free abelian group of rank $r + s - 1$).

$$\lambda\big|_{\mathcal{O}_K^\times} : \mathcal{O}_K^\times \lhook\joinrel\longrightarrow K_{\mathbb{R}}^\times \xrightarrow{l} \mathbb{R}^{r+s} \qquad\qquad \langle,\rangle_{st}$$

$$\cup$$

$$H \qquad\qquad \langle,\rangle_H, \dim = r + s - 1$$

$t := r + s - 1$ and $\lambda_1 = \begin{bmatrix} \lambda_{1,1} \\ \vdots \\ \lambda_{1,t+1} \end{bmatrix}, \cdots, \lambda_t = \begin{bmatrix} \lambda_{t,1} \\ \vdots \\ \lambda_{t,t+1} \end{bmatrix}$ be a basis of H, so $\sum_{j=1}^{t+1} \lambda_{i,j} = 0$

Set $\lambda_0 := \frac{1}{\sqrt{t+1}} \begin{bmatrix} 1 \\ \vdots \\ 1 \end{bmatrix} \in \mathbb{R}^{r+s} \implies \mathbb{R}^{r+s} = H \overset{\perp}{\oplus} \mathbb{R}\lambda_0$ and $\|\lambda_0\| = 1$.

Set $\Phi = \left\{ \sum_{i=1}^t x_i \lambda_i \mid x_i \in [0,1) \right\}$ is a fundamental mesh in the lattice $\sum_{i=1}^t \mathbb{Z}\lambda_i$ and $\Phi_0 = \left\{ \sum_{i=0}^t x_i \lambda_i \mid x_i \in [0,1) \right\}$ is a fundamental mesh for $\sum_{i=0}^t \mathbb{Z}\lambda_i$
Thus, $\text{vol}_{\langle,\rangle_H}(\Phi) = \text{vol}_{\langle,\rangle_{st}}(\Phi_0)$ [exercise].

Ch3 $\implies \text{vol}_{\langle,\rangle_{st}} = \left| \det \begin{bmatrix} \lambda_{0,1} & \cdots & \lambda_{t,1} \\ \vdots & & \vdots \\ \lambda_{0,t+1} & \cdots & \lambda_{t,t+1} \end{bmatrix} \right|$

THEOREM 6.5 (Definition). Put $t = r + s - 1$ and let $\varepsilon_1, \cdots, \varepsilon_t \in \mathcal{O}_K^\times$ be such that $\mathcal{O}_K^\times = \mu_K \times \langle \varepsilon_1, \cdots, \varepsilon_t \rangle$. Then, every $\varepsilon \in \mathcal{O}_K^\times$ can be written uniquely as:

$$\varepsilon = \zeta \varepsilon_1^{a_1} \cdots \varepsilon_t^{a_t}$$

with unique $\zeta \in \mu_K$ and unique $(a_1, \cdots, a_t) \in \mathbb{Z}^t$.
Set $\lambda_i = \lambda(\varepsilon_i) \in H$. Then, $\text{vol}_{\langle,\rangle_H}(\underset{=\lambda(\mathcal{O}_K^\times)}{H}) = \sqrt{t+1} \cdot R_K$

where R_K is the absolute value of any $t \times t$ minor of the matrix:

$$\begin{bmatrix} \lambda_{1,1} & \cdots & \lambda_{t,1} \\ \vdots & & \vdots \\ \lambda_{1,t+1} & \cdots & \lambda_{t,t+1} \end{bmatrix} = \begin{bmatrix} \vdots & & \vdots \\ \lambda_1 & \cdots & \lambda_t \\ \vdots & & \vdots \end{bmatrix} \qquad (*)$$

R_K is called the regulator of K and $(\varepsilon_1, \cdots, \varepsilon_t)$ is called the fundamental system of units of $\mathcal{O}_K^\times$.

Written by Thanic Nur Samin

PROOF. Put $\Delta = \begin{bmatrix} \vdots & & \vdots \\ \lambda_0 & \cdots & \lambda_t \\ \vdots & & \vdots \end{bmatrix}, \lambda_0 = \frac{1}{\sqrt{t+1}} \begin{bmatrix} 1 \\ \vdots \\ 1 \end{bmatrix}$. Fix $1 \leq i \leq t+1$ and add all rows of Δ to

the i'th row. We get:

$$\begin{bmatrix} \frac{1}{\sqrt{t+1}} & \lambda_{1,1} & \cdots & \lambda_{t+1} \\ \vdots & \vdots & & \vdots \\ \sqrt{t+1} & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ \frac{1}{\sqrt{t+1}} & \lambda_{1,t+1} & \cdots & \lambda_{t,t+1} \end{bmatrix}$$

$$\implies |\det(\Delta)| = \sqrt{t+1} \left| \begin{matrix} t \times t \text{ -minor obtained by} \\ \text{removing the } i\text{th row from } (*) \end{matrix} \right|$$

$$= \sqrt{t+1} R_K.$$

$\square$

Examples:

1) $R_{\mathbb{Q}} : r = 1, s = 0, t = 0, \mathbb{Z}^\times = \{\pm 1\} \implies R_K = 1$.
2) $K = \mathbb{Q}(\sqrt{-D}), D > 0$ square free $\implies r = 0, s = 1 \implies t = 0 \implies R_K = 1$.
3) $K = \mathbb{Q}(\sqrt{D}), D > 1$ square free $\implies r = 2, s = 0, t = 1, \mu_K = \{\pm 1\} \implies \mathcal{O}_K^\times = \{\pm 1\} \times \langle \varepsilon \rangle$ with some $\varepsilon \in \mathcal{O}_K^\times$ of infinite order. We have $N(\varepsilon) = \varepsilon \sigma(\varepsilon) = \pm 1$.
   WLOG, we take $\varepsilon > 1$. This specifies ε uniquely!
   $$\implies R_K = \left| 1 \times 1\text{-minor of } \begin{bmatrix} \log|\varepsilon| \\ \log|\sigma(\varepsilon)| \end{bmatrix} \right| = \log(\varepsilon)$$

The smallest unit $\varepsilon \in \mathcal{O}_K^\times$ which is > 1 is called the <u>fundamental unit</u> of K.

D	2	3	5	7	11	13	15
ε	$1 + \sqrt{2}$	$2 + \sqrt{3}$	$\frac{1+\sqrt{5}}{2}$	$8 + 3\sqrt{7}$	$10 + 3\sqrt{11}$	$1 + \frac{1+\sqrt{3}}{2}$	$4 + \sqrt{15}$

TABLE 1. Fundamental Units of Quadratic Fields

A general result is the following: <u>if</u> $D \not\equiv 1 \pmod 4$ and $\sqrt{D} = [a_0; \overline{a_1, \cdots, a_l}]$

$= a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_l + \cfrac{1}{a_1 + \cfrac{1}{\ddots}}}}}$ and if the reduced fraction $\frac{p}{q} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_{l-1}}}}$

then the fundamental unit of $\mathbb{Q}(\sqrt{D})$ is $p + q\sqrt{D}$. See [Borerich-Shafarevich, Ch2, sec 7, Problem 5].

A general result of Hecke states:

$$\operatorname{res}_{s=1} \zeta_K(s) = \frac{2^r (2\pi)^s}{|\mu_K| \sqrt{|d_K|}} h_K R_k \quad \text{(class number formula)}$$

This formula assembles all <u>invariants</u> of K we have considered so far:

- Number of real embeddings
- Number of complex embeddings
- Number of roots of unity
- The discriminant

- The class number
- The regulator

CHAPTER 7

Extensions of Dedekind Domains

The most fundmanetal case is something we have done: $\mathbb{Z} \subset \mathcal{O}_K$. We generalize the concept.

THEOREM 7.1. Let $\mathcal{O}_K$ be a Dedekind domain with $K = \text{Frac}(\mathcal{O}_K)$. Let L/K be a finite extension, and deinfe $\mathcal{O}_L$ to be the integral closure of $\mathcal{O}_K$ in L.
Then, $\mathcal{O}_L$ is a Dedekind domain and $\text{Frac}(\mathcal{O}_L) = L$.
Moreover, If L/K is separable, $\mathcal{O}_L$ is finitely generated as $\mathcal{O}_K$-module.

Note: If L/K is not separable, $\mathcal{O}_L$ might not be a finitely generated $\mathcal{O}_K$-modle. An example of this kind has been given by Emil Artin in "Questions de base minimale dans la theorie des nombres algebriques", Colloque internationale du CNRS (Paris, 1950), 19-20. Independently, Oscar Zariski has also found such examples.

PROOF. We only prove it here under the assumption that L/K is separable.
Proposition 1.4 $\implies \mathcal{O}_L$ is integrally closed.
To see that $\text{Frac}(\mathcal{O}_L) = L$, since L/K is a finite extension, we write it as a linear combination. By multiplying by an appropriate integral number a, we can make sure every coefficient is integral.

$$a\beta^n + aa_1\beta^{n-1} + \cdots + aa_n = 0$$

$$\implies (a\beta)^n + aa_1(a\beta)^{n-1} + \cdots + a^n a_n = 0$$

$$\implies a\beta \in \mathcal{O}_L \implies \beta = \frac{b}{a}, b \in \mathcal{O}_L, a \in \mathcal{O}_K.$$

Let $0 \neq Q \subset \mathcal{O}_L$ bea prime ideal. Suppose $\alpha \in Q \setminus \{0\}$ and $\exists a_1, \cdots, a_n \in \mathcal{O}_K$ such that $\alpha^n + a_1\alpha^{n-1} + \cdots a_n = 0\,(1)$.
WLOG we may assume $a_n \neq 0 \implies a_n \in Q \cap \mathcal{O}_K =: P \setminus \{0\}$ and P is a prime ideal in $\mathcal{O}_K$. $\mathcal{O}_K$ is a Dedekind domain, thus $P \in \text{Max}(\mathcal{O}_K)$.
Consider $\underbrace{\mathcal{O}_K/P}_{\text{field}} \to \underbrace{\mathcal{O}_L/Q}_{\text{integral domain}}$.
Since $\mathcal{O}_L$ is integral over $\mathcal{O}_K$, it follows that $\mathcal{O}_L/Q$ is integral over $\mathcal{O}_K/P$ by taking modulo on equation (1).
$\implies \forall \beta \in \mathcal{O}_L/Q : (\mathcal{O}_K/P)[\beta]$ is a finite dimensonal vector space over the field $\mathcal{O}_K/P$. Since $(\mathcal{O}_K/P)[\beta] \subseteq \mathcal{O}_L/Q$, an integral domain, multiplication is injective and thus bijective. Thus $(\mathcal{O}_K/P)[\beta]$ must be a field. This implies that $\mathcal{O}_L/Q$ is a field.
Thus, $Q \in \text{Max}(L)$.
It shows that all nonzero prime ideals are maximal. Now we need to show that $\mathcal{O}_L$ is noetherian. We use the separable condition here.
L/K separable $\overset{1.9}{\implies} d(\alpha_1, \cdots, \alpha_n) \neq 0$ for any basis $(\alpha_1, \cdots, \alpha_n)$ of L/K.
Let $(\alpha_1, \cdots, \alpha_n)$ be such a basis with elements $\alpha_i \in \mathcal{O}_L$.
Lemma 1.10 $\implies \underbrace{d(\alpha_1, \cdots, \alpha_n)}_{\neq 0} \cdot \mathcal{O}_L \subset \mathcal{O}_K \alpha_1 + \cdots + \mathcal{O}_K \alpha_n$

$\implies \mathcal{O}_L \subset$ (f.g. $\mathcal{O}_K$-module). Since $\mathcal{O}_K$ is noetherian, $\mathcal{O}_L$ is finitely generated as $\mathcal{O}_K$-module.
$\implies \mathcal{O}_L$ is finitely generated as $\mathcal{O}_K$-algebra. Thus, $\mathcal{O}_L$ is noetherian. $\qquad \square$

LEMMA 7.2. $\forall P \in \text{Max}(\mathcal{O}_K)$ we have:

    i) $P \cdot \mathcal{O}_L \subsetneq \mathcal{O}_L$.
    ii) $P \cdot \mathcal{O}_L \cap \mathcal{O}_K = P$.

PROOF.   i) Theorem 2.4 $\implies P \neq P^2 \implies \exists \pi \in P \setminus P^2$. We write $\pi \cdot \mathcal{O}_K = P \cdot I \implies$ $I \subsetneq P \implies P + I = \mathcal{O}_K$ with $b + s = 1$ with $b \in P, s \in I$.

Then, $s \notin P$ and $sP \subset IP = \pi\mathcal{O}_K$.

$\implies s\mathcal{O}_L = s(P\mathcal{O}_L) = (sP)\mathcal{O}_L \subset \pi\mathcal{O}_L$.

$\implies \exists x \in \mathcal{O}_L \cap K = \mathcal{O}_K; s = \pi x \implies s \in \pi\mathcal{O}_K \subset P$.

This is a contradiction. So, $P\mathcal{O}_L = \mathcal{O}_L$ condition cannot be true. Hence, $P\mathcal{O}_L \subsetneq \mathcal{O}_L$.

Tuesday, 10/8/2024

ii) We have $P \subseteq P \cdot \mathcal{O}_L \cap \mathcal{O}_K$.

If $P \subsetneq P \cdot \mathcal{O}_K \cap \mathcal{O}_K$ then $P\mathcal{O}_L \cap \mathcal{O}_K = (1) \implies 1 \in P\mathcal{O}_L$ which contradicts i. $\qquad\square$

In the following, consider $P \in \mathrm{Max}(\mathcal{O}_K)$ and write $P\mathcal{O}_L = Q_1^{e_1} \cdots Q_r^{e_r}$ with pairwise distinct $Q_i \in \mathrm{Max}(\mathcal{O}_L)$ and $e_i > 0$. Define:

$$e_i =: \underline{\text{ramification index}} \text{ of } Q_i \text{ over } P$$

$$f_i := [\mathcal{O}_L/Q_i : \mathcal{O}_K/P](<\infty\text{by 7.1}) =: \underline{\text{residue class degree}}$$

THEOREM 7.3. If L/K is separable then the $\underline{\text{fundamental equation}}$ holds:

$$\sum_{i=1}^{r} e_i f_i = n = [L : K]$$

PROOF. Chinese Remainder Theorem implies $\mathcal{O}_L/P\mathcal{O}_L \cong \prod_{i=1}^{r} \mathcal{O}_L/Q_i^{e_i}$. Consider the field $k := \mathcal{O}_K/P$.

It suffices to show that $\dim_K(\mathcal{O}_L/P\mathcal{O}_L) = n$ and $\forall 1 \leq i \leq r : \dim_k(\mathcal{O}_L/Q_i^{e_i}) = e_i f_i$.

Consider $\omega_1, \cdots, \omega_n \in \mathcal{O}_L$ such that $\overline{\omega}_1 := P\mathcal{O}_L, \cdots, \overline{\omega}_m := \omega_m + P\mathcal{O}_L \in \mathcal{O}_L/P\mathcal{O}_L$ are a k-basis of $\mathcal{O}_L/P\mathcal{O}_L$.

Suppose $(\omega_1, \cdots, \omega_m)$ was K-linearly dependent. Then, $\exists a_1, \cdots, a_m \in K$ not all zero such that

$$\sum_{i=1}^{m} a_i \omega_i = 0 \quad (1)$$

Consider the nonzero fractional ideal $I := \sum_{i=1}^{m} \mathcal{O}_K \cdot a_i \subset K$.

2.7 $\implies \exists a \in I^{-1} \setminus I^{-1} \cdot P \implies aI \not\subset P \implies \exists i : aa_i \notin P$ (2).

Since $a \in I^{-1}, a_i \in I, aa_i \in \mathcal{O}_K$.

$$(1) \implies \sum_{i=1}^{m} \underbrace{(aa_i)}_{\in\mathcal{O}_K} \underbrace{\omega_i}_{\in\mathcal{O}_L} = 0$$

Thus, in $\mathcal{O}_L/P\mathcal{O}_K$:

$$\sum_{i=1}^{m} \overline{aa_i} \underbrace{\overline{\omega}_i}_{\text{basis}} = 0_{\mathcal{O}_L/P\mathcal{O}_L}$$

Therefore, $\overline{aa_i} = 0_k \implies aa_i \in P$ which is a contradiction to (2).

Now consider $M := \mathcal{O}_K \omega_1 + \cdots + \mathcal{O}_K \omega_m \subseteq \mathcal{O}_L$ and set $N := \mathcal{O}_L/M$.

$\overline{\omega}_1, \cdots \overline{\omega}_m$ generate $\mathcal{O}_L/P\mathcal{O}_L$ as a k-vector space. Consider arbitrary $\beta \in \mathcal{O}_L$, then there is $\overline{\beta} := \beta + P\mathcal{O}_L = \sum_{i=1}^{m} \overline{a}_i \overline{\omega}_i$ where $a_i \in \mathcal{O}_K, \overline{a}_i = a_i + P$. Then $\beta - \underbrace{\sum_{i=1}^{m} a_i \omega_i}_{\in M} + P\mathcal{O}_L = 0_{\mathcal{O}_L/P\mathcal{O}_L}$.

Thus,

$$\mathcal{O}_L = M + P\mathcal{O}_L$$

Apply Nakayama's Lemma:

Written by Thanic Nur Samin

$$\implies PN = (P\mathcal{O}_L + M)/M = \mathcal{O}_L/M = N$$

Also, $M = \sum_{i=1}^m \mathcal{O}_K \omega_i$ therefore $m \le \dim_K(KM) \le m$.

Let $\alpha_1, \cdots, \alpha_s$ be generators of N as $\mathcal{O}_K$-module.

$$PN = N \implies a_i = \sum_{j=1}^s a_{ij} a_j \quad (3)$$

Set $A = I_s - (a_{ij})_{1 \le i,j \le s}$. Then,

$$A \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix} \quad (4)$$

Let $B = A^{\mathrm{adj}}$ be the adjugate matrix of A. Multiplying on both sides, we see:

$$\det(A) \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_s \end{bmatrix} = BA \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_s \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}$$

Thus, $\det(A)\mathcal{O}_L \subset M$.

However, $A = I_s - (\underbrace{a_{ij}}_{\in P})$ so $A \equiv I \pmod{P}$.

Therefore, $\det(A) \pmod{P} = \det(A \pmod{P}) = 1$.

Thus $\det(A) \ne 0$ in K.

Thus, $KM = K \cdot \mathcal{O}_K = L \implies m = n = [L : K]$.

Therefore, $m = n = [L : K]$. Then,

$$[L : K] = n = m = \dim_k(\mathcal{O}_K/P\mathcal{O}_L) \underset{CRT}{=} \sum_{i=1}^r (\mathcal{O}_L/Q_i^{e_i}) \underset{HW4}{=} \sum_{i=1}^r [\mathcal{O}_L/Q_i : k] \cdot e_i = \sum_{i=1}^r e_i f_i$$

$\square$

THEOREM 7.4 (Dedekind). Let L/K be a finite separable extension and $\theta \in \mathcal{O}_L$ be such that $L = K(\theta)$ and let $C = \{\alpha \in \mathcal{O}_L \mid \alpha \cdot \mathcal{O}_L \subset \mathcal{O}_K[\theta]\}$ be the conductor of $\mathcal{O}_K[\theta]$. Let $\mu(x) = \mu_{\theta,K}(x) \in \mathcal{O}_K[x]$ be the minimal polynomial of θ over K. Choose $P \in \mathrm{Max}(\mathcal{O}_K)$ such that $P \cdot \mathcal{O}_L + C = \mathcal{O}_L$. Then, if

$$\mu(x) \mod P = \overline{\mu}_1(x)^{e_1} \cdots \overline{\mu}_r(x)^{e_r}$$

with pairwise distinct monic irreducible polynomials $\overline{\mu}_i(x) \in (\mathcal{O}_K/P)[x]$ then:

$$P \cdot \mathcal{O}_L = Q_1^{e_1} \cdots Q_r^{e_r}$$

with pairwise distinct maximal ideals and:

$$Q_i = P \cdot \mathcal{O}_L + \mu_i(\theta) \cdot \mathcal{O}_L$$

where $\mu_i(x) \in \mathcal{O}_K(x)$ is any lift of $\overline{\mu}_i$.

