LECTURE 35

(35.0) Overview.– Recall that for a Galois extension L/K with Galois group $\Gamma = \mathsf{G}(L/K)$, we established a bijection between the following two partially ordered sets (order is inclusion).

$$\boxed{\begin{array}{c}\text{Sub-}K\text{-extensions}\\ \text{of } L/K\end{array}} \longleftrightarrow \boxed{\text{Closed subgroups of } \Gamma}$$

Here, we view Γ with the canonical topology of an inverse limit of finite discrete groups. For the rest of the course, we will narrow our focus to the case of finite Γ (so topological considerations are no longer necessary).

We say a finite Galois extension L/K is *cyclic (resp. abelian, solvable, simple)* if $\mathsf{G}(L/K)$ is cyclic (resp. abelian, solvable, simple). Recall that a group G is said to be *solvable* if there exists a chain of normal subgroups:

$$G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_\ell = \{e\}\ ,$$

such that G_j/G_{j+1} is abelian, for every $0 \leq j < \ell$. Thus, every abelian group is solvable. Solvability of an extension L/K is equivalent to solvability by radicals of any minimal polynomial $\mathsf{m}_\alpha(x)$, where $\alpha \in L$.

We say a group G is *simple* if there are no non–trivial, proper normal subgroups of G. That is, $H \triangleleft G \Rightarrow H = \{e\}$ or G. By convention, we do not consider the trivial group to be simple. The only abelian, simple, finite groups are $\mathbb{Z}/p\mathbb{Z}$ where $p \in \mathbb{Z}_{\geq 2}$ is a prime number.

Our next topic is to study *abelian extensions*.

- For each $n \in \mathbb{Z}_{\geq 3}$, let $\mu_n \in \mathbb{C}^\times$ be the cyclic subgroup consisting of n^{th} roots of 1. Then $\mathsf{G}(\mathbb{Q}(\mu_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ is abelian.

- Let k be a finite field. Let K/k be the finite extension of degree n. Then $\mathsf{G}(K/k) \cong \mathbb{Z}/n\mathbb{Z}$ is cyclic, hence abelian.

We also know that, for instance, if K is the splitting extension over $\mathbb{Q}$ of $x^5 - 7$, then $\mathsf{G}(K/\mathbb{Q}) \cong \mathbb{Z}/5\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$ is not abelian. Here, $\mathbb{Z}/4\mathbb{Z} \cong (\mathbb{Z}/5\mathbb{Z})^\times \cong \mathrm{Aut}_{\mathrm{gp}}(\mathbb{Z}/5\mathbb{Z})$ acts naturall on $\mathbb{Z}/5\mathbb{Z}$. Note that $\mathsf{G}(K/\mathbb{Q}(\mu_5)) \cong \mathbb{Z}/5\mathbb{Z}$ is abelian. Thus, we will often have to assume that our base field contains a primitive n^{th} root of unity.

Definition. Let F be a field and let $n \in \mathbb{Z}_{\geq 3}$. Consider the subgroup (which we know to be cyclic):

$$\mu_n(F) := \{x \in F : x^n = 1\} \subset F^\times.$$

We say that F contains a primitive n^{th} root of unity if $\mu_n(F) \cong \mathbb{Z}/n\mathbb{Z}$. That is, there exists $\zeta \in F$ such that $\langle \zeta \rangle \cong \mathbb{Z}/n\mathbb{Z}$.

(35.1) Norm and trace.– Let F be a field and let A be an F–algebra, which is finite-dimensional as an F–vector space. Given an element $a \in A$, consider the F–linear endomorphism of left multiplication by a, $\mathcal{L}_a : A \to A$. That is, $\mathcal{L}_a(x) = ax$.

$$\boxed{\text{Norm of } a = \mathsf{N}_{A/K}(a) := \det(\mathcal{L}_a)}$$

$$\boxed{\text{Trace of } a = \mathrm{Tr}_{A/K}(a) := \mathrm{Tr}(\mathcal{L}_a)}$$

Example. Let $f(x) = x^n + a_1x^{n-1} + \cdots + a_n \in K[x]$, and let $A = K[x]/(f(x))$. Let $\alpha = \overline{x} \in A$. Then multiplication by α, in the basis $\{1, x, x^2, \ldots, x^{n-1}\}$ of A over K, has the following form:

$$\mathcal{L}_\alpha = \begin{bmatrix} 0 & 0 & \cdots & \cdots & 0 & -a_n \\ 1 & 0 & \cdots & \cdots & 0 & -a_{n-1} \\ 0 & 1 & \ddots & \cdots & 0 & \vdots \\ \vdots & 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & 0 & \cdots & 0 & 1 & -a_1 \end{bmatrix}$$

Hence, we get $\mathsf{N}_{A/K}(\alpha) = (-1)^n a_n = (-1)^{\deg(f)} f(0)$ and $\mathrm{Tr}_{A/K}(\alpha) = -a_1$.

