Lecture 26

Galois Theory

(26.0) Motivation -- Solvability by radicals.

Given a polynomial equation (say monic) of the form

$$x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0 = 0 \quad - (*)$$

the interest lies in giving an <u>explicit</u>* formula for x - in terms of

- rational expressions
- $(\ )^{\frac{1}{k}}$

involving $\{a_0, \dots, a_{n-1}\}$.

eg. $n=2$ $\quad x^2 + bx + c = 0 \Rightarrow x = \dfrac{-b \pm (b^2 - 4c)^{\frac{1}{2}}}{2}$

(goes back to Babylonians)

$n=3$ (Scipio del Ferro - early 1500's)

$$x^3 + ax = b \Rightarrow x = \left[\frac{b}{2} + \left(\left(\frac{b}{2}\right)^2 + \left(\frac{a}{3}\right)^3\right)^{\frac{1}{2}}\right]^{\frac{1}{3}} + \left[\frac{b}{2} - \left(\left(\frac{b}{2}\right)^2 + \left(\frac{a}{3}\right)^3\right)^{\frac{1}{2}}\right]^{\frac{1}{3}}$$

Note: an arbitrary degree 3 equation can be brought to this form as follows: in $y^3 + Ay^2 + By + C = 0$ set $y = x - \frac{A}{3}$

The resulting equation does not have x^2 term.

$n=4$ Cardona, Ferrari (around 1540)

(1824; Abel - Ruffini - after Galois) No such formula for $n \geq 5$.

Idea - Step 0. Make the statement precise. A general formula would realize the field containing roots of (*) (say L) as a field obtained from the base field ($K = \mathbb{Q}(a_0, \dots, a_{n-1})$) by adjoining roots of equations of the form $X^\ell - \alpha = 0$.

Step 1. Get necessary and sufficient conditions.

G = Automorphisms (field) of L over K would then be a successive extension of abelian groups, hence solvable.

Finally, for $n = 5$, this group is S_5 which is not solvable.

(26.1) Basic definitions.

Extension fields. Let E be a field and $F \subset E$ ($0, 1 \in F$) which is itself a field under the restriction of the operations of E. We say <u>F is a subfield of E</u>, or E is <u>an extension of F</u>.

Notations. $F \subset E$

E/F or $\begin{matrix} E \\ | \\ F \end{matrix}$

Note. If E/F is an extension, E can be viewed as a vector space over F

Definition: $(E : F) = \dim_F(E)$ dimension of E as an F-vector space

An extension E/F is said to be <u>finite</u> if $(E:F) < \infty$.

(26.2) Theorem. Let $F \subset E \subset K$ be fields. Then K/F is finite iff K/E and E/F are. In this case

$$(K:F) = (K:E)(E:F)$$

Proof. ($\Leftarrow$) Assume $(K:E) = m$ and $(E:F) = n$. Let

$\{\alpha_1, \dots, \alpha_m\}$ be a basis of K as an E-vector space

$\{\beta_1, \dots, \beta_n\}$ be a basis of E as an F-vector space

Claim. $\{\alpha_i \beta_j\}_{\substack{1 \le i \le m \\ 1 \le j \le n}}$ is a basis of K as an F-vector space.

Pf. Let $\lambda \in K$. Then $\lambda = \sum_{i=1}^{m} c_i \alpha_i$ (unique expression where $c_i \in E \ \forall i$)

$$= \sum_{i=1}^{m} \left(\sum_{j=1}^{n} d_{ij} \beta_j \right) \alpha_i \qquad \left(c_i = \sum_{j=1}^{n} d_{ij} \beta_j \text{ with } d_{ij} \in F \right)$$

Thus $\{\alpha_i \beta_j\}$ span K as an F-vector space ($\Rightarrow (K:F) < \infty$)

Linear independence:

If $\sum_{\substack{1 \le i \le m \\ 1 \le j \le n}} d_{ij} \alpha_i \beta_j = 0$ for some $d_{ij} \in F$

then $\sum_{i=1}^{m} \left(\sum_{j=1}^{n} d_{ij} \beta_j \right) \alpha_i = 0$. Linear independence of $\{\alpha_i\}$ over E implies

($\sum_{j=1}^{n} d_{ij} \beta_j \in E$)

that $\forall i$, $1 \le i \le m$, $\sum_{j=1}^{n} d_{ij}\beta_j = 0$. Again,

linear independence of $\{\beta_j\}$ over F implies $d_{ij} = 0$ $\forall i,j$.