PROOF. Same as the proof of theorem 2.9. $\square$

Again suppose $P \cdot \mathcal{O}_L = Q_1^{e_1} \cdots Q_r^{e_r}$ be the prime factorization of $P \cdot \mathcal{O}_L$ for $P \in \mathrm{Max}(\mathcal{O}_K)$.
Q_i is called:

- <u>unramified</u> over K if $e_i = 1$ and if residue field extension $\mathcal{O}_L/Q_i$ of $\mathcal{O}_K/P$ is separable.
- <u>ramified</u> otherwise.
- <u>purely ramified</u> if $e_i > 1$ and $[\mathcal{O}_L/Q_i : \mathcal{O}_K/P] = f_i = 1$.

P is called <u>unramified</u> in L if all Q_i are unramified. L/K is called <u>unramified</u> if all $P \in \mathrm{Max}(\mathcal{O}_K)$ are unramified in L.

THEOREM 7.5. Let L/K be finite separable. Then there are only at most finitely many $P \in \mathrm{Max}(\mathcal{O}_K)$ which ramify in L.

Written by Thanic Nur Samin

SKETCH. Suppose $\theta \in \mathcal{O}_L$ is a primitive element, then $C =$ conductor of $\mathcal{O}_K[\theta]$. The discriminant argument implies this is a non-zero ideal, thus it can be written as a product of prime ideals. Therefore, it is contained in only finitely many maximal ideals $Q \in \text{Max}(\mathcal{O}_L)$.

There are only finitely many maximal ideals in $\mathcal{O}_K$ that is contained in some Q. Eliminating these, we reduce to the ideals $P \in \text{Max}(\mathcal{O}_K)$ such that $P \cdot \mathcal{O}_L + C = \mathcal{O}_L$.

Whether they ramify or not is then determined by theorem 7.4. That is dependant on the discriminant of the minimal polynomial vanishing. So we eliminate $P \in \text{Max}(\mathcal{O}_K)$ such that $\text{disc}(\mu_{\theta,K}(x)) \in P$. $\qquad\square$

CHAPTER 8

Ramification Theory

In this chapter, $\mathcal{O}_K$ is a dedekind domain, $K = \text{Frac}(\mathcal{O}_K)$ and L/K is a finite Galois (thus separable) extension and $\mathcal{O}_K$ = integral closure of $\mathcal{O}_K$ in L.
Let $G = \text{Gal}(L|K)$. Then,

1) G acts on $\mathcal{O}_L$. If $\beta \in \mathcal{O}_L$ then β is a root of some monic polynomial, and $\sigma(\beta)$ must be a root of the same polynomial!
2) If $Q \in \text{Max}(\mathcal{O}_L)$ then $\forall \sigma \in G : \sigma(Q) \in \text{Max}(\mathcal{O}_L)$. It is an ideal by checking the definition, and it is maximal since $\mathcal{O}_L/Q \underset{\overline{a}}{\overset{\cong}{\to}} \mathcal{O}_L/\sigma(Q)$.
   $\underset{\overline{a} \mapsto \overline{\sigma(a)}}{}$

   If $P = Q \cap \mathcal{O}_K \implies \sigma(Q) \cap \mathcal{O}_K = \sigma(Q \cap \mathcal{O}_K) = \sigma(P) = P$.

Thus, G acts on the sets of $Q \in \text{Max}(\mathcal{O}_L)$ which lie over $P \in \text{Max}(\mathcal{O}_K)$. These are exactly the maximal ideals in the prime factorization of $P \cdot \mathcal{O}_L$.

Thursday, 10/10/2024

If $P \in \text{Max}(\mathcal{O}_K)$, then we set

$$\text{Max}(\mathcal{O}_L \mid P) = \{Q \in \text{Max}(\mathcal{O}_L) \mid Q \cap \mathcal{O}_K = P\}$$

$Q \in \text{Max}(\mathcal{O}_L|P)$ is said to "lie over" (or divide) P: $Q \mid P$.
G acts on $\text{Max}(\mathcal{O}_L \mid P) : Q \in \text{Max}(\mathcal{O}_L \mid P) \implies \sigma(Q) \cap \mathcal{O}_K = Q \cap \mathcal{O}_K = P$.

THEOREM 8.1. G acts transitively on $\text{Max}(\mathcal{O}_L \mid P)$.

PROOF. Suppose $Q' \in \text{Max}(\mathcal{O}_L \mid P) \setminus G \cdot Q$ for some $Q \in \text{Max}(\mathcal{O}_L \mid P)$.
Chinese Remainder Theorem $\implies \exists x \in \mathcal{O}_L : (x \equiv 0 \pmod{Q'}$ and $\forall \sigma \in G : x \equiv 1 \pmod{\sigma(Q)})$.

$$\implies N_{L|K}(x) = \prod_{\sigma \in G} \sigma(x) = x \prod_{\substack{\sigma \in G \\ \sigma \neq \text{id}}} \sigma(x) \in Q' \cap (K \cap \mathcal{O}_L) = Q' \cap \mathcal{O}_K = P \ (1)$$

Thus, $\forall \sigma \in G : x \notin \sigma^{-1}(Q) \implies \sigma(x) \notin Q \implies N_{L|K}(x) \notin Q$. This contradicts (1) since $P \subset Q$. $\square$

DEFINITION. Given $Q \in \text{Max}(\mathcal{O}_L)$ we call

$$G_Q = \{\sigma \in G \mid \sigma(Q) = Q\}$$

the <u>decomposition group</u> of Q. The fixed field

$$Z_Q := L^{G_Q} = \{x \in L \mid G_Q \cdot x = x\}$$

is called the <u>decomposition field</u> of Q.
Z comes from the German word 'Zerlegung' roughly meaning decomposition.

<u>Note</u>: $\text{Gal}(L/Z_Q) = G_Q$.
<u>Remark</u>:

1) The groups G_Q for $Q \in \text{Max}(\mathcal{O}_L \mid P)$ are all conjugate in G.
2) $\forall Q \in \text{Max}(\mathcal{O}_L \mid P), [G : G_Q] = |\text{Max}(\mathcal{O}_L \mid P)| = r$ if $P = Q_1^{e_1} \cdots Q_r^{e_r}$ with pairwise distinct $Q_i \in \text{Max}(\mathcal{O}_L)$.
3) $G_Q = \{1\} \iff \underset{=[L:K]}{|G|} = |\text{Max}(\mathcal{O}_L \mid P)| \underset{\text{fundamental eqn}}{\implies} e_1 = \cdots = e_r = 1 = f_1 = \cdots = f_r \iff P$ is totally split.
4) $G_Q = G \iff |\text{Max}(\mathcal{O}_L \mid P)| = 1$.

40

PROPOSITION 8.2. If $P \in \mathrm{Max}(\mathcal{O}_K)$ and $P\mathcal{O}_L = Q_1^{e_1} \cdots Q_r^{e_r}$ with pairwise distinct $Q_i \in \mathrm{Max}(\mathcal{O}_L)$, then $e_1 = \cdots = e_r$ and $f_1 = \cdots = f_r$.

PROOF.
$$\implies P\mathcal{O}_L = Q_1^{e_1} \cdots Q_r^{e_r} = \sigma(P\mathcal{O}_L) = Q_i^{e_1} \sigma(Q_2)^{e_2} \cdots \sigma(Q_r)^{e_r}$$
This happens since $\sigma(Q^e) = \sigma(Q)^e$.
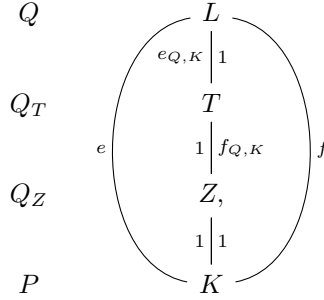This implies that $e_1 = e_i$.
Moreover, $\mathcal{O}_L/Q_1 \xrightarrow{\cong} \mathcal{O}_L/\sigma(Q_1) = \mathcal{O}_L/Q_i$ is an isomorphism of $\mathcal{O}_K/P$ vector spaces.

$$\implies f_1 = [\mathcal{O}_L/Q_1 : \mathcal{O}_K/P] = [\mathcal{O}_L/Q_i : \mathcal{O}_K/P] = f_i$$

$\square$

PROPOSITION 8.3. Let $Q \in \mathrm{Max}(\mathcal{O}_L)$ and $Z = Z_Q = L^{G_Q}$. Set $Q_Z := Q \cap \mathcal{O}_Z$ where $\mathcal{O}_Z$ is the integral closure of $\mathcal{O}_K$ in Z and $P = Q \cap \mathcal{O}_K$. Then,

   i) Q is the only prime ideal lying over Q_Z.
   ii) $Q_Z\mathcal{O}_L = Q^e$ where $e = e_{Q,K} = $ ramification index of Q over K and $f_{Q,Z} = [\mathcal{O}_L/Q : \mathcal{O}_Z/Q_Z] = f_{Q,K}(= [\mathcal{O}_L/Q : \mathcal{O}_K/P])$
   iii) $f_{Q_Z,K} = 1 = e_{Q_Z,K}$.

$$
\begin{array}{ccc}
Q & & L \\[4pt]
 & & \ \ e_{Q,K}\Big| 1 \\[4pt]
Q_T & & T \\[4pt]
 & e\left(\begin{array}{c} \\ 1\Big| f_{Q,K} \\ \\ 1\Big| 1 \end{array}\right)f & \\[4pt]
Q_Z & & Z, \\[4pt]
P & & K
\end{array}
$$

PROOF. i) Galois theory: $\mathrm{Gal}(L/Z) = G_Q$.
Theorem 8.1 $\implies$ G_Q acts transitively on $\mathrm{Max}(\mathcal{O}_L \mid Q_Z)(\ni Q)$ $\implies$ $\mathrm{Max}(\mathcal{O}_L \mid Q_Z) = G_Q \cdot Q = \{Q\}$, hence (i).
ii) By the fundamental equation 7.3: $[L : K]e_{Q,K} \cdot f_{Q,K} [G \cdot G_Q]$
$\implies [L : K] = |G| = [G : G_Q]|G_Q| = [G : G_Q][L : Z]$.
$\implies [L : Z] = e_{Q,K}f_{Q,K}$.
Further: $P \cdot \mathcal{O}_Z = Q_Z^{e_{Q_Z,K}} \cdot (\cdots)$

$$\implies P\mathcal{O}_L = (P\mathcal{O}_Z) \cdot \mathcal{O}_L = (Q_Z \cdot \mathcal{O}_L)^{e_{Q_Z,K}}(\cdots) \underset{(i)}{=} (Q^{e_{Q,Z}})^{e_{Q_Z,K}}(\underbrace{\cdots}_{\substack{Q \text{ does not} \\ \text{appear here}}})$$

$$\implies e_{Q,K} = e_{Q,Z}e_{Q_Z,K} \ (2)$$

Also:

$$f_{Q,K} = [\mathcal{O}_L/Q : \mathcal{O}_K/P] = [\mathcal{O}_L/Q : \mathcal{O}_Z/Q_Z][\mathcal{O}_Z/Q_Z : \mathcal{O}_K/P] = f_{Q,Z}f_{Q_Z,K} \ (3)$$

Now:

$$e_{Q,Z}f_{Q,Z} \underset{7.3}{\overset{(i)}{=}} [L : Z] \underset{(1)}{=} e_{Q,K}f_{Q,K} \underset{(3)}{\overset{(2)}{=}} e_{Q,Z}e_{Q_Z,K}f_{Q,Z}f_{Q_Z,K}$$

$$\implies 1 = e_{Q_Z,K}f_{Q_Z,K}$$

$$Q_Z\mathcal{O}_L = Q^e \implies e_{Q_Z,K} = 1 = f_{Q_Z,K}$$

Thus proving (ii) and (iii).

$\square$

$$P\mathcal{O}_Z = Q_Z(\cdots)$$

$$\tilde{k}$$
$$\cup$$
$$\tilde{k}_{\text{sep}} \quad \circlearrowleft \tau$$
$$\cup$$
$$k$$

THEOREM 8.4.   1) The residue field extension $\mathcal{O}_L/Q/\mathcal{O}_K/P$ is normal.
          2) The homomorphism:

$$\begin{array}{ccc} G_Q & \to & \text{Aut}(\mathcal{O}_L/Q \mid \mathcal{O}_K/P) \\ \sigma & \mapsto & \overline{\sigma} \end{array}$$

with $\overline{\sigma}(a + Q) = \sigma(a) + Q$ is $\underline{\text{surjective}}$.

PROOF.   1) Proposition 8.3 $\implies k \coloneqq k(P) = \mathcal{O}_K/P \overset{\cong}{\to} \mathcal{O}_Z/Q_Z \ (f_{Q_z,K} = 1)$. WLOG we may assume that $K = Z$ and $G = G_Q$
          Let $\overline{\theta} = \theta + Q \in k(Q) = \mathcal{O}_L/Q$ be any element, let $\mu(x) = \mu_{\theta,K}(x)$ be the minimal polynomial of θ over K. Set $\overline{\mu}(x) = \mu(x) \mod P$.
          Let $\mu_{\overline{\theta}}(x) \in k[x]$ be the minimal polynomial of $\overline{\theta}$ over k

$$\overline{\mu}(\overline{\theta}) = 0 \implies \mu_{\overline{\theta}} \mid \overline{\mu}$$

          L/K is Galois, so $\mu = \mu_\theta$ decomposes into linear polynomials in $\mathcal{O}_L[x]$.
          $\implies \overline{\mu}$ decomposes into monic linear polynomials in $k(Q)[x]$
          $\implies \mu_{\overline{\theta}}$ decomposes into monic linear polynomials in $k(Q)[x]$
          $\implies$ all roots of $\mu_{\overline{\theta}}$ are in $k(Q) \implies k(Q)$ is normal over k.
          2) Now let $\overline{\theta}$ be a $\underline{\text{primitive}}$ element for the maximal seperable subextension $k(Q)_{\text{sep}}$ over k. Thus, $k(Q)_{\text{sep}} = k(\overline{\theta})$
          Given $\tau \in \text{Aut}(k(Q) \mid k) = \text{Gal}(k(\overline{\theta}) \mid k) \implies \tau(\overline{\theta})$ is a root of $\mu_{\overline{\theta}}(x) \in k[x]$.
          $\mu_{\overline{\theta}} \mid \overline{\mu_\theta} \implies \exists \alpha \in \mathcal{O}_L : (\mu_\theta(\alpha) = 0$ and $\overline{\alpha} = \alpha + Q = \tau(\overline{\theta}))$.
          μ_θ is irreducible, thus $\exists \sigma \in G : \sigma(\theta) = \alpha$.
          Then, $\overline{\sigma}(\overline{\theta}) = \tau(\overline{\theta}) \implies \overline{\sigma} = \tau$

$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad$ $\square$

DEFINITION. $I_Q = \ker(G_Q \to \text{Aut}(k(\theta) \mid k(P)))$ is called the $\underline{\text{intertia group of}}$ (or at) Q and $T_Q \coloneqq L^{I_Q}$ is called the $\underline{\text{intertia field}}$ of (or at) Q.
In other words: $I_Q = \{\sigma \in G_Q \mid \forall \alpha \in \mathcal{O}_L, \sigma(\alpha) \equiv \alpha \pmod{Q}\}$.

We have a tower of fields:

$$
\begin{array}{cc}
\begin{array}{c} L \\ I_Q \left(\begin{array}{c} \| \\ \\ T \\ G_Q/I_Q \left(\begin{array}{c} \| \\ \\ Z \\ | \\ \\ K \end{array} \right) \end{array} \right) G_Q \\ G \end{array} &
\begin{array}{c} Q \\ \\ \\ Q_T \\ \\ \\ Q_Z \\ \\ \\ P \end{array}
\end{array}
$$

$$G_Q/I_Q \cong \text{Aut}(k(Q)/k(P))$$

Tuesday, 10/15/2024

Suppose $Q \mid P$.

G_Q = decomposition group = $\{\sigma \in G \mid \sigma(Q) = Q\} = \mathrm{Stab}(Q)$.

$G_Q \stackrel{8.4}{\twoheadrightarrow} \mathrm{Aut}(k(Q)/k(P))$

$I_Q = \ker(G_Q \to \mathrm{Aut}(k(Q)/k(P))), T_Q = L^{I_Q} \supset L^{G_Q} = Z_Q$

I_Q = inertial subgroup at Q

T_Q = inertia field

Z_Q = decomposotion field

$$1 \to I_Q \to G_Q \to \mathrm{Aut}(k(Q)/k(P)) \to 1$$

$\mathrm{Gal}(L/Z_Q) = G_Q$

$\mathrm{Gal}(L/T_Q) = I_Q$

$\mathrm{Gal}(T_Q/Z_Q) \cong G_Q/I_Q$

THEOREM 8.5.   i) The extention T_Q/Z_Q is Galois.
$\qquad \mathrm{Gal}(T_Q/Z_Q) \cong G_Q/I_Q \cong \mathrm{Aut}(k(Q)/k(P))$.

   ii) If the extention $k(Q)/k(P)$ is separable, then:

    a) $f_{Q,K} = [G_Q : I_Q] = [T_Q : Z_q]$

    b) $e_{Q,K} = |I_Q| = [L : T_Q]$

     We have for the prime ideal $Q_T := \mathcal{O}_T \cap Q$:

    c) $e_{Q,T} = e_{Q,K}$ and $f_{Q,T_Q} = 1$

    d) $e_{Q_T,K} = 1$ and $f_{Q_T,K} = f_{Q,K}(= f_{Q_T,Z})$

Note; $f_{Q,K} = f_{Q,T} \cdot f_{Q_T,Z} \cdot f_{Q_Z,K}$.

Since $[k(Q) : k[P]] = [k(Q) : k(Q_T)][k(Q_T) : k(Q_Z)][k(Q_Z) : k(P)]$.

$f_{Q_T,K} = f_{Q_T,Z}f_{Q_Z,K}, Q_K = P$.

  PROOF.   i) we already have this.

   ii) Set $k = k(P), T = T_Q, Z = Z_Q$. Then $f_{Q,K} = [k(Q) : k] = |\mathrm{Gal}(k(Q) \mid k)| = [G_Q : I_Q] = [T : Z]$ which proves part a.

    Moreover, $e_{Q,K}f_{Q,K} \stackrel{8.3}{=} e_{Q,Z}f_{Q,Z} \stackrel{7.3}{=} [L : Z] = [L : T][T : Z] \stackrel{(a)}{=} [L : T]f_{Q,K}$ (1)
$\implies e_{Q,K} = [L : T] = |I_Q|$, hence (b) is proved.

    Consider L/T and note: $Q_Z \subset Q_T \subset Q \implies \mathrm{Max}(\mathcal{O}_L \mid Q_T) = \{Q\}$.

    Again, $\stackrel{7.3}{\implies} [L : T] = e_{Q,T}f_{Q,T}$ (2).

    $I_Q = \mathrm{Gal}(L \mid T) = \mathrm{Gal}(L \mid T)_Q \stackrel{8.4}{\twoheadrightarrow} \mathrm{Aut}(k(Q) \mid k(Q_T)) \underset{\mathrm{assumption}}{=} \mathrm{Gal}(k(Q) \mid k(Q_T))$

  acts trivially on $k(Q)$ over $k(Q_T)$.

$$
\begin{array}{ccc}
I_Q = \mathrm{Gal}(L \mid T) = \mathrm{Gal}(L \mid T)_Q & \xrightarrow{\ 8.4\ } & \mathrm{Aut}(k(Q) \mid k(Q_T)) = \mathrm{Gal}(k(Q) \mid k(Q_T)) \\
\downarrow & & \downarrow \\
\mathrm{Gal}(L \mid Z) \qquad = \underset{\subset \mathrm{Gal}(L \mid K)}{G_Q} & \longrightarrow & \mathrm{Aut}(k(Q) \mid K)
\end{array}
$$

Then, $k(Q) = k(Q_T)$.

