LECTURE 34

(34.0) Overview.– In this lecture we will see some equations (Noether's equations) related to the cohomology of the Galois group. Theorem 34.4 and Corollary 34.5 are the main results of these notes. Theorem 34.4 is proved using some basic facts about *rationalily over the base field* - which was outlined in Homework 10, problems 10 and 11. The theorem itself, and its proof are not part of the syllabus. In that sense it is somewhat optional. However, its application (Corollary 34.5) is needed later in studying cyclic (and more generally abelian) extensions. For this reason, I have included a "direct proof" of this corollary, not assuming Theorem 34.4. In the end these results rely heavily on *Dedekind's independence of characters*, see Lecture 29, Sections 29.1 and 29.2.

(34.1) Rationality over the base field.– Recall the notion of a K–*structure* on a vector space. Namely, let L/K be a Galois extension, and let V be an L–vector space.

Definition. A K–*structure* on V is a sub-K-vector space $V^0 \subset V$ such that extension of scalars $\varphi : V^0 \otimes_K L \to V$ is an isomorphism of L–vector spaces.

Assuming (V, V^0) is a K–structure on V as above, a vector $x \in V$ is said to be *rational over* K if $x \in V^0$. Similarly, a sub-L-vector space $W \subset V$ is said to be rational over K if $W^0 := W \cap V^0$ is a K–structure on W.

Let (V_ℓ, V_ℓ^0), $\ell = 1, 2$ be two L–vector spaces together with their respective K–structures. Let $f : V_1 \to V_2$ be an L–linear map. We say that f is rational over K if $f(V_1^0) \subset V_2^0$.

Remark. A K–structure on V is essentially same as a choice of a basis of V. Namely, if $\{v_i\} \subset V$ is a basis of V (over L), we can define V^0 to be the K–span of $\{v_i\}$. Conversely, if $\{e_i\}$ is a basis of V^0, it is clear from the definition that $\{e_i\}$ will be a basis (over L) of V.

(34.2) Rationality via Γ–action.– Now, let $\Gamma = \mathsf{G}(L/K)$. Given a K–structure V^0 on an L–vector space V, we can define an action of $\Gamma = \mathsf{G}(L/K)$ on V, via K–linear automorphisms:

$$u : \Gamma \to \mathrm{Aut}_{K\text{–vs}}(V)$$

as follows. If $\{e_i\}_{i\in I}$ is a basis of V^0, then every $x \in V$ can be written as $x = \sum_{i\in I} \lambda_i e_i$, where $\lambda_i \in L$. Set:

$$u_\sigma(x) = \sum_{i\in I} \sigma(\lambda_i) e_i, \ \forall\ \sigma \in \Gamma.$$

Alternately, via the identification $\varphi : V^0 \otimes_K L \xrightarrow{\sim} V$, we have:

$$\text{For every } \sigma \in \Gamma,\ u_\sigma = \mathrm{Id}_{V^0} \otimes \sigma \in \mathrm{Aut}_{K\text{–vs}}(V^0 \otimes_K L).$$

This way of defining u_σ makes it clear that it is independent of the choice of the basis $\{e_i\}_{i\in I}$ of V^0. Moreover, the following equation follows directly from the definitions

(Γ–linear) $$\boxed{u_\sigma(\lambda v) = \sigma(\lambda) u_\sigma(v)} \ \forall\ \sigma \in \Gamma, \lambda \in L, v \in V.$$

Theorem.

(1) *$x \in V$ is rational over K if and only if $u_\sigma(x) = x$ for every $\sigma \in \Gamma$. In other words, $V^0 = V^\Gamma := \{v \in V : u_\sigma(v) = v,\ \forall\ \sigma \in \Gamma\}$.*

(2) *Let $f : V_1 \to V_2$ be an L–linear map between two L–vector spaces. Asssume that $V_\ell^0 \subset V_\ell$ is a K–structure ($\ell = 1, 2$). Then f is rational over K if, and only if it commutes with the Γ–action. That is,*

$$f(u_\sigma(x)) = u_\sigma(f(x)), \quad \text{for every } \sigma \in \Gamma, x \in V_1.$$

(3) *With the same notational set up of the previous part, let $\mathcal{G}(f) \subset V_1 \oplus V_2$ be the graph of f. Then f is rational over K if and only if $\mathcal{G}(f)$ is rational over K, where the K–structure on $V_1 \oplus V_2$ is given by $V_1^0 \oplus V_2^0$.*

