LECTURE 36

(36.0) Kummer's theorem.– In this set of notes, we fix a field K, an integer $n \geq 2$, and assume that $\mu_n(K) \cong \mathbb{Z}/n\mathbb{Z}$. That is, K contains a primitive n^{th} root of unity.

Consider the following two sets:

- Let $\mathcal{E}_n^{\text{ab}}(K)$ be the set of all finite, abelian, Galois extensions L/K such that the exponent of $\mathsf{G}(L/K)$ divides n. In other words, $\sigma^n = \text{Id}$ for every $\sigma \in \mathsf{G}(L/K)$.

  In order to avois logical fallacies, let $\Omega = \overline{K}$ be the algebraic closure of K. We can view each $L \in \mathcal{E}_n^{\text{ab}}(K)$ as a subfield of Ω, which makes it clear that $\mathcal{E}_n^{\text{ab}}(K)$ is a set (subset of the power set of Ω).

- Let $\mathcal{G}_n(K^\times)$ consist of all subgroups $H \subset K^\times$ containing
$$\mathcal{P}_n\left(K^\times\right) := \{z^n : z \in K^\times\} \subset H \subset K^\times,$$
  such that $H/\mathcal{P}_n\left(K\right)$ is finite.

Theorem. *The following assignments are mutually inverse to each other, inclusion preserving bijections between $\mathcal{E}_n^{\text{ab}}(K)$ and $\mathcal{G}_n(K^\times)$.*

$$H \subset K^\times \mapsto K(H^{1/n}) = \{z \in \Omega : z^n \in H\},$$
$$L \in \mathcal{E}_n^{\text{ab}}(K) \mapsto H_L := \mathcal{P}_n\left(L^\times\right) \cap K^\times.$$

Moreover, for every $H \in \mathcal{G}_n(K^\times)$, there is a group isomorphism:
$$\psi : \mathsf{G}\left(K(H^{1/n})/K\right) \xrightarrow{\sim} \text{Hom}_{gp}(H/\mathcal{P}_n\left(K^\times\right), \mu_n(K))$$
given as follows. For $\sigma \in \mathsf{G}\left(K(H^{1/n})/K\right)$ and $\theta \in K(H^{1/n})$ such that $\theta^n \in H$, let $t = \overline{\theta^n} \in H/\mathcal{P}_n\left(K^\times\right)$. Then
$$\psi(\sigma) : t \mapsto \frac{\sigma(\theta)}{\theta}.$$
In particular, we have $[K(H^{1/n}) : K] = \left|H/\mathcal{P}_n\left(K^\times\right)\right|$.

Remark. The first assertion is true without the finiteness hypothesis, with the same proof as we give below. The second assertion, without finiteness hypothesis, is proved by taking the inverse limit over finite subextensions, and claims that ψ is an isomorphism of topological groups. We will only give a proof in the finite case here, which is the heart of the argument anyway.

(36.1) Pairing for Galois extensions.– Let L/K be a Galois extension. Let $H_L = \mathcal{P}_n(L^\times) \cap K^\times$. We consider the following map:

$$\langle \cdot, \cdot \rangle : \mathsf{G}(L/K) \times H_L/\mathcal{P}_n\left(K^\times\right) \to \mu_n(K),$$

given as follows. Let $\sigma \in \mathsf{G}(L/K)$ and $t \in H_L/\mathcal{P}_n(K^\times)$. Choose an element $\theta \in L^\times$ such that $\theta^n \equiv t$ modulo $\mathcal{P}_n(K^\times)$. Then:

$$\langle \sigma, t \rangle = \frac{\sigma(\theta)}{\theta} \in L^\times.$$

Note that if $\tau \in L^\times$ is such that $\tau^n \equiv \theta^n$ modulo $\mathcal{P}_n(K^\times)$, then $(\theta/\tau)^n = a^n$ for some $a \in K^\times$. Thus, θ/τ is a solution of

$$x^n - a^n = \prod_{j=0}^{n-1} x - \zeta^j a,$$

showing that there is $0 \leq j \leq n-1$, such that $\theta/\tau = \zeta^j a \in K$. Hence $\sigma(\theta/\tau) = \theta/\tau$ for every $\sigma \in \mathsf{G}(L/K)$. This proves that $\langle \cdot, \cdot \rangle$ is unambiguous. We still have to show that it takes values in $\mu_n(K)$.

Let $\theta \in L^\times$ be such that $t = \theta^n \in K^\times$. Thus θ is a solution of $x^n - t$. This implies:

$$x^n - t = \prod_{j=0}^{n-1} x - \zeta^j \theta.$$

For any $\sigma \in \mathsf{G}(L/K)$, $\sigma(\theta)$ is another root of $x^n - t$ showing that there exists j with $\sigma(\theta) = \zeta^j \theta$. Hence, $\sigma(\theta)/\theta \in \mu_n(K)$.