$\implies f_{Q,T} = 1 \stackrel{(2)}{\implies} e_{Q,T} = [L : T] = e_{Q,K}$. hence c is proved.

Proof of 8.3 $\implies e_{Q,K} = e_{Q,T}e_{Q_T,K}$ and $f_{Q,K} = f_{Q,T}f_{Q_T,K}$. Since $f_{Q,T} = 1$ we have $f_{Q,K} = f_{Q_T,K}$, and since $e_{Q,K} = e_{Q,T}$ we have $e_{Q_T,K} = 1$.

                          $\square$

Written by Thanic Nur Samin

Absolute Values on Fields

<u>Reference</u>: Lorenz, Algebra II, sec. 23 [IUCAT].
<u>Notation</u>: In this chapter, K, L, M will always denote fields.

DEFINITION. A map $|\cdot| : K \to \mathbb{R}_{\geq 0}$ is called an <u>absolute value</u> if:
1) $|x| = 0 \iff x = 0$
2) $\forall x, y \in K : |xy| = |x| \cdot |y|$
3) $\forall x, y \in K : |x + y| \leq |x| + |y|$ [triangle inequality].

The set $|K^\times| = \{n|x| \mid x \in K^\times\}$ is called the <u>value group</u> of $|\cdot|$.

<u>Remark</u>: $|1_K| = 1$ and $|x^{-1}| = |x|^{-1}$
<u>Example</u>:
1) Let $K = \mathbb{Q}$, then $|a + ib|_\infty = |a + ib|_\mathbb{C} = \sqrt{a^2 + b^2}$ is an absolute value.
   We also write $|\cdot| = |\cdot|_\infty\big|_\mathbb{R}$ and $|\cdot|_\infty = |\cdot|_\infty\big|_\mathbb{Q}$.
2) Let K be any field, then:
$$|x| = \begin{cases} 0, & \text{if } x = 0; \\ 1, & \text{if } x \neq 0. \end{cases}$$
   is an absolute value on K called the <u>trivial absolute value</u>.
3) if $|\cdot|$ is an absolute value and $\rho \in (0, 1]$ there we have for $s, r \in \mathbb{R}_{>0}$:
$$\frac{s^\rho + r^\rho}{(s + r)^\rho} = \left(\frac{s}{s + r}\right)^\rho + \left(\frac{r}{s + r}\right)^\rho \geq \frac{s}{s + r} + \frac{r}{s + r} \geq 1$$
$$\implies s^\rho + r^\rho \geq (s + r)^\rho \quad \text{also true if } r = 0 \text{ or } s = 0$$

$$\implies |x + y|^\rho \leq (|x| + |y|)^\rho \leq |x|^\rho + |y|^\rho$$
   It follows that $|\cdot|^\rho$ is again an absolute value.
4) Let $D > 1$ be square-free integer. On $K = \mathbb{Q}(\sqrt{D})$ the maps $|a + b\sqrt{D}|_1 := |a + b\sqrt{D}|_\infty, |a + b\sqrt{D}|_2 := |a - b\sqrt{D}|_\infty$ are absolute values.
5) Let p be a prime. Write $x \in \mathbb{Q}^\times$ as $x = p^m \frac{a}{b}$ with $\gcd(p, a) = \gcd(p, b) = 1$ and set $v_p(x) = m$ and $v_p(0) = \infty$.
   Exercise (HW9): $\forall x, y \in \mathbb{Q}$: we have:
   a) $v_p(xy) = v_p(x) + v_p(y)$
   b) $v_p(x, y) \geq \min(v_p(x), v_p(y))$
   v_p is called the p-adic valuation.
   Then one obtains from the p-adic valuation an absolute value on $\mathbb{Q}$:
   $$|x|_p = \begin{cases} p^{-v_p(x)}, & \text{if } x \neq 0; \\ 0, & \text{if } x = 0. \end{cases} \text{ called } \underline{\text{the } p\text{-adic absolute value}}.$$
   Property (b) implies the strong triangle inequality: $|x + y|_p \leq \max\{|x|_p, |y|_p\} \leq |x|_p + |y|_p$

9.1. Topology

Let $|\cdot|$ be an absolute value on K. Then, $d(x, y) := |x - y|$ is a metric on K and (K, d) is a metric space.
The associated <u>metric topology</u> on K is the one which has the discs:

$$B^-(a, \varepsilon) := \{ x \in K \mid |x - a| < \varepsilon \}$$

as a basis of the topology, where a runs through K and $\varepsilon \in \mathbb{R}_{>0}$.

The maps $K \times K \xrightarrow{+} K, K \times K \xrightarrow{\cdot} K$ and $K^\times \xrightarrow{x \mapsto x^{-1}} K^\times$ are the $\underline{\text{continuous maps}}$ under this topology.

A sequence $(x_n)_{n \geq 0}$ in K $\underline{\text{converges to } a \in K}$ if $\lim_{n \to \infty} |x_n - a| = 0$.

A $\underline{\text{null sequence}}$ is a sequence which converges to 0_K.

DEFINITION. Two absolute values $|\cdot|_1, |\cdot|_2$ are said to be $\underline{\text{equivalent}}$ if every null sequence for $|\cdot|_1$ is a null sequence for $|\cdot|_2$ and vice versa.

$\underline{\text{Remark}}$: $|\cdot|_1$ and $|\cdot|_2$ are equivalent $\iff$ the topologies on K associated to $|\cdot|_1$ and $|\cdot|_2$ are the same (HW9).

$\underline{\text{Example}}$: We give example of absolute values that are not equivalent.

Suppose p is a prime. Then, $(p^n)_{n \geq 1}$ is a null sequence for $|\cdot|_p$, but unbounded for $|\cdot|_\infty$ and thus not a null sequene. It is not a null sequence for any other l-adic absolute value $|\cdot|_l$ with a prime $l \neq p$.

$\implies$ the set of $\{|\cdot|_p \mid p \text{ is a prime}\} \cup \{|\cdot|_\infty\}$ containsonly inequivalent absolute values.

LEMMA 9.1. Suppose $|\cdot|_1$ and $|\cdot|_2$ are two non-trivial absolute values on K. Then TFAE:

    i) $|\cdot|_1$ and $|\cdot|_2$ are equivalent.
    ii) $\exists \rho \in \mathbb{R}_{>0}$ such that $|\cdot|_2 = |\cdot|_1^\rho$
    iii) $\forall a \in K : |a|_1 < 1 \iff |a|_2 < 1$.

    PROOF. ii $\implies$ i is clear from the zero sequence condition.

i $\implies$ iii: if $|a|_1 < 1 \implies (a^n)_{n \geq 1}$ is a null sequence for $|\cdot|_1 \implies (a^n)_{n \geq 1}$ is a null sequence for $|\cdot|_2 \implies |a^n|_2 \to 0 \implies |a|_2 < 1$ and vice versa.

Thursday, 10/17/2024

iii $\implies$ ii: $|\cdot|$, non-trivial $\implies \exists c \in K^\times : |c|_1 > 1 \implies |c^{-1}|_1 < 1 \underset{\text{iii}}{\implies} |c^{-1}|_2 < 1 \implies \exists \rho > 0 :$ $|c|_2 = |c|_1^\rho$

Given $a \in K^\times$ and write $|a|_1 = |c|_1^\alpha$ for some $\alpha \in \mathbb{R}$. For $m, n \in \mathbb{Z}, n \neq 0$ and $\frac{m}{n} > \alpha$ we have:

$$|a|_1 = |c|_1^\alpha < |c|_1^{\frac{m}{n}} \implies \left| \frac{a^n}{c^m} \right|_1 < 1 \underset{\text{iii}}{\implies} \left| \frac{a^n}{c^m} \right|_2 < 1 \implies |a|_2 < |c|_2^{\frac{m}{n}}$$

Similarly, if $\frac{m}{n} < \alpha$ we find:

$$|a|_2 > |c|_2^{\frac{m}{n}}$$

Choose a sequence of rational numbers $\frac{m}{n}$ converging to α. Then,

$$|a|_2 = |c|_2^\alpha = |c|_\rho^{\rho \alpha} = |a|_1^\rho$$

$\square$

$\underline{\text{Remark}}$: 9.1 $\implies$ equivalent absolute values induce the same topology on K. The converse is also true: if the topology defined on K by two absolute values is the same, then they're equivalent.

DEFINITION. An absolute value $|\cdot|$ on K is called $\underline{\text{archimedean}}$ if $\{|n \cdot 1_K| \mid n \in \mathbb{Z}_{\geq 0}\}$ is $\underline{\text{unbounded}}$. It is called $\underline{\text{non-archimedean}}$ otherwise.

$\underline{\text{Remark}}$: "Archimedean" means $\forall x \in \mathbb{R} \exists n \in \mathbb{Z} : n \geq x$. We could also say $|x| \leq |n|$ instead, and this is where the concept comes from.

LEMMA 9.2. Let $|\cdot|$ be an absolute value on K. Then TFAE:

    i) $|\cdot|$ is non-archimedean.
    ii) $\forall n \in \mathbb{Z}_{\geq 1} : |n| \leq 1$.
    iii) $\forall a, b \in K : |a + b| \leq \max(|a|, |b|)$
    iv) $\forall \rho \in \mathbb{R}_{>0} : |\cdot|^\rho$ is an absolute value.

PROOF. Ommitted. Key idea: for i $\implies$ ii, in non-archimedean fields, we have:

$$\left| \binom{n}{k} \right| \leq C$$

for some constant C. $\square$

THEOREM 9.3. Every non-trivial absolute value on the field of rational numbers is equivalent to $|\cdot|_p$ for a unique prime p, or it is equivalent to $|\cdot|_\infty$

PROOF. <u>Case 1</u>: Suppose $|\cdot|$ is non-archimedean. $9.2 \implies \forall m \in \mathbb{Z}_{\geq 1}, |m| \leq 1$. In fact, $\forall m \in \mathbb{Z}_{\neq 0}, |m| \leq 1$.

Since $|\cdot|$ is non-trivial, there must exist some $m \in \mathbb{Z}_{>0}$ so that $|m| < 1$.

$\implies I = \{m \in \mathbb{Z} \mid |m| < 1\}$ is a non-zero ideal in $\mathbb{Z}$ by using 9.2.

Furthermore, I is a prime ideal: $|ab| < 1 \implies |a||b| < 1 \implies |a| < 1$ or $|b| < 1$.

Thus, $\exists$ prime p such that $I = (p)$.

Consider $a \in \mathbb{Z} \setminus \{0\}$ and write $a = p^m b$ where $p \nmid b$. Then $b \notin I$ and thus $|b| = 1$.

Therefore, $|a| = |p|^m = |p|_p^{m\rho}$ for some $\rho > 0 [|p|_p = \frac{1}{p}]$.

Thus $|a| = |a|_p^\rho$.

Therefore, $|x| = |x|_p^\rho$ for all $x \in \mathbb{Q}$.

<u>Case 2</u>: $|\cdot|$ is archimedean. Suppose $|\cdot|$ is <u>not</u> equivalent to $|\cdot|_\infty$.

Lemma 9.1 $\implies \exists x \in \mathbb{Q} : |x| < 1, |x|_\infty \geq 1$.

WLOG assume $x > 0$. So $x > 1$ but $|x| < 1$.

Write $x = \frac{a}{s}$ with $a, s \in \mathbb{Z}_{>0}$ with $\gcd(a, s) = 1, a > s$.

<u>Claim</u>: Every $n \in \mathbb{Z}_{\geq 0}$ can be written as:

$$n = c_0 + c_1 x + \cdots + c_r x^r \text{ with } c_i \in \mathbb{Z} \cap [0, a-1]$$

Proof of the claim is HW.

Using this, we have:

$$|n| \leq \sum_{i=0}^{r} |c_i| |x|^i \leq a \cdot \sum_{i=0}^{r} |x^i| \leq a \sum_{i=0}^{\infty} |x|^i = \frac{a}{1 - |x|}$$

This contradicts the fact that $|\cdot|$ is archimedean.

                                                                                          $\square$

<u>Exercise</u>: If $|\cdot|$ is non-archimedean and $|a| \neq |b|$ then $|a + b| = \max(|a|, |b|)$.

PROPOSITION 9.4 (Valuation Ring and Valuation ideal). Let $|\cdot|$ be a non-archimedean absolute value on K. Then,

   i) $R = \{a \in K \mid |a| \leq 1\}$ is a subring of K called the <u>valuation ring</u> of $|\cdot|$.
   ii) $K = \text{Frac}(R)$.
   iii) $P = \{a \in K \mid |a| < 1\}$ is the unique maximal ideal of R called the <u>valuation ideal</u>.
   iv) $R^\times = R \setminus P$.
   v) R/P is a field called the <u>residue field</u> of $|\cdot|$ (or of K, or of R).
   vi) $\forall a, b \in R: \quad a \mid b \quad \Longleftrightarrow \quad |b| \leq |a|$
         $ \Longleftrightarrow \exists c \in R: b = ac$

PROOF.   i) $a, b \in R \implies |a + b| \underset{9.2}{\leq} \max\{|a|, |b|\} \leq 1$ and $|ab| = |a||b| \leq 1$.

   ii) $x \in K \setminus R \implies |x| > 1 \underset{x \neq 0}{\implies} |x^{-1}| < 1 \implies x^{-1} \in R$

   iii) See next

   iv) Note: $P \subsetneq R$. Same argument as in the proof by 9.3: P is a prime ideal. Given $x \in R \setminus P \implies |x| = 1 \implies |x^{-1}| = 1 \implies x^{-1} \in R \implies x \in R^\times \implies R^\times = R \setminus P$ so P is maximal.

   v) Immediate

   vi) $a \mid b \implies \exists c \in R: b = ac \implies |b| = |a|\underset{\leq 1}{|c|} \leq |a|$.

   $$|b| \leq |a| \neq 0 \implies \left| \frac{b}{a} \right| \leq 1 \implies \frac{b}{a} \in R, b = \left(\frac{b}{a} \right) \cdot a \implies a \mid b$$

                                                                                          $\square$

<u>Example</u>: For $|\cdot|_p$ on $\mathbb{Q}$ we have:

i)

$$R = \left\{ x = \frac{a}{b} \in \mathbb{Q} \mid |x|_p \le 1 \right\} = \left\{ \frac{a}{b} \in \mathbb{Q} \mid a, b \in \mathbb{Z}, \gcd(a, b) = 1, b \notin p\mathbb{Z} \right\} = \mathbb{Z}_{(p)}$$

The localization of $\mathbb{Z}$ at (p), $(\mathbb{Z} \setminus (p))^{-1}\mathbb{Z}$.

ii) $P = p\mathbb{Z}_{(p)}$

iii) Residue field $\mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} \overset{\cong}{\to} \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ where $\frac{a}{b} \mod p\mathbb{Z}_{(p)} \mapsto (a \mod p)(b \mod p)^{-1}$.

Definition. A function $w : K \to \mathbb{R} \cup \{\infty\}$ is called a <u>valuation</u> if it has the following properties:

i) $w(x) = \infty \iff x = 0$

ii) $w(x + y) \ge \min\{w(x), w(y)\}$

iii) $w(xy) = w(x) + w(y)$

$w(K^\times)$ is called the <u>value group</u> of w.

Valuations w and v are called <u>equivalent</u> if $\forall x \in K : (w(x) > 0 \iff v(x) > 0)$.

Given a valuation w we define <u>an absolute value</u> $|\cdot|_w$ as follows

$$|x|_w := \begin{cases} e^{-w(x)}, & \text{if } x \ne 0; \\ 0, & \text{if } x = 0; \end{cases}$$

Then $|\cdot|_w$ is a non-archimedean absolute value on K.

This gives rise to a commutative diagram:

$$
\begin{Bmatrix} \text{valuations} \\ \text{on } K \end{Bmatrix}
\xrightarrow{\;\; w \mapsto |\cdot|_w \;\;}
\begin{Bmatrix} \text{non-archimedean} \\ \text{abs. values on } K \end{Bmatrix}
$$

$$\downarrow \qquad\qquad\qquad\qquad\qquad \downarrow$$

$$
\begin{Bmatrix} \text{equivalence classes} \\ \text{of valuations on } K \end{Bmatrix}
\longrightarrow
\begin{Bmatrix} \text{equivalence classes} \\ \text{of non-arch. abs. values on } K \end{Bmatrix}
$$

$$[w] \longmapsto [|\cdot|_w]$$

9.2. Completions

Fix an absolute value on K.

Definition. A sequence $(a_n)_{n \ge 0}$ in K is called a <u>Cauchy sequence w.r.t. $|\cdot|$</u> if $\forall \varepsilon > 0 \exists n_0 \forall n, m \ge n_0 : |a_n - a_m| < \varepsilon$.

We call K <u>complete</u> if every Cauchy sequence converges (in K) in which case we also call $|\cdot|$ a <u>complete</u> absolute value on K.

<u>Remark</u>:

i) Every convergent sequence is a Cauchy sequence.

ii) If $(a_n)_n$ is Cauchy in K, then $(|a_n|)_n$ is a Cauchy sequence in $\mathbb{R}$.

iii) If $(a_n)_n$ is Cauchy then it is bounded: $\exists C > 0 \forall n \ge 0 : |a_n| \le C$.

iv) If $(a_n)_n$ is Cauchy and if a subsequence $(a_{n_k})_{k \ge 0}$ is a null sequence, then $(a_n)_n$ is a null sequence.

v) The set of all Cauchy sequences:

$$\mathcal{C} = \{(a_n)_{n \ge 0} \mid (a_n)_{n \ge 0} \text{ is Cauchy in } K \text{ w.r.t. } |\cdot|\}$$

is a unital ring w.r.t. componentwise addition and multiplication.

vi) The set $\mathcal{N} \subset \mathcal{C}$ of null sequences is an ideal in $\mathcal{C}$.

Definition. A <u>completion</u> of K w.r.t. $|\cdot|$ is a pair $K^\wedge, |\cdot|^\wedge$ consisting of a field extension $K \underset{x \,\mapsto\, x}{\to} K^\wedge$ and an absolute value $|\cdot|^\wedge$ such that:

i) $\forall x \in K : |x|^\wedge = |x|$

ii) K is dense in $K^\wedge$.

iii) $K^\wedge$ is complete w.r.t. $|\cdot|^\wedge$

Written by Thanic Nur Samin

Tuesday, 10/22/2024

THEOREM 9.5.   i) $\exists$ a completion $K^\wedge, |\cdot|^\wedge$ of $(K, |\cdot|)$

   ii) If $(K_1, |\cdot|_1)$ and $K_2, |\cdot|_2$ are completions of $(K, |\cdot|)$ then there is a unique isomorphism $\sigma : K_1 \to K_2$ over K such that $\forall x \in K_1 : |\sigma(x)|_2 = |x|_1$.

PROOF. LEt $\mathcal{C}$ be the set of cauchy equences in K, $\mathcal{N}$ = set of null sequences in K. Set $K^\wedge := \mathcal{C}/\mathcal{N}$.

Claim: $K^\wedge$ is a field.

Proof of Claim:

$\mathbb{1} = (1, 1, \cdots) \in \mathcal{C}/\mathcal{N} \implies \mathcal{N} \subsetneq \mathcal{C}$. Let $(a_n)_n \in \mathcal{C}/\mathcal{N} \implies \exists \delta > 0 \exists n_0 \forall n \geq n_0 : |a_n| \geq \delta$.

Set $b_n = \begin{cases} 1, & \text{if } n < n_0; \\ \dfrac{1}{a_n}, & \text{if } n \geq n_0. \end{cases} \implies \forall n, m \geq n_0 : |b_n - b_m| = \dfrac{|a_m - a_n|}{|a_n||a_m|} \leq \dfrac{|a_n - a_m|}{\delta^2} \to 0$ as $m, n \to \infty$

$\implies (b_n) \in \mathcal{C}$ and $(b_n)_n(a_n)_n - \mathbb{1} \in \mathcal{N}$

$\implies ((a_n)_n + \mathcal{N})((b_n)_n + \mathcal{N}) = \mathbb{1} + \mathcal{N}$.