(4) *Let $W \subset V$ be a sub-L-vector space of V. Then W is rational over K if and only if $u_\sigma(W) \subset W$ for every $\sigma \in \Gamma$.*

Proof. (1). Let us choose a basis $\{e_i\}_{i\in I}$ of V^0. Given $x \in V$, we can write it, uniquely, as a finite sum $x = \sum_{i\in I} \lambda_i e_i$, where $\lambda_i \in L$. The condition $u_\sigma(x) = x$ is then equivalent to

$$\sum_{i\in I} (\sigma(\lambda_i) - \lambda_i) e_i = 0,$$

which implies (since $\{e_i\}$ is a basis of V as an L–vector space) that $\sigma(\lambda_i) = \lambda_i$. Thus, $u_\sigma(x) = x$ for every σ, if and only if $\sigma(\lambda_i) = \lambda_i$ for every σ and $i \in I$. As L/K is a Galois extension, this implies that $\lambda_i \in K$ for every $i \in I$, and hence $x \in V^0$.

(2). Assume that f commutes with Γ–actions. Let $v \in V_1^0$. Then we have:

$$f(v) = f(u_\sigma(v)) = u_\sigma(f(v)),$$

showing that $f(v) \in V_2^0$ by the previous part. Conversely, assume that f is rational over K, i.e, $f(V_1^0) \subset V_2^0$. Choose a basis $\{e_i\}_{i\in I}$ of V_1^0. Then, for every $v = \sum_{i\in I} \lambda_i e_i \in V$, and $\sigma \in \Gamma$, we have:

$$f(u_\sigma(v)) = \sum_{i\in I} \sigma(\lambda_i) f(e_i) = u_\sigma(\sum_{i\in I} \lambda_i f(e_i)) = u_\sigma(f(v)).$$

Here, we have used L–linearity of f, K–linearity of u_σ and equation (Γ–linear).

(3) is obvious from the definitions.

(4) Let $W \subset V$ be a sub-L-vector space of V.

Claim. There exist two sub-L-vector spaces $V_1, V_2 \subset V$, each rational over K, an L–linear map $f : V_1 \to V_2$ such that $V = V_1 \oplus V_2$ and $W \subset V$ is identified with the graph of f, $W = \mathcal{G}(f) \subset V_1 \oplus V_2$.

Proof of the claim. We need to make some choices.

- Let $\{w_j\}_{j\in J}$ be a basis of W (over L).
- Let $\{e_b\}_{b\in B} \subset V^0$ be such that $\{w_j\} \cup \{e_b\}$ is a basis of V.
- Let $\{e_a\}_{a\in A} \subset V^0$ be such that $\{e_a\} \cup \{e_b\}$ is a basis of V.

The fact that these choices can be made is a foundational result of linear algebra.

Now let $V_1 = L - \mathrm{Span}\{e_a\}$ and $V_2 = L - \mathrm{Span}\{e_b\}$. These sub-$L$-vector spaces of V are rational over K by construction. Moreover, $V = V_1 \oplus V_2$ and for every $v_1 \in V_1$, there exists a unique $f(v_1) \in V_2$ such that $v_1 + f(v_1) \in W$. This is because each e_a can be written uniquely in the basis $\{w_j\} \cup \{e_b\}$. In other words, we have:

$$V_1 \hookrightarrow V \twoheadrightarrow V/W \cong V_2.$$

Thus, $f : V_1 \to V_2$ defined as: $f(v_1)$ is the unique vector in V_2 so that $v_1 + f(v_1) \in W$ satisfies the requirements of the claim.

Now part (4) follows from parts (2) and (3) (left as an easy exercise). □

(34.3) K**–structures via** Γ**–actions.–** Now assume that Γ is finite. Let V be an L–vector space together with a group homomorphism $u : \Gamma \to \mathrm{Aut}_{K\text{–vs}}(V)$ satisfying:

$$u_\sigma(\lambda v) = \sigma(\lambda) u_\sigma(v),\ \forall\ \sigma \in \Gamma,\ \lambda \in L,\ v \in V.$$

Theorem. *$V^0 = V^\Gamma$ is a K–structure on V.*

Proof. Let $\varphi : V^0 \otimes_K L \to V$ be the canonical L–linear map. Let $u'_\sigma = \mathrm{Id}_{V^0} \otimes \sigma \in \mathrm{Aut}_K(V^0 \otimes_K L)$ be the Γ–action on $V^0 \otimes_K L$ (associated to the canonical K–structure $V^0 = V^0 \otimes_K K \subset V^0 \otimes L$). Let $W = \mathrm{Ker}(\varphi) \subset V^0 \otimes_K L$. It is clear that $u'_\sigma(W) \subset W$, for every $\sigma \in \Gamma$, since φ commutes with Γ–actions. Theorem 34.2 (4) implies that $W^0 = W \cap V^0$ spans W as an L–vector space. But for every $w \in W^0$, we have $w = \varphi(w) = 0$, proving that $W = \{0\}$, i.e, φ is injective. Note that we did not use $|\Gamma| < \infty$ hypothesis for this part.

