Lecture Notes from Differential Geometry (Michaelmas 2021)

Isaac Martin

Last compiled March 9, 2022

Contents

§ *Lecture 1*

Recorded: 2022-03-09 Notes: 2022-03-09

Corollary 0.1. If $E[n] \subseteq K(K)$ then $\mu_n \subseteq K$, where μ_n is the set of nth roots of unity in $\overline{K}$.

> *Proof:* If e_n is nondegenerate then there exist $S,T \in E[n]$ such that $e_n(S,T)$ is a primitive n^{th} root of unit, say ζ_n. Then $\sigma(\zeta_n) = e_n(\sigma S, \sigma T) = e_n(S,T) = \zeta_n$ for all $\sigma \in \mathrm{Gal}(\overline{K}/K)$. The first equality follows from Galois equivalence and the second since $S,T \in E(K)$. Therefore $\zeta_n \in K$. $\square$

Example 0.2. There exists no $E/\mathbb{Q}$ such that $E(\mathbb{Q})_{tors} \cong (\mathbb{Z}/3\mathbb{Z})^2$.

Remark 0.3. In fact, the Weil pairing is alternating, i.e. $e_n(T,T) = 1$ for all $T \in E[n]$. In particular, expanding $e_n(S+T,S+T)$ show $e_n(S,T) = e_n(T,S)^{-1}$.

1 Galois Cohomology

Throughout this section, G is a group and A is a G-module, i.e. and abelian group with an action of G via group homomorphisms. That is, we have a map $G \to \mathrm{Aut}(A)$ where $\mathrm{Aut}(A)$ is the group of abelian group homomorphisms of A, and $g \cdot a = g(a)$. To say that A is a G=module is equivalent to saying that A is a $\mathbb{Z}[G]$-module.

Definition 1.1. We set

$$H^0(G,A) = A^G = \{a \in A \mid \sigma(a) = a,\ \forall \sigma \in G\}.$$

We further set

$$\begin{aligned}
C^1(G,A) &= \{\text{maps } G \longrightarrow A\} && \text{“cochains”}\\
Z^1(G,A) &= \{(a_\sigma)_{\sigma \in G} \mid a_{\sigma\tau} = \sigma(a_\tau) + a_\sigma\} && \text{“\textit{cocycles}''}\\
B^1(G,A) &= \{(\sigma b - b)_{\sigma \in G} \mid b \in A\} && \text{“coboundaries”}
\end{aligned}$$

and we have inclusions $B^1(G,A) \subseteq Z^1(G,A) \subseteq C^1(G,A)$. We define $H^1(G,A) = Z^1(G,A)/B^1(G,A)$.

Remark 1.2. If G acts trivially on A, then $H^1(G,A) = \mathrm{Hom}(G,A)$.

Theorem 1.3. *A short exact sequence of G-modules*

$$0 \longrightarrow A \xrightarrow{\phi} B \xrightarrow{\psi} C \longrightarrow 0$$

gives rise to a long exact sequence of abelian groups

$$0 \longrightarrow A^G \xrightarrow[\phi]{} B^G \xrightarrow[\psi]{} C^G \xrightarrow[\delta]{} H^1(G,A) \xrightarrow[\phi_*]{} H^1(G,B) \xrightarrow[\psi_*]{} H^1(G,C) \longrightarrow \dots$$

where we stop before $H^2(G,A)$ because we have yet to define it. The map δ arises from the snake lemma.

Definition 1.4. Let $c \in C^G$. Then there exists a $b \in B$ such that $\psi(b) = c$. Then

$$\psi(\sigma b - b) = \sigma(c) - c = 0$$

for all $\sigma \in G$. This means $\sigma b - b = \phi(a_\sigma)$ for some $a_\sigma \in A$. One checks that $(a_\sigma)_{\sigma \in G} \in Z^1(G,A)$. We define $\delta(c) =$ chars of $(a_\sigma)_{\sigma \in G}$ in $H^1(G,A)$.

Theorem 1.5. *Let A be a G-module $H \subseteq G$ a normal subgroup. Then there is an inflation-restriction exact sequence*

$$0 \longrightarrow H^1(G/H, A^H) \xrightarrow{\text{inf}} H^1(G,A) \xrightarrow{\text{res}} H^1(H,A)$$

Proof: Omitted. □

Let K be a perfect field. $\mathrm{Gal}(\overline{K}/K)$ is then a topological group with basis of open subgroups. The sets $\mathrm{Gal}(\overline{K}/L)$ for $[L:K] < \infty$.