Therefore, $(a_n)_n + \mathcal{N} \in (\mathcal{C}/\mathcal{N})^\times \implies \mathcal{C}/\mathcal{N}$ is a field.

Define: $\iota : K \to K^\wedge$ by $\iota(a) = (a, \cdots, a) + \mathcal{N}$. This is a homomorphism of fields. Given $[(a_n)_n] := (a_n)_n + \mathcal{N} \in K^\wedge$ we set:

$$|[(a_n)_n]|^\wedge := \lim_{n \to \infty} \underbrace{|a_n|_n}_{\text{Cauchy in } \mathbb{R}} \quad \text{(converges)}$$

This extends the absolute value $|\cdot|$ in K.

Density of K in $K^\wedge$:

Let $\underbrace{[(a_n)_n]}_{\alpha} \in K^\wedge$ then the sequence $(\iota(a_n))_n$ converges to:

$$|\alpha - \iota(a_n)|^\wedge = \lim_{n \to \infty} |a_n - a_m|_K \to 0$$

as $m \to \infty$.

$K^\wedge$ is complete: Let $(\alpha_n)_n$ be a Cauchy sequence in $K^\wedge$. By density of K in $K^\wedge$ there is for any $n \geq 0 \exists a_n \in K : |\alpha_n - \iota(a_n)|^\wedge < \frac{1}{n}$.

$$\implies |a_n - a_m|_K = |\iota(a_n) - \iota(a_m)|^\wedge \leq \underbrace{|\iota(a_n) - \alpha_n|^\wedge}_{<1/n} + \underbrace{|\alpha_n = \alpha_m|^\wedge}_{\to 0} + \underbrace{|\alpha_m - \iota(a_m)|^\wedge}_{<1/m} \to 0$$

as $\min\{m, n\} \to \infty$.

$\implies \alpha = [(a_n)_n] \in K^\wedge$

Check: $(\alpha_n)_n$ converges to α. This shows (i). (ii) follows from the next statement.

$\square$

PROPOSITION 9.6. Let $(K_1, |\cdot|_1)$ be a completion of $K = (K, |\cdot|)$ and let $(K_2, |\cdot|_2)$ be another completely valued field.

Every homomorphism of fields $\tau : K \to K_2$ such that $\forall a \in K : |\tau(a)|_2 = |a| (= |\iota(a)|_1)$ extends uniquely to a homomorphism $\sigma : K_1 \to K_2$ such that $\forall a \in K_1 : |\sigma(a)|_2 = |a|_1$.

PROOF. Given $a \in K_1$ choose a sequence $(a_n)_n$ in K converging to a.

$\implies (\tau(a_n))_n$ is a Cauchy sequence in K_2. Since K_2 is complete, $\lim_{n \to \infty} \tau(a_n) =: \sigma(a)$ exists in K_2.

Check: $\sigma(a)$ is independent of the chosen sequence $(a_n)_n$ and σ is a ring homomoprhism satisfying:

$$\forall a \in K_1 : |\sigma(a)|_2 = |a|_1$$

$\square$

EXAMPLE.   1) $(\mathbb{Q}, |\cdot|_p) =: \mathbb{Q}_p$ called the field of p-adic numbers. We also have an evaluation ring: $\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid |x|_p^\wedge \leq 1\}$ is the ring of p-adic integers.

EXERCISE. $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$

2) Let k be any field. Define an evaluation $w_t : k(t) \to \mathbb{Z} \cup \{\infty\}$ given by $w_t(f) =$ vanishing order at $t = 0$ of $f(t) \in k[t] = \min\{n \geq 0 \mid f \in t^n k[t]\}, w_t(0) = \infty, w_t\left(\frac{f}{g}\right) = w_t(f) - w_t(g)$. Let $|\cdot|_t$ be the t-adic absolute value on $k(t)$ associated to w_t.

The completion of $(k(t), |\cdot|_t)^\wedge$ is the field of formal Laurent series $k((t)) := k[[t]]\left[\frac{1}{t}\right]$.

3) $\mathbb{Q}_\infty = (\mathbb{Q}, |\cdot|_\infty)^\wedge \cong \mathbb{R}$.

LEMMA 9.7. Let $K^\wedge$ be a completion of K. Then if $|\cdot|$ is non-archimedean, K and $K^\wedge$ have the same value group.

PROOF. Clearly: $|K^\times| = |K^\times|^\wedge \subset |(K^\wedge)^\times|^\wedge$.

Given $a \in K^{\wedge, \times}$ choose $(a_n)_n$ in K converging to $a \implies \exists n_0 \, \forall n \geq n_0 : |a - a_n| < \underbrace{|a_n|}_{\neq 0}$.

$$\implies |a| = |\underbrace{a - a_n}_{\text{small}} + \underbrace{a_n}_{\text{not so small}}| \overset{\text{HW } 9}{=} \max\{|a - a_n|, |a_n|\} = |a_n| \in |K^\times| \qquad \square$$

PROPOSITION 9.8. Suppose $|\cdot|$ is a non-archimedean absolute value on K. Then,

i) A series $\sum_{n=0}^\infty a_n$ converges $\iff (a_n)_n$ is a null sequence
ii) A power series $\sum_{n=0}^\infty a_n x^n \in R[[x]]$ [the valuation ring] has the property that $\forall a \in P_\infty (=$ valuation ideal$) : \sum_{n=0}^\infty a_n a^n$ converges in R.

PROOF. (ii) follows from (i).
(i): If $(a_n)_n$ is a null sequence then,

$$\left| \sum_{n=0}^{m_1} a_n - \sum_{n=0}^{m_2} a_n \right| = \left| \sum_{n=m_2+1}^{m_1} a_n \right| \overset{\text{non-arch}}{\leq} \max\{|a_n| \mid m_2 < n \leq m_1\}$$

for $m_1 \geq m_2 \geq 0$. RHS $\to 0$ as $m_2 \to \infty$ so partial sums $\sum_{n=0}^m a_n$ form a Cauchy sequnce, which converges since K is complete w.r.t. $|\cdot|$. $\qquad \square$

REMARK.   i) For every $a \in \mathbb{Q}_p$ there exists a unique "power series expansion"

$$a = \sum_{n=m}^\infty a_n p^n$$

with $a_n \in \{0, \cdots, p-1\}$ and $a_m \neq 0$. This is called the p-adic expansion of a.
ii) $a \in \mathbb{Q} \iff$ this expansion is eventually periodic.
We have the following unintuive fact:

$$1 + p + p^2 + \cdots = \frac{1}{1-p}$$

This makes complete sense because $|p|_p < 1$.
We also have:

$$\frac{p^n}{1+p^n} \to \begin{cases} 0, & \text{w.r.t. } |\cdot|_p; \\ 1, & \text{w.r.t. } |\cdot|_\infty. \end{cases}$$

9.3. Extension of Absolute Values

Let $(K, |\cdot|)$ be a (not necessarily completely) valued field.

DEFINITION. Let V be a K-vector space. Then a map $\|\cdot\| : V \to \mathbb{R}_{\geq 0}$ is called a $|\cdot|$-norm if:

i) $\|v\| = 0 \iff v = 0$
ii) $\forall v \in V \, \forall a \in K : \|av\| = |a|\|v\|$
iii) $\forall v, w \in V : \|v + w\| \leq \|v\| + \|w\|$

Given V with a norm $\|\cdot\|$ we get a metric $d(v, w) = \|v - w\|$ which gives us a topological space with open balls given by this norm.

One has concepts of Cauchy sequence, null sequence, convergence and completeness.

Written by Thanic Nur Samin

REMARK.   1) If $\dim_K(V) = n(< \infty)$ and $(e_1, \cdots, e_n)$ is a K-basis of V, then

$$\left\| \sum_{i=1}^n a_i e_i \right\| := \max_{1 \leq i \leq n} \{|a_i|\} \quad \text{is a } |\cdot|\text{-norm on } V.$$

2) If E/K is a field extension and $|\cdot|_E$ extends the absolute value $|\cdot|$ on K then $|\cdot|_E$ is a $|\cdot|$-norm on K.

3) On $K[x]$ we get a $|\cdot|$-norm by:

$$\left\| \sum_{i=0}^n a_i x^i \right\| = \max\{|a_i|\}$$

Suppose $|\cdot|$ is non-archimedean. Then this norm is multiplicative: $\|fg\| = \|f\|\|g\|$. It also satisfies the strong triangle inequality: $\|f + g\| \leq \overline{\max\{\|f\|, \|g\|\}}$ and one can extend to $K(x) = \text{Frac}(x)$ by

$$\left\| \frac{f}{g} \right\| = \frac{\|f\|}{\|g\|}.$$

This is called the Gauss norm on $K[x]$ associated to $|\cdot|$.

THEOREM 9.9. Let $\|\cdot\|_0$ be a $|\cdot|$-norm on V and suppose that $\dim_K(V) < \infty$ and K is complete w.r.t. $|\cdot|$. Then, if $\|\cdot\|_1$ is another $|\cdot|$-norm on V then $\exists 0 < c_1 \leq c_2$ such that $\forall v \in V$:

$$c_1 \|v\|_0 \leq \|v\|_1 \leq c_2 \|v\|_0.$$

Furthermore, V is complete w.r.t. $\|\cdot\|_0$ and $\|\cdot\|_1$.

PROOF. Idea: use induction on $\dim_K(V)$. If $\dim_K(V) = 1$ it is straightforward. Induction step: HW.

Warning: do not assume that K is locally compact. $\square$

PROPOSITION 9.10. Let E be a field extension of K, and let $|\cdot|_1$ and $|\cdot|_2$ be absolute values on E extending $|\cdot| = |\cdot|_K$.

i) If $|\cdot|$ is non-trivial then $|\cdot|_1 = |\cdot|_2$ if $|\cdot|_1$ and $|\cdot|_2$ are equivalent.

ii) If E/K is finite and K is complete w.r.t. $|\cdot|$, then $|\cdot|_1 = |\cdot|_2$ and E is complete w.r.t. $|\cdot|_1$.

Thursday, 10/24/2024

PROOF.   i) If $|\cdot|_1$ and $|\cdot|_2$ are equivalent then $\overset{9.1}{\Longrightarrow} \exists \rho > 0 : |\cdot|_2 = |\cdot|_1^\rho$.

Assumption $\implies \exists a \in K^\times : |a| \neq 1 \implies |a| = |a|_2 = |a|_1^\rho = |a|^\rho \implies \rho = 1 \implies |\cdot|_1 = |\cdot|_2$.

ii) We consider E as a finite dimensional K vector space. Then we can $|\cdot|_1$ and $|\cdot|_2$ as $|\cdot|$-norm on E.

Theorem 9.9 implies $\exists 0 < c_1 \leq c_2 \forall \alpha \in E$:

$$c_1 |\alpha|_1 \leq |\alpha|_2 \leq c_2 |\alpha|_1$$

Therefore, null sequence for $|\cdot|_1$ are null seqeunces for $|\cdot|_2$ and vice-versa.

Therefore, $|\cdot|_1$ and $|\cdot|_2$ are equivalent as absolute values.

If $|\cdot|$ is nontrivial then $\overset{i}{\implies} |\cdot|_1 = |\cdot|_2$.

Now assume $|\cdot|$ is trivial. Choose a basis $(\alpha_1)_{i=1}^n$ of E/K and define a vector space norm $\|\sum_i a_i \alpha_i\| := \max\{|a_i|\}$.

$\overset{9.9}{\implies} \|\cdot\|$ is equivalent as norm to $|\cdot|_1$ and $|\cdot|_2$.

Theorem 9.9 $\implies |\cdot|_1$ and $|\cdot|_2$ are both bounded above $[|\cdot|_i \leq c\|\cdot\| \leq c]$.

Therefore, they are both trivial and hence equal.

$\square$

THEOREM 9.11 (Ostrowski, 1918). A field K that is complete w.r.t. an archemdean absolute value $|\cdot|$ is either isomorphic to $\mathbb{R}$ or $\mathbb{C}$ by an isomorphism which makes $|\cdot|$ equivalent to (the pull-back) of $|\cdot|_\infty$.

PROOF. See Lorenz, appendix 23.9, 23.10, 23.11.   □

<u>Notation</u>: For the following lemma, let $|\cdot|$ be a non-archimedean absolute value on K, let $R \subset K$ be the valuation ring (elements of absolute value ≤ 1), let $P \subset R$ the valuation ideal (element of absolute value < 1) and $\overline{R} = R/P$ the residue field. Define $\overline{} : R \to \overline{R}|$ by $\overline{a} := a + P$. Extend this map to the polynomial rings $R[x] \to \overline{R}[x], f = \sum_i a_i x^i \mapsto \overline{f} = \sum_i \overline{a_i} x^i$. We also write for $f, g \in R[x]$ and $c \in R : f \equiv g\,(c) \iff f - g \in c \cdot R[x]$.

THEOREM 9.12 (Hensel's Lemma). Let K be complete w.r.t. $|\cdot|$. Given $f \in R[x]$ and a factorization $\overline{f} = \phi\psi$ with coprime polynomials $\phi, \psi \in \overline{R}[x] \setminus \{0\}$:
We can 'lift' this factorization back to R: there exists $g, h \in R[x]$ such that $f = gh$ and $\overline{g} = \phi, \overline{h} = \psi$ and $\deg(g) = \deg(\phi)$.

REMARK. We don't necessarily add the condition $\deg(h) = \deg(\psi)$ since we allow $\overline{f}$ to have degree smaller than f. If they do have the same degree, then we have $\deg(h) = \deg(\psi)$.

PROOF. Set $m = \deg(f), r = \deg(\phi)$.
$\exists g_0, h_0 \in R[x] : \overline{g_0} = \phi, \overline{h_0} = \psi, \deg(g_0) = r, \deg(h_0) \leq m - r$ and $f \equiv g_0 h_0 \mod P[\iff \overline{f} = \overline{g_0 h_0}]$.
Since ϕ, ψ are coprime, $\exists$ polynomials $a, b \in R[x] : ah_0 + bg_0 \equiv 1 \mod P[\iff \overline{a}\psi + \overline{b}\phi = \overline{1}]$.
$f - g_0 h_0$ and $ah_0 + bg_0 - 1$ have all coefficients in P.
Let $\pi \in P$ be such that $\overline{\pi} \geq \max\{\|f - g_0 h_0\|, \|ah_0 + bg_0 - 1\|\}$ where $\|\sum_i a_i x^i\| = \max\{|a_i|\}$.
$\implies f \equiv g_0 h_0 \pmod{\pi}$ and $ah_0 + bg_0 \equiv 1 \pmod{\pi}$.
<u>Induction Hypothesis</u>: $\exists a_1, \cdots, a_n, b_1, \cdots, b_n \in R[x]$ such that $\deg(a_i) \leq r, \deg(b_i) \leq m - r$ and $f \equiv g_n h_n \mod \pi^{n+1}$, where $g_n = g_0 \sum_{i=1}^n a_i \pi^i, h_n = h_0 + \sum_{i=1}^n b_i \pi^i$.
Case $n = 0$ we have just completed.
For $n - 1 \rightsquigarrow n$: Assume the induction hypothesis is true for $n - 1$ Then, $f \equiv g_{n-1} h_{n-1} \mod \pi^n$.
Then, $\exists d_n \in R[x]$ such that $f = g_{n-1} h_{n-1} + d_n \pi^n, \deg(d_n) \leq m = \deg(f)$.
Set $g_n = g_{n-1} + a_n \pi^n$ and $h_n = h_{n-1} + b_n \pi^n$ with polynomials a_n, b_n which we need to find.
$\implies g_n h_n \equiv g_{n-1} h_{n-1} + a_n h_0 \pi^n + b_n g_0 \pi^n \mod \pi^{n+1}$
$\equiv f + (-d_n + a_n h_0 + b_n g_0)\pi^n \mod \pi^{n+1}$
Hence we need to show $\exists a_n, b_n \in R[x]$ so that $\deg(a_n) \leq r, \deg(b_n) \leq m - r$ and $a_n h_0 + b_n g_0 \equiv d_n \mod \pi$.
The existence of a_n and b_n follows from the fact that $ah_0 + bg_0 \equiv 1 \mod \pi$.
It follows after some work that it also satisfies the degree condition.   □

EXAMPLE. Let $K = \mathbb{Q}_p$ hence $R = \mathbb{Z}_p = \{a \in \mathbb{Q}_p \mid |a|_p \leq 1\}$.
1) Set $f(x) = x^{p-1} - 1 \implies \overline{f}(x) = f(x) \mod p\mathbb{Z}_p = \prod_{a=1}^{p-1}(x - \overline{a}) = \underbrace{x - \overline{a_0}}_{\phi(x)} \psi(x)$.

$\implies \exists g(x), h(x) \in \mathbb{Z}_p[x] : g(x)h(x) = x^{p-1} - 1, \deg(g(x)) = \deg(\phi) = 1 \implies$
WLOG: $g(x) = x - \zeta$ for some $\zeta \in \mathbb{Z}_p \subset \mathbb{Q}_p \implies \zeta^{p-1} = 1$.
We can keep doing this with h. Again, $\overline{h}(x) = \prod_{1 \leq a \leq p-1, a \neq a_0}(x - \overline{a})$ and we can split another factor. Therefore,

$$x^{p-1} - 1 = \prod_{a=1}^{p-1}(x - \zeta_a)$$

with $\zeta_a \equiv a \mod p\mathbb{Z}_p$.
Therefore, $\mathbb{Q}_p$ contains all roots of unity of order dividing $p - 1$.
2) $f(x) = x^n + (1 + pm), p \nmid n, m \in \mathbb{Z}$ (or $m \in \mathbb{Z}_p$).
$p = 2, n = 5, m = 3 \implies f(x) = x^5 - 7$.
$\implies \overline{f} = f \mod p\mathbb{Z}_p = x^n - 1 = (x - 1)\psi(x)$ with $\psi(1) \neq 0$ over the residue field $\mathbb{F}_p[x]$ since $p \nmid n$.
Then there is some lift $g(x) \in \mathbb{Z}_p[x]$ of degree 1 such that $\overline{g}(x) = x - 1$ and $f(x) = g(x)h(x)$ for some $\overline{h}(x) = \psi(x)$.
WLOG $g(x) = x - \lambda, \overline{\lambda} = 1$ for some $\lambda \in \mathbb{Z}_p$.
$\implies \lambda^n = 1 + pm$.
Therefore, $1 + pm$ has n'th root in $\mathbb{Z}_p$.

Written by Thanic Nur Samin

$$\lambda \overset{!}{=} \sqrt[n]{1+pm}$$

For example, $\sqrt[5]{7} \in \mathbb{Q}_2$.

REMARK. The proof of Hensel's lemma is not purely algebraic.

$$g = g_\infty = g_0 + \sum_{n=1}^\infty a_n \pi^n$$

so there is some non-archimedean analysis going on.
We can use this fact to 'calculate' roots in $\mathbb{Z}_p$:

$$\sqrt[n]{1+pm} = (1+pm)^{1/n} = \sum_{j=0}^\infty \binom{\frac{1}{n}}{j}(pm)^j$$

If $p \nmid n$ then $\frac{1}{n} \in \mathbb{Z}_p^\times$ since $\left|\frac{1}{n}\right| = 1$. The binomial coefficients are in fact p-adic integer. $(pm)^j$ has small p-adic absolute value so the sum converges in $\mathbb{Q}_p$.

Tuesday, 10/29/2024

COROLLARY 9.13. Let $(K, |\cdot|)$ be a complete non-archemedean field. If

$$f = a_0 x^n + a_1 x^{n-1} + \cdots + a_n \in K[x]$$

with $n > 0, a_0 \neq 0$ and $a_0 < \|f\| = \max\{|a_i| \mid 0 \leq i \leq n\}$, where maximum is achieved not only for the constant term. then f is reducible.