Proposition. *Let L/K be a finite field extension, A a finite–dimensional L–algebra. Let $m = \dim_L(A)$. For $\alpha \in L$, we have:*

$$\mathsf{N}_{A/K}(\alpha) = \left(\mathsf{N}_{L/K}(\alpha)\right)^m, \qquad \mathrm{Tr}_{A/K}(\alpha) = m\,\mathrm{Tr}_{L/K}(\alpha).$$

Proof. Let $\ell = \dim_K(L)$ and let $X = (x_{i,i'})_{1 \le i,i' \le \ell} \in \mathrm{Mat}_{\ell \times \ell}(K)$ be the matrix of $\mathcal{L}_\alpha : L \to L$, in a chosen basis $\{\lambda_i\}_{1 \le i \le \ell}$.

Let $\{a_j\}_{1 \le j \le m}$ be a basis of A as an L–vector space. Recall that $\{\lambda_i\alpha_j\}$ is a basis of A as a K–vector space. In this basis, the matrix of left multiplication by α, say $\widetilde{\mathcal{L}}_\alpha : A \to A$ is a block $m\ell \times m\ell$ size matrix with X on the diagonals. The proposition follows. $\square$

(35.2) Norm and trace via the Galois group.– Let L/K be a finite Galois extension. Let $\Gamma = \mathsf{G}(L/K)$.

Proposition. *For every $\alpha \in L$, we have:*

$$\boxed{\mathsf{N}_{L/K}(\alpha) = \prod_{\sigma \in \Gamma} \sigma(\alpha)} \qquad \boxed{\mathrm{Tr}_{L/K}(\alpha) = \sum_{\sigma \in \Gamma} \sigma(\alpha)}$$

Proof. Let $f(x) = \mathsf{m}_\alpha(x) \in K[x]$ and $n = \deg f$. Note that $f(x)$ splits over L since L is Galois. That is, we have:

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_n) = \prod_{\beta \in \Gamma\alpha} (x - \beta)$$

Since $K(\alpha) \cong K[x]/(f(x))$, by Example from the previous paragraph, we have:

$$\mathsf{N}_{K(\alpha)/K}(\alpha) = (-1)^n \prod_{\beta \in \Gamma\alpha} \beta,$$

$$\mathrm{Tr}_{K(\alpha)/K}(\alpha) = -\sum_{\beta \in \Gamma\alpha} \beta$$

Let $rn = [L : K]$, where $r = [L : K(\alpha)]$. Note that $L/K(\alpha)$ is also Galois, hence $\mathsf{G}\,(L/K(\alpha))$ has order r, and is isomorphic to the subgroup $\mathrm{Stab}_\Gamma(\alpha) \subset \Gamma$. This observation leads to the following identity:

$$\prod_{\sigma \in \Gamma} \sigma(\alpha) = \left(\prod_{\beta \in \Gamma\alpha} \beta \right)^{|\,\mathrm{Stab}_\Gamma(\alpha)|} = \mathsf{N}_{K(\alpha)/K}(\alpha)^r.$$

$$\sum_{\sigma \in \Gamma} \sigma(\alpha) = |\,\mathrm{Stab}_\Gamma(\alpha)| \sum_{\beta \in \Gamma\alpha} \beta = r\,\mathrm{Tr}_{K(\alpha)/K}(\alpha).$$

The right–hand sides of these two equations are respectively $\mathsf{N}_{L/K}(\alpha)$ and $\mathrm{Tr}_{L/K}(\alpha)$, by Proposition 35.1, and the result follows. □

(35.3) Hilbert's $90^{\mathbf{th}}$ problem.– The following result is the key step in classifying cyclic extensions.

