LECTURE 37

(37.0) Overview.– In these notes we will prove two theorems: *primitive element theorem* and *normal basis theorem.*

For a field extension L/K, a primitive element is any *algebraic* $\alpha \in L$ such that $L = K(\alpha)$. A necessary condition for the existence of such an element is that the extension is finite (of degree given by the degree of the minimal polynomial of α). This condition is not sufficient as the following example from Homework 10, Problem 3 demonstrates.

Example. Let $K = \mathbb{F}_p(\lambda, \mu)$ and $L = \mathbb{F}_p(\lambda_1, \mu_1)$ be its extension generated by roots λ_1 of $x^p - \lambda$ and μ_1 of $x^p - \mu$. We claim that L does not have any primitive element (it is easy to see that $[L : K] = p^2$ is finite). For the sake of a contradiction, let us assume that $\gamma \in L$ is a primitive element. Note that γ can be written as: $\gamma = \dfrac{P(\lambda_1, \mu_1)}{Q(\lambda_1, \mu_1)}$, where P and Q are polynomials in two variables, with coefficients from $\mathbb{F}_p$. Applying σ_p to both sides of the equation, we get

$$\gamma^p = \frac{P(\lambda_1^p, \mu_1^p)}{Q(\lambda_1^p, \mu_1^p)} = \frac{P(\lambda, \mu)}{Q(\lambda, \mu)} \in K.$$

Therefore, γ satisfies a polynomial of degree p, showing that $K(\gamma)/K$ can have degree at most p, so $K(\gamma) \neq L$.

(37.1) Primitive element theorem.–

Theorem. *Let L/K be a finite extension. Then the following two conditions are equivalent.*

(1) *There are only finitely many intermediate extensions $K \subset E \subset L$.*

(2) *There exists $\alpha \in L$ such that $L = K(\alpha)$.*

Remark. It is clear that if an extension is infinite, then it would certainly contain infinitely many intermediate extensions.

Condition (1) holds for finite Galois extensions, since subextensions correspond to subgroups of the (finite) Galois group. More generally, if L/K is a finite, separable extension, we can consider the splitting extension of the minimal polynomials of a finite system of generators of L, say $\Omega \supset L$, which is then finite and Galois. Thus L/K necessarily has finitely many intermediate extensions (since so does Ω/K). In particular, every finite extension over a perfect field satisfies the hypothesis (1) of the theorem above, hence contains a primitive element.

Proof. (1)$\Rightarrow$(2). If K is a finite field, then so is L, and we already know $L^\times$ is a cyclic group, say generated by $\alpha \in L^\times$. Then $L = K(\alpha)$ as claimed.

Now assume that K is infinite. As L/K is a finite extension, there exist $\alpha_1, \ldots, \alpha_r \in L$ such that $L = K(\alpha_1, \ldots, \alpha_r)$. An easy induction argument reduces the task of proving (2) to the case when $r = 2$, that is $L = K(\alpha, \beta)$.

Consider the infinite family of subextensions $L_t = K(\alpha + t\beta)$, where $t \in K$. As there are only finitely many intermediate extensions, there must exist $s \neq t \in L$ so that $L_s = L_t =: K'$. But then $\alpha, \beta \in K'$ showing that $K' = L$. Moreover, $K' = K(\gamma)$ with $\gamma = \alpha + t\beta$.

(2)⇒(1). Now we assume that $L = K(\alpha)$, where α is an algebraic element (otherwise the extension wouldn't be finite). Let $f(x) = \mathsf{m}_\alpha(x) \in K[x]$. Consider the (finite) set of monic factors of $f(x)$ in $L[x]$:

$$P = \{g(x) \in L[x] \text{ monic, such that } g(x) | f(x)\}.$$

We claim that every intermediate extension $K \subset E \subset L$ is generated by coefficients of $g(x)$ for some $g(x) \in P$. This clearly implies that there are finitely many such choices.

To prove the claim, consider the minimal polynomial of $\alpha \in L$ over E, $p(x) = \mathsf{m}_\alpha^E(x) \in E[x] \subset L[x]$. Note that $p(x)$ divides $f(x)$ and hence $p(x) \in P$. Let $F \subset E$ be generated by the coefficients of $p(x)$. It remains to show that $F = E$. Since $L = K(\alpha)$, we also have $L = F(\alpha) = E(\alpha)$. Moreover, the minimal polynomial of α over F is also $p(x)$, showing that $[L : F] = [L : E] = \deg(p)$. Hence $F = E$. □

(37.2) Normal basis theorem.–

Theorem. *Let L/K be a finite Galois extension and $\Gamma = \mathsf{G}(L/K)$. Then there exists $\theta \in L$ such that $\{g(\theta)\}_{g\in\Gamma}$ is a basis of L as a K–vector space (called* normal basis*).*

Remark.

(1) It is clear that such an element $\theta \in L$ will also generate L, i.e, will be a primitive element $L = K(\theta)$. This is because $\mathsf{m}_\theta(x) = \prod_{g\in\Gamma} x - g(\theta)$ is guarenteed to have degree $n = |\Gamma| = [L : K]$.

