bezeichnet, dann gilt

$$Fr^k = Id_{\mathbb{F}_{p^n}}$$

Aber $Fr^k(x) = x^{p^k}$ und somit

ist jedes $x \in \mathbb{F}_{p^n}$ Nullstelle von $X^{p^k} - X$

Woraus $p^n \leq p^k$ und somit $k = n$ folgt.

[Z]

Nun wenden wir uns einer Familie von Polynomen zu deren Galois Gruppe so gross wie möglich ist.

Thm 2.20 Sei p eine Primzahl und $f \in \mathbb{Q}[X]$ ein Polynom mit $deg(f) = p$ und Zerfällungskörper E. Annahme:

(1) f ist irreduzibel.

(2) f hat genau $p-2$ reelle Nullstellen.

Dann folgt $Gal(E/\mathbb{Q}) \cong S_p$.

Aus Korollar 2.18 folgt $p \mid |\mathrm{Gal}(E/\mathbb{Q})|$.
Dies impliziert im allgemeinen folgendes:

Lemma 2.21. (Cauchy) *Sei G eine endliche Gruppe und p eine Primzahl mit $p \mid |G|$. Dann enthält G ein Element der Ordnung p.*

Beweis:

Wir betrachten $\Gamma_p = \{(g_1, \dots, g_p) \in G^p : g_1 \cdot \dots \cdot g_p = e\}$.

Die symmetrische Gruppe S_p wirkt auf G^p via:

$$\tau_\sigma(g_1, \dots, g_p) = (g_{\tau(1)}, \dots, g_{\tau(p)})$$

Sei $\sigma = (1, 2, \dots, p)$ der p-Zyklus:

$$\begin{matrix} 1 & 2 & \cdots & p \\ 2 & 3 & \cdots & 1 \end{matrix}$$

und $C_p = \{\mathrm{id} = \sigma^0, \sigma, \sigma^2, \dots, \sigma^{p-1}\}$

die durch σ erzeugte zyklische Gruppe:

sie hat Ordnung p. Wir behaupten, dass die Wirkung von C_p auf G^p die Teilmenge Γ_p erhält: in der Tat aus

$$g_1 \cdot g_2 \cdot g_3 \cdots \cdot g_p = e$$

folgt

$$\underbrace{g_1^{-1}(g_1 \cdots g_p) g_1}_{g_2 \cdot g_3 \cdots \cdot g_p \cdot g_1} = e$$

und somit

$$\tau_*(g_1, \ldots, g_p) \in \Gamma_p$$

falls $(g_1, \ldots, g_p) \in \Gamma_p$.

Daraus folgt, dass Γ_p disjunkte Vereinigung der C_p-Bahnen in Γ_p ist; da p Primzahl ist die Kardinalität einer solchen Bahn 1 oder p. ∎

$$\Gamma_p = \bigcup_{i \in I} \bigcup_{j \in J_i} \ldots$$

Sei jetzt I die Menge der Bahnen der ~~Ordnung~~ Kardinalität 1 und J die der Kardinalität p. Dann ist:

$$\Gamma_p = \bigsqcup_{i \in I} \mathcal{O}_i \quad \bigsqcup \bigsqcup_{j \in J} \mathcal{O}_j .$$

Wobei $\bigsqcup$ angibt, dass die Vereinigung disjunkt ist. Somit:

$$|\Gamma_p| = |I| + |J| \cdot p \quad . \quad (*)$$

Nun bemerken wir:

(1) $|\Gamma_p| = |G|^{p-1}$, folglich teilt p die Kardinalität $|\Gamma_p|$ von Γ_p.

(2) $|I| \geq 1$ denn $(e, \dots, e) \in \Gamma_p$ ist eine Bahn mit Kardinalität 1.

Aus $(*)$ folgt dann p teilt $|I|$ insbesondere $|I| \geq 2$.

Es gibt also $h \neq e$ mit $(h, \dots, h) \in T_p$
d.h. $h^p = e$. Folglich hat h Ordnung p.

□

Beweis von Thm 2.20.

Sei $\mathbb{Q} \subset E \subset \mathbb{C}$ ein in $\mathbb{C}$ enthaltener Zerfällungskörper von f und

$$R(f) = \{\alpha_1, \dots, \alpha_n\}$$

die Nullstellen von f geordnet so dass $\{\alpha_3, \alpha_4, \dots, \alpha_p\} \subset \mathbb{R}$.