Pf. of the claim $\rightarrow$ □

($\Rightarrow$) If K/F is finite then, as $E \subset K$ is in particular a sub-F-vector space, we get $(E:F) \le (K:F) < \infty$. Moreover a basis of K as an F-vector space ~~and~~ spans K as an E-vector space $\Rightarrow$ $(K:E) \le (K:F) < \infty$.

□

Corollary. If $F_0 \subset F_1 \subset \dots \subset F_n$ is a chain of extensions then $(F_n : F_0) = (F_n : F_{n-1})(F_{n-1} : F_{n-2}) \cdots (F_1 : F_0)$.

(26.3) Let E/F be an extension of fields. and let $S \subset E$.

$F[S]$:= subring of E generated by F and S.

$F(S)$:= subfield of E generated by F and S.

If $S = \{\alpha_1, \dots, \alpha_\ell\}$ is finite then

$F[S]$ = Image of $F[x_1, \dots, x_\ell] \longrightarrow E$

$x_j \longmapsto \alpha_j$

and $F(S)$ = Image of $F(x_1, \ldots, x_\ell) \longrightarrow E$

(26.4) Again, let E/F be a field extension and $\alpha \in E$.

We have a ring homomorphism (evaluation at α)

$$ev_\alpha : F[x] \longrightarrow E$$
$$x \longmapsto \alpha$$

Let $I_\alpha \subset F[x]$ be the kernel of ev_α.

If $I_\alpha = (0)$ we say α is <u>transcendental</u> (over F). Otherwise, we say that α is <u>algebraic</u> and since $F[x]$ is a PID, $I_\alpha = (f_\alpha(x))$ where $f_\alpha(x)$ is a monic polynomial, called the <u>minimal polynomial</u> of α.

- $I_\alpha = (0)$, ev_α extends to an injective hom. of fields

$$F(x) \hookrightarrow E$$

(hence $F[\alpha] \cong F[x]$ and $F(\alpha) = F(x)$)

- $I_\alpha = (f_\alpha)$, we get $F[x]/(f_\alpha) \hookrightarrow E$

$\Rightarrow$ f_α is irreducible. Hence $F[\alpha] = F(\alpha) \simeq F[x]/(f_\alpha)$

Theorem. $\alpha \in E$ is algebraic over $F \iff (F(\alpha) : F) < \infty$

Proof. ($\Rightarrow$) Let $\alpha \in E$ be algebraic over F and assume that

$$f_\alpha(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0 \in F[x]$$ be its min'l poly.

Then $F(\alpha) \simeq F[x]/(f_\alpha)$ has a basis $\{1, \alpha, \dots, \alpha^{n-1}\}$

$$\left(\alpha^n = -a_{n-1}\alpha^{n-1} - \dots - a_0 \right)$$

so $(F(\alpha) : F) = n$ = degree of f_α.

($\Leftarrow$) If α is not algebraic then $\forall N$, $\{1, \alpha, \dots, \alpha^N\}$ is a linearly independent set (over F) of elements of $F[\alpha] \subset F(\alpha)$

Hence $(F(\alpha) : F) = \infty$. □

(26.5) For example, let $F = \mathbb{Q}$, $S = \{\sqrt{2}, \sqrt{3}\} \subset \mathbb{R}$

$$F(\sqrt{2}, \sqrt{3}) \ni \sqrt{2} + \sqrt{3} = \alpha$$

$$f_\alpha(x) = x^4 - 10x^2 + 1$$ Minimal polynomial.

$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Cor $\Rightarrow$ $(\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}) = 4$

(page 4)

(26.6) Theorem (Kronecker). If $f(x) \in F[x]$ is a polynomial, $\deg(f) \geq 1$, then there exists an extension E/F and $\alpha \in E$ s.t. $f(\alpha) = 0$.

Proof. It is enough to show this for an irreducible (monic) polynomial $f(x)$. Since, in general, we can apply our result to an irreducible factor of $f(x)$.

Now if $f(x) \in F[x]$ is irreducible, $E := F[x]/(f(x))$ is a field, and $\alpha = x + (f(x))$ satisfies $f(\alpha) = 0$ □

Theorem (26.7) Let $\sigma : F \xrightarrow{\sim} F'$ be an iso. of fields.

Assume E/F and E'/F' are two field extns., s.t.

- $E = F(\beta)$, $E' = F'(\beta')$
- β is algebraic with min'l poly $f(x) \in F[x]$
  β' " " " " " $g(x) = \sigma(f(x)) \in F'[x]$

Then σ extends to a field iso $E \xrightarrow{\sim} E'$.