Due: Feb 2, 2024

Math 6030 / Problem Set 1 (two pages)

More about Trace/Norm/Discriminant. Recall that for a finite field extension $L|K$ one has the (i) relative trace $\mathrm{Tr}_{L|K} : L \to K$, which is a K-linear map, and (ii) the relative norm $\mathrm{N}_{L|K} : L \to K$, which is multiplicative. See HW 12 from Math 6020, Problems 7, 8, 9.

The map $\boldsymbol{T}_{L|K} : L \times L \to K$, $(x, y) \mapsto \mathrm{Tr}_{L|K}(xy)$ is symmetric K-bilinear (WHY). Given a K-basis $\mathcal{A} = (\alpha_i)_{i \leqslant n}$ of $L|K$ and $B_{\mathcal{A}} = \mathrm{Tr}_{L|K}(\mathcal{A}^\tau \cdot \mathcal{A}) := \big(\mathrm{Tr}_{L|K}(\alpha_i \alpha_j)\big)_{i,j}$, define/consider:

- $\partial_{\mathcal{A}} := \det(B_{\mathcal{A}})$, called the discriminant of the basis $\mathcal{A}$ w.r.t. $\boldsymbol{T}_{L|K}$
- The dual basis $\mathcal{A}^* = (\alpha_i^*)_{i \leqslant n}$ of $\mathcal{A}$ w.r.t. $\boldsymbol{T}_{L|K}$ (if it exists), i.e., $\boldsymbol{T}_{L|K}(\alpha_i, \alpha_j^*) = \delta_{ij}$.

1) In the above notation, let $\mathcal{B} = (\beta_1, \dots, \beta_n)$ be further K-basis of $L|K$. Prove:

a) There is $S \in \mathrm{GL}_n(K)$ with $\mathcal{B} = \mathcal{A}S$.

b) $\partial_{\mathcal{B}} = \det(S)^2 \partial_{\mathcal{A}}$, concluding the following:

$\partial_{L|K} := \partial_{\mathcal{A}} \in K^\times / K^{\times 2}$ *is independent of* $\mathcal{A}$ *modulo the group of squares* $K^{\times 2} \leqslant K^\times$.

2) Let $L = K[x]$ be separable, $p(t) = \mathrm{Mipo}_K(x)$, and $\mathcal{A} = (x^i)_{0 \leqslant i < n}$. Prove:

a) $\mathcal{A}$ is a K-basis of $L|K$ and $\partial_{\mathcal{A}} = \prod_{i<j}(x_i - x_j)^2 = (-1)^{\frac{n(n-1)}{2}} \mathrm{N}_{L|K}\big(p'(x)\big)$.

b) **Euler's Theorem**. Set $p(t) = (t - x)\sum_{i<n} b_i t^i \in L[t]$. Then $\mathcal{A}^* = \big(b_i / p'(x)\big)_{0 \leqslant i < n}$.

[**Hints**. To a): Set $A_x := (x_j^i)_{i,j} \in \overline{K}^{n \times n}$. Then $\partial_{\mathcal{A}} \overset{\text{why}}{=} \det(A_x A_x^\tau) = \det(A_x)^2$ (WHY), etc. To b): Last resort Google it!…]

3) In the above notation, prove that the following are equivalent:

(i) $L|K$ is separable.

(ii) $\mathrm{Tr}_{L|K}$ is non-trivial, i.e., $\exists\, x \in L$ s.t. $\mathrm{Tr}_{L|K}(x) \neq 0$.

(iii) $\boldsymbol{T}_{L|K}$ is non-degenerate, i.e., $\forall\, x \in L\ \exists\, y \in L$ s.t. $\boldsymbol{T}_{L|K}(x, y) \neq 0$.

(iv) $\mathcal{A} = (\alpha_1, \dots, \alpha_n)$ has a dual basis $\mathcal{A}^* = (\alpha_1^*, \dots, \alpha_n^*)$.

(v) $\partial_{\mathcal{A}} \neq 0$.

