LECTURE 26

(26.0) Splitting extensions and statement of the main theorem.– Let K be a field. For a set of polynomials $P \subset K[x]$, we define *a splitting extension of* P as a field extension L/K such that:

- Every $p(x) \in P$ splits as a product of linear factors in $L[x]$:
$$p(x) = c \prod_{i=1}^{\deg(p)} (x - r_i^{(p)}), \quad \text{where } c \in K^\times = K \setminus \{0\}, \text{ and } r_1^{(p)}, \dots, r_{\deg(p)}^{(p)} \in L.$$
- $L = K\left(r_i^{(p)} : p \in P, 1 \leq i \leq \deg(p)\right)$.

Theorem. *Let K be a field and let $P \subset K[x]$.*

(1) *There exists a splitting extension L/K of P.*
(2) *Let L'/K' be another field extension, and assume that there is a homomorphism $f : K \to K'$. Further assume that for every $p(x) \in P$, $f(p(x))$ splits into a product of linear factors in $L'[x]$. Then there exists a homomorphism $\widetilde{f} : L \to L'$ such that $\widetilde{f}|_K = f$.*

In particular splitting extensions are unique up to (non-unique in general) isomorphism. We will denote this field extension by $\mathcal{E}(P, K)$.

We begin by giving a proof of this theorem, based on an argument due to Kronecker (1823-1891). A different proof via symmetric group actions will be presented in the next lecture.

The following observation is going to be crucial in this part of the course.

Let K be a field and $p(x) \in K[x]$. For $\alpha \in K$, we have:

$$\boxed{p(\alpha) = 0 \iff x - \alpha \text{ divides } p(x)}$$

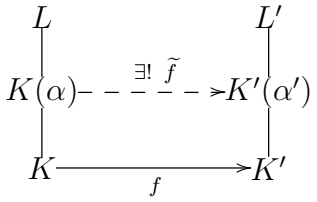
For a proof, use Euclidean division algorithm to write $p(x) = (x - \alpha)q(x) + r$, where $q(x) \in K[x]$ and $r \in K$. Then, both assertions written above are equivalent to $r = 0$.

(26.1) Kronecker's theorem.– The key step in the proof is the following result.

Theorem. *Let K be a field and $p(x) \in K[x]$ be an irreducible polynomial. Then there exists a field extension $\widetilde{K}/K$ and an element $\alpha \in \widetilde{K}$ such that: (i) $p(\alpha) = 0$ (ii) $\widetilde{K} = K(\alpha)$.*

Assume that there are two field extensions L/K and L'/K', and a homomorphism $f : K \to K'$. Further assume that there exist $\alpha \in L$ and $\alpha' \in L'$ which are algebraic over K and K' respectively, and $f(\mathsf{m}_\alpha(x))$ is divisible by $\mathsf{m}_{\alpha'}(x)$.

Then there exist a unique $\widetilde{f} : K(\alpha) \to K'(\alpha')$ *such that* $\widetilde{f}|_K = f$ *and* $\widetilde{f}(\alpha) = \alpha'$.



Remark. Note that the element α' is allowed to be in K'. However, our assumptions make sure that $\alpha' \notin f(K)$. To see this assume that $\alpha' = f(\beta)$, for some $\beta \in K$. Then $f(\mathsf{m}_\alpha(\beta)) = 0$ since $\mathsf{m}_{\alpha'}(\alpha') = 0$ and $\mathsf{m}_{\alpha'}(x)$ divides $f(\mathsf{m}_\alpha(x))$. Since f is injective, we conclude that $\mathsf{m}_\alpha(\beta) = 0$. In other words, $\mathsf{m}_\alpha(x)$ is divisible by $x - \beta$, which contradicts its irreducibility.

Proof. Let $\widetilde{K} = K[x]/(p(x))$. It is a field since $p(x)$ is irreducible. Let $\alpha := x + (p(x)) \in \widetilde{K}$. Then $\widetilde{K} = K(\alpha)$ and $p(\alpha) = p(x) + (p(x)) = 0$ in $\widetilde{K}$.

For the second part, we have unique isomorphisms sending x to α and α' respectively:

$$K(\alpha) = K[x]/(\mathsf{m}_\alpha(x)), \qquad K'(\alpha') = K'[x]/(\mathsf{m}_{\alpha'}(x))$$

As $(f(\mathsf{m}_\alpha(x))) \subset (\mathsf{m}_{\alpha'}(x))$, f extends to a unique homomorphism $\overline{f} : K[x]/(\mathsf{m}_\alpha(x)) \to K'[x]/(\mathsf{m}_{\alpha'}(x))$. Composing with the two isomorphisms above, we obtain:

$$\widetilde{f} : K(\alpha) \to K'(\alpha')$$

uniquely determined by the requirement that $\widetilde{f}|_K = K'$ and $\widetilde{f}(\alpha) = \alpha'$. □

(26.2) Proof of Theorem 26.0 (2).– Theorem 26.1 finishes the proof of the second part of Theorem 26.0 as follows. Assume L/K, L'/K', $f : K \to K'$, $P \subset K[x]$, $P' \subset K'[x]$ be as in the statement of Theorem 26.0 above. Consider the following set:

$$\mathcal{F} = \{(K_1, f_1) : K_1 \subset L \text{ is a subfield containing } K \text{ and } f_1 : K_1 \to L' \text{ such that } f_1|_K = f\},$$

(partially) ordered by inclusion.