PROOF. WLOG assume $\|f\| = 1 \implies f \in R[x]$. Let P be the valuation ideal. Then,
$\overline{f} = f \mod P$ has degree $< n$ and is not constant.
Write $\overline{f} = \overline{f} \cdot 1$. Set $\phi = \overline{f}$ and $\psi = 1 \in \overline{R}[x]$ where $\overline{R} = R/P$.
Trivially, ϕ, ψ are coprime.
Since K is complete, Hensel's Lemma implies that $\exists g, h \in R[x]$ so that $f = gh$, $\overline{g} = \phi, \overline{h} = \psi$ and $\deg g = \deg \phi \implies \deg(h) = \deg(f) - \deg(g) > 0$.
Thus we have found a nontrivial decomposition. $\qquad\square$

EXAMPLE. In $\mathbb{Q}_p$ the polynomial $px^n + x + 1$ has a root in $\mathbb{Z}_p$.

THEOREM 9.14. Let $(K, |\cdot|)$ bea completely valued field [we allow $|\cdot|_\infty$]. If E/K is a finite extension then $|\cdot|$ extends uniquely to an absolute value $|\cdot|_E$ which is given by:

$$\forall \alpha \in E : |\alpha|_E := \left|N_{E/K}(\alpha)\right|_K^{\frac{1}{n}}, \text{ where } n = [E:K] \quad (*)$$

Moreover, E is complete w.r.t. $|\cdot|_E$.

PROOF. 9.10 implies uniqueness and completeness.
If $|\cdot|$ is archimedean then Ostrowski's Theorem (9.11) says that $(K, |\cdot| = (\mathbb{R}, |\cdot|_\infty))$ or $(K, |\cdot|) = (\mathbb{C}, |\cdot|_\infty)$ upto equivalent absolute values. This takes care of the archimedean case. We are interested about the non-archimedean case.

Suppose $|\cdot|$ is non-archimedean. $(*)$ defines a function satisfying $\begin{cases} |\alpha|_E = 0 \iff \alpha = 0 \\ |\alpha\beta|_E = |\alpha|_E |\beta|_E \end{cases}$

Thus it suffices to show that it satisfies the strong triangle inequality.
It suffices to show, given $|y| \geq |x|$ that:

$$\left|\frac{x}{y} + 1\right| \leq 1$$

Since WLOG assuming $|x| \leq |y|$,
$|x+y| \leq \max\{|x|, |y|\} \iff |x+y| \leq |y| \iff \left|\frac{x}{y}+1\right| \leq 1$ when $|y| \neq 0$. The 0 case is trivial.
This is equivalent to:

$$\forall \alpha \in E : |\alpha|_E \leq 1 \implies |\alpha + 1|_E \leq 1$$

$$N_{E|K}(\alpha) \overset{1.8}{=} N_{K(\alpha)|K}(N_{E|K(\alpha)}(\alpha))$$

$$= N_{K(\alpha)|K}(\alpha^{[E:K(\alpha)]}) = N_{K(\alpha)|K}(\alpha)^{[E:K(\alpha)]}$$

Thus, WLOG we may assume $E = K(\alpha)$. Let $\alpha \in E$ be such that $|\alpha|_E \leq 1$ and let $\mu(x) = x^n + a_1 x^{n-1} + \cdots + a_n \in K[x]$ be the minimal polynomial of α/K.
$a_n = \pm N_{K(\alpha)|K}(\alpha) \implies |a_n|_K \leq 1$ by assumption.
If $\exists 0 < i < n : |a_i| > 1 \underset{9.13}{\implies} \mu_\alpha(x)$ is reducible.
Thus, $\|\mu_\alpha(x)\| \leq 1$. Note that $p(x) = \mu_\alpha(x - 1)$ is the minimal polynomial of $\alpha + 1$ with constant coefficient $p(0) = \mu_\alpha(-1) \in R$ and thus it is $\pm N_{K(\alpha)/K}(\alpha + 1)$.

$$\implies \left| N_{K(\alpha)|K}(\alpha + 1) \right|_K \leq 1$$

<div align="right">□</div>

COROLLARY 9.15. Let $(K, |\cdot|)$ be complete and $|\cdot|$ be non-archimedic. Let C be an algebraic closure of K. Then,

  i) $|\cdot|$ has a unique extension $|\cdot|_C$ to C given by $|\alpha|_C = |N_{K(\alpha)|K}(\alpha)|_K^{1/[K(\alpha):K]}$.
  ii) Let R be the valuation ring of $|\cdot|$. For $\alpha \in C$ TFAE:
   a) $|\alpha|_C \leq 1$.
   b) $\mu_{\alpha,K}(x) \in R[x]$.
   c) α is integral $/R$.

 PROOF. $9.14 \implies$ i since $C = \bigcup_{K \subset E \subset C, [E:K] < \infty} E$.
For ii:
(a) $\implies$ (b): $|\mu_{\alpha,K}(0)|_K = \left| N_{K(\alpha)|K}(\alpha)(\alpha) \right|_K = |\alpha|_C^{[K(\alpha):K]} \leq 1$ [by assumption].
$\mu_{\alpha,K}(x)$ is irreducible and leading term has absolute value $= 1 \underset{9.13}{\implies}$ all coeffiients of $\mu_\alpha(x)$ are in R.
(b) $\implies$ (c) by definition.
(c) $\implies$ (a): $\exists a_i \in R : \alpha^n + a_i \alpha^{n-1} + \cdots + a_n = 0$.
If $|\alpha|_C > 1$ then $|\alpha^n|_C = \left| -a_1 \alpha^{n-1} - \cdots - a_n \right|_C \leq \max\{ |a_i \alpha^{n-i}| \mid i = 1 \cdots n \} \leq |\alpha|_C^{n-1}$.
which is a contradiction. <div align="right">□</div>

REMARK.   1) Consider the unique extension of $|\cdot|_p$ to $\overline{\mathbb{Q}_p}$, then $(\overline{\mathbb{Q}_p}, |\cdot|_p)$ is <u>not</u> complete [HW11]. <u>However</u>:

$$(\mathbb{C}_p, |\cdot|_p) := (\overline{\mathbb{Q}_p}, |\cdot|_p)^{\wedge} \text{ is complete and algebraically closed}$$

  2) A <u>valuation ring</u> is an integral domain R such that $\forall x \in \text{Frac}(R) \setminus R : x^{-1} \in R$.

A valuation ring R is called <u>Henselian</u> if Hensel's Lemma holds for R.
Hensel's Lemma, as we have proved it, says: the valuation ring of a complete non-archimedean field is Henselian.

EXAMPLE (Henselian Valuation Ring, not complete).

$$\mathbb{Z}_{(p)}^h = \{ \alpha \in \mathbb{Q}_p \mid \alpha \text{ is inegral over } \mathbb{Z}_{(p)} \}$$

We have $\mathbb{Z} \subseteq \mathbb{Z}_{(p)}^h \subseteq \mathbb{Z}_p$.

The following follows from Proposition 9.10 and Theorem 9.14 given a non-archimedean absolute value $|\cdot|$ on K (K not necessarily complete w.r.t. $|\cdot|$). Then,

  $|\cdot|$ has a unique extension to any finite extension $E/K \iff R = R(|\cdot|)$ is Henselian

THEOREM 9.16. Let E/K be a finite extension of degree n and let $|\cdot|$ be an absolute value on K. Then:

  i) $|\cdot|$ can be extended to an absolute value on E.
  ii) There are at most n extensions of $|\cdot|$ to distinct absolute values on E.

           Written by Thanic Nur Samin

iii) Let $|\cdot|_1, \cdots, |\cdot|_r$ be the set of all distinct extensions of $|\cdot|$ to E. For each $1 \le j \le r$ let $E_j^\wedge := (E, |\cdot|_j)^\wedge$ and $K^\wedge = (K, |\cdot|)^\wedge$, which embeds canonically into $E_j^\wedge$. This canonical homomorphism of $K^\wedge$-algebras:

$$E \otimes_K K^\wedge \to \prod_{j=1}^r E_j^\wedge \ (*)$$

$$\alpha \otimes a \mapsto (\iota_j(\alpha)a)_{j=1}^r$$

where $\iota_j : E \to E_j^\wedge$ is the canonical map, is surjective and hence

$$\sum_{j=1}^r [E_j^\wedge : K^\wedge] \le n \, (= \dim_{K^\wedge}(E \otimes_K K^\wedge))$$

If E/K is separable, then $(*)$ is an isomorphism and hence $\sum_j [E_j^\wedge : K^\wedge] = n$.

Thursday, 10/31/2024

PROOF. Proof has four pats.

a) Set $C = \overline{K^\wedge}$ [algebraic closure]. Corollary 9.15 $\implies$ $|\cdot|$ on $K^\wedge$ extends uniquely to an absolute value $|\cdot|_C$ on C [since $K^\wedge$ is complete].

Let $\sigma_1, \cdots, \sigma_m : E \to C$ be all K-embeddings into C. Then $m \le n[= \deg[E/K]]$, and if E/K is separable, we can write E as being generated by primitive element whose minimal polynomial has degree n, and we get embeddings by permuting the roots and therefore $m = n$.

Define [not necessarily distinct] absolute values $|\cdot|_j$ on E by $|\alpha_j| := |\sigma_j(\alpha)|_C$, these extend $|\cdot|$ on K.

Let $|\cdot|'$ be any extension of $|\cdot|$ on K to E. We show that this is one of $|\cdot|_j$.

Let $E' = (E, |\cdot|')^\wedge$ and $K' = (K, |\cdot|)^\wedge$ which is just the closure of K in E'.

Then, the composite field $E.K'/K'$ is a finite extension and since it is a finite extension of a completely valued field, $\stackrel{9.10}{\implies} E.K'$ is complete (w.r.t. the unique extension of $|\cdot|'$). Since E maps canonically into E' and K' is a subfield of E', $E.K'$ canonically embeds into E'

Therefore, since E is dense in E', $EK' = E'$.

Proposition 9.6 $\implies$ $\exists$ isometric isomorphism $K' \underset{\rho}{\to} K^\wedge$ such that $\forall a \in K' :$ $|\rho(a)|_C = |a|'$.

C is algebraically closed, thus ρ extends to a field homomorphism $\sigma : E' \to C$.

$$
\begin{array}{ccccc}
K & \longrightarrow & K' & \stackrel{\rho}{\longrightarrow} & K^\wedge \\
\downarrow & & \downarrow & & \downarrow \\
E & \longrightarrow & E' & \stackrel{\sigma}{\cdots\cdots\cdots} & C
\end{array}
$$

Set another absolute value on E' by $|\alpha|'' = |\sigma(a)|_C$. $|\cdot|''$ restricts to $|\cdot|'$ on K'.

9.10 $\implies$ $\forall \alpha \in E'$ we have fma$|\sigma(\alpha)|_C = |\alpha|' \implies |\alpha|'' = |\alpha|'$.

Thus, $\forall \alpha \in E : |\alpha|' = |\sigma(\alpha)|_C = |\sigma_j(\alpha)|_C = |\alpha|_j$ if the map $E \underset{\text{canonical}}{\hookrightarrow} E' \underset{\sigma}{\to} C$ is equal to σ_j.

Upshot: every extension of $|\cdot|$ to E is one of $|\cdot|_j = |\sigma_j(\cdot)|$.

This shows (i) and (ii).

b) Let $(E_1^\wedge, |\cdot|_1), \cdots, (E_r^\wedge, |\cdot|_r)$ be the completions w.r.t. $|\cdot|_1, \cdots, |\cdot|_r$.

We know by part a that $r \le m \le n$. $\exists K6\wedge \underset{\text{canonical}}{\to} E_j^\wedge$ and the diagonal map $E \to \prod_{j=1}^r E_j^\wedge, \alpha \mapsto (\iota_j(\alpha))_{j=1}^r$ extends uniquely to a homomorphism of $K^\wedge$ algebras:

$$E \otimes_K K^\wedge \to \prod_{j=1}^r E_j^\wedge$$

$$\alpha \otimes a \mapsto (\iota_j(\alpha)a)_{j=1}^r \quad (1)$$

We have seen in (a) that image of $E.K^\wedge$ in $E_j^\wedge$ is $E_j^\wedge$.

Thus, composition of (1) with projection onto $E_j^\wedge$ is surjective.

If E/K is purely inseparable then $m = 1 \implies r = 1 \implies$ (1) is surjective. Hence (iii) in this case.

c) Let F/K be the maximal separable subextension of $E/K \implies E/F$ is purely inseparable.

Note: $E \otimes_K K^\wedge = E \otimes_F \underbrace{\left(F \otimes_K K^\wedge \right)}_{\overset{?}{\cong} \prod F_j^\wedge}$.

$$\underbrace{\qquad\qquad\qquad\qquad\qquad\qquad}_{\overset{?}{\cong} \prod (E \otimes_F F_j^\wedge) \twoheadrightarrow E_j^\wedge}$$

Thus, it suffices to show that (iii) is true for F/K separable. We thus assume E/K is separable.

Then, $E = K(\alpha)$ for some $\alpha \in E$ and let $\mu(x) = \mu_{\alpha,K}(x)$ be the minimal polynomial of α over K. We can decompose into distinct [since separable] irreducible factors $\mu_i(x) \in K^\wedge[x]$:

$$\mu(x) = \mu_1(x) \cdots \mu_s(x)$$

eg $x^2 + 1$ is irreducible over $\mathbb{Q}$ but $x^2 + 1 = (x - \alpha)(x - \beta)$ in $\mathbb{Q}_p$ if $p \equiv 1 \mod 4$

Choose for $1 \le j \le s$ a root α_j of μ_j in $C = \overline{K^\wedge}$.

The map $\alpha \mapsto \alpha_j$ induces a K embedding $E \to C$ equal to σ_j [renumbering if needed].

For $k > s$, $\sigma_k(\alpha)$ is a root of $\mu(x)$ and thus must be a root of sone $\mu_j(x)$. Hence $\sigma_k(\alpha)$ is a conjugate to α_j over $K^\wedge$.

$\implies \exists \tau \in \text{Aut}(C/K^\wedge) : \tau(\sigma_k(\alpha)) = \alpha_j = \sigma_j(\alpha)$.

$\implies |\sigma_j(\alpha)|_C = |\tau(\sigma_k(\alpha))|_C \overset{9.15}{=} |\sigma_k(\alpha)| \implies r = $ number of distinct extensions of $|\cdot| \le s$.

For $1 \le i \le s$ defined $\forall \gamma \in E : |\gamma|_i := |\sigma_i(\gamma)|_C$.

$K^\wedge(\alpha_i)$ is complete $\implies$ the K-homomorphism $E = K(\alpha) \underset{\sigma_i}{\to} K^\wedge(\alpha_i)$ given by

$\alpha \mapsto \sigma_i(\alpha) = \alpha_i$ extends to $E_i^\wedge = (K(\alpha), |\cdot|_i)^\wedge \overset{\hat{\sigma}_i}{\to} K^\wedge(\alpha_i)$.

If $|\cdot|_k = |\cdot|_j$ for some $1 \le k \le j \le s$ then $E_k^\wedge$ is isometric isomorphic to $E_j^\wedge$.

Therefore, $\hat{\sigma}_k \circ \hat{\sigma}_i^{-1} : K^\wedge(\alpha_i) \to K^\wedge(\alpha_k)$ isomorphism over $K^\wedge$. Thus, α_i and α_k have the same minimal polynomial. Thus, $k = j$.

d) CRT $\implies$ the top horizontal map

$$\begin{array}{ccc} K^\wedge[x]/\mu_\alpha(x) & \overset{\cong}{\longrightarrow} & \prod K^\wedge[x]/(\mu_i(x)) \\ \cong \uparrow & & \cong \uparrow \\ E \otimes_K K^\wedge & \longrightarrow & \prod E_j^\wedge \end{array}$$

[Since $R[x]/(f) \otimes_R A = A[x]/fA[x]$ and $E = K[x]/(\mu_\alpha(x))$].

Thus, the bottom map is an isomorphism.

$\square$

EXAMPLE. Let $K = \mathbb{Q}, E = $ number field, $|\cdot| = |\cdot|_\infty$, let $\rho_1, \cdots, \rho_r : E \to \mathbb{R}, \sigma_1, \cdots, \sigma_s, \overline{\sigma}_1, \cdots, \overline{\sigma}_s : E \to \mathbb{C}$ be real and complex embeddings.

Then, $|\cdot|_\infty$ has precisely $r + s$ distinct extensions to E, namely

$$|\alpha|_\phi = |\phi(\alpha)|_\mathbb{C} \text{ for } \phi \in \{\rho_1, \cdots, \rho_r, \sigma_1, \cdots, \sigma_s\}$$

If $E = \mathbb{Q}(\alpha)$ then $\mu_{\alpha,\mathbb{Q}}(x) = \mu_1(x) \cdots \mu_r(x)\mu_{r+1}(x) \cdots \mu_{r+s}(x)$.

Here $\deg(\mu_i(x)) = \begin{cases} 1, & \text{if } 1 \le i \le r; \\ 2, & \text{if } r + 1 < i \le r + s. \end{cases}$

$$\mu_i(x) = x - \alpha_i \quad \alpha_i \, in \, \mathbb{R}$$

$$\mu_i(x) = (x - \alpha_i)(x - \overline{\alpha_i}) \quad \alpha \in \mathbb{C} \setminus \mathbb{R}$$

Hence $s = r$.

EXAMPLE (Inseparable). Suppose $\text{char}(K) = p > 0, E = K(\sqrt[p]{t}), t \notin K^p$ [not a p'th power].
Then, $x^p - t$ is irreducble and inseparable $= (x - \sqrt[p]{t})^p$.
<u>Two cases</u>: $x^p - t$ splits over $K^\wedge$. Then $\sqrt[p]{t} \in K^\wedge \implies E \otimes_K K^\wedge = K[x]/(x^p - t) \otimes_K K^\wedge = K^\wedge[x]/(x^p - t) = K^\wedge[x]/((x - \sqrt[p]{t})^p)$ which has nilpotent elements. If we divide by the ideal consisting of the nilpotent element, we get $\twoheadrightarrow K^\wedge$ back.
In characteristic p we have unique p'th root in the algebraic closure.

$$E \lhook\joinrel\longrightarrow C = \overline{K^\wedge}$$

$$\sqrt[p]{t} \longmapsto \text{ some root of } t$$

Sine there is only one root, there is only one embedding!

$$(E, |\cdot|_C)^\wedge = K^\wedge$$

2nd Case: $x^p - t$ stays irreducible over $K^\wedge$.
Then we get $K^\wedge[x]/(x^p - t)$ which will remain a field. Thus,

$$K^\wedge[x]/(x^p - t) = E \otimes_K K^\wedge \overset{\cong}{\to} E^\wedge$$

Residue Class Degree and Ramification Index

Tuesday, 11/5/2024

In this chapter: E/K will be a field extension, and $|\cdot|$ a non-archimedean absolute value on E.
$\mathcal{O}_K$ = valuation of K w.r.t. $|\cdot| \supset P_K$ = valuation ideal.
$\mathcal{O}_E$ = valuation of E w.r.t. $|\cdot| \supset P_E$ = valuation ideal.
$\overline{K}$ = residue field of $K = \mathcal{O}_K/P_K, \overline{E} = \mathcal{O}_E/P_E$.
The canonical injection $\overline{K} \to \overline{E}$ is called the <u>residue field extension</u>.

DEFINITION. $f = f(E \mid K) := [\overline{E} : \overline{K}]$, called the <u>residue class degree</u>.
$e = e(E \mid K) := [|E^\times| : |K^\times|]$, called the <u>ramification index</u>.

