Lecture 9: Some number theory

NB: most result stated (& proved) in any textbook on algebraic number theory, except perhaps with some finiteness assumptions (easy to remove).

Cohomology of the additive group

Thm (normal basis theorem) If L/k is a finite Galois extension, then $\exists\, x \in L$ s.t. $\{gx \mid g \in Gal(L/k)\}$ forms a basis of L as a k-v.s.

Pf omitted.

Corollary L/k any Galois ext^n. Then

$$H^*(Gal(L/k), L^+) = 0 \quad \text{for } * > 0.$$

Here L^+ is the discrete $Gal(L/k)$-module with underlying set L, abelian gp. structure addition in L, canonical Galois action.

Pf If L/k is finite, then $L^+ \cong M_{Gal(L/k)} k$ by prev. thm & $\therefore H^* = 0$ for $* > 0$.

General case: $\mathrm{Gal}(L/K) = \lim\limits_{L'} \mathrm{Gal}(L'/K)$,

limit over $L/L'/K$, where L'/K is finite Galois

& $\operatorname{colim}\limits_{L'} L'^{+} = L^{+}$.

$\therefore H^{*}(\mathrm{Gal}(L/K), L^{+}) = \operatorname{colim}\limits_{L'} H^{*}(\mathrm{Gal}(L'/K), L'^{+})$

$= 0$ for $* > 0$. $\square$

Hilbert 90

<u>Thm</u> If L/K any Galois ext^n, then

$$H^1(\mathrm{Gal}(L/K), L^{\times}) = 0.$$

$L^{\times}$ is the discrete $\mathrm{Gal}(L/K)$-module with underlying set $L \setminus \{0\}$, as gp. structure coming from mult^n, & canonical $\mathrm{Gal}(L/K)$-action.

<u>Pf</u> WMA that L/K is finite. Let $f: G \to L^{\times}$, $G = \mathrm{Gal}(L/K)$, be a crossed-hom^m.

For $a \in L^{\times}$ let $b(a) = \sum f(g) \cdot ga \in L^{\times}$.

$g \in G$

Then $G \ni h$: $h \cdot b(a) \cdot f(h) = \sum_{g \in G} h\left[f(g) \cdot ga\right] \cdot f(h)$

$\left[\, f(hg) = f(h) \cdot h f(g) \right.$

$$= \sum_{g} \frac{f(hg)}{\cancel{f(h)}}\, hga \cdot \cancel{f(h)}$$

$$= \sum_{g} f(g) \cdot ga = b(a)$$

If $b(a) \neq 0$ then $f(h) = \dfrac{b(a)}{h\, b(a)}$ which is a coboundary.

Let $1, a, \ldots, a^{n-1}$ be a basis for L/K.

Consider the sys of eq^{ns}

$$\sum_{g \in G} x_g \cdot g a^{\nu} = 0 \quad , \quad \nu = 0, 1, \ldots, n-1$$

Compute the ("Vandermonde") determinant $\rightsquigarrow \neq 0$.

I.e. if all eq^{ns} are satisfied then $x_g = 0$ $\forall g$.

Hence if $b(a) = 0$ $\forall a \in L^*$, then $f(g) = 0$ $\forall g \in G$.

$\square$

NB $H^*(\mathrm{Gal}(L/K), L^\times) \neq 0$ for $* > 1$ in general.

Standard terminology

Let K be a field.

An <u>absolute value</u> on K is a function

$|\cdot| : K \to \mathbb{R}_{\geq 0}$ s.t.

(i) $|a| = 0 \iff a = 0$

(ii) $|ab| = |a||b|$

(iii) $|a+b| \leq |a| + |b|$.

Call $|\cdot|$ <u>non-archimedean</u> (or <u>finite</u>) if we have

(iii') $|a+b| \leq \max(|a|, |b|)$

Otherwise call $|\cdot|$ <u>archimedean</u> (or <u>infinite</u>).

Call $|\cdot|, |\cdot|'$ equivalent if $\exists\, r \in \mathbb{R}_{>0}$ s.t. $|\cdot|^r = |\cdot|'$.

An equivalence class of absolute values of K is called a <u>place</u>. If v is a place, denote by $|\cdot|_v$ a choice of representing absolute value.

<u>Ex</u> Given $\sigma : K \hookrightarrow \mathbb{C}$. Obtain $|a|_\sigma = |\sigma a|$

(where $|x+iy| = \sqrt{x^2+y^2}$ is std abs. value on $\mathbb{C}$).
This is an archimedean absolute value (or place).

Ex Let $K/\mathbb{Q}$ be a finite ext^n, $\mathcal{O}_K$ the ring of integers, P a max ideal of $\mathcal{O}_K$. Then $(\mathcal{O}_K)_P =: \mathcal{O}_{K,P}$ is a dvr, i.e. $P\mathcal{O}_{K,P} = (\pi)$ & every $x \in K$ can be written uniquely as $x = u \cdot \pi^n$, where $u \in (\mathcal{O}_{K,P})^+$, $n \in \mathbb{Z}$.

