LECTURE 25

(25.0) Galois theory: sketch.– Last time we started our study of Galois theory. A brief sketch of the main ideas of this theory is as follows.

Let K be a field and $f(x) \in K[x]$ a monic polynomial. Recall that *monic* means that the coefficient of $x^{\deg(f)}$ (called leading coefficient) is 1. Assume $n = \deg(f) \in \mathbb{Z}_{\geq 1}$.

- Construct a field L containing K so that $f(x)$ splits into a product of linear terms:

$$f(x) = \prod_{j=1}^{n}(x - \alpha_j) \qquad \text{in } L[x],$$

  and $L = K(\alpha_1, \ldots, \alpha_n)$. Such extensions will be called *splitting extensions* and we will have to show that they exist and are uniquely determined by f. This will be done next week when we will also establish the existence of an *algebraic closure.*

- Define a group (in honour of Galois, we will call them *Galois groups*)

$$G = \{\sigma : L \to L \text{ field isomorphism such that } \sigma|_K = \mathrm{Id}_K\}.$$

The fundamental theorem of Galois theory will establish a dictionary between *field extensions* and *groups.* We will carefully translate the properties of one to the other.

Remark. It is worth noticing the similarity between the construction of a group associated to a field extension L/K, and the group of *deck transformations of a covering space.* In fact this is more than an analogy, and in algebraic geometry fundamental group of algebraic schemes is defined via Galois theory.

(25.1) Terms introduced last time.–

Prime fields are $\mathbb{Q}$ and $\mathbb{F}_p$ where $p \in \mathbb{Z}_{\geq 2}$ is a prime number. For any field K, there is only one prime field P and only one homomorphism (necessarily injective) $P \hookrightarrow K$. We say K is of characteristic zero (resp. p) if $P = \mathbb{Q}$ (resp. $P = \mathbb{F}_p$).

A *field extension* is a pair consisting of a field L and a subfield K. We denote a field extension by $K \subset L$, or L/K. In some textbooks, a field extension is also denoted by (implying authors' fondness for covering spaces) $\begin{array}{c} L \\ | \\ K \end{array}$.

- Degree of an extension L/K is defined as the dimension of L as a K–vector space

$$\boxed{[L : K] = \dim_K(L)}$$

  We say L/K is a *finite extension* if $[L : K] < \infty$.

- For a set of elements $\{\alpha_i\}_{i\in I} \subset L$, we denote by $K(\alpha_i : i \in I) \subset L$ the smallest subfield containing K and the set $\{\alpha_i\}_{i\in I}$.

- An element $\alpha \in L$ is said to be *algebraic* over K if there exists $p(x) \in K[x]$ such that $p(\alpha) = 0$. *Transcendental* elements are the ones which are not algebraic.

- For $\alpha \in L$, we defined a homomorphism (evaluation at α) $\mathrm{ev}_\alpha : K[x] \to L$, by $p(x) \mapsto p(\alpha)$. We observed from the definition that:

$$\boxed{\alpha \text{ is algebraic} \iff \mathrm{Ker}(\mathrm{ev}_\alpha) \neq \{0\}}$$

  The *minimal polynomial* of α is defined as the unique monic polynomial $\mathsf{m}_\alpha(x) \in K[x]$ such that $\mathrm{Ker}(\mathrm{ev}_\alpha) = (\mathsf{m}_\alpha(x))$.

(25.2) Equivalent characterizations of algebraic elements.– Again, let L/K be a field extension, and let $\alpha \in L$.

Proposition. *The following three statements are equivalent:*
(1) *α is algebraic.* (2) $\mathrm{Ker}(\mathrm{ev}_\alpha) \neq \{0\}$. (3) $K[\alpha] = K(\alpha)$.

In this case, we have:

$$\boxed{[K(\alpha) : K] = \deg(\mathsf{m}_\alpha(x))}$$

The last equation was proved in the previous lecture (see Proposition 24.5 on page 5).

Proof. As observed above, (1) $\iff$ (2) by definition. (2)⇒(3) is also proved in Proposition 24.5. Let us check (3)⇒(2). By $K[\alpha] = K(\alpha)$ we know that α^{-1} exists in $K[\alpha]$. That is, there is a polynomial $p(x) \in K[x]$ such that $p(\alpha) = \alpha^{-1}$. But then, we have $xp(x) - 1 \in \mathrm{Ker}(\mathrm{ev}_\alpha)$, hence it is non–zero. □

(25.3) Degree of successive extensions.–

Theorem. *Let us assume that $K_1 \subset K_2 \subset K_3$ are field extensions. Then we have:*

$$\boxed{[K_3 : K_1] = [K_3 : K_2] \cdot [K_2 : K_1]}$$

Proof. Note that the equation written above is only meaningful when the three degrees involved are finite. Our proof however will not assume this.

Let $\{\alpha_i\}_{i\in I}$ be a basis of K_2 as a K_1–vector space, and let $\{\beta_j\}_{j\in J}$ be a basis of K_3 as a K_2–vector space. The equation claimed in the theorem above is an easy consequence of the following claim.

Claim: $\{\alpha_i\beta_j\}_{i\in I, j\in J}$ is a basis of K_3 as a K_1 vector space.