$\mathcal{F} \neq \emptyset$ since $(K, f) \in \mathcal{F}$. Moreover, it is easy to see that every totally ordered subset of $\mathcal{F}$ has a supremum (left as an easy exercise).

Let (E, g) be a maximal element of $\mathcal{F}$. We claim that $E = L$. If $E \subsetneq L$, then, using the fact that L is a splitting extension of $P \subset K[x]$, there must exist some $p(x) \in P$ and $\alpha \in L$ such that $p(\alpha) = 0$ and $\alpha \notin E$. For the rest of the argument, we consider $p(x) \in E[x]$, and take the minimal polynomial $\mathsf{m}_\alpha(x)$ of α over E, which is irreducible of degree ≥ 2 (otherwise α would be in E) and divides $p(x)$ (because $p(\alpha) = 0$).

Let $E' = g(E) \subset L'$ and $q(x) = g(\mathsf{m}_\alpha(x)) \in E'[x]$. Note that $q(x)$ divides $g(p(x))$. By the assumption on L', there exists $\alpha' \in L'$ such that $q(\alpha') = 0$. Thus $\mathsf{m}_{\alpha'}(x) \in E'[x]$ divides $q(x)$. Using Theorem 26.1 above, we can extend g to $\widetilde{g} : E(\alpha) \to E'(\alpha')$ contradicting the

maximality of E.

(26.3) Existence of splitting extensions: finite case.– Let us assume that $P \subset K[x]$ is a finite set. Let $p(x) = \prod_{q(x)\in P} q(x)$, which reduces the task of proving the existence of a splitting extension for P to that of a single polynomial $p(x)$. We will do so by induction on $\deg(p)$.

If $\deg(p) = 1$, then $L = K$ is its splitting extension. Assume that $\deg(p) \geq 2$. Let $p_1(x)$ be an irreducible factor of $p(x)$. By Theorem 26.1, first part, there exists $\widetilde{K}/K$ with $\alpha \in \widetilde{K}$ such that $p_1(\alpha) = 0$ and $\widetilde{K} = K(\alpha)$. Therefore, $p(x)$ is divisible by $x - \alpha$ in $\widetilde{K}[x]$, say $p(x) = (x - \alpha)q(x)$. Since $\deg(q) < \deg(p)$, by induction hypothesis there exists a splitting extension $L/\widetilde{K}$ of $q(x)$. It is easy to see that L/K is then a splitting extension of $p(x)$.

(26.4) Existence of splitting extensions: general case.– Now we can finish the proof of Theorem 26.0. Let $P \subset K[x]$ be an arbitrary set. Define a (right directed) partially ordered set:

$$\mathcal{I}_P = \{I \subset P : I \text{ is finite}\}, \qquad \text{ordered by inclusion.}$$

By the proof for the finite case given above, for every $I \in \mathcal{I}_P$, we have a splitting extension $\mathcal{E}(I, K)$. Moreover, for $I \subset J$, we can fix a homomorphism $\varphi_{JI} : \mathcal{E}(I, K) \to \mathcal{E}(J, K)$, by viewing $\mathcal{E}(I, K)$ as a subfield of $\mathcal{E}(J, K)$ generated by the roots of polynomials from the set I.

Thus we have a direct system $\{(\mathcal{E}(I, K))_{I\in\mathcal{I}_P}, (\varphi_{JI} : \mathcal{E}(I, K) \to \mathcal{E}(J, K))_{I\subset J}\}$. Define:

$$\boxed{\mathcal{E}(P, K) = \varinjlim_{I\in\mathcal{I}_P} \mathcal{E}(I, K)}$$

(see Theorem 7.1 from Lecture 7). The routine verification of the fact that $\mathcal{E}(P, K)$ is a splitting extension of $P \subset K[x]$ is left for the reader.

(26.5) Algebraic closure of a field.– Let K be a field and let us take $P = K[x]$. The splitting extension $\mathcal{E}(K[x], K)$ is denoted by $\overline{K}$, and is called *the algebraic closure of* K. By definition, every $f(x) \in K[x]$ splits into a product of linear factors in $\overline{K}$. We will need the following lemma in order to show that $\overline{K}$ is the *universal algebraic extension* of K.