Proposition. *The map $\langle \cdot, \cdot \rangle$ is bi–multiplicative. That is, for every $g_1, g_2, g \in \mathsf{G}(L/K)$ and $t_1, t_2, t \in H_L/\mathcal{P}_n(K^\times)$, we have:*

$$\langle g_1 g_2, t \rangle = \langle g_1, t \rangle \langle g_2, t \rangle, \qquad \langle g, t_1 t_2 \rangle = \langle g, t_1 \rangle \langle g, t_2 \rangle.$$

Let $\phi : H_L/\mathcal{P}_n(K^\times) \to \mathrm{Hom}_{gp}(\mathsf{G}(L/K), \mu_n(K))$ be given by $\phi(t) = \langle -, t \rangle$. Then ϕ is a bijection.

Proof. The proof of bi–multiplicativity is left as an easy exercise. It essentially follows from the discussion preceding the proposition.

Let us prove that ϕ is a bijection. Let $\bar{t} \in H_L/\mathcal{P}_n(K^\times)$. Let $\theta \in L^\times$ be such that $\theta^n = t \in K^\times$. If $\phi(\bar{t}) = e$, then $\sigma(\theta) = \theta$ for every $\sigma \in \mathsf{G}(L/K)$, showing that $\theta \in K^\times$, i.e, $\bar{t} = \bar{1}$. This proves that ϕ is injective.

To show surjectivity, let $\chi \in \mathrm{Hom}_{gp}(\mathsf{G}(L/K), \mu_n(K))$. Then $\chi(\sigma\tau) = \chi(\sigma)\chi(\tau) = \chi(\sigma)\sigma(\chi(\tau))$, since σ acts trivially on K. By Corollary 34.5, we can find $\theta \in L^\times$ such that $\chi(\sigma) = \sigma(\theta)/\theta$ for every $\sigma \in \mathsf{G}(L/K)$. It remains to check that $\theta^n \in K^\times$.

Note that $\chi(\sigma)^n = 1$, for every $\sigma \in \mathsf{G}(L/K)$. This means, $\frac{\sigma(\theta)^n}{\theta^n} = 1$, that is, $\sigma(\theta^n) = \theta^n$ for every $\sigma \in \mathsf{G}(L/K)$. Since the extension is Galois, we get $\theta^n \in K^\times$ as claimed. □

Remark. When $\mathsf{G}\left(L/K\right)$ is finite, abelian and of exponent dividing n, then

$$\mathrm{Hom}_{gp}(\mathsf{G}\left(L/K\right), \mu_n(K)) \cong \mathsf{G}\left(L/K\right) \text{ (non–canonically).}$$

This claim uses the structure theorem of finite abelian groups, and is verified as follows. Since all the groups involved are abelian, we may revert to the additive notation. A finite abelian group G of exponent r has the following form:

$$G \cong \mathbb{Z}/r_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/r_t\mathbb{Z}, \quad \text{where } r_t = r \text{ and } r_1|r_2|\cdots|r_t.$$

Thus it suffices to prove that $\mathrm{Hom}(\mathbb{Z}/r\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/r\mathbb{Z}$, where $r|n$. Let us write $n = rd$, and let $\chi : \mathbb{Z}/r\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ be given by $\chi(\overline{1}) = \overline{d}$. It is left as an easy exercise that $\mathrm{Hom}(\mathbb{Z}/r\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$ is generated by χ and order of χ is r.

(36.2) Proof of Theorem 36.0 - I.– We begin by checking the assignments given in the statement of Theorem 36.0. Let $A \subset K^\times$ and let $K(A^{1/n})$ be the extension generated by the roots of the set of polynomials $\{x^n - a\}_{a\in A}$.

Proposition.

(1) *$K(A^{1/n})$ is an abelian, Galois extension of K. Moreover, $\sigma^n = 1$ for every $\sigma \in \mathsf{G}\left(K(A^{1/n})/K\right)$. That is, $\mathsf{G}\left(K(A^{1/n})/n\right)$ has a finite exponent which divides n.*

(2) *Let H be the smallest subgroup of $K^\times$ containing A and $\mathcal{P}_n\left(K^\times\right)$. Then $K(H^{1/n}) = K(A^{1/n})$.*

(3) *If $H/\mathcal{P}_n\left(K^\times\right)$ is finite, then $K(H^{1/n})/K$ is a finite extension.*

Proof. (1). For each $a \in K^\times$, let L_a be the splitting extension of $x^n - a$. Let $\alpha \in L_a$ be a root of $x^n - a$. Then:

$$x^n - a = \prod_{j=0}^{n-1} x - \zeta^j\alpha, \ \in \ L_a[x]$$

proving that $x^n - a$ is a separable polynomial. This shows that $K(A^{1/n})/K$ is a Galois extension.