Infinite Galois Theory. Make sure that you checked all the details from the *Fundamental Thm of Galois Theory*: For a Galois extension $L|K$, let $L_\alpha|K$, $\alpha \in I$ be the set of finite Galois subextensions, and $p_\alpha : G := G(L|K) \to G(L_\alpha|K) =: G_\alpha$, $\sigma \mapsto \sigma_\alpha = \sigma|_{L_\alpha}$. Then p_α is surjective (WHY), and setting $\mathcal{F} := \mathcal{F}(L|K)$, $\mathcal{F}_\alpha := \mathcal{F}(L_\alpha|K)$, $\mathcal{G} := \{H \in \mathrm{Sg}(G) \mid H \text{ closed}\}$, $\mathcal{G}_\alpha = \mathcal{G}(L_\alpha|K)$, one has surjective projective systems (s.p.s.) and canonical maps as follows:

- $(G_\alpha, p_{\gamma\beta})_{\alpha, \gamma \geqslant \beta}$ is a s.p.s. and $p : G \to \widehat{G} := \varprojlim_\alpha G_\alpha$, $\sigma \mapsto (\sigma_\alpha)_\alpha$ is an isomorphism.
- $(\mathcal{F}_\alpha, \varphi_{\gamma\beta})_{\alpha, \gamma \geqslant \beta}$ is a s.p.s. and $\varphi : \mathcal{F} \to \widehat{\mathcal{F}} := \varprojlim_\alpha \mathcal{F}_\alpha$, $L' \mapsto (L'_\alpha)_\alpha$, $L'_\alpha := \cap L_\alpha$ is bijective.
- $(\mathcal{G}_\alpha, \phi_{\gamma\beta})_{\alpha, \gamma \geqslant \beta}$ is a s.p.s. and $\phi : \mathcal{G} \to \widehat{\mathcal{G}} := \varprojlim_\alpha \mathcal{G}_\alpha$, $H \mapsto (H_\alpha)_\alpha$, $H_\alpha := H|_{L_\alpha}$ is bijective.
- The isomorphism of s.p.s. $(\mathrm{gal}_\alpha : \mathcal{F}_\alpha \to \mathcal{G}_\alpha)_\alpha$ defines an isomorphism $\mathrm{gal} : \mathcal{F} \to \mathcal{G}$ (HOW).
- etc.

Cyclotomic extensions/character. Let K be a field, $m > 0$ with $\mathrm{char}(K) \nmid m$, $\overline{K}|K$ a fixed algebraic closure, and $K_m := K(\mu_m) \subset \overline{K}$ be the splitting field of the m^{th} cyclotomic polynomial Φ_m. Define the cyclotomic character $\chi_{K,m}$ of $K_m|K$ as follows: Let $\zeta \in \mu_m$

be a fixed primitive m^{th} root of unity. Then $\sigma(\zeta)$ is a primitive root of unity for each $\sigma \in G(K_m|K)$ (WHY), hence there is $\overline{n}_\sigma \in (\mathbb{Z}/m\mathbb{Z})^\times$ s.t. $\sigma(\zeta) = \zeta^{n_\sigma}$ for any $\mathbb{Z} \ni n_\sigma \mapsto \overline{n}_\sigma$ (WHY).

4) In the above notation prove the following:

a) $\chi_m : G(K_m|K) \to (\mathbb{Z}/m\mathbb{Z})^\times$, $\sigma \mapsto \overline{n}_\sigma$ is injective and independent of ζ.

b) If $K = \mathbb{Q}$, then $\chi_m : G(\mathbb{Q}_m|\mathbb{Q}) \to (\mathbb{Z}/m\mathbb{Z})^\times$ is an isomorphism.

c) If $K = \mathbb{F}_p$, then $\mathrm{Im}(\chi_m)$ is the cyclic group generated by $\overline{p} \in (\mathbb{Z}/m\mathbb{Z})^\times$.

• Recall: (i) The ring of p-adic integers $\mathbb{Z}_p = \varprojlim_e \mathbb{Z}/p^e\mathbb{Z}$ is a profinite ring having group of units $\mathbb{Z}_p^\times = \varprojlim_e (\mathbb{Z}/p^e\mathbb{Z})^\times$ (WHY). (ii) The adic completion $\widehat{\mathbb{Z}} := \varprojlim_m \mathbb{Z}/m\mathbb{Z}$ of $\mathbb{Z}$ is a compact ring (WHY) and canonically: $\widehat{\mathbb{Z}} \cong \prod_p \mathbb{Z}_p$ as rings and $\widehat{\mathbb{Z}}^\times = \varprojlim_m (\mathbb{Z}/m\mathbb{Z})^\times \cong \prod_p \mathbb{Z}_p^\times$ as groups (WHY).

