Übung II.6 Zeige, dass wenn E und E' Zerfällungskörper von f sind, dann sind die Gruppen $Gal(E|k)$ und $Gal(E'|k)$ isomorph.

Sei X eine Menge; wir bezeichnen mit S_X die Gruppe der Bijektionen von X und falls $X = \{1, 2, \dots, n\}$, $n \in \mathbb{N}$ setzen wir $S_X = S_n$.

Lemma II.7 (Lemma 3.2 + Thm 3.3)

Sei $E|k$ ein Zerfällungskörper eines Polynoms $f \in k[X]$. Dann ist die Restriktionsabbildung

$$\begin{aligned} Gal(E|k) &\longrightarrow S_{R(f)} \\ \sigma &\longmapsto \sigma|_{R(f)} \end{aligned}$$

ein injektiver Gruppenhomomorphismus. 26.2.21

Insbesondere ist $Gal(E|k)$ zu einer Untergruppe von $S_{R(f)}$ isomorph.

Beweis: Aus Lemma II.4 folgt dass jedes $\sigma \in Gal(E|k)$ eine Permutation von $R(f)$ definiert. Somit ist für alle $\sigma, \tau \in Gal(E|k)$

$$(\sigma\tau)|_{R(f)} = \sigma|_{R(f)} \cdot \tau|_{R(f)}$$

und $\sigma \longmapsto \sigma|_{R(f)}$ ist ein Homomorphismus.

Sei $R(f) = \{\alpha_1, \dots, \alpha_n\}$. Da E ein Zerfällungskörper von f ist folgt (siehe Algebra 1)

$$E = k[\alpha_1, \dots, \alpha_n] .$$

Sei nun $\sigma \in Gal(E|k)$ und $P \in k[X_1, \dots, X_n]$. Dann ist $\sigma(P(\alpha_1, \dots, \alpha_n)) = P(\sigma(\alpha_1), \dots, \sigma(\alpha_n))$ und somit folgt, dass falls $\sigma(\alpha_i) = \alpha_i$, $1 \le i \le n$, dann ist $\sigma = id_E$. [$\S$]

Es ist klar dass $|\mathcal{R}(f)| \leq \deg f$.

Es gibt Beispiele wo $|\mathcal{R}(f)| < \deg f$ mit f irreduzibel:

Beispiel II.8 $k = \mathbb{F}_p(t)$, $f \in k[X]$

$f = X^p - t$. Dann ist f irreduzibel und $|\mathcal{R}(f)| = 1$.

Sei $E \supset k$ ein Zerfällungskörper von f und $\alpha \in \mathcal{R}(f)$. Somit ist $\alpha^p = t$ und da E charakteristik p ist folgt

$$(X-\alpha)^p = X^p - \alpha^p = X^p - t = f$$

woraus $\mathcal{R}(f) = \{\alpha\}$ folgt. Dass $\alpha \notin k$ ist eine Übung. Aus dem folgt, dass f irreduzibel ist.

Also folgt aus Lemma I.7, dass die Galois Gruppe von $X^p - t$ die triviale Gruppe ist.

Wir werden im Verlauf dieses Kapitels sehen, dass für ein irreduzibles Polynom $f \in k[X]$, dass in einem Zerfällungskörper E/k keine mehrfachen Nullstellen besitzt

$$|\mathrm{Gal}(E/k)| = [E:k]$$

Dies ist ein zentraler Satz dieses Kapitels. Wir beginnen in dem wir ein Kriterium herleiten, dass entscheidet wenn ein Polynom keine mehrfachen Wurzeln besitzt.

Def. II.9 Ein Polynome $f \in k[X]$ hat keine mehrfachen Nullstellen Wurzeln, falls in einem Zerfällungskörper E:

$$|R(f)| = \deg f.$$

Es ist eine bemerkenswerte Tatsache dass man diese Eigenschaft von f nachweisen kann ohne einen Zerfällungs-

körper zu berechnen:

Lemma II.10 (siehe nächstes Übungsblatt)

Sei $f \in k[X]$ und $f' \in k[X]$ seine erste Ableitung. Dann hat f keine mehrfachen Wurzeln (Nullstellen) genau dann wenn $ggT(f, f') = 1$.

Aus dem folgt ein nützliches Kriterium für Einfachheit der Nullstellen.

Korollar II.11 (Rotman Lemma 3.4)

Sei $f \in k[X]$ irreduzibel (unitär) und eine der folgenden Eigenschaften ist erfüllt:

(1) $\operatorname{char} k = 0$

(2) $\operatorname{char} k > 0$ und teilt nicht $d = \deg(f)$

Dann hat f keine mehrfachen Nullstellen.