Now given $\sigma \in \mathsf{G}\left(K(A^{1/n})/K\right)$ and $\alpha \in K(A^{1/n})$ such that $\alpha^n \in A$, we have:

$$\sigma(\alpha^n) = \alpha^n \Rightarrow \left(\frac{\sigma(\alpha)}{\alpha}\right)^n = 1$$

that is, $\sigma(\alpha) = \zeta^j\alpha$ for some $0 \leq j \leq n-1$. This shows that $\sigma^n(\alpha) = \alpha$ for every $\alpha \in K(A^{1/n})$ such that $\alpha^n \in A$. Since such elements generate the field $K(A^{1/n})$ we conclude that $\sigma^n = \mathrm{Id}$.

It remains to check that $\mathsf{G}\left(K(A^{1/n})/K\right)$ is abelian. Let $\sigma, \tau \in \mathsf{G}\left(K(A^{1/n})/K\right)$ and $\alpha \in K(A^{1/n})$ such that $\alpha^n \in A$ (as above). By the previous argument, there exist j, k such that $\sigma(\alpha) = \zeta^j\alpha$ and $\tau(\alpha) = \zeta^k\alpha$. It is now clear that $\sigma(\tau(\alpha)) = \tau(\sigma(\alpha))$. Again the extension is generated by such α, showing that σ and τ commute.

(2) follows from the fact that if α_ℓ is a root of $x^n - a_\ell$ $(1 \leq \ell \leq r)$, then $\alpha = \alpha_1 \cdots \alpha_r$ is a root of $x^n - a$, with $a = a_1 \cdots a_r$.

To prove (3), let us choose finite number of coset representatives

$$H = a_1\mathcal{P}_n\left(K^\times\right) \sqcup \cdots \sqcup a_r\mathcal{P}_n\left(K^\times\right).$$

Let L be the splitting extension of $\{x^n - a_\ell\}_{1\le\ell\le r}$. It is clear that $L = K(H^{1/n})$ and L is finite.

□

This proposition shows that the map $\mathcal{G}_n(K^\times) \to \mathcal{E}_n^{\mathrm{ab}}(K)$, given by $H \mapsto K(H^{1/n})$, is well–defined. For the converse, $L \mapsto H_L = \mathcal{P}_n\left(L^\times\right) \cap K^\times$, it only remains to check that $H_L/\mathcal{P}_n\left(K^\times\right)$ is finite. But this group is isomorphic to $\mathrm{Hom}_{gp}(\mathsf{G}\left(L/K\right), \mu_n(K))$ by Proposition 36.1 above, and the latter is finite.

(36.3) Proof of Theorem 36.0 - II.– Now we will check that the two assignments are mutually inverse to each other. That these preserve inclusions follows from the definitions.

Let $L \in \mathcal{E}_n^{\mathrm{ab}}(K)$. Set $H_L := \mathcal{P}_n\left(L^\times\right) \cap K^\times$. Let $L' = K(H_L^{1/n})$. Clearly $L' \subset L$ is a sub-K-extension. Moreover, it is obvious from the definitions that $H_{L'} = H_L$. By Proposition 36.1 and Remark 36.1, we obtain an identification between $\mathsf{G}\left(L'/K\right)$ and $\mathsf{G}\left(L/K\right)$, showing that $L' = L$.

Conversely, let $H \in \mathcal{G}_n(K^\times)$ and let $L = K(H^{1/n})$. Clearly $H \subset H_L = \mathcal{P}_n\left(L^\times\right) \cap K^\times$. To show that $H = H_L$, it is enough to establish that the restriction homomorphism

$$u : \mathrm{Hom}_{gp}(H_L/\mathcal{P}_n\left(K^\times\right), \mu_n(K)) \to \mathrm{Hom}_{gp}(H/\mathcal{P}_n\left(K^\times\right), \mu_n(K))$$

is injective. This is because, we already know that $|H/\mathcal{P}_n\left(K^\times\right)| \le |H_L/\mathcal{P}_n\left(K^\times\right)|$. If u is injective, by remark 36.1, we will also have the other way inequality, establishing that $H = H_L$.

Now identifying $\mathrm{Hom}_{gp}(H_L/\mathcal{P}_n\left(K^\times\right), \mu_n(K))$ with $\mathsf{G}\left(L/K\right)$, by the same remark, it is easy to see that $u(\sigma) = 1$ means $\sigma(\theta) = \theta$ for every $\theta \in L$ such that $\theta^n \in H$. Since such elements generate L, we get $\sigma = \mathrm{Id}$ showing that u is injective.

The last part of the theorem now follows from the established bijection and Proposition (and Remark) 36.1.