Woche 1

14. Grundbegriffe

Def. (a) Körpererweiterung $L : K$

(b) Zwischenkörper $M : L$, $L : K$

(c) $K[A]$, $K(A)$ für $A \subseteq L$

(d) einfach, primitives Element

(e) Grad, endl. Körpererw.

Bsp. ...

Gradsatz für Körpererw. 14.1: $[M : K] = [M : L] \cdot [L : K]$

Erinnerung an universelle Eigenschaft etc.

Def. alg. / trans. Körpererweiterungen

Satz 14.2 $L : K$, $a \in L$ trans. $\Rightarrow$ $K(a) \cong K(X) := \mathrm{Quot}(K[X])$

Satz 14.3 $L : K$, $a \in L$ alg.

(a) $K(a) = K[a]$

(b) $K(a) \cong K[X]/(f)$ Def. f Minimalpolynom

(c) $[K(a) : K] = \mathrm{grad}(f) = n$

(d) $1, a^1, \dots, a^{n-1}$ ist Basis von $K(a)$ als K-VR.

Woche 2

[Beweis von Satz 14.3 fertig]

Satz 14.4 Seien K, K' Körper, $\varphi: K \xrightarrow{\sim} K'$, $L:K$, $L':K'$, $a \in L$, $a' \in L'$ beide trans. oder $f(a)=0$ und $(\varphi f)(a')=0$, dann ex. $\tilde{\varphi}: K(a) \xrightarrow{\sim} K'(a')$ mit $\tilde{\varphi}(a) = a'$ und $\tilde{\varphi}|_K = \varphi$.

Folgerung 14.5 $K = K'$ und $\varphi = id$.

a, b dasselbe Minimalpolynom $\Leftrightarrow K(a) \cong K(b)$.

Satz 14.6 K Körper, $f \in K[X]$ mit $\text{grad}(f) = n \geq 1$. Dann ex einfache Erweiterung $L = K(a)$ mit
- a Nullstelle von f.
- $[K(a):K] \leq n$ ($=n$ gdw. f irred.).

Satz 14.7 $L:K$, $A \subseteq L$, $L = K(A)$, jedes Element aus A ist alg. über K.

(a) $L:K$ ist alg.

(b) $|A| < \infty \Rightarrow [L:K] < \infty$.

Korollar 14.8 $M:L$ und $L:K$ alg., so auch $M:K$.

[Übung]

Satz 14.9 $M:K$, $L := \{a \in M : a \text{ alg. über } K\}$, dann ist L ein Körper.

Woche 3

15. Zerfällungskörper

Kor. 15.1 [Stammbach III Kor. 2.8] $f \in K[X]$, $\mathrm{grad}(f) = n$, es ex. $L \supseteq K$ sodass f zerfällt in L in lin. Fakt. dann $[L:K] \leq n!$

Def. Zerfällungskörper von f über K.

Satz 15.2 [Stammbach III 2.10] Zerfällungskörper bis auf Isom. eindeutig.

Beispiel $X^3 - 2$ über $\mathbb{Q}$ mit SAGE.

16. Endliche Körper

Bemerkung: [Sb III 4.1]

Def. Formale Ableitung

Satz 16.1 [Sb III 4.2]

Def. separabel / inseparabel

Faktum 16.2 (a) [Sb Kor. 4.3]
(b) [Sb Kor. 4.4]

Satz 16.3 [Sb Satz 4.5] / Beweis nächste Woche

Woche 4

Beweis von Satz 16.3

Satz 16.4 $\mathbb{F}_{p^n}^*$ ist zyklisch [Serie 8; Afg 54]

Satz 16.5 [Sb III. 4.6]

Lemma 16.6 $a^p = a \iff a \in \mathbb{F}_p \quad (a \in \mathbb{F}_{p^n})$

Proposition 16.7 [Sb III. 4.7]

Satz 16.8 $a \in \mathbb{F}_{p^n}$, NS von $X^{p^n} - X$, h Min.-Poly. von a.
[Sb III. 4.8] $\Rightarrow \underbrace{\mathrm{grad}(h)}_{=m} \mid n$ und $a^{p^0}, \dots, a^{p^{m-1}}$ NS von h.