Put $|x|_P = e^{-n}$ any number > 1.

This is a non-archimedean place.

NB: $\mathcal{O}_{K,P} = \{x \in K \,/\, |x|_P \leq 1\}$

Th^m (Ostrowski) If $K/\mathbb{Q}$ is finite, then all places are of the form $|\cdot|_P$ or $|\cdot|_\sigma$.

Rmk $K/\mathbb{Q}$ infinite, P a prime of $\mathcal{O}_K$ = integral closure of $\mathbb{Z}$ in K.

For $K/K'/\mathbb{Q}$ a finite subextension, $K' \cap P$ is a prime of $\mathcal{O}_{K'}$ & hence have associated absolute value $|\cdot|_{K'}$ & place $v_{K'}$.

One may show that "$\exists$ place v of K s.t. $v_{K'} = v|_{K'}$ $\forall K'$."

NB: $\mathcal{O}_{K,\mathfrak{p}}$ need not be a dvr.

Namely $\mathfrak{p} \cdot \mathcal{O}_{K,\mathfrak{p}}$ need not be principal anymore.

(It is a "valuation ring of rk 1".)

Given K/k alg. & place v of K, the (algebraic) completion $K_v = \underset{\underbrace{K/K'/k}_{\text{finite subextensions}}}{\operatorname{colim}} K'_{v|_{K'}}$

where $K'_{v|_{K'}}$ is the usual completion using Cauchy sequences.

If v is infinite one may show that $K_v = \mathbb{R}$ or $K_v = \mathbb{C}$. Call v real or complex, respectively.

If v is finite then

$$\mathcal{O}_{K,v} = \mathcal{O}_v = \{x \in K \mid |x|_v \leq 1\}$$

is a "valuation ring" (a special kind of local ring) with max ideal $\mathfrak{m}_v = \{x \in K \mid |x|_v < 1\}$.

Denote by $k(v)$ the residue field $\mathcal{O}_v/_{m_v}$.

If K/k is an algebraic extension & v is a finite place of K, say that K/k is <u>unramified</u> at v if $|K|_v = |k|_v$ (i.e. equality as subsets of $\mathbb{R}$), otherwise say K is <u>ramified at v</u>.

An infinite place v is called <u>unramified</u> if $K_v = k_v$, else ramified.

<u>Galois extensions</u>

Let K/k be Galois, v a finite place of K, $G = \mathrm{Gal}(K/k)$.

We have subgroups $I_v \subset D_v \subset G$ called <u>inertia</u> & <u>decomposition</u> groups, respectively.

ov. $\mathfrak{p}_v$

$$D_v = \{ g \in G \mid |\alpha|_v = |g\alpha| \ \forall \alpha \in K \}$$
$$I_v = \{ g \in G / \ |g\alpha - \alpha| < 1 \ \forall \alpha \in K \}.$$

One may show that $I_v \trianglelefteq D_v$ is a normal subgp.

<u>Thm</u> Let K/k be Galois, $K/L/k$ a subextension,

v a finite place of K. Then:

$$D_v(K/L) = D_v(K/k) \cap \mathrm{Gal}(K/L)$$

$$I_v(K/L) = I_v(K/k) \cap \mathrm{Gal}(K/L).$$

If L/k is Galois & $v' := v|_L$ then

$$\frac{D_v(K/k)}{D_v(K/L)} = D_{v'}(L/k) \subset \mathrm{Gal}(L/k) = \frac{\mathrm{Gal}(K/k)}{\mathrm{Gal}(K/L)}$$

& $$\frac{I_v(K/k)}{I_v(K/L)} = I_{v'}(L/k).$$

Pf omitted.

In particular $$D_v(K/k) = \varprojlim_{\substack{L \\ \text{finite, subext'} \\ \text{Gal}}} D_{v'}(L/k)$$

$$I_v(K/k) = \varprojlim_{L} I_{v'}(L/k)$$

are profinite, i.e. closed subgroups.

Let K/k Galois, v any place of K, $v' := v|_k$.

Have embeddings
$$\begin{tikzcd} K \arrow[r, hook] & K_v \\ k \arrow[u, hook] \arrow[r, hook] & k_{v'} \arrow[u, hook] \end{tikzcd},$$

& hence $\varphi_v : \mathrm{Gal}(K_v/k_v) \longrightarrow \mathrm{Gal}(K/k)$.

<u>Thm</u> φ_v is an injection. If v is finite, the image of φ_v is D_v.

Pf omitted.

If v is infinite, we <u>define</u> $I_v = D_v = \mathrm{im}(\varphi_v)$.

<u>Thm</u> K^{I_v} is the largest subextension of k in which v is unramified.

Pf omitted.

<u>Frobenius</u>

<u>Thm</u> K/k Galois, v a finite place.

$$D_v \longrightarrow \mathrm{Gal}(K_v/k_v)$$

is surjective with kernel I_v.

NB: $g \in D_v \Rightarrow |\cdot|_v$ is g-inv. $\Rightarrow$ g extends to an auto^n of K_v.

Pf omitted.

fix (?) next time.