More on ramification

HW 4 to be posted later today.

Reminder: Daylight Saving Time ends in San Diego this weekend. Starting next week, all course times are UTC-8 rather than UTC-7.

Reminder: voting in the US election closes on Tuesday, November 3 (and in the AMS election on Sunday, November 1).

Reminder: the fundamental identity

$\mathcal{O}_K$ = Dedekind domain

$\mathrm{Frac}\,\mathcal{O}_K = K$

L = finite separable ext of K

$\mathcal{O}_L$ = integral closure of $\mathcal{O}_K$ in L

$\mathfrak{p} \subset \mathcal{O}_K$ nonzero prime

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r}$$

$$f_i = \left[\mathcal{O}_L/\mathfrak{q}_i : \mathcal{O}_K/\mathfrak{p} \right] \quad \underline{\text{inertia degree}}$$

then $$\sum_i e_i f_i = n = [L : K]$$

e_i = $\underline{\text{ramification index}}$

f_i = $\underline{\text{inertia degree}}$ of $\mathfrak{q}_i$ over $\mathfrak{p}$.

Polynomial factorization and the fundamental identity

Pf: Suppose $\alpha \in \mathcal{O}_L$ is such that $L = K(\alpha)$
$g(x)$ = minimal polynomial of α $\in \mathcal{O}_K[x]$

For $\mathfrak{p}$ coprime to $\{\beta \in \mathcal{O}_L : \beta \mathcal{O}_L \subseteq \mathcal{O}_K[\alpha]\}$ (in $\mathcal{O}_L$)
then e_i, f_i are given by factoring
$\bar{g}(x) \in (\mathcal{O}_K/\mathfrak{p})[x]$ as $\prod \bar{g}_i(x)^{e_i}$, $\deg = f_i$

more precisely, $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \cong \mathcal{O}_K[\alpha]/\mathfrak{p}\mathcal{O}_K[\alpha]$

$\cong \mathcal{O}_K[x]/(\mathfrak{p}, g(x))$

$\cong (\mathcal{O}_K/\mathfrak{p})[x]/(\bar{g}(x)) \overset{CRT}{\cong} \bigoplus_i (\mathcal{O}_K/\mathfrak{p})[x]/(\bar{g}_i(x)^{e_i})$

Polynomial factorization and the fundamental identity

On the other hand

$$p\mathcal{O}_L = \prod \mathfrak{q}_i^{e_i} \Rightarrow \mathcal{O}_L/p\mathcal{O}_L = \bigoplus \mathcal{O}_L/\mathfrak{q}_i^{e_i}$$

$$\cong \bigoplus \mathcal{O}_K/_p[x]/(\bar{g}_i(x)^{e_i})$$

To match things up,

Let $\mathfrak{q}_i = \{\beta \in \mathcal{O}_L :$ image of β in $\mathcal{O}_L/p \cong \bigoplus \mathcal{O}_K/_p[x]/(\bar{g}(x))$ is divisible by $\bar{g}_i\}$

This is a prime ideal

and $\prod \mathfrak{q}_i^{e_i} = p\mathcal{O}_L$.

Ramification and the discriminant (ideal)

$K = \#$ field

Note: only finitely many prime ideals of $\mathcal{O}_K$ can have ramification above them.

Namely, if $\mathfrak{p}$ coprime to $\{\beta \in \mathcal{O}_K : \beta\mathcal{O}_L \subset \mathcal{O}_K(\alpha)\}$ and to discriminant $d(1, \alpha, \ldots, \alpha^{n-1})$

$= \mathrm{disc}(g)$

then $e_i = 1 \ \forall i$.

i.e. $\mathfrak{p}$ does not ramify if $\mathfrak{p}$ coprime to the discriminant ideal, generated by $d(\omega_1, \ldots, \omega_n)$ where $\omega_1, \ldots, \omega_n$ runs over all choices of basis of L/K consisting of elements of $\mathcal{O}_L$.

(and conversely ....)

Example: quadratic fields

D: square free

$K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{D})$

$[\mathcal{O}_L : \mathbb{Z}[\sqrt{D}]] \mid 2$.

minpoly of $\sqrt{D}$ $= x^2 - D$

$p \neq 2$ ramifies iff $p \mid D$

$f_1 = f_2 = 1$ (split) $\iff \left(\frac{D}{p}\right) = +1$

$f_2 = 1$ (inert) $\iff \left(\frac{D}{p}\right) = -1$

by quadratic reciprocity, this is related to $p \bmod 4D$

Example: prime cyclotomic fields

$K = \mathbb{Q}$

$L = \mathbb{Q}(\zeta_p)$ p odd prime $\quad \mathbb{Z}[\zeta_p] = \mathcal{O}_L$

min poly is $x^{p-1} + \dots + x + 1$

Only p ramifies.

Let $q \neq p, 2$ be another prime

mod q, factorization of $x^{p-1} + \dots + x + 1$ is determined by q mod p

e.g. splits completely $\iff q \equiv 1 \bmod p$

$\iff p \mid \mathbb{F}_q^\times$

more precisely, all f_i are equal to order of q in $\mathbb{F}_p^\times$

(e.g. if $q \not\equiv 1 \bmod p$, $q^2 \equiv 1 \bmod p \Rightarrow \zeta_p \notin \mathbb{F}_q$, $\zeta_p \in \mathbb{F}_{q^2}$)

Relationship between these two examples (Gauss sums)

Gauss: $\mathbb{Q} \subset$ some quadratic $\subset \mathbb{Q}(\zeta_p)$ — degree $p-1$, Galois group $(\mathbb{Z}/p\mathbb{Z})^\times$ cyclic

this is $\mathbb{Q}\left(\sqrt{(-1)^{\frac{p-1}{2}}\, p}\right)$

exercise: this is $\underbrace{\sqrt{(-1)^{\frac{p-1}{2}}\, p}}$ $= \sum_{a \in \mathbb{F}_p^\times} \left(\frac{a}{p}\right) \zeta_p^{\,a}$

if q splits completely in $\mathbb{Q}(\zeta_p)$
then it also splits completely in $\mathbb{Q}\left(\sqrt{(-1)^{\frac{p-1}{2}}\, p}\right)$

can recover all of quadratic reciprocity this way!

One more example

$K = \mathbb{Q}$

$L = \mathbb{Q}(\alpha)$ $\quad \alpha^3 - \alpha - 1 = 0$ $\quad$ not Galois.

(S_3)

can have $\quad f_1 = 1, f_2 = 2$

there is no congruence condition on p

that determines splitting of p in $\mathcal{O}_L$.

(bc L not abelian Galois extension)

class field theory

Artin reciprocity

(can use modular forms)