Da f reelle Koeffizienten in $\mathbb{Q} \subset \mathbb{R}$ hat folgt

$$\alpha_2 = \overline{\alpha_1}$$

wobei $\varepsilon : z \mapsto \overline{z}$ komplexe Konjugation von $\mathbb{C}$ bezeichnet.

Mit Lemma II.7 können wir

$Gal(E/\mathbb{Q})$ mit einer Untergruppe von

$$S_{R(f)} = S_p$$

identifizieren.

Beachte, dass $\varepsilon(\alpha_i) = \alpha_i \quad 3 \le i \le p$

$$\varepsilon(\alpha_1) = \alpha_2$$

$$\varepsilon(\alpha_2) = \alpha_1$$

und da $E = \mathbb{Q}(\alpha_0, \dots, \alpha_p)$

folgt $\varepsilon(E) = E$.

Folglich ist $\varepsilon|_E \in Gal(E/\mathbb{Q})$ und

entspricht der Transposition (12).

Andererseits folgt aus Korollar 2. VS, dass

$$p \mid |Gal(E/\mathbb{Q})|$$

und folglich (Lemma II.2.1) enthält

$Gal(E/\mathbb{Q})$ ein Element η der Ordnung p.

Dann ist η ein p-Cykel und da

p Primzahl folgt daß ein p-Cykel und

eine Transposition S_p ergeben. ∎

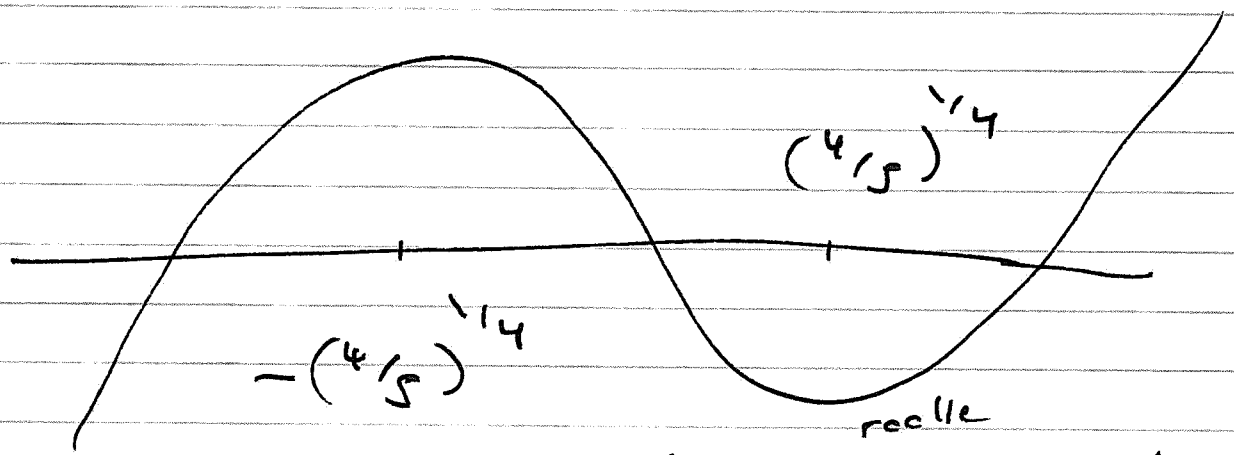
Korollar 2.22. Die Galois Gruppe von

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

ist isomorph zu S_5.

Beweis: Eisenstein Kriterium mit $p = 2$ impliziert, daß $X^5 - 4X + 2$ irreduzibel ist.

Sei $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto x^5 - 4x + 2$.



~~Dann ist $f'(x) = 5x^4 - 4$, Nullstellen $(4/5)^{1/4}$, $-(4/5)^{1/4}$, $f''(x) = 20x^3 \neq 0$~~

Dann ist $f'(x) = 5x^4 - 4$: hat genau zwei reelle Nullstellen:

$$-(4/5)^{1/4}, \quad (4/5)^{1/4}.$$

Für $|x| > (4/5)^{1/4}$ folgt $f'(x) > 0$

$|x| < (4/5)^{1/4}$ folgt $f'(x) < 0$.

Also ist f strikt monoton wachsend auf $(-\infty, -(4/5)^{1/4})$ mit $f(x) < 0$ für $x \to -\infty$ und $f((-4/5)^{1/4}) > 0$.

