Example: cyclotomic fields

μ - primitive p^r-th root of unity, $r \geq 1$

p - prime number

$K = \mathbb{Q}(\mu)$

p^r-th roots of unity form a cyclic group $\mathbb{Z}/p^r\mathbb{Z}$, primitive roots of unity correspond to the elements of $(\mathbb{Z}/p^r\mathbb{Z})^\times$

$$|(\mathbb{Z}/p^r\mathbb{Z})^\times| = p^r - p^{r-1} = p^{r-1}(p-1) = e$$

K is Galois $/\mathbb{Q}$. The action of $g \in Gal(K/\mathbb{Q})$ is uniquely determined by the image of μ which is μ^n for some $n \in (\mathbb{Z}/p^r\mathbb{Z})^\times$

$\Rightarrow$ we get a group embedding

$$G = Gal(K/\mathbb{Q}) \hookrightarrow (\mathbb{Z}/p^r\mathbb{Z})^*$$
$$g \longmapsto n, \text{ s.t. } g\mu = \mu^n$$

$\Rightarrow G$ is abelian.

Consider $F \in \mathbb{Z}[x]$, $F = \dfrac{X^{p^r} - 1}{X^{p^{r-1}} - 1}$

$y = X^{p^{r-1}} \Rightarrow y^p = X^{p^r} \Rightarrow F = \dfrac{y^p - 1}{y - 1} =$

$= y^{p-1} + \ldots + 1 =$

$$= X^{p^{q-1}(p-1)} + \dots + 1 = X^{e} + \dots + 1$$

F is the cyclotomic polynomial.

$\deg F = e$.

μ is a root of F, because μ is a root of $X^{p^q} - 1$, but not of $X^{p^{q-1}} - 1$

If F is irred. $\Rightarrow K \cong \dfrac{\mathbb{Q}[x]}{(F)} \Rightarrow |G| = e$
$\Updownarrow$
$G \cong (\mathbb{Z}/p^q\mathbb{Z})^*$

Conversely, if $|G| = e$ then $F = \prod_{g \in G} (X - g \cdot \mu) \Rightarrow F$ is irred

<u>Prop. 14.4</u> $[K:\mathbb{Q}] = e$.

<u>Proof</u> Let $\mu_1, \dots, \mu_e$ be all prim. roots of unity, $\mu = \mu_1$.

Then $F = \prod_{i=1}^{e} (X - \mu_i)$ in $K[x]$

and $p = F(1) = \prod_{i=1}^{e} (1 - \mu_i)$ $\quad (*)$

We have $\mu_i \in \mathcal{O}_K$, consider the ideals

$$J_i = (1 - \mu_i) \subset \mathcal{O}_K$$

$\forall\, i \neq j \quad \mu_i = \mu_j^n$ for some n,

$$1 - \mu_i = 1 - \mu_j^n = (1-\mu_j)(1+\mu_j+\dots+\mu_j^{n-1})$$

$\Rightarrow 1-\mu_i \in I_j \Rightarrow I_i \subset I_j$

$\Rightarrow I_i = I_j$, actually all I_i are equal to I

From $(*)$: $\quad p \cdot \mathcal{O}_K = I^e$

If we decompose $I = \prod_{i=1}^{k} \mathfrak{p}_i^{m_i}$

$$\Rightarrow p \cdot \mathcal{O}_K = \prod_{i=1}^{k} \mathfrak{p}_i^{e m_i}$$

We know $e m_1 = \dots = e m_k = em$

and $[K:\mathbb{Q}] = k \cdot em \cdot f$

but $[K:\mathbb{Q}] \leq e$, because μ is a root of F, $\deg F = e$.

$\Rightarrow k = m = f = 1$, $\quad [K:\mathbb{Q}] = e$. $\square$

Note: $\mathfrak{p} = (1-\mu)$ is prime, s.t. $\mathcal{O}_K / \mathfrak{p} = \mathbb{F}_p$

So, p is totally ramified in K.

<u>Cor</u> F is irred, $\mathrm{Gal}(K/\mathbb{Q}) = (\mathbb{Z}/p^r\mathbb{Z})^\times$.

What other prime numbers ramify in K?

15. Discriminants and ramification

Recall the definition of the discriminant d_K of a number field K.

Let $e_1, \dots, e_n$ be a basis of $\mathcal{O}_K$ over $\mathbb{Z}$. $a_{ij} = \mathrm{Tr}(e_i e_j)$, then

$d_K = \det(a_{ij})$

Generalize this: we will work in the following setting:

$K \subset L$ ext. of number fields

R is a Dedekind domain with field of fractions K

T = integral closure of R in L

$\mathcal{O}_K \subset R$ and $R = S^{-1}\mathcal{O}_K$ for some mult. closed subset $S \subset \mathcal{O}_K$ and $T = S^{-1}\mathcal{O}_L$

Recall: trace $\mathrm{Tr}_{L/K} : L \longrightarrow K$

and $\forall x \in T \quad Tr_{L/K}(x) \in K \cap T = R$

$\Big(x \in T \Rightarrow x$ is integral $/ R$ — because R is int. closed.