Beweis: Sei $f(x) = X^d + a_{d-1} X^{d-1} + \cdots + a_0$.

Dann ist $f'(x) = d X^{d-1} + \cdots$.

Unter den Annahmen des Lemmas ist $d \neq 0$ in k. Somit ist $\deg(f') = d-1$.

Falls jetzt $p \in k[X]$ f und f' dividiert folgt $\deg(p) \leq d-1$ und wegen irreduzibel von f folgt, dass p eine Konstante ist, d.h. $ggT(f, f') = 1$. ☐

Folgende Begriffe sind zentraler Bedeutung:

Def. II.12

(1) Ein irreduzibles Polynom ist separabel falls es keine mehrfachen Nullstellen besitzt.

(2) Ein Polynom ist separabel falls jeder seiner irreduziblen Faktoren separabel ist.

Beispiel II.13 $X^4+1 \in \mathbb{Q}[X]$ ist irreduzibel und da $\mathrm{char}\,\mathbb{Q} = 0$ auch separabel nach Korollar II.11. Dann ist $(X^4+1)^{13}$ auch separabel; ~~selbst wenn ich soll~~

~~Aufgabe~~

Unser nächstes Ziel ist Thm II.17, das insbesondere sagt, dass falls E/k der Zerfällungskörper eines separablen Polynoms $f \in k[X]$ ist dann gilt:

$$|\mathrm{Gal}(E/k)| = [E:k].$$

Zuerst rufen wir einige Tatsachen aus Algebra I in Erinnerung.

Sei E/k eine Körpererweiterung und $\alpha \in E$.

Die Auswertungsabbildung

$$\varphi_\alpha : k[X] \longrightarrow E$$
$$P \longmapsto P(\alpha)$$

ist ein Ring homomorphismus. Für dessen Kern $\ker \varphi_\alpha$, ein ideal in $k[X]$, gibt es zwei Möglichkeiten:

(1) $\ker \varphi_\alpha = (0)$, dann heißt α transzendent über k.

(2) $\ker \varphi_\alpha \neq (0)$: da $k[X]$ ein Hauptidealring ist gibt es genau ein unitäres Polynom $\mathrm{irr}(\alpha, k)$, das Minimalpolynom von α über k, das $\ker \varphi_\alpha$ erzeugt.

Aus der Tatsache, dass $k[X]$ ein euklidischer Ring ist folgt $k[X]/\ker \varphi_\alpha$ ist ein Körper und

Lemma II.14. φ_α induziert einen Körperisomorphismus

$$k[X]/\ker \varphi_\alpha \longrightarrow k(\alpha).$$

Ein Körperisomorphismus $\varphi : k \to k'$ induziert einen Ring isomorphismus

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

via $\varphi_*(a_n X^n + \dots + a_0) = \varphi(a_n) X^n + \dots + \varphi(a_0)$.

Da φ_* ein Ring isomorphismus ist, folgt dass $p \in k[X]$ genau dann irreduzibel ist falls $\varphi_*(p)$ irreduzibel ist.

Lemma 2.15 : Sei $p \in k[X]$ irreduzibel und $p_* := \varphi_*(p) \in k'[X]$. Seien E/k E'/k' Körpererweiterungen mit $E \supset R(p)$ und $E' \supset R(p_*)$. Dann gilt:

Für jedes $\alpha \in R(p)$ und $\alpha' \in R(p_*)$ gibt es einen isomorphismus

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

der φ' erweitert und so dass $\hat{\varphi}(\alpha) = \alpha'$.

Beweis: Betrachte folgendes Diagramm:

$$\begin{array}{ccc} k[x] & \xrightarrow{\varphi_*} & k'[x] \\ \varphi_\alpha \downarrow & & \downarrow \varphi_{\alpha'} \\ k(\alpha) & & k(\alpha') \\ \cap & & \cap \\ E & & E' \end{array}$$

wobei wie oben φ_α, $\varphi_{\alpha'}$ evaluation in α resp. α' bedeutet.

Da p irreduzibel ist und $p(\alpha) = 0$ folgt $\ker \varphi_\alpha = p \cdot k[x]$ und analog $\ker \varphi_{\alpha'} = p_* k'[x]$. Dies impliziert $\varphi_*(\ker \varphi_\alpha) = \ker \varphi_{\alpha'}$; folglich induziert φ_* einen Ring isomorphismus

$$\begin{array}{ccc} k[x]/_{\ker \varphi_\alpha} & \xrightarrow{\overline{\varphi_*}} & k'[x]/_{\ker \varphi_{\alpha'}} \\ \overline{\varphi_\alpha} \downarrow & & \downarrow \overline{\varphi}_{\alpha'} \\ k(\alpha) & & k'(\alpha') \end{array}$$

Zusammen mit den Isomorphismen von Lemma 2.14 ist dann

$$\hat{\varphi} := \bar{\varphi}_{\alpha'} \, \bar{\varphi}_{\alpha} \, \bar{\varphi}_{\alpha}^{-1}$$

die gesuchte Erweiterung von $\varphi : k \to k'$. ∎

Dieses Lemma impliziert folgende allgemeine Erweiterungseigenschaft die schon in Algebra I benutzt wurde.

