Corollary (from Prop 16.4) $K = \mathbb{Q}(\mu)$ μ - prim. n-th root of unity, then $\mathcal{O}_K = \mathbb{Z}[\mu]$, $[K:\mathbb{Q}] = \varphi(n)$ where φ is the Euler's function $Gal(K/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$; A prime $p > 2$ ramifies in $K \Leftrightarrow p$ divides n

Proof $n = p_1^{r_1} \cdot \ldots \cdot p_m^{r_m}$ μ_i primitive $p_i^{r_i}$-th root of unity

Using the proposition inductively, we get: $K \simeq K_1 \otimes \ldots \otimes K_m$

$K_i = \mathbb{Q}(\mu_i)$

$$Gal(K/\mathbb{Q}) = \prod_{i=1}^{m} Gal(K_i/\mathbb{Q}) \simeq \prod_{i=1}^{m} (\mathbb{Z}/p_i^{r_i}\mathbb{Z})^\times$$

$$\xrightarrow{CRT} = (\mathbb{Z}/n\mathbb{Z})^\times,$$

$\mathcal{O}_K$ is spanned/$\mathbb{Z}$ by $\prod_{i=1}^{m} \mu_i^{l_i}$

but they are all powers of μ

$\Rightarrow \mathcal{O}_K = \mathbb{Z}[\mu]$

$[K:\mathbb{Q}] = |(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(n)$ by def. of φ

$p>2$ divides $n \Rightarrow p$ ramifies in one of $K_i \Rightarrow p$ ramifies in K.
opposite implication – exercise $\square$

Rem 2 ramifies in $K \Leftrightarrow 4$ divides n.

What about the primes p, s.t. $(n,p)=1$?

Recall: $p \cdot \mathcal{O}_K = \prod_{i=1}^{k} p_i$ $\quad \mathcal{O}_K/p_i \simeq \mathbb{F}_{p^f}$

$[K:\mathbb{Q}] = kf$

$Gal(\mathbb{F}_{p^f}/\mathbb{F}_p)$ is generated by Frobenius $x \mapsto x^p$

We have defined a Frobenius element

$$\left(\frac{K/\mathbb{Q}}{p}\right) \in Gal(K/\mathbb{Q})$$

characterized by the property: $\forall x \in \mathcal{O}_K$

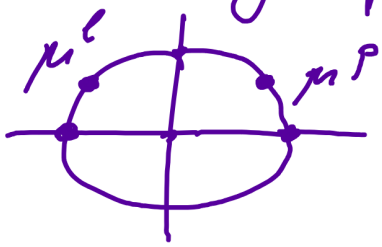
$$\left(\frac{K/\mathbb{Q}}{p}\right) \cdot x \equiv x^p \pmod{p}$$

take $x=\mu$; let $\left(\frac{K/\mathbb{Q}}{p}\right) = l \in (\mathbb{Z}/n\mathbb{Z})^\times$

$\Rightarrow \mu^l \equiv \mu^p \pmod{p}$

this only possible if $l=p$ in $(\mathbb{Z}/n\mathbb{Z})^\times$

$\Leftrightarrow l \equiv p \pmod{n}$



$\mu^l = \mu^p$

$\Rightarrow \left(\frac{K/\mathbb{Q}}{p}\right) \equiv p \pmod{n} \in (\mathbb{Z}/n\mathbb{Z})^\times$

f = order of p in $(\mathbb{Z}/n\mathbb{Z})^\times$

If we fix $n \in \mathbb{Z}$ $(n, m) = 1$

are there prime numbers with

$p \equiv m \pmod{n}$

<u>Thm</u> (Dirichlet) Fix n and m are coprime, consider the set

$$P_{n,m} = \{p \in \mathbb{Z} \text{ prime} \mid p \equiv m \pmod{n}\}$$

Then $P_{n,m}$ has density $\frac{1}{\varphi(n)}$ in particular it is infinite.

<u>Def</u> If $P \subset \{p \in \mathbb{Z} \text{ prime}\}$ a subset. We say P has density δ if $\exists \lim_{k \to \infty} \frac{\{p \in P \mid p \leq k\}}{\{p \in \mathbb{Z} \text{ prime} \mid p \leq k\}} = \delta$

More generally, for arbitrary number field K, $Gal(K/\mathbb{Q})$ not abelian

am $\left(\frac{K/\mathbb{Q}}{p}\right)$ is only a conjugacy class in $Gal(K/\mathbb{Q})$

$Gal(K/\mathbb{Q}) = C_1 \amalg \dots \amalg C_m$ conjugacy classes.

Thm (Chebotarev's density thm)
Fix a conj. class C in $Gal(K/\mathbb{Q})$
Let $P_C = \{p \in \mathbb{Z} \text{ prime} \mid p \text{ does not ramify in } K \text{ and } \left(\frac{K/\mathbb{Q}}{p}\right) = C\}$
Then P_C has density $\frac{|C|}{|Gal(K/\mathbb{Q})|}$

For example: $\{1\} \subset Gal(K/\mathbb{Q})$ a conj. class. The thm tells us that
$\exists$ inf. many primes p, s.t.

$$\left(\frac{K/\mathbb{Q}}{p}\right) = \{1\}.$$

This means $f = 1 \Rightarrow p$ splits completely in K:

$$p \cdot \mathcal{O}_K = \prod_{i=1}^{[K:\mathbb{Q}]} p_i$$

$$\mathcal{O}_K/p_i \cong \mathbb{F}_p$$

17. Absolute values and completions

Let K be a field

Def An absolute value on K is a map $|\cdot| : K \longrightarrow \mathbb{R}_{\geq 0}$ satisfying

1) $|x| = 0 \iff x = 0$

2) $\forall x, y \in K \quad |xy| = |x| \cdot |y|$

3) $\forall x, y \in K \quad |x+y| \leq |x| + |y|$

If $|\cdot|$ satisfies the stronger condition

3') $|x+y| \leq \max\{|x|, |y|\}$

then $|\cdot|$ is called non-archimedian, otherwise it is archimedian.

