III Solvability by radicals and solvable groups.

We will now formalize the intuitive idea of when the roots of a polynomial are expressible in terms of radicals. This requires the concepts of pure and radical extension.

Given $K = k(u)$ a field extension. Then the subset $\{n \in \mathbb{Z} : u^n \in k\}$ is a subgroup of $\mathbb{Z}$ and hence of the form $m \cdot \mathbb{Z}$ for a unique $m \geq 0$.

Definition III.1: $k(u)/k$ is called a pure extension of type m if $m \geq 1$.

Definition III.2 An extension K/k is a radical extension if there is a finite tower of intermediate fields

$$k = K_0 \subset K_1 \subset \cdots \subset K_t = K$$

where for every $0 \leq i \leq t-1$, K_{i+1}/K_i is a pure extension.

And

Definition III.3 A polynomial $f \in k[x]$ is solvable by radicals if its splitting field is contained in a radical extension of k.

Example III.4 $f(x) = x^2 + bx + c \in k[x]$.

Let E be a splitting field of f and assume $E \neq k$; but $R(f) = \{\alpha_1, \alpha_2\}$.

For $\alpha \in \mathfrak{L}(f)$: $0 = \alpha^2 + b\alpha + c = \left(\alpha + \frac{b}{2}\right)^2 + c - \frac{b^2}{4}$

Set $u := \alpha_1 + \frac{b}{2}$; then $k(u)/k$ is a pure extension of type 2. We claim that $F = k(u)$: indeed $\alpha_1 = u - \frac{b}{2} \in k(u)$ and $\alpha_2 = -b - \alpha_1 \in k(u)$. Thus $F = k(u)$ is a pure extension and f is solvable by radicals.

To proceed with the study of pure extensions we make the following observation:

Let $K(u)/k$ be a pure extension of type m and let $m = p_1 \cdots p_r$ be the factorization in primes, possibly with repeated prime factors; example: $24 = 2 \cdot 2 \cdot 2 \cdot 3$.

Then we have a tower:

$$k(u) \supset k(u^{p_1}) \supset k(u^{p_1 p_2}) \supset \cdots \supset k(u^{p_1 \cdots p_r}) = k.$$

and $k(u^{p_1 \cdots p_{i-1}})$ is a pure extension of $k(u^{p_1 \cdots p_i})$ of prime type p_i.

This leads us to the study of the polynomial $X^p - c \in k[X]$:

Lemma III.5 Let p be a prime and

$$f(X) = X^p - c \in k[X].$$

(1) The following dichotomy holds:

(a) f is irreducible.

(b) c is a p^{th} power in k.

(2) Assume that k contains a ℓ p^{th} root of 1 and u is a root of f, $k(u)/k$ is a splitting field of f.

(2.1) Assume f irreducible.

If $\mathrm{char}(k) \neq p$, $\mathrm{Gal}(k(u)/k) \simeq \mathbb{Z}/p\mathbb{Z}$

If $\mathrm{char}(k) = p$, $\mathrm{Gal}(k(u)/k) \simeq (e)$

(2.2) Assume f reducible.

Then $k(u) = k$ and $\mathrm{Gal}(k(u)/k) \simeq (e)$.

Proof:

(1) Assume $f = g \cdot h$ with

$$g(X) = X^d + b_{d-1}X^{d-1} + \cdots + b_0$$

and $1 \leq d < p$.

Let $E \supset k$ be a splitting field of f

and $u \in R(f)$. Then

$$R(f) = \{ u \cdot \zeta : \zeta^p = 1, \zeta \in E \}.$$

Hence $b_0 = u^d \cdot \eta$ for some $\eta \in E$ with $\eta^p = 1$. Thus:

$$b_0^p = u^{dp} = c^d.$$

Since d, p are coprime pick $r, s \in \mathbb{Z}$ with $rp + sd = 1$. Then

$$c = c^{rp} c^{ds} = c^{rp} b_0^{ps} = (c^r b_0^s)^p.$$

This shows (1).

(2) The first assertion is clear.

If $\mathrm{char} k \neq p$, f is separable and since $k(w)/k$ is the splitting field of f and f is irreducible,

$$|Gal(k(u)/k)| = [k(u):k] = p$$

↑ Thm II.17.(2) ↑ Irred.

But a group of prime order p is $\cong \mathbb{Z}/p\mathbb{Z}$.

If $\mathrm{char}\, k = p$, $X^p - c = X^p - u^p = (X-u)^p$

and hence $Gal(k(u)/k) \simeq (e)$.

Finally if f is reducible we have by (1) that c is a p^{th} power and since k contains all p^{th} roots of 1, $k(u) = k$.

∎

In order to relate the question of solvability by radicals to Galois groups and hence to group theory we need to show that a radical extension is always contained in a radical extension that is normal.