Korollar 16.9 [Aufgabe 92]

Def. Frobeniushomomorphismus

Proposition 16.10 [Aufgabe 91. (a)]

Woche 5

[Einschub: Rechnen in endl. Körpern mit SAGE]

17. Der algebraische Abschluss

Def. alg. abgeschlossen

Lemma 17.1 äquivalent
- (a) alg. abg. K
- (b) jedes $f \in K[X]$ zerfällt
- (c) irred. Polynome haben Grad $= 1$
- (d) $L : K$ alg. $\rightarrow L = K$
- (e) es ex. $K_0 \subseteq K$ mit $K : K_0$ alg. und jedes Polynom $f \in K_0[X]$ zerf. über K.

[(a) $\Leftrightarrow$ (e) Aufgabe 96]

Korollar 17.2 Umformulierung von Lem. 17.1 (e).

Bem. / Bsp. / Def. von alg. Abschluss

Lemma 17.3 äquiv.
- (a) L alg. Abschluss von K
- (b) $L : K$ ist alg. und L ist alg. abg.

Satz 17.4 Jeder Körper K besitzt einen alg. Abschluss.

[Beweis mit Teichmüller Prinzip]

Satz 17.5 Der alg. Abschluss ist bis auf Isom. eindeutig. (etwas allg. formuliert)

nächsten Montag

[Beweis mit Wohlordnungssatz bzw. transfiniter Induktion und Satz 14.4.]

Woche 6

[Beweis von Satz 17.5 mit transfiniter Induktion und Wohlordnungssatz]

18. Normale und separable Körpererweiterungen

<u>Def.</u> Normale Körpererweiterungen

<u>Bsp.</u> $\mathbb{C}:\mathbb{R}$, $\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}$ (Unbeispiel)

<u>Satz 18.1</u> [Sb VI 2.1]

<u>Def.</u> separable Polynome / Körpererweiterungen

<u>Def.</u> perfekte Körper (nach R. Pink)

<u>Proposition 18.2</u> [Sb VI 3.1]

wird nächste Woche behandelt

<u>Proposition 18.3</u> [Sb VI 3.2]

<u>Proposition 18.4</u> [Sb VI 3.3] [Beweis folgt direkt aus Satz 16.8]

<u>Def.</u> α separabel über K ; separable Körpererweiterungen

Woche 7

Propositionen 18.3 & 18.4 formuliert und bewiesen.

Satz 18.5 [Sb VI 3.4]

Korollar 18.6 Jeder endl. Körper ist perfekt.

19. Die Galoisgruppe

Def. $L:K$; $\sigma: L \xrightarrow{\sim} L$; K-Autom. von L,
Galoisgruppe $\mathrm{Gal}(L:K)$ von L über K.

Bsp. $\mathrm{Gal}(\mathbb{Q}(i):\mathbb{Q})$

Satz 19.1 $L:K$; $G = \mathrm{Gal}(L:K)$; $H \leq G$.

[Sb VI 5.1] $L^H := \{a \in L : \forall \sigma \in H \ (\sigma(a) = a)\} \leq L$

$H \leq \mathrm{Gal}(L:L^H)$

Def. Fixkörper zur UG H; L^H

Satz 19.2 [Sb VI 5.2]

Def. $L:K$; $f \in K[X]$; $\alpha \in L$; $f(\alpha) = 0$
in L zu α konjugierte Elemente

Korollar 19.3 [Sb VI 5.3]

wird nächstes Mal behandelt

Satz 19.4 [Sb VI 5.4]

Def. Galoisgruppe von $g \in K[X]$

Bem. [Sb p. 166]
$L:K$; L Zerfällungskörper von $g \in K[X]$, ...
$\mathrm{Gal}(L:K)$ ist isom. zu einer Untergr. von S_n.