Examples 1) Let $|x| = \begin{cases} 1, & x \neq 0 \\ 0, & x = 0 \end{cases}$

this is called trivial abs. value.

2) $K = \mathbb{Q}$, $|x|_\infty = |x|$ abs. value of x as a real number

$|\cdot|_\infty$ is an archimedian abs. val

(e.g. $|1+1| = 2 > \max\{|1|, |1|\}$

$\Rightarrow$ no stronger inequality 3')

3) $K = \mathbb{Q}$, $p \in \mathbb{Z}$ prime

We have the DVR $\mathbb{Z}_{(p)} \subset \mathbb{Q}$

and a valuation $\nu_p : \mathbb{Q}^\times \longrightarrow \mathbb{Z}$

$\nu_p\left(p^n \frac{a}{b}\right) = n$ for $(a,p)=1$, $(b,p)=1$

$\mathbb{Z}_{(p)} = \{x \in \mathbb{Q} \mid \nu_p(x) \geq 0\}$ (formally $\nu_p(0) = +\infty$)

Let $\alpha \in \mathbb{R}$ $0 < \alpha < 1$

Define $|x|_p = \alpha^{\nu_p(x)}$ $|0|_p = 0$

$\nu_p(xy) = \nu_p(x) + \nu_p(y)$ $\Rightarrow$ property 2) for $|\cdot|_p$

$\nu_p(x+y) \geq \min\{\nu_p(x), \nu_p(y)\}$ $\Rightarrow$ property 3') for $|\cdot|_p$

$\Rightarrow |\cdot|_p$ is a non-archimedean abs. value.

<u>Def</u> 1) if $|\cdot|_1$, $|\cdot|_2$ are abs. values on K, they are called equivalent if $\exists \lambda \in \mathbb{R}_{>0}$: $\forall x \in K$ $|x|_1 = |x|_2^\lambda$

2) An equivalence class of abs. values on K is called a <u>place</u> of K

$\Rightarrow |\cdot|_p$ is a well-defined place of $\mathbb{Q}$

(for two different d_1, d_2 we get equivalent abs. values)

<u>Thm</u> (Ostrowski) A non-trivial place of $\mathbb{Q}$ is either given by $|\cdot|_p$ or $|\cdot|_\infty$

Archimedian places are also called "infinite places"

If $|\cdot|_v$ is an abs. value on K define a metric $\rho(x,y) = |x-y|_v$
$\Rightarrow K$ is a metric space

<u>Def</u> K is complete w.r.t. $|\cdot|_v$ if this metric space is complete (i.e. all Cauchy-sequences have limits)

If K is not complete, we can produce its completion K_v

$K_v = \{\text{Cauchy sequences in } K \text{ w.r.t. } |\cdot|_v\}/\sim$

(similar to the construction of $\mathbb{R}$ from $\mathbb{Q}$)

K_v is complete w.r.t. to the natural extension of $|\cdot|_v$ to K_v

Remark: if $|\cdot|_{v_1} \sim |\cdot|_{v_2}$, then $K_{v_1} \simeq K_{v_2}$

$\Rightarrow$ the completion of K in a place is well-defined up to isomorp.

$\mathbb{Q}_\infty = \mathbb{R}$ (completion w.r.t. $|\cdot|_\infty$)

$\mathbb{Q}_p$ = the field of p-adic rationals

$\cup$

$\mathbb{Z}_p$ = ring of p-adic integers.

Alternative description of $\mathbb{Z}_p$

Assume that $(x_i)_{i\geq 1}$ is a Cauchy seq. in $\mathbb{Z}$ w.r.t. $|\cdot|_p$

$\Rightarrow \forall \varepsilon > 0 \quad \exists i_0 : \forall i,j \geq i_0$

$|x_i - x_j|_p < \varepsilon$

$\| \alpha^{v_p(x_i - x_j)}$

$\Leftrightarrow \forall n > 0 \quad \exists i_0 : \forall i,j \geq i_0$

$x_i - x_j = p^n a$ for some $a \in \mathbb{Z}$

$\Leftrightarrow x_i \equiv x_j \pmod{p^n}$

$\Rightarrow (x_i)_{i \geq 1}$ gives us a well-defined residue class in $\mathbb{Z}/p^n\mathbb{Z}$

$x_i \pmod{p^n}$ for $i \gg 0$

These residue classes are compatible with the quotient maps

$$\mathbb{Z}/p^{n+1}\mathbb{Z} \longrightarrow \mathbb{Z}/p^n\mathbb{Z}$$

$$\mathbb{Z}_p \simeq \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$$

<u>Def</u> $\varprojlim_n \mathbb{Z}/p^n\mathbb{Z} = \{(y_n)_{n \geq 1}, y_n \in \mathbb{Z}/p^n\mathbb{Z}$

s.t. $y_{n+1} \equiv y_n \pmod{p^n}\}$