(2) It is not true that every primitive element will give rise to a normal basis. For instance, let us consider a cyclic extension of degree n as follows. Let $K = \mathbb{Q}(\mu_n)$ and choose $r \in K$ such that $x^n - r$ is irreducible. We know (from Kummer's theorem, or Homework 11, Problem 9) that $L =$ splitting extension of $x^n - r$ is a cyclic extension: $L = K(\alpha)$, where $\alpha^n = r$. Moreover,

$$x^n - r = \prod_{j=0}^{n-1} x - \zeta^j\alpha, \qquad \text{where } \zeta = e^{\frac{2\pi\iota}{n}}.$$

Choose a generator $\sigma \in \mathsf{G}(L/K) \cong \mathbb{Z}/n\mathbb{Z}$ so that $\sigma(\alpha) = \zeta\alpha$. Then

$$\Gamma\alpha = \{\alpha, \zeta\alpha, \ldots, \zeta^{n-1}\alpha\}$$

is not a linearly independent set (their sum is zero). So, α is a primitive element which does not give rise to a normal basis.

To get normal basis, we can take $\theta = \sum_{j=0}^{n-1} \alpha^j$. In order to show that $\{\sigma^j(\theta)\}_{j=0}^{n-1}$ is a linearly independent set, we use the fact that $\{\alpha^j\}_{j=0}^{n-1}$ is, and the change of basis matrix from the latter to the former is given by $X = (\zeta^{ij})_{0\le i,j\le n-1}$. This matrix is known to be invertible (for instance, with $n = 3$, its determinant is $\zeta(\zeta-1)^2(\zeta^2-1)$). I am going to leave the computation of the determinant of this matrix in general as a fun exercise.

(3) Another way to think about having a normal basis is to ask for an isomorphism between L and the group algebra $K[\Gamma]$. Recall that $K[\Gamma]$, as a K–vector space, has basis $\{\delta_g : g \in \Gamma\}$, with multiplication given by:

$$\delta_g \cdot \delta_h = \delta_{gh}.$$

If $\{g(\theta)\}$ is a basis of L as a K–vector space, then we can write an isomorphism (of K–vector spaces) $\psi : K[\Gamma] \to L$, given by $\psi(\delta_g) = g(\theta)$, which is then "$\Gamma$–equivariant", that is commutes with the action of Γ on both sides. The action on L is the natural one, since $\Gamma = \mathsf{G}\,(L/K)$, while on $K[\Gamma]$ is given by: $\sigma(\delta_g) = \delta_{\sigma g}$.

(37.3) Proof of the normal basis theorem: infinite case.– Let us assume that K and hence L are infinite fields. The proof of the normal basis theorem rests on the following lemma.

Lemma. *For an element $\beta \in L$, the set $\{g(\beta)\}_{g\in\Gamma}$ is a basis if and only if the matrix $X = (gh(\beta))_{g,h\in\Gamma}$ is invertible.*

Given this lemma, we can view $D(\beta) = \det((gh(\beta))_{g,h\in\Gamma})$ as a polynomial map on L. As L is infinite, there exists θ such that $D(\theta) \neq 0$.

Proof. Let $n = [L : K] = |\Gamma|$. Let $\{\omega_1, \ldots, \omega_n\}$ be a basis of L (as a K–vector space) and let $\Gamma = \{g_1, \ldots, g_n\}$. Recall that we showed (Lecture 29) that the matrix $(g_i(\omega_j))$ is invertible. This shows the forward implication of the lemma.

For the converse, assume that $(gh(\beta))_{g,h\in\Gamma}$ is invertible. If there exists a linear relation

$$\sum_{h\in\Gamma} a_h h(\theta) = 0, \quad \text{where } a_h \in K \ \forall\ h \in \Gamma,$$

then applying $g \in \Gamma$ on both sides we get:

$$\sum_{h\in\Gamma} a_h gh(\theta) = 0, \ \text{ for every } g \in \Gamma.$$

That is, $(a_h)_{h\in\Gamma}$ is annihilated by X, which proves that $a_h = 0$ for every $h \in \Gamma$. □

(37.4) Proof of normal basis theorem: finite case.– If K is finite, then $K = \mathbb{F}_q$ for some q, a power of a prime. In this case $L = \mathbb{F}_{q^n}$ with $\mathsf{G}\,(L/K) = \langle\sigma_q\rangle \cong \mathbb{Z}/n\mathbb{Z}$, where $\sigma_q(z) = z^q$ is the Frobenius automorphism.

Let us view L as a module over $K[x]$ via:

$$\left(\sum_{j=0}^{N} c_j x^j\right) \cdot z = \sum_{j=0}^{N} c_j \sigma_q^j(z),$$

where $c_0, \ldots, c_N \in K$ and $z \in L$.

Since $\sigma_q^n = \mathrm{Id}_L$, we get that $(x^n - 1) \subset \mathfrak{a} = \mathrm{Ann}_{K[x]}(L)$.

$$\mathfrak{a} = \{f(x) \in K[x] : f(\sigma_q) \cdot z = 0, \ \forall \ z \in L\}$$

Conversely, if $F(x) \in \mathfrak{a}$, then dividing by $x^n - 1$ gives:

$$F(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1} + (x^n - 1)G(x).$$

Now $F(x) \cdot z = 0$ for every $z \in L$ implies that

$$\sum_{j=0}^{n-1} c_j \sigma_q^j \equiv 0.$$

Using Dedekind's independence of characters, we conclude that $c_j = 0$ for every $0 \leq j \leq n-1$. Hence $\mathfrak{a} = (x^n - 1)$.

From Homework 10, problem 12, there exists $\theta \in L$ such that $\mathrm{Ann}_{K[x]}(\theta) = \mathfrak{a} = (x^n - 1)$. That is, $\{\sigma_q^j(\theta)\}_{0 \leq j \leq n-1}$ is linearly independent, as we wanted.