Proof of the claim. Let $\alpha \in K_3$. Then we can write it as a (finite) linear combination

$$\alpha = \sum_{j\in J} \beta_j c_j,$$

where the sum is finite, and $c_j \in K_2$. Each c_j can be written as a finite sum $c_j = \sum_{i\in I} \alpha_i d_{ij}$, where $d_{ij} \in K_1$. This implies:

$$\alpha = \sum_{i,j\in I\times J}^{\text{finite}} d_{ij} \cdot \alpha_i\beta_j,$$

proving that $\{\alpha_i\beta_j\}$ span K_3 as a K_1–vector space.

Now we will check that this set is linearly independent. Consider a linear dependence relation:

$$\sum_{i,j\in I\times J}^{\text{finite}} x_{ij} \cdot \alpha_i\beta_j = 0,$$

where $x_{ij} \in K_1$. Collect terms with same j subscript to write it as

$$\sum_{j\in J} \beta_j \left(\sum_{i\in I} x_{ij}\alpha_i\right) = 0.$$

Now $\{\beta_j\}_{j\in J}$ are linearly independent over K_2, proving that for each $j \in J$, we have:

$$\sum_{i\in I} x_{ij}\alpha_i = 0.$$

We get $x_{ij} = 0$ for each $i \in I$ by using linear independence of $\{\alpha_i\}$ over K_1. □

Corollary. *If $K_1 \subset K_2 \subset \cdots \subset K_\ell$ are field extensions, then*

$$[K_\ell : K_1] = \prod_{j=1}^{\ell-1} [K_{j+1} : K_j].$$

(25.4) Algebraic extensions.– A field extension L/K is said to be an *algebraic extension* if every $\alpha \in L$ is algebraic over K.

Theorem.

(1) *Every finite extension is algebraic.*

(2) *If L/K is any field extension, then:*

$$L^{\text{alg}} := \{\alpha \in L : \alpha \text{ is algberaic over } K\} \subset L$$

is a subfield of L. L^{alg}/K is an algberaic extension.

Proof. (1). Let L/K be a finite extension, and let $\alpha \in L$. Since L is a finite–dimensional vector space over K, the infinite set $\{\alpha^n : n \in \mathbb{Z}_{\geq 0}\}$ has to be linearly dependent. A dependence relation $\sum_{n=0}^{N} c_n\alpha^n = 0$ gives us a non–zero polynomial $p(x) = \sum_{n=0}^{N} c_n x^n \in \text{Ker}(\text{ev}_\alpha)$, proving that α is algebraic over K.

(2). Now we assume L/K is an arbitrary extension. We have to show that given two (say, non–zero) algebraic elements $\alpha, \beta \in L^{\text{alg}}$, $\alpha\beta$, $\alpha + \beta$ and α^{-1} are again algebraic. The last one is obvious, since:

$$\sum_{j=0}^{n} c_j \alpha^j = 0 \iff \sum_{j=0}^{n} c_j (\alpha^{-1})^{n-j} = 0.$$

As for the first two, consider the successive extensions:

$$K = K_1 \subset K(\alpha) = K_2 \subset K(\alpha, \beta) = K_3.$$

As α, β are algebraic, each of the extensions K_2/K_1 and K_3/K_2 is finite by Proposition 25.2 (note that β being algebraic over K implies that it is algebraic over $K(\alpha) \supset K$). Hence, using Theorem 25.3, we know K_3/K_1 is finite, hence algebraic by (1). So $\alpha+\beta, \alpha\beta \in K(\alpha, \beta)$ are algebraic over K. □

Remark. In general it is a bit non–trivial to get the minimal polynomial of $\alpha + \beta$ from that of α and β. For instance, let $\alpha = 2^{\frac{1}{3}}$ and $\beta = \sqrt{3}$. Over $\mathbb{Q}$, the minimal polynomials are easily computable:

$$\mathsf{m}_\alpha(x) = x^3 - 2, \qquad \mathsf{m}_\beta(x) = x^2 - 3.$$

(I am leaving as an easy exercise to prove that these polynomials are irreducible over $\mathbb{Q}$).

Let $\gamma = \alpha + \beta$ and try to compute the minimal polynomial of γ. Our proof of the theorem above implies that its degree will be ≤ 6.

$$(\gamma - \sqrt{3})^3 = 2 \;\Rightarrow\; \gamma^3 - 3\sqrt{3}\gamma^2 + 9\gamma - 3\sqrt{3} = 2.$$

We have to eliminate radicals from $3\sqrt{3}(\gamma^2 + 1) = \gamma^3 + 9\gamma - 2$ to get:

$$27(\gamma^2 + 1)^2 = (\gamma^3 + 9\gamma - 2)^2.$$

Expanding this out, we get:

$$\gamma^6 - 9\gamma^4 - 4\gamma^3 + 27\gamma^2 - 36\gamma - 23 = 0.$$

(I am also leaving, not so easy, exercise of proving that this is irreducible).

Example. There exist algebraic extensions which are not finite. A typical example is obtained by taking $\mathbb{Q} \subset \mathbb{C}$ and looking at all algebraic elements of $\mathbb{C}$ (called *algebraic numbers* and denoted by $\overline{\mathbb{Q}}$):

$$\overline{\mathbb{Q}} = \mathbb{C}^{\text{alg}} = \{z \in \mathbb{C} : z \text{ is algebraic over } \mathbb{Q}\}.$$

(2) of the theorem above implies that $\overline{\mathbb{Q}} \subset \mathbb{C}$ is a field, clearly algebraic over $\mathbb{Q}$. It is not hard to see that this field is infinite–dimensional as a $\mathbb{Q}$–vector space.