$\Rightarrow gx$ is integral $/ R$

for all $g \in Gal(L/K)$

$\Rightarrow Tr(x) \in T \Big)$

<u>Def</u> For any elements $v_1, \dots, v_n \in L$ where $n = [L:K]$ form a matrix

$$A = \left(Tr_{L/K}(v_i v_j) \right)$$

write $D(v_1, \dots, v_n) = \det(A)$

Note: if $v_1, \dots v_n \in T$, then

$$D(v_1, \dots, v_n) \in R$$

<u>Lemma 15.1</u> If $v_i' = \sum_j b_{ij} v_j$ with $b_{ij} \in K$ then

$$D(v_1', \dots, v_n') = (\det B)^2 D(v_1, \dots v_n)$$

where $B = (b_{ij})$

<u>Proof</u> $\underbrace{Tr(v_i' v_j')}_{a_{ij}'} = \sum_{\alpha, \beta} b_{i\alpha} b_{j\beta} \underbrace{Tr(v_\alpha v_\beta)}_{a_{\alpha\beta}}$

$\Rightarrow A' = B \cdot A \cdot B^t \Rightarrow \det A' = (\det B)^2 \det A$ $\square$

Def In the above setting, let the ideal $\delta_{T/R} \subset R$ be generated by $D(v_1, \dots v_n)$ for all n-tuples $v_1, \dots v_n \in T$

Lemma 15.2 Assume that T is a free R-module, i.e. $T \simeq R^{\oplus n}$ and $e_1 \dots e_n$ - a basis of T/R. Then $\delta_{T/R} = (D(e_1, \dots, e_n))$

Proof Clearly for $v_1, \dots, v_n \in T$ we have $v_i = \sum_j b_{ij} e_j$ for some $b_{ij} \in R$. By Lemma 15.1:

$$D(v_1, \dots, v_n) = (\det B)^2 D(e_1, \dots e_n)$$

so $D(e_1, \dots e_n)$ generates $\delta_{T/R}$ $\square$

Lemma 15.3 Assume that $S \subset R$ is a mult. closed subset. Then

$$\delta_{S^{-1}T/S^{-1}R} = S^{-1} \delta_{T/R}$$

Proof if $v_1 \dots v_n \in T \subset S^{-1}T$

$\Rightarrow D(v_1 \dots v_n) \in \delta_{S^{-1}T/S^{-1}R}$

$\Rightarrow S^{-1}\delta_{T/R} \subset \delta_{S^{-1}T/S^{-1}R}$

Assume: $\frac{v_1}{s_1}, \dots, \frac{v_n}{s_n} \in S^{-1}T$

Then by Lemma 15.1

$$D\left(\frac{v_1}{s_1}, \dots, \frac{v_n}{s_n}\right) = \left(\frac{1}{s_1 \cdot \dots \cdot s_n}\right)^2 D(v_1 \dots v_n)$$

$(s_1 \cdot \dots \cdot s_n)^2 \in S \Rightarrow$

$\Rightarrow D\left(\frac{v_1}{s_1} \dots \frac{v_n}{s_n}\right) \in S^{-1}\delta_{T/R}$

$\Rightarrow \delta_{S^{-1}T/S^{-1}R} \subset S^{-1}\delta_{T/R}$ $\square$

Assume now that R is a DVR with maximal ideal $\mathfrak{m}$.

Then T is a free R-module (because R is PID, see the lecture last week)

Let $e_1, \dots, e_n$ be a basis of T/R

If we reduce mod $\mathfrak{m}$ we get:

$\mathbb{F}_q = R/m \hookrightarrow T/mT = F$

and F is a fin. dimensional $\mathbb{F}_q$-algebra with a basis $\bar{e}_1, .., \bar{e}_n$

Recall, that the trace of $x \in T$ $Tr_{L/K}(x)$ is the trace of the matrix that defines multiplic. by x in the basis $e_1 ... e_n$, i.e. write $x \cdot e_i = \sum_j a_{ij} e_j$, $a_{ij} \in R$

$\Rightarrow Tr_{L/K}(x) = \sum_{i=1}^{n} a_{ii}$

It is clear that $\overline{Tr_{L/K}(x)} = Tr_{F/\mathbb{F}_q}(\bar{x})$ (bar denotes reduction mod m)