Lemma. *Let K_3/K_2 and K_2/K_1 be two field extensions. Assume that K_2 is algebraic over K_1 and let $\alpha \in K_3$ be algebraic over K_2. Then α is algebraic over K_1.*

Proof. We will use Theorem 25.3 for this. As α is algebraic over K_2, we can consider its minimal polynomial in $K_2[x]$.

$$\mathsf{m}_\alpha(x) = x^n + \sum_{j=0}^{n-1} c_j x^j \in K_2[x].$$

Let $F = K_1(c_0, \ldots, c_{n-1})$. As each c_j is algebraic over K_1, $[F : K_1] < \infty$ using Theorem 25.3 and its corollary. Morever, $[F(\alpha) : F] < \infty$. By the same results, we know that $[F(\alpha) : K_1] < \infty$ which proves that α is algebraic over K_1. □

Proposition. *Let K be a field and $\overline{K}$ its algebraic closure.*

(1) *Let $E/\overline{K}$ be a field extension and let $\alpha \in E$ be algebraic over $\overline{K}$. Then $\alpha \in \overline{K}$.*

(2) *Every irreducible polynomial in $\overline{K}[x]$ is of degree 1.*

(3) *Let L/K be an algebraic extension. Then there exists an embedding $L \hookrightarrow \overline{K}$.*

Proof. (1). By the lemma above, α is algebraic over K. By definition of $\overline{K}$, $\mathsf{m}_\alpha(x) \in K[x]$ splits into a product of linear factors in $\overline{K}[x]$.

$$\mathsf{m}_\alpha(x) = \prod_{i=1}^{N}(x - \beta_i), \qquad \text{where } \beta_1, \ldots, \beta_N \in \overline{K}.$$

Now $\mathsf{m}_\alpha(\alpha) = 0$, which proves that there is some $1 \leq i \leq N$ such that $\alpha = \beta_i \in \overline{K}$.

(2) follows from (1).

(3). If L/K is any algebraic extension, then it is a subfield of the splitting extension of $P(L) = \{\mathsf{m}_\alpha(x) : \alpha \in L\}$. That is, $L \subset \mathcal{E}(P(L), K)$. Applying the second part of Theorem 26.0, we get the existence of a homomorphism $\mathcal{E}(P(L), K) \hookrightarrow \overline{K}$. Hence there exists an embedding $L \hookrightarrow \overline{K}$ as claimed. □

(26.6) Algebraically closed fields.–

Proposition. *The following conditions are equivalent, for a field L.*

(1) *Every irreducible polynomial in $L[x]$ is of degree 1.*

(2) *If E/L is an algebraic extension, then $E = L$.*

(3) *For every $p(x) \in L[x]$, there exists some $r \in L$ such that $p(r) = 0$.*

Proof. (1)⇒(2). Let $\alpha \in E$ and let $\mathsf{m}_\alpha(x) \in L[x]$ be its minimal polynomial. As it is irreducible, by (1), $\deg(\mathsf{m}_\alpha(x)) = 1$. So $\mathsf{m}_\alpha(x) = x - a$, where $a \in L$. Now $0 = \mathsf{m}_\alpha(\alpha) = \alpha - a$ proving that $\alpha = a \in L$.

(2)⇒(3). It is enough to show this for a monic irreducible polynomial $p(x)$. By Theorem 26.1, we know that there exists E/L generated by a root r of $p(x) = 0$. By (2), $E = L$, hence there exists $r \in L$ so that $p(r) = 0$.

(3)⇒(1). Let $p(x)$ be a monic irreducible polynomial in $L[x]$. By (3) there exists $r \in L$ so that $x - r$ divides $p(x)$. By irreducibility, we conclude that $p(x) = x - r$ is of degree 1.
□

Definition. A field L is said to be *algberaically closed* if it satisfies one of the three equivalent conditions of the proposition above.

(26.7) Remarks.–

I. If F is a finite field, then F cannot be algebraically closed. This is because we can form a polynomial $p(x) = \left(\prod_{a \in F}(x-a)\right) + 1 \in F[x]$ such that $p(r) = 1$ for every $r \in F$.

II. For any field K, its algebraic closure $\overline{K}$ is algebraically closed by Proposition 26.5.

III. The field of complex numbers $\mathbb{C}$ is a degree 2 extension of $\mathbb{R}$: $\mathbb{C} \cong \mathbb{R}[x]/(x^2+1)$. There are several proofs of what is now called the *fundamental theorem of algebra*, namely

$$\boxed{\mathbb{C} \text{ is algebraically closed}}$$

For instance, the most familiar proof is from complex analysis, and uses *Louiville's theorem*: bounded holomorphic functions of one complex variable are nothing but constants. A different proof will be given next time using the intermediate value theorem (Bolzano–Weierstrass).

All the known proofs of the fundamental theorem of algebra use some topological argument at some point, in a crucial way. A few mathematicians have searched, in vain, for a *purely algebraic proof*, but the general consensus at the time is that no such proof could possibly exist.