In particular the Galois group of $X^p - t$ is the trivial group, since by Lemma II.7 the restriction map

$$Gal(E/k) \longrightarrow S_{R(f)}$$

is injective and $|R(f)| = 1$.

We will see that essentially if an irreducible polynomial f has at least 2 distinct roots in a splitting field, its Galois group is non-trivial; thus we need a handy criterion to decide when a polynomial has no multiple-roots.

Definition II.9 A polynomial $f \in k[X]$ has no multiple roots if in a splitting field E, $|R(f)| = \deg f$.

It is a remarkable fact that this property can be checked without having to compute the splitting field.

Lemma II.10 (see Algebra I and exercise sheet 2). Let $f \in k[x]$ and f' its derivative. Then f has no multiple roots $\iff \gcd(f, f') = 1$.

We deduce

Corollary II.11 (lemma A-5.4)

Assume $f \in k[x]$ is irreducible and either $\mathrm{char}\, k = 0$ or $\mathrm{char}(k)$ does not divide $d := \deg(f)$. Then f has no multiple roots.

Proof: $f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0$

$f'(x) = d\,x^{d-1} + \cdots$

Under the above hypothesis, $d \neq 0$. Hence any polynomial p dividing f and f' must have $\deg(p) \leq d-1$. Since f is irreducible that implies that p is a constant, hence $\gcd(f, f') = 1$ and by lemma II.10, f has no mult. roots. ∎

The following concepts are central:

Def. II.12 (1) An irreducible polynomial is separable if it has no repeated roots.

(2) An arbitrary polynomial is separable if each of its irreducible factors is.

Example II.13 $X^4+1 \in \mathbb{Q}[x]$ is irreducible

$\mathrm{char}\,\mathbb{Q} = 0$, hence separable. Then $(x^4+1)^{115}$

is separable as well. ~~Another example~~

~~FF~~

Let now E/k be a field extension

and $\alpha \in E$. We recall some facts from

Algebra I. Consider the evaluation map

$$\varphi_\alpha : k[x] \longrightarrow E$$
$$p \longmapsto p(\alpha)$$

This is a ring homomorphism sending X to α,

and its kernel $\ker \varphi_\alpha$ is an ideal in $k[x]$.

Recall that

(1) If $\ker \varphi_\alpha = (0)$ then α is called

transcendental over k.

(2) If $\ker \varphi_\alpha \neq (0)$ then α is called algebraic over k.

In the second case, $\ker \varphi_\alpha$ is generated by a unique monic polynomial denoted $\mathrm{irr}(\alpha, k)$, called the minimal polynomial of α; that is $\ker \varphi_\alpha = \mathrm{irr}(\alpha, k) \cdot k[X]$.

Observe that φ_α induces an injective ring homomorphism

$$f_\alpha : k[X]/\ker \varphi_\alpha \longrightarrow E.$$

~~where irr~~.

In particular $k[X]/\ker \varphi_\alpha$ is an integral domain and hence, if $\alpha \neq 0$, $\mathrm{irr}(\alpha, k)$ is an irreducible polynomial.

The second observation is that the image of f_α is contained in $k(\alpha)$.

In fact (exercise):

Lemma II.14: $\tilde{f}_\alpha : k[x]/\ker\varphi_\alpha \longrightarrow k(\alpha)$

is an isomorphism.

Our main goal next is to show a result that relates the degree $[E:k]$ of the splitting field E of a separable polynomial $f \in k[x]$ to the order of its Galois group.

To this end we recall certain extension properties not involving the separability assumption and which have been treated in Algebra I in the context of the uniqueness of algebraic closure.

Let $\varphi : k \to k'$ be a field isomorphism.

This induces a ring isomorphism

$$\varphi_* : k[x] \to k'[x]$$

by $\varphi_*(a_n x^n + \cdots + a_0) = \varphi(a_n)x^n + \cdots + \varphi(a_0)$.

Clearly $p \in k[x]$ is irreducible $\iff$

$\varphi_*(p) \in k'[x]$ is.

Lemma II.15 Let $p \in k[x]$ be irreducible

$p_* := \varphi_*(p)$ and let E/k, E'/k' be field

extensions with $E \supset R(p)$, $E' \supset R(p_*)$.

Then given $\alpha \in R(p)$, $\alpha' \in R(p_*)$ there

is an isomorphism

$$\hat{\varphi} : k(\alpha) \to k'(\alpha')$$

extending φ, with $\hat{\varphi}(\alpha) = \alpha'$.

Proof: Since p is irreducible and $p \neq 1 = 0$, we have $p = c \cdot \mathrm{irr}(\alpha, k)$, $c \in k$, $c \neq 0$.

Thus $p \cdot k[x] = \mathrm{irr}(\alpha, k) \cdot k[x]$ and the evaluation map

$$\varphi_\alpha : k[x] \longrightarrow E$$
$$f \longmapsto f(\alpha)$$

induces an isomorphism

$$f_\alpha : k[x]/p\,k[x] \longrightarrow k(\alpha).$$

Similarly, since p_* is irreducible

$$f_{\alpha'} : k'[x]/p_*\,k'[x] \longrightarrow k'(\alpha')$$

is an isomorphism. Now observe that

$\varphi_\alpha(p\,k[x]) = p_*\,k'[x]$ and hence

induces a ring isomorphism

$$\gamma : k[x]/(p\,k[x]) \longrightarrow k'[x]/(p_\alpha\, k'[x])$$

Then: $\hat{\varphi} := f_{\alpha'} \circ \gamma \circ f_\alpha^{-1}$ is an isomorphism

$$\hat{\varphi} : k(\alpha) \to k'(\alpha')$$

and

$$\hat{\varphi}(\alpha) = f_{\alpha'} \circ \gamma\left(f_\alpha^{-1}(\alpha)\right)$$

$$= f_{\alpha'} \circ \gamma\left(X + (p\,k[x])\right) = f_{\alpha'}\left(X + (p_\alpha\, k'[x])\right)$$

$$= \alpha'. \qquad \square$$

This lemma implies the following extension property used already in Algebra I:

Prop. I.16 (Lemma A-8.38)

With the above notations, let $f \in k[x]$,

$f_* = \varphi_* f \mid \in k'[x]$, E/k a splitting field of f, E_*/k' a splitting field of f_*.

Then there is an isomorphism

$$\Phi : E \to E_*$$

extending $\varphi : k \to k'$.

Now we turn to the central extension thm:

Thm II.17 (Thm A-5.7) With the notations of Prop II.16.

(1) Assume f is separable. Then there are exactly $[E:k]$ isomorphisms

$$\begin{array}{ccc} E & \xrightarrow{\Phi} & E_* \\ \uparrow & & \uparrow \\ k & \xrightarrow{\varphi} & k' \end{array}$$

extending φ.

(2.) If $E|k$ is the splitting field of a separable polynomial,

$$|Gal(E|k)| = [E:k].$$

1.3.18