Therefore $D(\bar{e}_1, .., \bar{e}_n) = \overline{D(e_1, .., e_n)}$ where $D(\bar{e}_1, .., \bar{e}_n)$ is the determinant of the trace form of $F/\mathbb{F}_q$ in the basis $\bar{e}_1, ..., \bar{e}_n$

<u>Prop. 15.4</u> The $\mathbb{F}_q$-algebra F is reduced (i.e. has no non-zero nilpotent

elements) if and only if

$$D(\bar{e}_1, \ldots, \bar{e}_n) \neq 0$$

$$\Leftrightarrow D(e_1, \ldots, e_n) \notin \mathfrak{m}$$

<u>Proof</u> If we decompose

$$\mathfrak{m} \cdot T = \prod_i \mathfrak{p}_i^{m_i}$$

Then $F \cong \prod_i T/\mathfrak{p}_i^{m_i}$

all $m_i = 1 \Leftrightarrow F$ contains no non-zero nilp. elements. (if e.g. $m_1 > 1$, then $\exists x \in \mathfrak{p}_1 \setminus \mathfrak{p}_1^{m_1}$, then the image of x is a non-zero nilp. in $T/\mathfrak{p}_1^{m_1}$)

$D(\bar{e}_1, \ldots, \bar{e}_n) \neq 0 \Leftrightarrow D(e_1', \ldots, e_n') \neq 0$ for any basis $e_1', \ldots e_n'$ of $F/\mathbb{F}_q$

$\Rightarrow$ we can choose a basis in each factor $T/\mathfrak{p}_1^{m_i}$ separately, so it is enough to show that

$m_i = 1 \Leftrightarrow$ the trace form on $T/\mathfrak{p}_i^{m_i}$ is non-degenerate.

$\Rightarrow$ if $m_i = 1$, then $T/_{p_i}$ is a field, extension of $\mathbb{F}_q$

$\Rightarrow$ the trace form is non-deg

(Thm 4.5 in lecture 3)

$\Leftarrow$ if $m_i \geq 2$, then $\exists$ a nilpotent element $0 \neq y \in T/_{p_i^{m_i}}$. We claim

that y is in the kernel of the trace form, i.e. $Tr(xy) = 0$ $\forall x \in T/_{p_i^{m_i}}$.

Assume: $y^d = 0$, $y^{d-1} \neq 0$, then

$\forall x \in T/_{p_i^{m_i}}$ multiplication by xy is a nilpotent endomorphism of $T/_{p_i^{m_i}}$

because $(xy)^d = 0$ $\Rightarrow$ $Tr(xy) = 0$

$\Rightarrow$ the matrix of the trace form is degenerate

$\square$

<u>Thm 15.5</u> Assume $K \subset L$ number fields R Dedekind domain with fraction field K, T the int. closure of R

in L. A non-zero prime ideal $\mathfrak{p} \subset R$ ramifies in L if and only if $\delta_{T/R} \subset \mathfrak{p}$, i.e. $\mathfrak{p}$ divides $\delta_{T/R}$

<u>Proof</u> We localize at $\mathfrak{p}$, i.e. consider $S = R \setminus \mathfrak{p}$

then $$S^{-1}\delta_{T/R} \underset{\text{Lemma 15.5}}{=} \delta_{S^{-1}T/S^{-1}R} \subset S^{-1}\mathfrak{p}$$

$$\Updownarrow$$

$$\delta_{T/R} \subset \mathfrak{p}$$

$\mathfrak{p}$ is ramified in L $\iff$ $S^{-1}\mathfrak{p}$ is ramified in L.

$\Rightarrow$ we can consider the case R is a DVR with max. ideal $\mathfrak{p}$.

$\mathfrak{p}$ ramifies $\iff$ $T/\mathfrak{m}T$ is non-reduced

$\overset{\text{Prop. 15.4}}{\iff}$ $D(e_1, \dots, e_n) \in \mathfrak{m}$

$\overset{\text{Lemma 15.2}}{\iff}$ $\delta_{T/R} \subset \mathfrak{m}$ $\square$

<u>Cor. 1</u> In the above setting $\exists$ only finitely many primes in R that ramify in L.

Proof those primes appear in the decomposition $\delta_{T/R} = \prod \mathfrak{p}_i^{m_i}$ □

Cor. 2 In the case $\mathbb{Q} \subsetneq K$:

1) $p \in \mathbb{Z}$ ramifies in $K \iff p$ divides d_K
2) $\exists$ at least one p that ramifies in K

Proof 1) clear: $\delta_{K/\mathbb{Q}}$ is generated by d_K

2) follows from Minkowski's bound (lecture 12): $d_K > 1 \Rightarrow \exists$ at least one prime divisor. □