5) Let $K^{\text{cycl}} := \cup_m K_m \subset \overline{K}$, the cyclotomic extension of K. Prove/disprove/answer:

a) $G(K^{\text{cycl}}|K) = \varprojlim_m G(K_m|K)$ (HOW) and the cyclotomic character $\chi_K = \varprojlim_m \chi_{K,m}$ of K is an embedding of profinite groups $\chi_K : G(K^{\text{cycl}}|K) \to \widehat{\mathbb{Z}}^\times$ (HOW).

b) $\chi_\mathbb{Q} : G(\mathbb{Q}^{\text{cycl}}|\mathbb{Q}) \to \widehat{\mathbb{Z}}^\times$ is an isomorphism of profinite groups.

c) $\overline{\mathbb{F}}_p = \mathbb{F}_p^{\text{cycl}}$ and $\mathrm{Im}(\chi_{\mathbb{F}_p}) \subset \prod_{q \neq p} \mathbb{Z}_q^\times$, but $\mathrm{Im}(\chi_{\mathbb{F}_p}) \not\subset \prod_{q \in \Sigma} \mathbb{Z}_q^\times$ if $\exists\, \ell \neq p$, $\ell \notin \Sigma$.

6) Prove the following "*initial form*" of the Hilbert 90 (as proven in Hilbert's *Zahlbericht*). Let $L|K$ be a finite cyclic extension with Galois group $G = \langle \sigma \rangle$. Then for $a \in L$ one has:

a) $\mathrm{Tr}_{L|K}(a) = 0$ iff $\exists\, a_0 \in L$ s.t. $a = \sigma(a_0) - a_0$.

b) $\mathrm{N}_{L|K}(a) = 1$ iff $\exists\, a_0 \in L$ s.t. $a = \sigma(a_0)/a_0$.

Cohomology of profinite groups. If G is a topological group, e.g. a profinite group, a G-module is by definition a topological abelian group A, e.g. a discrete abelian group, on which G acts continuously. If so, one also considers the "*topological*" variants of cocycles $Z^i_{top}(G, A)$ and coboundaries $B^i_{top}(G, A)$ of G with values in A, thus the resulting "*topological*" cohomology groups $H^i_{top}(G, A)$. In the case of profinite groups, e.g. $G = G(L|K)$ the Galois group of Galois extensions $L|K$ acting on—usually—discrete abelian groups A, e.g. L^+ and/or $L^\times$, the result are *cohomology groups $H^i(G, A)$ of profinite groups.*

7) Let profinite groups G act continuously on discrete abelian groups A and $G \xrightarrow{p_\alpha} \overline{G}_\alpha = G/G_\alpha$ be the finite quotients of G. Then $\overline{G}_\alpha$ acts on $A_\alpha := A^{G_\alpha}$ (HOW), and further, $A = \cup_\alpha A^\alpha$ (WHY). For $i > 0$, let $\mathcal{C}(G^i, A) \supset Z^i(G, A) \supset B^i(G, A)$ be the continuous maps on G^i, respectively the continuous i^{th} cocycles/coboundaries. Prove the following:

a) $\mathcal{C}(G^i_\alpha, A_\alpha) = \mathsf{Maps}(\overline{G}^i_\alpha, A_\alpha) \hookrightarrow \mathcal{C}(G^i, A)$ by $\overline{f} \mapsto \overline{f} \circ p^i_\alpha$, and $\mathcal{C}(G^i, A) = \varinjlim_\alpha \mathcal{C}(\overline{G}^i_\alpha, A_\alpha)$.

b) $B^i(G, A) = \varinjlim_\alpha B^i(\overline{G}_\alpha, A_\alpha) \subset \varinjlim_\alpha Z^i(\overline{G}_\alpha, A_\alpha) = Z^i(G, A)$ for $i = 1, 2$.[1]

c) For $0 \to A \to B \to C \to 0$ exact seq. of discrete G-modules, one has a long exact seq.:

$$0 \to A^G \to B^G \to C^G \to H^1(G, A) \to H^1(G, B) \to H^1(G, C) \to H^2(G, A) \to \dots$$

<u>*Conclude*</u>: $G = G(L|K)$ acts continuoulsy on the discrete groups $A = L^+, L^\times$ and one has:

Generalized Hilbert 90. $Z^1(G, A) = B^1(G, A)$, *hence* $H^1(G, L^+) = 0$ *and* $H^1(G, L^\times) = 1$.

[1] Actually, this holds for all $i > 0$, but we did not define the objects for $i > 2$.