Prop. I.16. *Sei $f \in k[x]$, $f_\alpha = \varphi_\alpha(f) \in k'[x]$, E/k ein Zerfällungskörper von f, E'/k' ein Zerfällungskörper von f_α. Dann gibt es einen Isomorphismus*

$$\bar{\Phi} : E \to E'$$

der $\varphi : k \to k'$ erweitert.

Nun kommen wir zum zentralen Erweiterungssatz:

Thm II.17 (Rotman Thm 3.7)

Mit den Notationen der Prop. II.16:

(1) Sei f separabel. Dann gibt es genau $[E:k]$ Isomorphismen

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

die φ erweitern.

(2) Sei E/k der Zerfällungskörper eines separablen Polynoms. Dann gilt:

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

Beweis: (1) Induktion über $[E:k]$.

Falls $[E:k]=1$ zerfällt f in lineare Faktoren in $k[x]$; das selbe gilt für $f_* = \varphi(f)$, somit $[E_*:k']=1$ und $\Phi = \varphi$.

Sei $[E:k] > 1$. Dann zerfällt f nicht in lineare Faktoren über $k[x]$; sei $f = p \cdot g$ wobei p ein irreduzibler Faktor von f mit höchstem grad d ist; also ist $d > 1$. Es folgt $f_* = \underbrace{\varphi_*(p)}_{p_*} \underbrace{\varphi_*(g)}_{g_*}$

Dann ist f_* ~~separabel~~ und somit p_* separabel.

Da p_* irreduzibel mit ~~dem~~ $\deg(p_*) = d$ hat p_* genau d Nullstellen

$$\alpha_1^*, \dots, \alpha_d^*$$

alle in E^* enthalten.

Sei $\alpha \in R(p)$. Aus ~~Lemma~~ 2.15 folgt, dass es für jede ~~der~~ Nullstelle α_i^* eine Erweiterung

$$\hat{\varphi}_i : k(\alpha) \longrightarrow E_*$$

von $\varphi : k \longrightarrow k' \subset E_*$ mit $\hat{\varphi}_i(\alpha) = \alpha_i^*$ gibt. Es ist eine einfache

Übung, dass jede Erweiterung $\hat{\varphi} : k(\alpha) \longrightarrow E_*$ von $\varphi : k \to k' \subset E_*$ von dieser Form ist.

Es gibt also genau d Erweiterungen

$$\hat{\varphi} : k(\alpha) \longrightarrow E_*$$

von $\varphi : k \to k'$, eine für jede Nullstelle von p_*. D.h. $\hat{\varphi} : k(\alpha) \longrightarrow k'(\alpha_*^*)$, $\alpha_*^* \in \{\alpha_1^*, \dots, \alpha_d^*\}$ eine solche Erweiterung.

Dann:

$$[E : k(\alpha)] = [E:k]/d \quad < [E:k].$$

Nun ist E auch ein Zerfällungs-körper von $f \in k(\alpha)[X]$, $\hat{\varphi}_*(f) = f_*$ und E_* ist ein Zerfällungskörper von $f_* \in k'(\alpha_*)[X]$. Bemerke auch, dass $f \in k(\alpha)[X]$ wieder separabel ist.

Induktionshypothese impliziert, dass

$$\hat{\varphi} : k(\alpha) \longrightarrow k'(\alpha^*)$$

$[E : k(\alpha)] = [E:k]/d$ Erweiterungen $E \to E_*$

besitzt und somit hat $\varphi : k \to k'$,

$[E : k(\alpha)]\, d = [E : k]$ Erweiterungen.

(2) $k = k'$, $\varphi = id_k$, $E = E_x$. ▯

Erste Anwendung des Erweiterungsgrades:

Thm 2.19 (Rotman Thm 3.13)

Sei p eine Primzahl und $n \in \mathbb{N}$, $n \geq 1$.

Dann ist

$$G = \mathrm{Gal}(F_{p^n} / F_p) \cong \mathbb{Z}/n\mathbb{Z}$$

und ein ~~Generator~~ Erzeugendes Element ist der Frobenius Automorphismus:

$$Fr : F_{p^n} \to F_{p^n}$$

$$x \mapsto x^p.$$