REMARK.   1) For $K \subset F \subset E$ we have $\overline{K} \subset \overline{F} \subset \overline{E} \implies f(E \mid K) = f(E \mid F)f(F \mid K)$.
$|K^\times| \subset |F^\times| \subset |E^\times| \implies e(E \mid K) = e(E \mid F)e(F \mid K)$.
    2) $E^\wedge = (E, |\cdot|)^\wedge \overset{\text{exercise}}{\implies} \overline{E} \overset{\cong}{\to} \overline{E^\wedge}$ and $|E^\times| \overset{9.7}{=} |(E^\wedge)^\times|$.
        $\implies f(E \mid K) = f(E^\wedge \mid K^\wedge)$ and $e(E \mid K) = e(E^\wedge \mid K^\wedge)$.
    3) E/K finite $\overset{9.16}{\implies} [E^\wedge : K^\wedge] \leq [E : K]$.
        $[E^\wedge : K^\wedge] =:$ local degree of E/K w.r.t. $|\cdot|$.

LEMMA 10.1. If $[E : K] = n < \infty$ then $e(E \mid K)f(E \mid K) \leq n$.

PROOF. Let $\alpha_1, \cdots, \alpha_r \in \mathcal{O}_E$ be such that $\overline{\alpha}_1, \cdots, \overline{\alpha}_r(\overline{\alpha}_i := \alpha_i + P_E \in \overline{E})$ are linearly independent over $\overline{K}$.
<u>Claim:</u> For all $a_1, \cdots, a_r \in K : |a_1\alpha_1 + \cdots + a_r\alpha_r| = \max\{|a_i|\}$
<u>Proof:</u> WLOG we may assume $\max\{|a_i|\} = 1$.
Strong Triangle inequality $\implies |\sum_i a_i\alpha_i| \leq \max\{|a_i\alpha_i|\} \leq 1 = \max\{|a_i|\}$.
Assume by contradiction that $|\sum_i a_i\alpha_i| < 1$. Then, $\overline{0} = 0_{\overline{E}} = \overline{\sum_i a_i\alpha_i} = \sum_i \overline{a_i\alpha_i}$, linear independence $\implies |a_i| = 0 \iff a_i \in P_K \forall i$. Contradition!
Now choose $\pi_1, \cdots, \pi_s \in E^\times$ s.t. $\forall i \neq j : |\pi_i||K^\times| \neq |\pi_j||K^\times|$ (different elements in $|E^\times|/|K^\times|$).

Suppose $0 = \sum_{\substack{1 \leq i \leq r \\ 1 \leq j \leq s}} a_{ij}\alpha_i\pi_j$ with $a_{ij} \in K$. Set $b_j = \sum_{i=1}^r a_{ij}\alpha_i \implies 0 \overset{(1)}{=} \sum_{j=1}^s b_j\pi_j$.
WLOG: $|b_1\pi_1| = \max\{|b_j\pi_j| \mid 1 \leq j \leq s\} > 0$.
$(1) \implies |b_1\pi_1| = \left|\sum_{j=2}^s b_j\pi_j\right|$.
$\implies \exists 2 \leq j \leq s$ such that $|b_1\pi_1| = |b_j\pi_j|$.
$\implies |\pi_1| \overset{(2)}{=} \left|\frac{b_j}{b_1}\right||\pi_j|$
As we've seen before: $|b_j| = \max\{|a_{ij}| \mid 1 \leq i \leq r\} \in |K^\times|$.
(2) contradicts the previous assumption on the $|\pi_j|$.
$\implies r \cdot s \leq n \implies e \cdot f \leq n$. $\qquad\square$

REMARK.   1) If $[E : K] = n < \infty$ and $|\cdot|_1, \cdots, |\cdot|_r$ are pairwise distinct extensions of a
        given absolute value $|\cdot|$ on K. Then,

$$\sum_{i=1}^r e(E \mid K, |\cdot|_i)f(E \mid K, |\cdot|_i) \overset{\text{Previous Remark}}{\leq} \sum_{i=1}^r e((E, |\cdot|)^\wedge/K^\wedge)f((E, |\cdot|_i)^\wedge/K^\wedge).$$

$$\overset{10.1}{\leq} \sum_{i=1}^r [(E, |\cdot|_i)^\wedge : K^\wedge] \overset{9.16}{\leq} [E : K] = n.$$

2) Even if K is complete and E/K is finite, it can happen that $e(E \mid K)f(E \mid K) < [E : K]$. However, this cannot happen if $|\cdot|$ is a discrete absolute value.

DEFINITION. An absolute value $|\cdot|$ on a field K is called <u>discrete</u>, if $|K^\times|$ is a non-trivial discrete subgroup of $\mathbb{R}_{>0}$.

REMARK.   1) If $|\cdot|$ is discrete then $|\cdot|$ is non-archimedean (otherwise $\mathbb{Q} \hookrightarrow K$ and $|\cdot|\big|_{\mathbb{Q}}$ is non-trivial and archimedean $\implies$ $|\cdot|\big|_{\mathbb{Q}}$ is equivalent to $|\cdot|_\infty$ whose value group is dense.)

2) Some authors allow the trivial absolute value to be discrete.

3) $|\cdot|$ is discrete $\implies \exists c \in \mathbb{R}_{>1}$ such that $|K^\times| = c^{\mathbb{Z}}$.
   Set $w(x) = -\log_c(|x|) \implies |x| = c^{-w(x)}$ and w is a <u>normalized valuation</u> $K \to \mathbb{Z} \cup \{\infty\}$.
   Any $\pi \in K$ with $\mathrm{w}(\pi) = 1 = C^{-1}$ is called a <u>prime element</u> or <u>funiformizer</u> of K w.r.t. $|\cdot|$.
   Then, $\forall x \in K^\times \exists! n \in \mathbb{Z} \exists! v \in K^x : (|u| = 1$ and $n = w(x))$.
   $(|u| = 1)$ and $x = \pi^n \cdot v$.

4) If E/K is an extension and $|\cdot|$ is an absolute value on E with $e(E/K) < \infty$,

$$|\cdot| \text{ is discrete} \iff |\cdot|\bigg|_K \text{ is discrete.}$$

THEOREM 10.2. Suppose that K is complete w.r.t. a discrete absolute value $|\cdot|$, and let w be the associated normalized variation. Let $S \subset \mathcal{O}_K$ be any fixed set of representatives of $\overline{K} = \mathcal{O}_K/P_K$. Asume $\mathcal{O} \in S$.
Let π be a uniformizer of K. Then every $x \in K^\times$ can be written as $x = \sum_{i=w(x)}^\infty a_i \pi^i$ with uniquely determined $a_i = \mathcal{S}$ and $w(x) \coloneqq \min\{i \in \mathbb{Z} \mid a_i \neq 0 \}$.

LEMMA 10.3. Let E/K and $|\cdot|$ be as above. Let $\pi \in K$ be such that $0 < |\pi| < 1$, and assume K is complete w.r.t. $|\cdot|$. If $\beta_1, \cdots, \beta_r \in \mathcal{O}_E$ are represantatives of a generating set of $\mathcal{O}_E/\pi\mathcal{O}_E$ as a $\mathcal{O}_K/\pi\mathcal{O}_K$-module. Then $\beta_1, \cdots, \beta_r$ generate $mathcalO_E$ over $\mathcal{O}_K$.

PROOF. Let $M = \sum_{i=1}^r \mathcal{O}_K\beta_i \subset \mathcal{O}_E$. By assumption, $\mathcal{O}_E \overset{(1)}{=} M + \pi\mathcal{O}_E$.
For any $x \in \mathcal{O}_E$ we get from (1) sequences $(x_i^{(n)})_{i=1}^r$ in $\mathcal{O}_K$ such that:

$$\forall n \geq 1 : \sum_{i=1}^r x_i^{(n)}\beta_i \equiv x \mod \pi^n$$

$$x_i^{(n+1)} \equiv x_i^{(n)} \mod \pi^{n+1}\mathcal{O}_K$$

$\implies x_i = \lim_{n \to \infty} x_i^{(n)}$ exists in K [and is an element of $\mathcal{O}_K$], and $\sum_{i=1}^r x_i\beta_i = x$ $\qquad \square$

THEOREM 10.4. Let E/K and $|\cdot|$ be as before, and $[E : K] < \infty$, and $|\cdot|$ is discrete, and K is complete w.r.t. $|\cdot|$. Then,

$$e(E \mid K)f(E \mid K) = [E : K]$$

PROOF. Let π be a uniformizer of K and ω a uniformizer of E. Then $\exists m \geq 1 : |\pi| = |\omega|^m \implies |E^\times| = |\omega|^{\mathbb{Z}}$.
$\implies |K^\times| = |\pi|^{\mathbb{Z}} = |\omega|^{m\mathbb{Z}} \subset |\omega|^{\mathbb{Z}} = |E^\times|$.
$\implies m = e(E \mid K) = e \implies \pi = u \cdot \omega^m$ for some $u \in E, |u| = 1$.
Let $\alpha_i, \cdots, \alpha_f \in \mathcal{O}_E$ be representatives of a basis of $\overline{E}$ over $\overline{K}$.
<u>Claim:</u>

$$M = \sum_{\substack{1 \leq i \leq f \\ 0 \leq j < e}} \mathcal{O}_K\alpha_i\omega^j = \mathcal{O}_E$$

<u>Proof of Claim:</u> Let $N = \sum_{i=1}^f \mathcal{O}_K\alpha_i$.
The composition $N \hookrightarrow \mathcal{O}_E \twoheadrightarrow \overline{E} = \mathcal{O}_E/\omega\mathcal{O}_E$ is <u>surjective</u>.
Therefore, $\mathcal{O}_E = N + \omega\mathcal{O}_E$ (1).

Thursday, 11/7/2024

<u>Claim:</u> $M := \sum_{j=0}^{e-1} \omega^j N = \sum_{\substack{1 \le i \le f \\ 0 \le j \le e-1}} \mathcal{O}_K \alpha_j \omega^j = \mathcal{O}_E$.

<u>Proof of Claim:</u>

$$\mathcal{O}_E \stackrel{(1)}{=} N + \omega \mathcal{O}_E \stackrel{(1)}{=} N + \omega(N + \omega \mathcal{O}_E) = N + \omega N + \omega^2 \mathcal{O}_E$$

$$= \cdots = N + \omega N + \cdots + \omega^{e-1} N + \underbrace{\omega^e \mathcal{O}_E}_{\pi \mathcal{O}_E} = M + \pi \mathcal{O}_E$$

Lemma 10.3 $\implies M = \mathcal{O}_E$.

Therefore, $E = \mathcal{O}_E\left[\frac{1}{\pi}\right] = \sum_{\substack{1 \le i \le f \\ 0 \le j < e}} \underbrace{K}_{\mathcal{O}_K\left[\frac{1}{\pi}\right]} \cdot \alpha_i \omega^j \implies e \cdot f \ge [E : K]$.

10.1 $\implies e \cdot f \le [E : K]$.

$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

REMARK. The elements $\alpha_i \omega_j, 1 \le i \le f, 0 \le j < e$ form a basis of E over K.

THEOREM 10.5. Let E/K be a finite separable extension, let $|\cdot|_1, \cdots, |\cdot|_r$ be pairwise distinct extensions of the given absolute value $|\cdot|$ on K.
Let $e_i =$ ramification inde of E/K w.r.t. $|\cdot|_i$.
$f_i =$ residue class degree of E/K w.r.t. $|\cdot|_i$.
Then,

$$\sum_{i=1}^{r} e_i f_i = [E : K]$$

PROOF. Recall that $E \otimes_K K^\wedge \cong \prod_{i=1}^{r} E_i^\wedge$.

$$[E : K] = \dim_{K^\wedge}(E \otimes_K K^\wedge) \stackrel{9.16}{=} \sum_{i=1}^{r} [E_i^\wedge : K^\wedge] \stackrel{10.4}{=} \sum_{i=1}^{r} e(E_i^\wedge/K^\wedge) f(E_i^\wedge/K^\wedge)$$

9.7 and Residue field doesn't change upon completition implies:

$$= \sum_{i=1}^{r} e_i f_i$$

$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

DEFINITION. Assume E/K is finite. Then E/K is unramified w.r.t. the non archimedean absolute value $|\cdot|$ on E, if:
  i) $\overline{E}/\overline{K}$ is separable.
  ii) $[E^\wedge : K^\wedge] = [\overline{E} : \overline{K}]$.

REMARK.   1) Since $e(E/K, |\cdot|) f(E/K, |\cdot|) \stackrel{10.1}{\le} [E^\wedge : K^\wedge]$. If E/K is unramified then $e(E/K, |\cdot|) = 1$.
  2) If $|\cdot|$ is discrete and separable, then E/K is unramified $\stackrel{10.4}{\iff} e(E/K, |\cdot| = 1 \iff P_K \mathcal{O}_E = P_E)$.

THEOREM 10.6. Let $|\cdot|$ be non-arch and K complete w.r.t. $|\cdot|$. Extend $|\cdot|$ uniquely to the algebraic closure C of K. Then,
  i) $\overline{C}$ (=residue field) is an algebraic closure of $\overline{K}$.
  ii) For every finite subextension $F/\overline{K} \subseteq \overline{C}/\overline{K} \exists$ subextension $L/K \subseteq C/K$ such that $\overline{L} = F$ and $[L : K] = [F : \overline{K}]$.
  iii) The map from finite subextension of C/K to finite subetensions of $\overline{C}/\overline{K}$ induces an inclusion preserving bijection between the unramified subextensions $L/K \subseteq C/K$ and the finite separale subextensions $L/K \subseteq C/K$ and the finite separable subextensions $F/\overline{K} \subseteq \overline{C}/\overline{K}$. Every unramified extension of K is separable.

Written by Thanic Nur Samin

   iv) Every finite subextensions $E/K \subseteq C/K$ has a largest unramified subextension L/K. If $\overline{E}/\overline{K}$ is separable, then this maximal unramified subextension L satisfies $\overline{L} = \overline{E}$ and $[L : K] = [\overline{L} : \overline{K}]$.

   v) If L/K is unramified, then it is Galois $\iff$ $\overline{L}/\overline{K}$ is Galois, and in this case there is a canonical isomorphism $\operatorname{Gal}(L/K) \to \operatorname{Gal}(\overline{L}/\overline{K})$.

PROOF.   i) Corollary 9.15 $\implies$ $\overline{C}$ is algebraic over $\overline{K}$.

     $f(x) \in \overline{K}[x]$ monic $\implies$ $\exists$ monic $g(x) \in \mathcal{O}_K[x]$ with $\overline{g} = f$ [reduction modulo P_K].

     C is algebraically closed, so $g(x) = \prod_i (x - \alpha_i) \in C[x] \stackrel{9.15}{\implies} |\alpha_i| \leq 1 \implies \alpha_i \in \mathcal{O}_C$.

     $\implies f(x) = \overline{g}(x) = \prod_i(x - \overline{\alpha_i}) \in \overline{C}[x] \implies \overline{C}$ is an algebraic closure of $\overline{K}$.

   ii) Given $\beta \in \overline{C}$ and $F = \overline{K}(\beta)$ and minimal polynomial $\mu_{\beta, \overline{K}} \in \overline{K}[x] = $ min. poly of $\beta/\overline{K}$. $\exists$ monic $g(x) \in \mathcal{O}_K[x] : \overline{g}(x) = \mu_{\beta, \overline{K}}(x)$.

     9.15 (same as before) $\implies$ $g(x) = \prod_i(x - \alpha_i)$ with $\alpha_i \in \mathcal{O}_C \implies \exists i : \overline{\alpha_i} = \beta$.

     Set $L = K(\alpha_i) \implies [\overline{L} : \overline{K}] \stackrel{10.1}{\leq} [L : K] \stackrel{g \text{ irr.}}{=} \deg g = \deg(\mu_{\beta, \overline{K}}) \leq [\overline{L} : \overline{K}]$.

     The general case of a finitely generated field extension $\overline{F}/\overline{K} \subseteq \overline{C}/\overline{K}$ is reduced to the case of a monogenic extension by replacing $\overline{K}$ by $\overline{K}(\beta)$.

   iii) L/K finite unramified $\implies$ $\overline{L}/\overline{K}$ is finite (by 10.1) and separable (by definition of "unramified").

     Conversely, suppose $F/\overline{K}$ is finite separable and $L/K \subseteq C/K$ is a finite extension such that $\overline{L} = F$ and $[L : K] = [\overline{L} : \overline{K}] = [F : \overline{K}]$ [exists by ii]. Then, L/K is unramified.

     It suffices to show that this map is injective on the set of finite unramified extensions.

     Suppose E_1 and E_2 are unramified subextensions of C/K and $\overline{E_1} = \overline{E_2} = \overline{K}(\beta)$ for some $\beta \in \overline{C}$.

     Thus, β is separable over $\overline{K} \implies \mu_{\beta, K}$ is separable. Let $g(x) = \mathcal{O}_K[x]$ be monic and $\overline{g} = \mu_{\beta, \overline{K}}(x)$ $(*)$

     Theorem 9.1 (Hensel) $\implies$ $\exists$ factorization $g(x) = (x - \alpha_1)h_1(x)$ in $\mathcal{O}_{E_1}$, $(x - a_2)h_2(x)$ is in $\mathcal{O}_{E_2}$ with $\overline{\alpha_1} = \overline{\alpha_2} = \beta$.

     Roots of g in C lie on $\mathcal{O}_C$ and they reduce to pairwise distinct elements in $\overline{C}$ since $\mu_{\beta, \overline{K}}$ is separable $g(\alpha_1, \alpha_2) = 0 \implies \alpha_1 = \alpha_2$.

     $K(\alpha) \subset E, \overline{K}(\beta) \subset E2$

     $\implies [E_1 : K] \stackrel{\text{unramifieid}}{=} [\overline{E_i} : \overline{K}] = [\overline{K}(\beta) : \overline{K}] = \deg(\mu_{\beta, \overline{K}}) = \deg(g) = [K(\alpha_1) : K] \leq [E_i : K] \implies K(\alpha_1) = E_1$. Similarly, $K(\alpha_2) = E_2$

     Since $\alpha_1 = \alpha_2$ we have $E_1 = E_2$.

   iv) Let $E/K \subseteq C/K$ be any finite subextension, and $\overline{E}_s \subset \overline{E}$ be the maximal separable over $\overline{K}$ subextension of $\overline{E}/\overline{K} \implies \exists \beta \in \overline{E}_s : \overline{E}_s = \overline{K}(\beta)$.

     Choose $\alpha \in \mathcal{O}_E$ as in (ii) [$\overline{\alpha} = \beta$ and $g(\alpha) = 0$ for a monic lift of $\mu_{\beta, \overline{K}}$ to $\mathcal{O}_K[x]$].

     ii $\implies L := K(\alpha) \subseteq E$ is unramified $/K$ and $\overline{L} = \overline{E}_s$.

     If $L \subseteq \widetilde{L} \subset E$ and $\widetilde{L}/K$ unramified,

     $\implies \overline{L} \subseteq \overline{\widetilde{L}} \subseteq \overline{E}_s \implies \overline{L} = \overline{\widetilde{L}}$ and since $[\widetilde{L} : K] = [\overline{\widetilde{L}} : \overline{K}] = [\overline{L} : \overline{K}] = [L : K] \implies \widetilde{L} = L$.

     eg $K = \mathbb{Q}_p \implies \overline{K} = \mathbb{F}_p, \overline{C} \cong \overline{\mathbb{F}_p}$.

Tuesday, 11/12/2024

$$\left\{ \begin{array}{c} \text{subextensions } E/K \subset C/K \\ [E : K] < \infty \end{array} \right\} \xrightarrow[E \mapsto \overline{E}]{} \left\{ \begin{array}{c} \text{subextensions } F/\overline{K} \subset \overline{C}/\overline{K} \\ [E : K] < \infty \end{array} \right\}$$

$$\cup \qquad\qquad\qquad\qquad\qquad \cup$$

$$\{\text{unramified } E/K\} \xrightarrow[b_{ij}]{} \{\text{separable } F/\overline{K}\}$$

$E \mapsto \overline{E}, [E : K] = [\overline{E} : \overline{K}]$.

       Written by Thanic Nur Samin

v) Let L/K be unframified, $\sigma \in \operatorname{Aut}(L/K)$.

9.14 (uniqueness of extending absolute values) $\implies \forall a \in L, |\sigma(a)| = |a|$.