Woche 8

Satz 19.4 formuliert.

Def. Gal(g)

Korollar 19.5 $|\mathrm{Gal}(g)| \mid n!$ [Bew. Übung]

Proposition 19.6 $|\mathrm{Gal}(L:K)| \leq [L:K]$ [Sb VI 5.6]

Satz 19.7 [Sb VI 5.7] [Bew. zum Teil in den Übungen]

Bem. Prp. 19.6 folgt aus Satz 19.7.

Proposition 19.8 [Sb VI 5.8]

Satz 19.9 [Sb VI 5.9]

Bsp. $[\mathbb{F}_{p^{12}} : \mathbb{F}_{p^3}] = 4 = |\mathrm{Gal}(\mathbb{F}_{p^{12}} : \mathbb{F}_{p^3})|$ $G \cong C_2 \times C_2$ ~~✓~~ / $G \cong C_4$ ✓

20. Der Hauptsatz der Galoistheorie

Lemma 20.1 [Sb VI 7.1]

Korollar 20.2 [Sb VI 7.2] ; Bem. zu Galoiserweiterung

Lemma 20.3 [Sb VI 7.3] (Beweis nach den Osterferien)

Satz 20.4 [Sb VI 7.4]

Woche 9

[Beweis von Lem. 20.3]

Korollar 20.5 [Sb $\overline{\text{VI}}$ 7.5]

Korollar 20.6 [Sb $\overline{\text{VI}}$ 7.6]

Korollar 20.7 [Sb $\overline{\text{VI}}$ 7.7]

Korollar 20.8 [Sb $\overline{\text{VI}}$ 7.8]

Korollar 20.9 [Sb $\overline{\text{VI}}$ 7.9]

Beispiel $X^6 - 2X^3 - 1$ über $\mathbb{Q}$ [Exercise 13.8 aus I. Stewart]

Woche 10

[1. Mai]

Woche 11

21. Zwei Anwendungen der Galoistheorie

(A) Konstruktionen mit Zirkel und Lineal

- Definitionen und Konstruktionen [analog zu Sb III.3, aber ausführlicher]

<u>Konstruierbarkeit geometrisch:</u> $\alpha \in \mathbb{R}$ konstruierbar genau dann wenn es pos. reelle Zahlen $\omega_0, \ldots, \omega_k \in \mathbb{R}$ gibt mit $\omega_0 \in \mathbb{Q}$, $\omega_i \in \mathbb{Q}(\sqrt{\omega_0}, \ldots, \sqrt{\omega_{i-1}})$ (für $1 \leq i \leq k$) und $\alpha \in \mathbb{Q}(\sqrt{\omega_0}, \ldots, \sqrt{\omega_k})$.

<u>Konstruierbarkeit algebraisch:</u> [Sb VI.9, p. 177]

Woche 12

Konstruierbarkeit mit Zirkel und Lineal abgeschlossen.

Letztes Resultat:

Satz 21.6 Das reguläre n-Eck ist genau dann konstruierbar, wenn $\varphi(n) = 2^l$ für ein $l \in \mathbb{N}$.

Woche 13

(B) Radikalerweiterungen und Lösungsformeln

Def. von Radikalerweiterung, normale Hülle, f durch Radikale auflösbar...

Ich folge "Galois Theory" (von Ian Stewart) (3rd ed.), Chapter 15 und habe mit Lemma 15.7 aufgehört (Beweis von Lem. 15.7 sowie "An Insoluble Quintic" wird nächstes Mal behandelt.)

Woche 14

- Beweis von Lem. 15.7 (Ian Stewart)
- Theorem 15.9
- Lemma 15.2

$\left.\begin{array}{l}\text{Theorem 15.9}\\ \text{Lemma 15.2}\end{array}\right\}$ aus "Galois Theory" (von Ian Stewart)