Also hat f in $(-\infty, (4/5)^{1/4}]$ genau eine reelle Nullstelle. Das gleiche gilt für

$$[-(4/5)^{1/4}, (4/5)^{1/4}], \quad [(4/5)^{1/4}, \infty)$$

Folglich hat f genau $3 = 5 - 2$ reelle Nullstellen. □

Die nächste Anwendung der Erweiterungssätze betrifft den Zusammenhang zwischen transitivitäts-eigenschaften der Galois Gruppe eines Polynoms und der irreduzibilität desen.

Korollar II.23 (Reitmon Prop. 3.14)

Sei $f \in k[x]$ und E ein Zerfällungskörper von f. Annahme: f hat keine mehrfachen Nullstellen. Dann gilt:

f irreduzibel $\iff$ $Gal(E/k)$ wirkt transitiv auf $R(f)$.

Beweis:

($\Longrightarrow$) Seien $\alpha, \beta \in R(f)$. Wir wenden jetzt Lemma 2.15 an auf $\varphi = id_k : k \to k$, da f irreduzibel ist gibt es

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

Erweiterung von id_k mit $\hat{\varphi}(\alpha) = \beta$.

Bemerke $f = (\hat{\varphi})_*(f)$. Wir können Thm II.17 (1) auf $f_* = f$, $E_* = E$ und $\hat{\varphi} : k(\alpha) \to k(\beta)$ anwenden und erhalten $\sigma \in Gal(E/k)$ mit $\sigma(\alpha) = \beta$.

($\Longleftarrow$) Wir nehmen an, $Gal(E/k)$ wirkt transitiv auf $R(f)$. Sei $f = p \cdot q$ mit $p, q \in k[x]$. Dann folgt:

$$R(p) \subset R(f), \quad R(q) \subset R(f)$$

und $Gal(E/k)$ lässt $R(p)$ und $R(q)$ invariant. Da f keine mehrfachen Nullstellen hat folgt $R(p) \cap R(q) = \emptyset$ und aus der Transitivität von $Gal(E/k)$ auf $R(f)$ folgt $R(p) = \emptyset$ oder $R(q) = \emptyset$ d.h. p oder q sind Konstant. □

Def. II.24. Eine Erweiterung E/k ist genannt normal falls sie Zerfällungs-körper eines Polynoms in $k[X]$ ist.

Bemerkung II.25 Seien $E \supset B \supset k$ Körpererweiterungen. Falls E/k normal ist, so ist E/B. Offensichtlich gilt:

$$Gal(E/B) < Gal(E/k).$$

Wir beenden dieses Kapitel mit einem Fundamentalen Resultat, das einen Zusammenhang herstellt zwischen den Galois Gruppen eines Turmes

$$E \supset B \supset k$$

von normalen Erweiterungen.

Thm II.26. (Rotman Thm 3.17)

Seien $k \subset B \subset E$ Erweiterungen mit der Eigenschaft, dass sowohl E/k wie B/k normal sind. Dann folgt

$\sigma(B) = B \quad \forall \sigma \in Gal(E/k)$

und der Homomorphismus

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

ist surjektiv mit Kern:

$$Gal(E/B).$$

Beweis: Sei $f \in k[X]$ mit ~~separ~~ B als Zerfällungskörper. Aus Lemma 2.4 folgt $\sigma(R(f)) = R(f) \quad \forall \sigma \in Gal(E/k)$; da $B = k(R(f))$ folgt

$$\sigma(B) = B \quad \forall \sigma \in Gal(E/k).$$

Damit ist $\sigma \longmapsto \sigma|_B$ ein wohldefinierter

Gruppenhomomorphismen mit Kern $Gal(E|B)$.

Surjektivität: Sei $g \in k[x]$ mit Zerfällungskörper E und $\sigma \in Gal(B|k)$.

Dann ist $\sigma_*(g) = g$, $\sigma: B \longrightarrow B$

$\cup \quad \cup$

$E \quad E$

und nach Prop. 2.16 gibt es eine Erweiterung von σ zu $\sigma': E \to E$;

insbesondere:

$$\sigma'|_K = \sigma|_k = id_k$$

und deshalb ist $\sigma' \in Gal(E|k)$ mit

$$\sigma'|_B = \sigma. \qquad \square$$

In der Übungsserie 4, Übung 6 werden sie folgende Charakterisierung normaler Erweiterungen herleiten:

Thm 2.27 Eine (endliche) Körpererweiterung E/k ist genau dann normal falls jedes irreduzible Polynom in $k[x]$ das eine Nullstelle in E besitzt, in $E[x]$ in lineare Faktoren zerfällt.