$l - r \geq 1$. On the other hand

$|\Gamma_p| = |G|^{p-1}$ hence $p \mid |\Gamma_p|$, which implies $l - r \geq 2$; that is there is $(h, \ldots, h) \in \Gamma_p$ with $h \neq e$ which proves the lemma. ∎ 8.3.18

Proof of Thm 2.20

Let $\mathbb{Q} \subset E \subset \mathbb{C}$ be a splitting field of f and $\mathcal{R}(f) = \{\alpha_1, \ldots, \alpha_p\}$ numbered in such a way that $\{\alpha_3, \ldots, \alpha_p\} \subset \mathbb{R}$.

~~Now the complex conjugation $\mathbb{C} \to \mathbb{C}$~~
~~$z \mapsto \bar{z}$~~

~~fixes $\alpha_3, \ldots, \alpha_p$ and interchanges α_1, α_2.~~

~~Thus $E \cap \mathbb{R} = E$ and~~

Using lemma II.7 we consider $Gal(E/\mathbb{Q})$ as a subgroup of S_p.

Notice that the complex conjugation $\varepsilon : \mathbb{C} \to \mathbb{C}$, $z \mapsto \bar{z}$, fixes $\alpha_3, \ldots, \alpha_p$ and interchanges α_1, α_2. Since $E = \mathbb{Q}(\alpha_1, \ldots, \alpha_p)$ this implies $\varepsilon(E) = E$ and that $\varepsilon|_E \in Gal(E/\mathbb{Q}) < S_p$ is the transposition (12).

Since f is irreducible, Corollary II.18 implies $p \mid |Gal(E/\mathbb{Q})|$ and by Cauchy's theorem (lemma II.21) $Gal(E/\mathbb{Q})$ contains an element η of order p. Thus η is a p-cycle (exercise) and since p is prime, a transposition and a p-cycle generate S_p (exercise).

$\square$

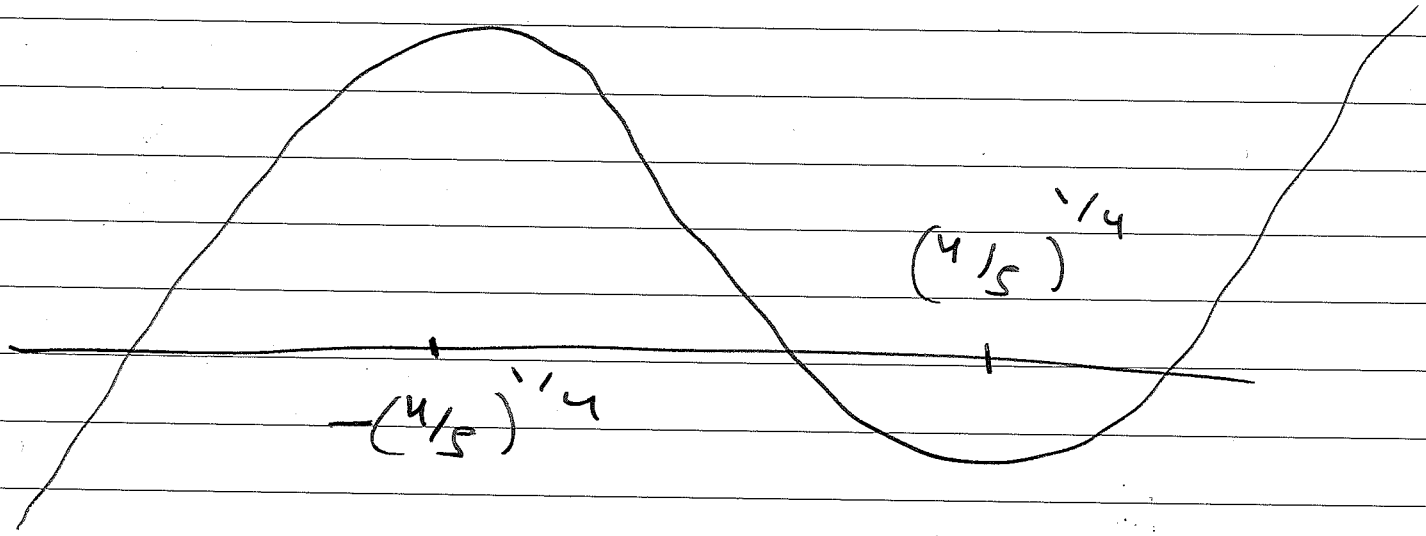
Corollary II.22 The Galois group of $x^5 - 4x + 2$ is isomorphic to S_5.