$\implies \sigma(\mathcal{O}_L) \subset \mathcal{O}_L, \sigma(P_L) \subset P_L \implies \sigma$ induces $\overline{\sigma} : \overline{L} \to \overline{L}$ over $\overline{K}$.

This gives us a group hoomorphism $\phi : \operatorname{Aut}(L/K) \to \operatorname{Aut}(\overline{L}/\overline{K})$.

Write $\overline{L} = \overline{K}(\beta)$. Let $g(x) \in \mathcal{O}_K[x]$ be a monic lift of $\mu_{\beta,\overline{K}}(x) \in \overline{K}[x]$.

9.12 (Hensel's Lemma) $\implies \exists \alpha \in \mathcal{O}_L$ such that $g(x) = (x - \alpha)h(x)$ in $\mathcal{O}_L[x]$ with $\overline{\alpha} = \beta$.

By part iii: $K(\alpha) = L$ (consider residue fields).

<u>Claim</u>: ϕ is injective.

<u>Proof of Claim</u>: Suppose $\overline{\sigma} = \operatorname{id}_{\overline{L}} \implies \beta = \overline{\sigma}(\beta) = \overline{\sigma}(\overline{\alpha}) = \overline{\sigma(\alpha)}$.

$g(\alpha) = 0 \implies g(\sigma(\alpha)) = 0$ and $\sigma(\alpha)$ has the same reduction mod P_L as α [namely β].

$\mu_{\beta,\overline{K}}$ separable $\implies \sigma(\alpha) = \alpha \implies \sigma = \operatorname{id}_L$. This proves the claim.

Now suppose L/K is Galois. Then $[\overline{L} : \overline{K}] \geq |\operatorname{Aut}(\overline{L}/\overline{K})| \overset{\text{Claim}}{\geq} |\operatorname{Aut}(L/K)| \overset{\text{Galois}}{=} [L : K]$.

$\implies [\overline{L} : \overline{K}] = |\operatorname{Aut}(\overline{L}/\overline{K})| \implies \overline{L}/\overline{K}$ is Galois.

Conversely, if $\overline{L}/\overline{K}$ is Galois $\implies \mu_{\beta,\overline{K}}$ splits into distinct linear monic factors in $\overline{L}[x]$.

9.12 (Hensel's Lemma) $\implies g(x)$ splits into distinct linear factors in $L[x] \implies L$ is obtained by adjoining all roots of $g(x)$ to K.

$\implies L/K$ is normal and since $g(x)$ is separable ($\impliedby \mu_{\beta,\overline{K}}(x)$ is separable) we have L/K is Galois.

$\square$

THEOREM 10.7. Suppose K is complete w.r.t. a non-archimedean absolute value $|\cdot|$ and the residue field $\overline{K}$ is finite with q elements. Let the notation be as in the previous theorem. Then,

i) $\forall n \in \mathbb{Z}_{\geq 1} \exists!$ unramified subextension of C/K which is of degree n over K. This subextension is generated by a primitive root of unity ζ_{q^n-1} of order $q^n - 1$.

ii) Suppose $m \in \mathbb{Z}_{\geq 1}$ is not divisible by $p := \operatorname{char}(\overline{K})$. Let $\zeta_m \in C$ be a primitive m'th root of unity. Then $K(\zeta_m)/K$ is unramified and $[K(\zeta_m) : K]$ is equal to the order of q modulo m in $(\mathbb{Z}/m\mathbb{Z})^{\times}$. In particular,

$$\mu^p(K) = \{\zeta \in J \mid \zeta \text{ is root of unity of order prime to } p\}$$

is cyclic of order $q - 1$ and is a set of representatives of $\overline{K}^{\times}$.

iii) Every unramified extension of L/K is Galois and $\operatorname{Gal}(L/K)$ is cyclic and is generated by a unique element $\varphi_{L/K}$ which induces the map $x \mapsto x^q$ on $\overline{L}$. $\varphi_{L/K}$ is called the <u>Frobenius</u> of L/K.

PROOF. $\mathbb{F}_{q^n} = $ splitting field of $x^{q^n} - x$ over $\mathbb{F}_q = \prod_{\alpha \in \mathbb{F}_{q^n}}(x - \alpha)$. $|\mathbb{F}_{q^n}^{\times}| = q^n - 1$. $\mathbb{F}_{q^n}^{\times} = \langle \zeta_{q^n-1} \rangle$.

i) $|\overline{K}| = q \implies \forall n \in \mathbb{Z}_{\geq 1}, \exists! \overline{K}_n/\overline{K} \subset \overline{C}/\overline{K}$ such that $[\overline{K}_n : \overline{K}] = n$ and $\overline{K}_n = \overline{K}(\overline{\zeta}_{q^n-1})$ where $\overline{\zeta}_{q^n-1}$ is a primitive root of unity of orer q$^n - 1$.

$g(x) = x^{q^n-1} - 1$ splits into distinct linear factors over $\overline{K}_n$.

9.12 (Hensel's Lemma) $f(x) := x^{q^n-1} - 1 \in \mathcal{O}_{L_n}[x]$ splits into distinct linear factors where $L_n \subset C/K$ is the unique unramified extension with $\overline{L}_n = \overline{K}_n$.

Let $\zeta \in \mathcal{O}_{L_n}$ be a root of $f(x)$ with $\overline{\zeta} = \overline{\zeta}_{q^n-1}$.

$f(\zeta) = 0 \implies \zeta^{q^n-1} = 1 \implies \operatorname{ord}(\zeta) \mid q^n - 1$ but $q^n - 1 = \operatorname{ord}(\overline{\zeta}) \mid \operatorname{ord}(\zeta)$.

Therefore, ζ is a primitive <u>root</u> of unity of order $q^n - 1$.

$\implies K(\zeta) = L_n$ ($\overline{\zeta}_{q^n-1} \in \overline{K(\zeta)} \subset \overline{L}_n = \overline{K}_n = \overline{K}(\overline{\zeta}_{q^n-1})$).

$\implies L_n$ is the unique unramified extension with residue field $\overline{K}_n$ and it is generated by a root of unity of order $q^n - 1$.

ii) Suppose $p \nmid m$ and let $\zeta_m \in C$ be a primitive m'th root of 1. Set $n := \min\{l \in \mathbb{Z}_{>0} \mid q^k \equiv 1\,(m)\}$.

$\implies \zeta_m \in \langle \zeta_{q^n-1} \rangle$.

$\implies K(\zeta_m) \subset K(\zeta_{p^n-1})$.

and $\zeta_m = \zeta_{q^n-1}^{ra}$ where $r = \frac{q^n-1}{m}$ and $\gcd(a, m) = 1$.

Therefore, $\overline{\zeta_m} = \overline{\zeta}_{q^n-1}^{ra} \implies \text{ord}(\overline{\zeta_m}) = m$.

If $\overline{\zeta}_m^{q^k} = \overline{\zeta}_m$ for $k \leq n$ then $\overline{\zeta}^{q^k-1} = 1 \implies m \mid q^k - 1 \implies q^k \equiv 1 \pmod{m}$ for some $k \geq 1$.

$\implies k \geq n \implies \overline{K}(\overline{\zeta}_m) = \overline{K}_n.$

$\implies [K(\zeta_m) : K] = [\overline{K}[\overline{\zeta}_m] : \overline{K}] = n.$

iii) $\impliedby$ Theorem 10.6 v and i.

$\square$

PROPOSITION 10.8. Let $|\cdot|$ be discrete absolute value on K with normalized valuation $w : K \to \mathbb{Z} \cup \{\infty\}$ (we do not assume K is complete).

i) Let $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n \in \mathcal{O}_K[x]$ be an Eisenstein polynomial ($w(a_i) \geq 1, w(a_n) = 1$) and let π be a root of f. Then $|\cdot|$ has unique extension $|\cdot|_1$ to $E := K(\pi)$ and E/K is purely ramified ($\underset{\text{dfn}}{\iff} e(E/K, |\cdot|_1) = [E : K]$), and fmf is ireudcible, and π is a prime element of E w.r.t. $|\cdot|_1$.

ii) Conversely any purely ramified extension E/K w.r.t. an extension $|\cdot|_1$ of $|\cdot|$ to E is of the form $E = K(\pi)$, where π is a prime element of E w.r.t. $|\cdot|_1$.

The minimal polynomial of π is an Eisenstein polynomial.

PROOF.   i) Let $|\cdot|_1$ be some extension of $|\cdot|$ to E. We have $\pi^n = -a_1 \pi^{n-1} - \cdots - a_n$ (1).

If $|\pi|_1 \geq 1$ then $|\pi|_1^n \geq |\pi|_1^{n-i} > |a_i \pi^{n-i}|_1$ by strong triangle inequality. This is a contradiction to (1).

Thus, $|\pi|_1 < 1$ and $|\pi|_1^n = |a_n| \implies |K^\times| \subseteq |a_n|^{\mathbb{Z}} = |\pi|_1^{n\mathbb{Z}} \subset |E^\times|_1$.

Therefore, $e(E/K, |\cdot|_1) \geq n = \deg(f) \geq [E : K] \underset{10.1}{\overset{9.16}{\implies}} \sum_{i=1}^r e_i f_i \geq e_1 = e(E/K, |\cdot|_1)$ (2) [same notation as in 9.16].

Then, $e(E/K, |\cdot|_1) = [E : K] \implies f$ is the minimal polynomial of $\pi, r = 1 \implies |\cdot|_1$ is the only extension of $|\cdot|$ to E.

ii) By assumption $[E : K] = e(E/K, |\cdot|_1)$.

(2) $\implies |\cdot|_1$ is the unique extension of $|\cdot|$ to E. Recall that $|E^\times| = |\pi|_1^{\mathbb{Z}}$.

Let π be a prime element of E. Then $[K(\pi) : K] \underset{10.1}{\geq} e(K(\pi)/K, |\cdot|_1) = e(E/K, |\cdot|_1) = [E : K] \implies E = K(\pi)$.

Let $f(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_n \in K[x]$ be the minimal polynomial of π/K with $a_0 = 1$.

$a_0 \pi^n + \cdots + a_{n-1}\pi + a_n = 0 \implies \exists 0 \leq i < j \leq n : |a_i \pi^{n-i}|_1 = |a_j \pi^{n-j}|_1 = \max\{|a_k \pi^{n-k}|_1 \mid 0 \leq k \leq n\} \neq 0 \implies |\pi|^{j-i} = \left|\frac{a_j}{a_i}\right| \in |K^\times| \implies j - i = n \implies j = n, i = 0.$

$\implies |\pi|^n = |a_n| \implies |a_n|^{\mathbb{Z}} = |K^\times| = |\pi|^{n\mathbb{Z}}.$

Thus, a_n is a uniformizer of K and $|a_i| \leq |a_n|$ for $1 \leq i \leq n$.

$\square$

Thursday, 11/14/2024

Recall: we hat $E = K(\pi), \pi = $ root of Eisenstein polynomial ($(K, |\cdot|)$ discretely valued) $\implies E/K$ purely ramified and $|\cdot|$ has a unique extension to E.

Example: $K = \mathbb{Q}, p = $ prime, $n \geq 1 : p$'th cyclotomic polynomial:

$$\Phi_{p^n}(x) = \frac{x^{p^n} - 1}{x^{p^{n-1}} - 1} = \frac{(x^{p^{n-1}} - 1 + 1)^p - 1}{x^{p^{n-1}} - 1} = \frac{1}{x^{p^{n-1}} - 1} \sum_{j=1}^p \binom{p}{j}(x^{p^{n-1}} - 1)^j$$

$$\implies f(x) := \Phi_{p^n}(x+1) = \sum_{j=1}^p \binom{p}{j}((x+1)^{p^{n-1}} - 1)^{j-1}$$

$$\implies f(x) \mod p = x^{p^{n-1}(p-1)} \text{ and } f(0) = p$$

Therefore, f is Eisenstein for the p-adic absolute value on $\mathbb{Q}$.

10.8 $\implies |\cdot|_P$ has a unique extension to $\mathbb{Q}(\zeta_{p^n} - 1)$ and $\zeta_{p^n} - 1$ is a uniformizer of $\mathbb{Q}(\zeta_{p^n})$.

It also follows that $p \cdot \underbrace{\mathcal{O}_{\mathbb{Q}(\zeta_{p^n})}}_{=\mathbb{Z}[\zeta_{p^n}]} = P^{\phi(p^n)}$ where P is generated by $(\zeta_{p^n} - 1)$.

CHAPTER 11

Local Fields

DEFINITION. A field K with absolute value $|\cdot|$ is called a <u>local field</u> if the topology on K induced by $|\cdot|$ is <u>locally compact but not discrete</u>.

REMARK.   1) The topology on K induced by $|\cdot|$ is discrete $\iff$ $|\cdot|$ is the trivial absolute value.
   2) K is locally compact $\iff$ $\forall c \in \mathbb{R}_{>0}$, the closed disk $D(0, \leq c) = \{x \in K \mid |x| \leq c\}$ is compact ($\implies$ every $a \in K$ has a compact neighborhood $a + D(0, \leq c)$).
      $\iff \exists c \in \mathbb{R}_{>0} : D(0, \leq c)$ is compact.
   3) if K is localy compact then K is complete: given a cauchy sequence $(x_n)_{n \geq 0}, \exists c > 0$ such that $\forall n \geq 0, |x_n| \leq c$.
      Since K is locally compact, $D(0, \leq c)$ is compact. Thus, (x_n) has a convergent subsequence. But it is also a Cauchy sequence, so it is indeed convergent.
   4) K is complete and $|\cdot|$ is archimedean implies (by Ostrowksi) that $(K, |\cdot|) \cong \mathbb{R}, |\cdot|_\infty$ or $\cong (\mathbb{C}, |\cdot|_\infty)$. So we have local completeness automatically.
   5) If K is complete and $|\cdot|$ is non-archimedean, then $P_K = \{x \in K \mid |x| < 1\}$ is open. If K is also locally compact then $\mathcal{O}_K = \bigsqcup_{\overline{a} \subset \mathcal{O}_K \subset P_K} (\widetilde{a} + P_K)$ where $\widetilde{a}$ is a lift of $\overline{a}$ to $\mathcal{O}_K$. Thus, since K is locally compact, $\mathcal{O}_K$ is compact. The cosets are also open.
      Therefore, residue field $\mathcal{O}_K / P_K$ must be finite.
   6) <u>Claim</u>: if K is locally compact and $|\cdot|$ is non-archimedean then $|\cdot|$ is discrete.

   PROOF. Suppose $(x_n)_{n \geq 1}$ sequence in $K^\times$ with $|x_i| \neq |x_j|$ and $\lim_{n \to \infty} |x_n| = c > 0$. Then $(|x_n|)$ is bounded, and since K is locally compact we have $x_{n_i} \to a \in K^\times$. Then, $|\underset{\in K^\times}{a}| = \lim_{i \to \infty} |x_{n_i}| = c > 0$.
   $\implies |x_{n_i}| = |\underbrace{x_{n_i} - a}_{\to 0} + a| = |a|$ for all $i \gg 0$ which is a contradiction. $\qquad\square$

PROPOSITION 11.1. Let $|\cdot|$ be a non-archimedean absolute value on K. Then TFAE:
   i) $(K, |\cdot|)$ is a local field.
   ii)   a) $(K, |\cdot|)$ is complete.
         b) $\overline{K} = \mathcal{O}_K / P_K$ is finite.
         c) $|\cdot|$ is discrete.

   PROOF. i $\implies$ ii we have already completed.
ii $\implies$ i: Suppose $\exists$ open covering $(U_i)_{i \in I}$ of $\mathcal{O}_K$ which does not hve a finite subcovering.
Let π be uniformizer of $(K, |\cdot|)$ and $\mathcal{R}$ of $(K, |\cdot|)$ and $\mathcal{O}_K \supset \mathcal{R}$ complete system of representatives of $\overline{K}$ which contains 0.
$\implies \mathcal{O}_K = \bigsqcup_{a \in \mathcal{R}} (a + P_K)$.
$|\overline{K}| < \infty \implies \exists a_0 \in \mathcal{R} : a_0 + P_K = a_0 + (\pi)$ is not contained in a finite union of U_i's.
$(\pi) = \bigsqcup_{a \in \mathcal{R}} a\pi + (\pi^2) \implies \exists a_1 \in \mathcal{R}$ such that $a_0 + a_1\pi + (\pi)^2$ is not contained in a finite union of U_i's.
Continuing in this way we find a sequence $(a_i)_{i \geq 0}$ in $\mathcal{R}$ such that $\forall n \geq 0 : a_0 + a_1\pi + \cdots + a_n\pi^n + (\pi^{n+1})$ is not contained in a finite union of U_i's.
K complete so $a_0 + a_1\pi + a_2\pi^2 + \cdots$ converges in K to some $a \in \mathcal{O}_K$.
$\exists i \in I : a \in U_i, U_i$ open $\implies U_i$ contains neighborhood of $a \implies U_i$ contains a subset of the form $a + (\pi^m)$ for some $m \geq 0$. Then U_i contains $a_0 + a_1\pi + \cdots + a_{m-1}\pi^{m-1} + (\pi^m)$ which is a contradiction. $\qquad\square$

DEFINITION. A <u>non-archimedean local field</u> is a local field whose absolute value (uniquely determined by the topology up to equivalence) is non-archimedean.

THEOREM 11.2. Let $(K, |\cdot|)$ be a non-archimedean local field.
  i) $\mathrm{char}(K) = 0 \implies K$ is a finite extension of $\mathbb{Q}_p$ for a unique prime p.
  ii) $\mathrm{char}(K) = p > 0 \implies K$ is isomorphic to $\mathbb{F}_q((t))(= \mathrm{Frac}(\mathbb{F}_q[[t]]))$ where $q = |\overline{K}|$ is a power of p by an isomorphism which makes $|\cdot|$ equivalent to:
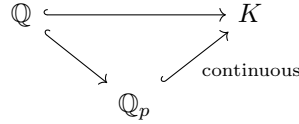
$$\left| \sum_{i \gg -\infty}^{\infty} a_i t^i \right| = q^{-v(f)}$$

    where $v(f) = \min\{i \in \mathbb{Z} \mid a_i \neq 0\}$.

PROOF.   i) Note $\mathbb{Q} \subset K$. If $|\cdot|\big|_{\mathbb{Q}}$ is trivial $\implies Q \hookrightarrow \overline{K}$, since $\overline{K}$ is finite it is not possible. Thus, the restriction cannot be trivial.
        Theorem 9.3 $\implies |\cdot|\big|_{\mathbb{Q}}$ is equivalent to $|\cdot|_p$ for a unique prime p.
        Proposition 9.6 $\implies \exists$ unique extension:

        $|K^\times| = |\pi|^{\mathbb{Z}} \supset |p|^{\mathbb{Z}} \neq \{1\}$.
        Therefore, $[|K^\times| : |\mathbb{Q}_p^\times|]$ is finite.
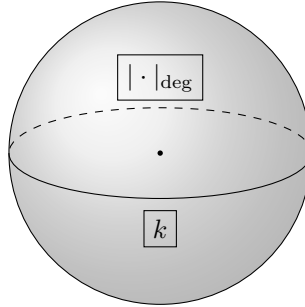 $\overline{K}$ finite $\implies f(K/\mathbb{Q}_p) = [\overline{K} : \mathbb{F}_p] < \infty$.
        K complete and $|\cdot|$ is discrete. This along with theorem 10.4 $(e \cdot f = n)$ implies $[K : \mathbb{Q}_p] < \infty$.
  ii) HW 13.

$\square$

REMARK. Every non-trivial absolute value $|\cdot|$ on $k(x)$ which is trivial on k is of one of the following form:
  i) $|\cdot|_f$ where $|g|_f = e^{-v_f(g)}$ where $f(x) \in k[x]$ is irreducible and $v_f(g) = m$ if $f^m \,||\, g$.
  ii) $|\cdot|_{\deg}$ where $|g|_{\deg} = e^{\deg(g)}$.

COROLLARY 11.3. The local fields (up to isomorphism) are:
  i) $\mathbb{R}$ and $\mathbb{C}$
  ii) The finite extensions of $\mathbb{Q}_p$ where p is any prime.
  iii) The fields $\mathbb{F}_q((t))$.