If $G = \mathrm{Gal}(\overline{K}/K)$ then we modify the definition of $H^1(G,A)$ by insisting

1. The stabilizer of each $a \in A$ is an open subgroup of G.
2. All cochains $G \longrightarrow A$ are continuous where A is given by the discrete topology.

Then

$$H^1(\mathrm{Gal}(\overline{K}/K), A) = \varinjlim_{L,\ L/K \text{finite Galois}} H^1(\mathrm{Gal}(L/K), A^{\mathrm{Gal}(\overline{K}/L)}).$$

The direct limit is with respect to inflation maps (what are inflation maps?).

Theorem 1.6 (Hilbert's Theorem 90)**.** *Let L/K be a finite Galois extension. Then $H^1(\mathrm{Gal}(L/K), L^*) = 0$.*

Proof: Let $G = \mathrm{Gal}(L/K)$. Let $(a_\sigma)_{\sigma \in G} \in Z^1(G, L^*)$. Distinct automorphisms are linearly independent, hence there exists some $y \in L$ such that

$$\underbrace{\sum_{\tau \in G} a_\tau^{-1} \tau(y)}_{x} \neq 0.$$

For $\sigma \in G$,

$$\sigma(x) = \sum_{\tau \in G} \sigma(a_\tau)^{-1} \sigma\tau(y) = a_\sigma \sum_{\tau \in G} a_\sigma^{-1} \sigma\tau(y) = a_\sigma \cdot x.$$

Therefore $a_\sigma = \sigma(x)/x \implies (a_\sigma)_{\sigma \in G} \in B^1(G, L^*)$. Hence $H^1(G, L^*)$. □

Corollary 1.7. $H^1(\mathrm{Gal}(\overline{K}/K), \overline{K}^*) = 0$.

Application: Assume $\mathrm{char}\, K \not| n$. There is an exact sequence of $\mathrm{Gal}(\overline{K}/K)$-modules

$$0 \longrightarrow \mu_n \longrightarrow \overline{K}^* \xrightarrow[x \longmapsto x^n]{} \overline{K}^* \longrightarrow 0.$$

Have a long exact sequence

$$K^* \xrightarrow[x\mapsto x^n]{} K^* \longrightarrow H^1(\mathrm{Gal}(\overline{K}/K), \mu_n) \longrightarrow H^1(\mathrm{Gal}(\overline{K}/K), \overline{K}^*),$$

but $H^1(\mathrm{Gal}(\overline{K}/K), \overline{K}^*) = 0$ by Theorem (1.6). Therefore $H^1(\mathrm{Gal}(\overline{K}/K), \mu_n) \cong K^*/(K^*)^n$.

If $\mu_n \subseteq K$ then $\mathrm{Hom}_{cts}(\mathrm{Gal}(\overline{K}/K), \mu_n) \cong K^*/(K^*)^n$.

If L/K is a finite Galois extension then $\mathrm{Gal}(\overline{K}/K) \xrightarrow{\pi} \mathrm{Gal}(L/K)$ and hence

$$\mathrm{Hom}(\mathrm{Gal}(L,K), \mu_n) \hookrightarrow \mathrm{Hom}_{cts}(\mathrm{Gal}(\overline{K}/K), \mu_n) \cong K^*/(K^*)^n,$$

where the above map is given by $\chi \mapsto \chi \circ \pi$. The image is a finite subgroup $\Delta \subseteq K^*/(K^*)^n$.

If $\mathrm{Gal}(L/K)$ is abelian of exponent dividing n then

$$[L:K] = |\mathrm{Gal}(L/K)| = |\mathrm{Hom}(\mathrm{Gal}(L/K), \mu_n)| = |\Delta|.$$

Compare to Theorem 11.2 from lectures Fix numbering.

Notation: We'll write $H^1(K, -) = H^1(\mathrm{Gal}(\overline{K}/K), -)$ to avoid writing Gal and $\overline{K}$ every time.

Lemma 1.8. Let $[K : \mathbb{Q}_p] < \infty$. Then

$$\ker(H^1(K, \mu_n) \longrightarrow H^1(K^{nr}, \mu_n)) \subseteq \{x \in K^*/(K^*) \mid v(x) \equiv 0 \pmod n\}.$$

remember that K^{nr} is the maximal unramified extension of K.

Proof: By Theorem (1.6), identify H^1 □