Theorem. *Let L/K be a cyclic extension, with $\Gamma = \mathsf{G}\,(L/K) \cong \mathbb{Z}/m\mathbb{Z}$. Choose a generator $\sigma \in \Gamma$.*

(1) *For $\beta \in L^\times$, $\mathsf{N}_{L/K}(\beta) = 1$ if and only if there exists $\alpha \in L^\times$ such that $\beta = \frac{\sigma(\alpha)}{\alpha}$.*
(2) *For $\beta \in L$, $\mathrm{Tr}_{L/K}(\beta) = 0$ if and only there exists $\alpha \in L$ such that $\beta = \sigma(\alpha) - \alpha$.*

Proof. (1). If $\beta = \frac{\sigma(\alpha)}{\alpha}$, then we have:

$$\mathsf{N}_{L/K}(\beta) = \prod_{j=0}^{m-1} \sigma^j \left(\frac{\sigma(\alpha)}{\alpha} \right) = \frac{\sigma(\alpha)\sigma^2(\alpha)\cdots\sigma^m(\alpha)}{\alpha\sigma(\alpha)\cdots\sigma^{m-1}(\alpha)} = 1,$$

using the fact that $\sigma^m = \mathrm{Id}$.

For the converse, define $u : \Gamma \to L^\times$ by

$$u_{\sigma^k} = \prod_{j=0}^{k-1} \sigma^j(\beta).$$

This definition is unambiguous, since

$$u_e = u_{\sigma^m} = \prod_{j=0}^{m-1} \sigma^j(\beta) = \mathsf{N}_{L/K}(\beta) = 1.$$

It is also easy to see that $u_{\sigma^{k+1}} = u_\sigma \sigma(u_{\sigma^k})$. This implies, by Corollary 34.5, that there exists $\alpha \in L^\times$ such that $u_\tau = \frac{\tau(\alpha)}{\alpha}$. For $\tau = \sigma$ we get the claimed result.

(2). As in the previous part, it is easy to see that if $\beta = \sigma(\alpha) - \alpha$, for some $\alpha \in L$, then $\mathrm{Tr}_{L/K}(\beta) = 0$.

Now we prove the converse. Define $u : \Gamma \to L$ by

$$u_{\sigma^k} = \sum_{j=0}^{k-1} \sigma^j(\beta).$$

Again, using $\mathrm{Tr}_{L/K}(\beta) = 0$, we can check that this definition is unambiguous. Moreover, $u_{\sigma^{k+1}} = u_\sigma + \sigma(u_{\sigma^k})$. Corollary 34.5 again implies the existence of an $\alpha \in L$ so that $\beta = \sigma(\alpha) - \alpha$. $\square$

(35.4) Cyclic extensions.– Again we assume that L/K is a cyclic extension, with $\Gamma = \mathsf{G}(L/K) \cong \mathbb{Z}/m\mathbb{Z}$. We choose a generator $\sigma \in \Gamma$. We further assume that K contains a primitive m^{th} root of unity, which we denote by ζ.

Theorem. *There exists $\alpha \in L^\times$ such that the following assertions hold.*

(1) $a = \alpha^m \in K^\times$.
(2) $\sigma(\alpha) = \zeta\alpha$. *Hence* $\Gamma\alpha = \{\alpha, \zeta\alpha, \dots, \zeta^{m-1}\alpha\}$.
(3) $L = K(\alpha)$. *Hence L is the splitting extension over K of* $x^m - a \in K[x]$

$$x^m - a = \prod_{j=0}^{m-1} x - \zeta^j\alpha \ , \qquad \textit{in } L[x].$$

Proof. Note that $\zeta \in K^\times$, and $\zeta^m = 1$, which implies:

$$\mathsf{N}_{L/K}(\zeta) = \zeta^m = 1.$$

Therefore, by Theorem 35.4, there exists $\alpha \in L^\times$ such that $\zeta = \frac{\sigma(\alpha)}{\alpha}$. (2) is proved.

As norm of any element of L is an element of K, we get

$$\mathsf{N}_{L/K}(\alpha) = \zeta^{\frac{m(m-1)}{2}}\alpha^m = (-1)^{m-1}\alpha^m \in K.$$

Here, we have used that $x^m - 1 = \prod_{j=0}^{m-1}(x - \zeta^j)$ in $K[x]$, which implies (upon setting $x = 0$) that $-1 = (-1)^m\zeta^{\frac{m(m-1)}{2}}$. Thus, $a = \alpha^m \in K$ as claimed in (1).

It remains to show that $L = K(\alpha)$. Note that the identity $x^m - a = \prod_{j=0}^{m-1} x - \zeta^j\alpha$ implies that $K(\alpha)/K$ is the splitting extension of $x^m - a$, which has m distinct roots in $K(\alpha)$. Hence $K(\alpha)/K$ is a Galois extension. The claim that $K(\alpha) = L$ follows from the fact that $\mathrm{Stab}_{\mathsf{G}(L/K)}(\alpha)$ is trivial (since $\sigma^j(\alpha) = \zeta^j\alpha \neq \alpha$ for $1 \leq j \leq m-1$). $\square$