DEFINITION. The following are called <u>global fields</u>:
  i) The finite extensions of $\mathbb{Q}$ (ie number fields)
  ii) The finite extensions of $\mathbb{F}_p(t) = \mathrm{Frac}(\mathbb{F}_p[t])$

PROPOSITION 11.4. The local fields are precisely the completions of global fields w.r.t. a non-trivial absolute value.

SKETCH.   1) We have seen: any completion of a global field is a local field (HW9, Problem 8 for $\mathbb{F}_q(t)$ and HW11, Problem 2 for number field).

2) Furthermore, $\mathbb{F}_q((t))$ is the t-adic completion of $\mathbb{F}_q(t)$.

3) Remaining case: for any finite extension K of $\mathbb{Q}_p$ $\exists$ number field $E/\mathbb{Q}$ and a non-archimedean absolute value $|\cdot|$ on E so that $(E, |\cdot|)^\wedge \cong K$.

This will be proved in 11.7.

$\square$

Note: we can have fields that are abstractly isomorphic but still extensions: $\mathbb{F}_q((t^{\frac{1}{n}}))$ and $\mathbb{F}_q((t))$ are isomorphic but $\mathbb{F}_q((t))[x]/(x^n - t) = \mathbb{F}_q((t^{\frac{1}{n}}))$

Tuesday, 11/19/2024

THEOREM 11.5 (Krasner's Lemma). Let K be complete w.r.t. a non-archimedean absolute value $|\cdot|$, and let C be an algeraic closure of K. Suppose $\alpha \in C$ has a separable min. poly. $\mu_{\alpha,K}(x) = \prod_{j=1}^{n}(x - \alpha_j)$ with $\alpha_1 = \alpha$.
Then, whenever $\beta \in C$ satisfies $|\beta - \alpha| < |\alpha_j - \alpha|$, for all $2 \le j \le n$.
Then, $K(\alpha) \subset K(\beta)$.

PROOF. Suppose $K(\alpha) \not\subset K(\beta)$. Then $\alpha \notin K(\beta) \implies L := K(\beta)(\alpha)$ is a proper extension of $K(\beta)$.
$\mu_{\alpha,K(\beta)} \mid \mu_{\alpha,K} \implies \alpha$ is separable over $K(\beta)$. Thus, $L/K(\beta)$ is separable and non-trivial.
Thus, $\exists \sigma : L \underset{K(\beta)}{\hookrightarrow} C \exists j > 1 : \sigma(\alpha) = \alpha_j$ extend σ to $\widetilde{\sigma} \in \text{Aut}(C/K(\beta))$, since K is complete, $|\cdot|$ extends uniquely to C.
Thus, $\widetilde{\sigma}$ preserves the absolute value on C since $|\gamma|_{\text{new}} := |\widetilde{\sigma}(\gamma)| \implies |\gamma|_{\text{new}} = |\gamma|$.
Therefore, $|\beta - \alpha| = |\widetilde{\sigma}(\beta - \alpha)| = |\beta - \widetilde{\sigma}(\alpha)| = |\beta - \alpha_j| = |\beta - \alpha + \alpha - \alpha_j| = \max\{|\beta - \alpha|, |\alpha - \alpha_j|\} = |\alpha - \alpha_j|$.
This is a contradiction to our assumption. Thus, $K(\alpha) \subset K(\beta)$.

$\square$

THEOREM 11.6. Let K be complete w.r.t. a non-archimedean absolute value $|\cdot|$ and let $f(x) = \sum_{\nu=0}^{n} a_\nu x^\nu$ be a <u>monic separable</u> polynomial over K of degree n. Then $\exists \delta = \delta(f) > 0$ such that if $g = \sum_{\nu=0}^{n} b_\nu x^\nu$ is another monic irreducible polynomial of degree n for which

$$|f - g| = \max\{|a_\nu - b_\nu| \mid 0 \le \nu \le n\} < \delta$$

Then g is irreducible and separable, and then for any root α of f, $\exists$ unique root β of g such that:

$$|\beta - \alpha| < \max\{|\alpha' - \alpha| \mid f(\alpha') = 0, \alpha' \in C\}$$

Where C is algebraic closure of K. Moreover, $K(\alpha) = K(\beta)$.

PROOF. Write $f(x) = \prod_{j=1}^{n}(x - \alpha_j)$ in $C[x]$ with $\alpha_i \ne \alpha_j$ for $i \ne j$.
Let $\alpha := \alpha_i$ be any root of f.
Claim: $|f| = \max\{|\alpha_\nu|\} \ge |\alpha|$.
<u>Proof of Claim:</u> Suppose $|\alpha| > |f|$. f monic $\implies |f| \ge 1 \implies |\alpha| > 1$.
$\implies \forall 0 \le j \le n-1 : |\alpha|^n = |\alpha||\alpha|^{n-1} > |f||\alpha|^{n-1} \ge |\alpha_j||\alpha|^{n-1} \underset{|\alpha|>1}{>} |a_j \alpha^j|$

$\implies 0 = |f(\alpha)| = \left|\alpha^n + \sum_{\nu=0}^{n-1} a_\nu \alpha^\nu\right| = |\alpha|^n > 1$ which is a contradiction.
Choose δ small eough so that $\sqrt[n]{\delta}|f| \le \min\{|\alpha_i - \alpha_j| \mid i \ne j\} =: M$.
Now assume $|f - g| < \delta$. Write $g(x) = \prod_{j=1}^{n}(x - \beta_j)$.
Fix $1 \le i \le n$. Then, $\left|\prod_{j=1}^{n}(\alpha_i - \beta_j)\right| = |g(\alpha_i)| = |g(\alpha_i) - f(\alpha_i)| = \left|\sum_{\nu=0}^{n-1}(b_\nu - a_\nu)\alpha_i^\nu\right| \le |f - g| \max\{|\alpha_i|^\nu\} < \delta|f|^n \le M^n$.
Then, $\exists$ at least one $j = j(i)$ so that $|\alpha_i - \beta_j| < M$.
Theorem 11.5 (Krasner's Lemma) with $\beta := \beta_j \implies K(\alpha_i) \subset K(\beta_j)$. But we know $[K(\alpha_i) : K] = \deg(f) = \deg(g) \ge [K(\beta_j) : K] \implies K(\alpha_i) = K(\beta_j)$.
We show that the map $\alpha_i \mapsto \beta_j = \beta_{j(i)} = \beta(\alpha_i)$ is injective, since for $i \ne k$ we have:

$$|\beta(\alpha_i) - \beta(\alpha_k)| = |\underbrace{\beta(\alpha_i) - \alpha_i}_{<M} + \underbrace{\alpha_i - \alpha_K}_{\ge M} + \underbrace{\alpha_k - \beta(\alpha_k)}_{<M}| = |\alpha_i - \alpha_k| \ne 0$$

$\implies \beta(\alpha_i) \ne \beta(\alpha_k)$ so the map is injective. We also have g is separable.

$\square$

COROLLARY 11.7. $\forall$ finite extension $K/\mathbb{Q}_p \exists$ subfield $F \subset K$ such that:
   i) $F/\mathbb{Q}$ is finite (hence F is a number field) and $[F : \mathbb{Q}] = [K : \mathbb{Q}_p]$.
   ii) F is closure of K w.r.t. the unique extension of the p-adic absolute value on $\mathbb{Q}_p$ to K, hence $(F, |\cdot|\big|_F)^\wedge = K$.

PROOF. It is a finite extension over characteristic 0, so this is a separable extenson. We write $K = \mathbb{Q}_p(\alpha)$ for some $\alpha \in K$ and we have minimal polynomial $\mu_{\alpha,\mathbb{Q}_p}(x) \in \mathbb{Q}_p[x]$ is irreducible and separable. Choose δ from previous theorem. Choose $g(x) \in \mathbb{Q}[x]$ monic of degree n such that $|f - g| < \delta$.
Theorem 11.6 $\implies \exists \beta \in \overline{\mathbb{Q}}_p \implies g(\beta) = 0$ and $\mathbb{Q}_p(\beta) = \mathbb{Q}_p(\alpha) = K$. Also, g is irreducible over $\mathbb{Q}_p$ and thus $\mathbb{Q}$.
Set $F = \mathbb{Q}(\beta) \subset K$. Then $[F : \mathbb{Q}] = \deg(g) = n = [K : \mathbb{Q}_p]$.
F contains $\mathbb{Q}$ and since $\mathbb{Q}$ is dense in $\mathbb{Q}_p$ we can deduce that closure of F in K contains $\mathbb{Q}_p$ and β. Therefore, β is dense in K. $\qquad\square$

We have the following diagram:

$$
\begin{array}{ccc}
 & & (F, |\cdot|\big|_F)^\wedge \\
 & \nearrow & \downarrow \\
F & & \\
 & \searrow & \downarrow \\
 & & K
\end{array}
$$
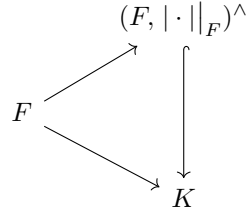
COROLLARY 11.8.   i) The algebraic closure of $\mathbb{Q}_p$ is not complete w.r.t. $|\cdot|_p$ [HW11/5].
   ii) The completion $\mathbb{C}_p = (\mathbb{Q}_p^{\mathrm{alg}}, |\cdot|_p)^\wedge$ is algebraically closed [HW13].

PROPOSITION 11.9. In a fixed algebraic closure of a local field K of characteristic 0, there are only finitely many finite extensions of a fixed degree.

PROOF. Application of Krasner's Lemma [Theorem 11.6]. HW13. $\qquad\square$

DEFINITION. Let E/K be a finite extension and $|\cdot|$ a discrete nontrivial absolute value on E. E/K is $\underline{\text{tamely ramified}}$ if $\mathrm{char}(\overline{E}) \nmid e(E/K, |\cdot|)$ We consider unramified extensions to be also tamely ramified. Otherwise it is called $\underline{\text{wildly ramified}}$.

EXAMPLE. $K = \mathbb{Q}_p, E = \mathbb{Q}_p(\zeta_{p^n})$ where $\zeta_{p^n} = $ primitive p^n th root of 1.
Then $[E_n : \mathbb{Q}_p] = \phi(p^n) = \deg(\Phi_{p^n}) = (p-1)p^{n-1} = e(E_n/\mathbb{Q}_p, |\cdot|_p)$.
$E_n/\mathbb{Q}_p$ is $\underline{\text{purely ramified}}$, and totally ramified $\iff n = 1$.
$\underbrace{E_n/E_1}_{p^{n-1}}$ is $\underline{\text{wildly ramified}}$.

Thursday, 11/21/2024

Recall:
   i) E/K $\underline{\text{purely ramified}}$: $e(E/K, |\cdot|) = [E : K]$.
   ii) E/K $\underline{\text{tamely ramified}}$: $\mathrm{char}(\overline{K}) \nmid e(E/K, |\cdot|)$

PROPOSITION 11.10. Let K be complete w.r.t. non-archimedean discrete absolute value $|\cdot|$ and let E/K be a finite, purely and tamely ramified extension.
   i) $\exists$ uniformizer π_K of K such that $E = K(\sqrt[e]{\pi_K})$ where $e = [E : K]$.
   ii) E/K is Galois $\iff K$ contains a primitive eth root of unity, in which case $\mathrm{Gal}(E/K)$ is isomorphic to $\mu_e = $ group of eth roots of unity $(\cong \mathbb{Z}/e\mathbb{Z})$.

EXAMPLE. Only roots of unity contained in $\mathbb{Q}_p$ ae the $(p-1)$ th roots of unity, if $p > 2$; then the only roots of unity in $\mathbb{Q}_2$ are ± 1
Only tamely ramified and purely ramified $\underline{\text{Galois}}$ extensions of $\mathbb{Q}_p$ are $\mathbb{Q}_p(\sqrt[e]{up})$ where $u \in \mathbb{Z}_p^\times, e \mid p - 1$.
If $\mathbb{Q}_{p,nr} = \widehat{\mathbb{Q}_p^{nr}}$ [$\mathbb{Q}_p^{nr} = $ maximal unramified extension] then $\mathbb{Q}_{p,nr}(\sqrt[e]{up} \mid |u| = 1, e \in \mathbb{Z}_{\geq 1}, p \nmid e) =: \mathbb{Q}_{p,\text{tame}}$.

Written by Thanic Nur Samin

$$\mathrm{Gal}(\mathbb{Q}_{p,\mathrm{tame}}/\mathbb{Q}_{p,nr}) \cong \varprojlim_{\substack{e \geq 1 \\ p \nmid e}} \mu_e \underset{\text{non. canonical}}{\cong} \prod_{\substack{\ell \text{ prime} \\ \ell \neq p}} \mathbb{Z}_\ell$$

$$1 \longrightarrow \mathrm{Gal}(\mathbb{Q}_{p,\mathrm{tame}}/\mathbb{Q}_{p,nr}) \longrightarrow \mathrm{Aut}(\mathbb{Q}_{p,\mathrm{tame}}/\mathbb{Q}_p) \longrightarrow \mathrm{Aut}(\mathbb{Q}_{p,nr}/\mathbb{Q}_p) \longrightarrow 1$$

$$\|\wr \qquad\qquad\qquad \|\wr$$

$$\varprojlim_{p \nmid e} \mu_e \qquad\qquad\qquad \varprojlim_n \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$$

$$\|\wr$$

$$\widehat{\mathbb{Z}}$$

Lubin-Tate Theory

Lubin, Tate (1965) Formal complex multiplication in local fields.
Serre: Local Class Field Theory in Cassels-Fröhlich.
Neukirch: ch V, section 4-5.
<u>Goal</u>: Generalize the tower of fields $(\mathbb{Q}_p(\zeta_{p^n}))_n$ and $\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p) \underset{\text{canonical}}{\cong} \mathrm{Aut}(\mu_{p^n}) \underset{\text{canonical}}{\cong}$
$(\mathbb{Z}/p^n)^\times$

Formal Groups

DEFINITION. A 1-dimensional commutative <u>formal group</u> (law) over a commutative ring $\mathcal{O}$ is a formal power sries $F(x,y) \in \mathcal{O}[[x,y]]$ satisfying:

   1) $F(x,y) \equiv x+y \bmod \deg 2$
   2) $F(x,y) = F(y,x)$
   3) $F(x,F(y,z)) = F(F(x,y),z)$

Intuitively, $x \underset{F}{+} y := F(x,y)$

REMARK. It can be shown that $\exists$ unique power series $\iota \in \mathcal{O}[[x]], \iota(x) \equiv -x \bmod \deg 2$ and $F(\iota(x),x) = F(x,\iota(x)) = 0$.

<u>Convention</u>: From now on, "formal group" means "1-dimensional commutative formal group".

EXAMPLE.   1) Additive Formal Group: $\widehat{\mathbb{G}}_a(x,y) = x+y$.
   2) Multiplicative Formal Group: $\widehat{\mathbb{G}_m}(x,y) = x+y+xy = (1+x)(1+y)-1$.
   3) E = elliptic curve over a field $k \rightsquigarrow$ we can express addition on E as a power series in x and $_y$.
   4) If $f(x) = a_1 x + a_2 x^2 + \cdots \in \mathcal{O}[x]$ with $a_1 \in \mathcal{O}^\times$ then $\exists! f^{-1}(x) = b_1 x + b_2 x^2 + \cdots \in \mathcal{O}[[x]]$ such that $b_1 = a_1^{-1}$ and $f(f^{-1}(x)) = f^{-1}(f(x)) = x$.
       Then, $F_f(x,y) := f^{-1}(\underbrace{f(x)+f(y)}_{\text{const. term} = 0}) \in \mathcal{O}[x,y]$ and $F_f(x,y)$ is a formal group over $\mathcal{O}$.

       For existence of f^{-1} compute $\sum_{i=1}^\infty a_i \left(\sum_{j=1}^\infty b_j x^j\right)^i$ and set this $= x$.
       $a_1 b_1 = 1 \implies b_1 = a_1^{-1}$.
       We work modulo some x^m inductively $\rightsquigarrow b_n \times (\text{unit}) = $ polynomial involving a_i and $b_1, \cdots b_{n-1}$, we can solve for b_n.

DEFINITION. Let F, G e formal groups over G. A <u>homomorphism</u> from F to G is a powerseries $f(x) \in x\mathcal{O}[[x]]$ such that $f(F(x,y)) = G(f(x),f(y))$.
A homomorphism $f : F \to G$ is an isomorphism if $\exists$ a homomorphism $g : G \to F$ such that $f(g(x)) = g(f(x)) = x$.

EXERCISE. $f(x) = \sum_{i=1}^\infty a_i x^i$ is an isomorphism iff $a_1 \in \mathcal{O}^\times$.

If $\mathcal{O}'/\mathcal{O}$ is a ring extension and $f(x) = x\mathcal{O}'[[x]]$ and $f(F(x,y)) = G(f(x),f(y))$ then we say f is a homomorphism from F to G <u>defined over $\mathcal{O}'$</u>

PROPOSITION 12.1. Let $F/\mathcal{O}$ be formal group. Then, the set:

$$\mathrm{End}_{\mathcal{O}}(F,F) = \{f : F \to F \mid f \text{ is a homomorphism defined over } \mathcal{O}\}$$

equipped with the addition $(f+g)(x) = F(f(x),g(x))$ and multiplication $(f \cdot g)(x) = f(g(x))$ [not necessarily equal to $g(f(x))$] is an associative ring with unit $1(= 1(x) = x)$

EXAMPLE. Let $f(x) = a_1 x + a_2 x^2 + \cdots$ with $a_1 \in \mathcal{O}^\times$ and f^{-1} defined as before, and $F_f(x,y) = f^{-1}(\underbrace{f(x) + f(y)}_{\widehat{\mathbb{G}}_a(f(x), f(y))})$.

Then, $f : F_f \to \widehat{\mathbb{G}}_a$ is an isomorphism, called a logarithm of F_f.

We also have $f^{-1} : \widehat{\mathbb{G}}_a \to F_f$ an isomorphism (exponential).

EXERCISE. If $\mathcal{O}$ is a field of characteristic 0 then every formal group has a logarithm, i.e. is isomorphic to $\widehat{\mathbb{G}}_a$

EXAMPLE. If $\mathcal{O} = \mathbb{F}_{p^2}$ and $F = \widehat{\mathbb{G}}_a$ over $\mathbb{F}_{p^2} \implies \forall \lambda \in \mathcal{O} : [\lambda](x) = \lambda x$ is an endomorphism of $\widehat{\mathbb{G}}_a$:

$$\widehat{\mathbb{G}}_a(\lambda x, \lambda y) = \lambda x + \lambda y = \lambda \widehat{\mathbb{G}}_a(x,y)$$

and $[\pi](x) := x^p$ is an endomorphism of $\widehat{\mathbb{G}}_a : \widehat{\mathbb{G}}_a(x^p, y^p) = x^p + y^p = (x+y)^p = \widehat{\mathbb{G}}(x,y)^p$.

Thus, if $\lambda \notin \mathbb{F}_p$ then $\underbrace{[\pi] \cdot [\lambda]}_{[\lambda^p] \cdot [\pi]} \neq [\lambda] \cdot [\pi]$.

Therefore, $\mathrm{End}_{\mathbb{F}_{p^2}}(\widehat{\mathbb{G}}_a)$ is $\underline{\text{not}}$ commutative.

Let K be a non-archimedean local field with ring of integers $\mathcal{O} = \mathcal{O}_K$ with maximal ideal P_K and residue field $k = \mathcal{O}/P_K$ of char p and $|k| = q$.

DEFINITION. A formal $\underline{\mathcal{O}\text{-module}}$ is a formal group F over $\mathcal{O}$ together with a ring homomorphism $[\cdot]_F : \mathcal{O} \to \mathrm{End}_{\mathcal{O}}(F)$ such that $\forall a \in \mathcal{O} : [a]_F(x) \equiv ax \mod \deg 2$.