To prove surjectivity, we have to show that $V^0 \subset V$ spans V as an L–vector space. If not, we will be able to find a non–zero linear form $\xi : V \to L$ (L–linear) such that $\xi|_{V_0} \equiv 0$. Let $v \in V$ be such that $\xi(v) \neq 0$. Then, for any $\alpha \in L$, $\sum_{\sigma\in\Gamma} u_\sigma(\alpha v)$ is in V^0, which implies:

$$0 = \xi(\sum_{\sigma\in\Gamma} u_\sigma(\alpha v)) = \xi(\sum_{\sigma\in\Gamma} \sigma(\alpha) u_\sigma(v)) = \sum_{\sigma\in\Gamma} \sigma(\alpha)\xi(u_\sigma(v))$$

By Dedekind's independence of characters, this means $\xi(u_\sigma(v)) = 0$ for every $\sigma \in \Gamma$. In particular, for $\sigma = e$, we get $\xi(v) = 0$ which is a contradiction. □

(34.4) Noether's equations.– Assume that L/K is a *finite* Galois extension, with $\Gamma = \mathsf{G}(L/K)$. Let $m, n \in \mathbb{Z}_{\geq 1}$. For an $m \times n$ matrix $X = (X_{ij}) \in \mathrm{Mat}_{m\times n}(L)$ and $\sigma \in \Gamma$, we denote by $\sigma(X) = (\sigma(X_{ij}))$.

Theorem. *Let $U : \Gamma \to \mathrm{GL}_n(L)$ be a set map. Then the following two conditions are equivalent.*

(1) *For every* $\sigma, \tau \in \Gamma$*, we have*

$$\boxed{U_{\sigma\tau} = U_\sigma \cdot \sigma(U_\tau)}$$

These equations for the set map U *are often called* Noether's equations.

(2) *There exists* $A \in \mathrm{GL}_n(L)$ *such that* $U_\sigma = A^{-1} \cdot \sigma(A)$ *for every* $\sigma \in \Gamma$.

Proof. (2)⇒(1) is easily verified as follows.

$$U_{\sigma\tau} = A^{-1} \cdot \sigma(\tau(A)) = A^{-1} \cdot \sigma(A) \cdot \sigma(A^{-1}) \cdot \sigma(\tau(A)) = U_\sigma \cdot \sigma(U_\tau).$$

Conversely, let $U : \Gamma \to \mathrm{GL}_n(L)$ be a set map satisfying Noether's equations. We can define $u_\sigma : L^n \to L^n$ as $u_\sigma(\xi) = U_\sigma \cdot \sigma(\xi)$. Here, we are viewing L^n as $n \times 1$ matrices (column vectors).

- $u_{\sigma\tau} = u_\sigma u_\tau$. This is clear, since for every $\xi \in L^n$, we have:

  $$u_{\sigma\tau}(\xi) = U_{\sigma\tau} \cdot \sigma(\tau(\xi)) = U_\sigma \cdot \sigma(U_\tau) \cdot \sigma(\tau(\xi)) = U_\sigma \cdot \sigma(U_\tau \cdot \tau(\xi)) = u_\sigma(u_\tau(\xi)).$$

- $u_\sigma(\lambda\xi) = \sigma(\lambda)u_\sigma(\xi)$, for every $\xi \in L^n$ and $\lambda \in L$. This is clear from the definition of u_σ.
- $u_e = \mathrm{Id}$, where $e \in \Gamma$ is the neutral element. Using Noether's equations with $\sigma = \tau = e$, we get $U_e = U_e^2$. Since U_e is invertible, this implies that U_e is the identity matrix.

Thus, we have verified the hypotheses of Theorem 34.3, showing that $V^0 = (L^n)^\Gamma$ is a K–structure on L^n. Unfolding the definitions, this means that $\dim_K(V^0) = n$. Let $B \in \mathrm{GL}_n(L)$ be an invertible matrix whose columns constitute a basis of V^0. The condition $u_\sigma(B) = B$ translates to $U_\sigma \cdot \sigma(B) = B$. Taking $A = B^{-1}$ proves our theorem. □

Remark. The statement of this theorem is often written as

$$\boxed{H^1(\Gamma, \mathrm{GL}_n(L)) = \{1\}}$$

where $H^1(\Gamma, M)$ is the first *Galois cohomology* group. We will learn more about this next week during Will Newman's presentation.