For later use we introduce

Definition III.6 Let K/k be an extension and $x \in K$ algebraic over k. We say that x is separable if its minimal polynomial $irr(x,k) \in k[X]$ is separable.

To extend a radical extension to a radical normal extension we'll need the following technical lemmas.

To set the stage, let $B = k(u_1, \dots, u_t)$ be a finite extension of k, let $p_i = irr(u_i, k)$ and $f = p_1 \cdots p_t \in k[X]$. Let E be the splitting field of f, which by definition is a normal extension and $G = Gal(E|k)$.

Lemma III.6

(1) $\Leftrightarrow E = k_0(\sigma(u_1), \dots, \sigma(u_t) : \sigma \in G)$.

(2) if $u_1, \dots, u_t$ are separable, f is separable.

Proof: (2) is the definition of separability for f!

(1) For every $1 \le i \le t$ and every pair u, u' of roots of p_i there is an isomorphism

$$\varphi : k(u) \to k(u')$$

with $\varphi(u) = u'$, extending id_{k_0}. Since $\varphi_*(f) = f$ and E is a splitting field of f over $k(u)$ and $k(u')$, φ extends to $\sigma \in G$ with $\sigma(u) = u'$. (Prop. II.16)

Hence

~~Since~~ every p_i splits over $k(\sigma(u_1), \dots, \sigma(u_t) : \sigma \in G)$

so does f and hence

$$E = k(\sigma(u_1), \dots, \sigma(u_t) : \sigma \in G).$$

□

Lemma III.7 Assume in the context of Lemma III.6 that

$$u_1^{m_1} \in k, \quad u_2^{m_2} \in k(u_1), \dots, \quad u_\ell^{m_\ell} \in k(u_1, \dots, u_{\ell-1}).$$

Then E/k is a radical extension.

Proof:

Let $G = Gal(E/k) = \{\sigma_1, \dots, \sigma_e\}$

and define:

$$B_1 = k(\sigma_1(u_1), \dots, \sigma_e(u_1))$$

and inductively for $j \geq 2$:

$$B_j = B_{j-1}(\sigma_1(u_j), \dots, \sigma_e(u_j)).$$

We are going to show that in the tower

$$k \subset B_1 \subset B_2 \dots \subset B_\ell = E$$

each B_j is a radical extension of B_{j-1} which will show (exercise) that E is a radical extension of k.

For B_1: we have $\sigma_i(u_1^{m_1}) = \sigma_i(u_1)^{m_1}$

$$= u_1^{m_1} \in k.$$

Thus we can write

~~$k \subset k(\sigma_1(u_1)) \subset k(\sigma_1(u_1), \sigma_2(u_1)) \subset \dots \subset B_1$~~

~~and each $k(\sigma_1(u_1), \sigma_2(u_1), \dots, \sigma$~~

$$k \subset k(\sigma_1(u_1)) \subset k(\sigma_1(u_1))(\sigma_2(u_1)) \subset k(\sigma_1(u_1), \sigma_2(u_1))$$

$$k(\sigma_1(u_1), \sigma_2(u_1)) \qquad (\sigma_3(u))$$

$$\subset B_1$$

and thus being a tower of pure extensions shows that B_1 is radical.

Observe inductively that $\forall \sigma \in G$,

$$\sigma(B_j) = B_j \quad \text{for } 1 \le j \le t.$$

Indeed this is o. for $B_1 = k(\sigma_1(u_1), \dots, \sigma_\ell(u_1))$ since σ permutes $\{\sigma_1(u_1), \dots, \sigma_\ell(u_1)\}$.

Assuming $\sigma(B_{j-1}) = B_{j-1}$, it follows by the same argument for B_j.

Finally: $u_j^{m_j} \in k(u_1, \dots, u_{j-1})$ and hence ~~$\sigma_i(u_j)^{m_j} \in k(\sigma_i(u_1), \dots, \sigma_i(u_{j-1}))$~~

$$u_j^{m_j} \in B_{j-1}$$

and thus $\sigma_i(u_j)^{m_j} = \sigma_i(u_j^{m_j}) \in \sigma_i(B_{j-1})$

$$= B_{j-1}.$$

Thus by the same argument than for B_1, B_j is a radical extension of B_{j-1}.

□

We draw the following important conclusion

Corollary III.8 Let E be the splitting field of a polynomial $f \in k[x]$ and assume $E \subset K$ where K/k is radical. Then $E \subset K \subset F$ where F/k is radical and normal.

22.3.18

In particular the Galois groups of F/E, E/k, F/k and ~~E/E~~ are related by Thm II.26:

$$e \to Gal(F/E) \to Gal(F/k) \to Gal(E/k) \to e$$
$$\sigma \longmapsto \sigma|_E .$$

Now our goal is two fold:

1. Show that $Gal(F/k)$ is a solvable group, a group theoretic property to be