Proof: By Eisenstein's criterion

$$x^5 - 4x + 2 \in \mathbb{Q}[x]$$

is irreducible.

By computing local extrema, we see that the graph of f has the following shape:



Thus f has exactly $3 = 5 - 2$ real zeros and the theorem II.20. applies. ∎

The next application of our extension theorem concerns the relation between the transitivity properties of the Galois group of a polynomial as permutation group and the irreducibility of said polynomial.

Corollary II.23 (Prop. A.5.14)

Let $f \in k[x]$ and E a splitting field of f. Assume that f has no multiple roots. Then

f is irreducible $\Leftrightarrow$ $Gal(E|k)$ acts transitively on $R(f)$.

Proof:

($\Rightarrow$) Let $\alpha, \beta \in R(f) \subset E$. Applying Lemma II.15 to $\varphi = id_k : k \to k$,

there is, since f is irreducible, an isomorphism $\hat{\varphi} : k(\alpha) \to k(\beta)$ extending id_k and $\hat{\varphi}(\alpha) = \beta$.

Now we apply Prop. II.16 to $f \in k(\alpha)[x]$ and $\hat{\varphi} : k(\alpha) \to k(\beta)$ taking into account that $\hat{\varphi}_*(f) = f$ and E is a splitting field of f over $k(\alpha)$. We obtain that $\hat{\varphi}$ extends to an automorphism $\sigma : E \to E$ such that $\sigma(\alpha) = \beta$ and $\sigma|_k = id_k$; thus $\sigma \in Gal(E|k)$ which proves $\Longrightarrow$.

($\Longleftarrow$) Conversely assume that $Gal(E|k)$ acts transitively on $R(f)$. If $f = p \cdot q$ with $p, q \in k[x]$, then $R(p) \subset R(f)$, $R(q) \subset R(f)$ and $Gal(E|k)$ keeps both

$R(p)$ and $R(q)$ invariant. But f has no multiple roots, hence $R(p) \cap R(q) = \phi$ which implies either $R(p) = \phi$ hence p is constant or $R(q) = \phi$ and q is constant. Hence f is irreducible. ∎

It will be convenient to give a name to splitting fields of polynomials without reference to said polynomial.

Def. II.24 An extension E/k is normal if it is the splitting field of a polynomial $f \in k[x]$.

Remark II.25 Let $E \supset B \supset k$ be field extensions. If E/k is normal then E/B is normal and $Gal(E/B) < Gal(E/k)$.

We close this chapter with a fundamental result relating the Galois groups of towers of normal extensions.

Thm II.26 (Thm A-5.17)

Let $k \subset B \subset E$ be extensions such that E/k and B/k are normal.

Then for every $\sigma \in Gal(E/k)$,

$$\sigma(B) = B$$

and the surjective homomorphism

$$Gal(E/k) \longrightarrow Gal(B/k)$$

$$\sigma \longmapsto \sigma|_B$$

is surjective with kernel $Gal(E/B)$.

Proof: Let $f \in k[X]$ such that B is a splitting field of f. By lemma II.4

We have for every $\sigma \in Gal(E|k)$ that $\sigma(R(f)) = R(f)$ and since $B = k(R(f))$ we conclude $\sigma|B = B$. Thus we obtain a group homomorphism

$$Gal(E|k) \to Gal(B|k),$$
$$\sigma \longmapsto \sigma|_B$$

whose kernel is obviously $Gal(E|B)$.

Now we prove surjectivity: let $g \in k[X]$ such that E is a splitting field of g and let $\sigma \in Gal(B|k)$. We apply Prop. II.16 with $\sigma: B \to B$, $f \in B[X]$ and observe $\sigma(f) = f$. Then E is a splitting field of $f \in B[X]$ and Prop II.16 gives an extension of σ to $\sigma': E \to E$ with $\sigma'|_R = id_R$, thus $\sigma' \in Gal(E|k)$. ∎

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

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 into 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 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