(34.5) Special cases.– The following result is a corollary of Theorem 34.4. Again, L/K is a finite Galois extension, with $\Gamma = \mathsf{G}(L/K)$.

Corollary.

(1) *Let* $\{c_\sigma \in L^\times\}_{\sigma\in\Gamma} \subset L^\times$*. Then there exists* $a \in L^\times$ *such that* $c_\sigma = \frac{\sigma(a)}{a}$ *(*$\forall\ \sigma \in \Gamma$*) if and only if* $c_{\sigma\tau} = c_\sigma\sigma(c_\tau)$ *(*$\forall\ \sigma, \tau \in \Gamma$*).*

(2) *Let* $\{x_\sigma \in L\}_{\sigma\in L} \subset L$*. Then there exists* $a \in L$ *such that* $x_\sigma = \sigma(a) - a$ *(*$\forall\sigma \in \Gamma$*) if and only if* $x_{\sigma\tau} = x_\sigma + \sigma(x_\tau)$ *(*$\forall\ \sigma, \tau \in \Gamma$*).*

PROOF. (1) is obtained by taking $n = 1$ in Theorem 34.4. (2) is proved using $n = 2$ and $U_\sigma = \begin{bmatrix} 1 & x_\sigma \\ 0 & 1 \end{bmatrix}$. We give a direct proof below, since this result is going to be crucial in our study of abelian extensions.

Proof of (1): As it was for the proof of Theorem 34.4, if there exists $a \in L^\times$ such that $c_\sigma = \sigma(a)/a$, then $c_{\sigma\tau} = c_\sigma \sigma(c_\tau)$. Let us prove the converse. Using Dedekind's independence of characters, $\sum_{\tau\in\Gamma} c_\tau \tau : L \to L$ is not identically zero. Meaning, there exists $x \in L^\times$ such that

$$b := \sum_{\tau\in\Gamma} c_\tau \tau(x) \neq 0.$$

Now, for every $\sigma \in \Gamma$, we have:

$$\sigma(b) = \sum_{\tau\in\Gamma} \sigma(c_\tau)\sigma(\tau(x)) = \sum_{\tau\in\Gamma} \frac{c_{\sigma\tau}}{c_\sigma}(\sigma\tau)(x) = \frac{1}{c_\sigma} \sum_{\tau'\in\Gamma} c_{\tau'}\tau'(x) = \frac{b}{c_\sigma}.$$

Here, we changed variables $\tau' = \sigma\tau$. We conclude that, for every $\sigma \in \Gamma$, $c_\sigma = \dfrac{b}{\sigma(b)}$. (1) is proved by taking $a = b^{-1}$.

Proof of (2): Again we only show the sufficiency of Noether's equations. Namely, assuming $x_{\sigma\tau} = x_\sigma + \sigma(x_\tau)$ we will establish the existence of $a \in L$ so that $x_\sigma = \sigma(a) - a$ for every $\sigma \in \Gamma$. Using Dedekind's independence of characters, we conclude the existence of an element $\theta \in L$ so that

$$y = \sum_{\tau\in\Gamma} \tau(\theta) \neq 0.$$

Note that $\sigma(y) = y$ for every $\sigma \in \Gamma$, which implies that $y \in K^\times$. Define:

$$b = \frac{1}{y} \sum_{\tau\in\Gamma} x_\tau \tau(\theta).$$

For any $\sigma \in \Gamma$, we get, using $\sigma(x_\tau) = x_{\sigma\tau} - x_\sigma$:

$$\begin{aligned} \sigma(b) &= \frac{1}{y} \sum_{\tau} \sigma(x_\tau)\sigma(\tau(\theta)) = \frac{1}{y} \sum_{\tau} (x_{\sigma\tau} - x_\sigma)(\sigma\tau)(\theta) \\ &= \frac{1}{y} \sum_{\tau'} x_{\tau'}\tau'(\theta) - \frac{x_\sigma}{y} \sum_{\tau'} \tau'(\theta) = b - x_\sigma. \end{aligned}$$

Thus, $x_\sigma = b - \sigma(b)$ for every $\sigma \in \Gamma$. (2) is proved by taking $a = -b$. □