Zusammenfassung zu Algebra A

Sara Adams

11. Juli 2004

Diese Zusammenfassung basiert auf der Vorlesung
Algebra A
gehalten im Wintersemester 2003/04
von Prof. Dr. Klaus Metsch
an der Justus-Liebig Universität Gießen

Inhaltsverzeichnis

1 Integritätsbereiche

1.1 Gruppen

Definitionen

- G **Gruppe** $\Leftrightarrow$
  - $\cdot$ Verknüpfung, $a \cdot b \in G \, \forall \, a, b \in G$
  - $a \cdot (b \cdot c) = (a \cdot b) \cdot c \; \forall \, a, b, c \in G$
  - $\exists \, 1 \in G : 1 \cdot a = a \; \forall \, a \in G$ (**neutrales Element**)
  - $\forall \, a \in G \, \exists \, a^{-1} \in G : a^{-1} \cdot a = 1$ (**Inverse**)
- G **abelsche Gruppe** $\Leftrightarrow$ G Gruppe, $a \cdot b = b \cdot a \; \forall \, a, b \in G$
- U **Untergruppe** von $G \Leftrightarrow \; U \subseteq G$, U Gruppe $(U \leq G)$
- G Gruppe, $M, N \subseteq G$: $M \cdot N = \{m \cdot n : m \in M, n \in N\}$
- U Untergruppe von G
  - **Linksnebenklasse** von U: $gU = \{g \cdot u : u \in U\}$
  - **Rechtsnebenklasse** von U: $Ug = \{u \cdot g : u \in U\}$
- N **Normalteiler** von G $(N \trianglelefteq G) \Leftrightarrow gN = Ng \, \forall \, g \in G$
- **Faktorgruppe** von G nach $N \Leftrightarrow N \trianglelefteq G, G/N = \{gN : g \in G\}$
- **Index** von U $[G : U]$: Anzahl der Linksnebenklassen von U
- **Erzeugnis** von g: $< g >= \{g^a : a \in \mathbb{Z}\}$
- **Erzeugnis** von $M \subseteq G$: $< M >= \bigcap_{U \leq G, M \subseteq U} U$
  $M = \{g_1, .., g_s\} \Rightarrow < M >= < g_1, .., g_s >$
- **Ordnung** von $g \in G$:
  - $\exists \, n \in \mathbb{N} : g^n = 1, g^m \neq 1 \, \forall \, \mathbb{N} \ni m < n \Rightarrow Ord(g) = n$
  - $\nexists \, n \in \mathbb{N} : g^n = 1 \Rightarrow Ord(g) = \infty$
- G **zyklische Gruppe** $\Leftrightarrow \; \exists \, g \in G : G =< g >$ (g **Erzeuger** von G)
- $\phi : G \to H$ **Gruppenhomomorphismus** $\Leftrightarrow$ G, H Gruppen, $\phi(g_1 \cdot g_2) = \phi(g_1) \cdot \phi(g_2) \, \forall g_1, g_2 \in G$
  - ϕ inj., surj., bij.: **Mono-, Epi-, Isomorphismus**
  - $G = H$: **Endomorphismus**, surj.: **Automorphismus**
  - **Kern**$(\phi) = \{g \in G : \phi(g) = 1\}$, **Bild**$(\phi) = \{\phi(g) : g \in G\}$

Sätze

- **Untergruppenkriterium**: U Untergruppe von $G \Leftrightarrow$
  - $1 \in G$
  - $a, b \in U \Rightarrow \; a \cdot b \in U$
  - $a \in U \Rightarrow \; a^{-1} \in U$
- U Untergruppe von G, $g, h \in G$:
  - $gU = hU \Leftrightarrow h^{-1} \cdot g \in U \Leftrightarrow g \in hU$
  - $gU \cap hU = \emptyset \Leftrightarrow h^{-1} \cdot g \notin U \Leftrightarrow g \notin hU$
  - $Ug = Uh \Leftrightarrow g \cdot h^{-1} \in U \Leftrightarrow g \in Uh$
  - $Ug \cap Uh = \emptyset \Leftrightarrow g \cdot h^{-1} \notin U \Leftrightarrow g \notin Uh$

  Die versch. Linksnebenklassen von U bilden eine Partition von G.
- $|G| < \infty, U$ Untergruppe von $G \Rightarrow |U| = |gU| \, \forall g \in G, \exists \, ! \, \frac{|G|}{|U|}$ Linksnebenklassen
- **Satz von Lagrange**: U Untergruppe von G, $|G| < \infty \Rightarrow |U| \; \big| \; |G|$
- $Ord(g) = n < \infty \Rightarrow < g >= \{1, g, .., g^{n-1}\}$
- $Ord(g) = \infty \Rightarrow g^a \neq g^b \, \forall \, a, b \, \mathbb{N}, \; a \neq b$
- G zyklisch $\Rightarrow \; G$ abelsch
- $N \trianglelefteq G, \; g, h \in G \Rightarrow (gN) \cdot (hN) = (g \cdot h)N$
- $\phi : G \to H$
  - $\phi(1) = 1, \; \phi(g^{-1}) = \phi(g)^{-1} \, \forall \, g \in G$
  - $Kern(\phi) \trianglelefteq G, \; Bild(\phi) \leq H$
  - ϕ injektiv $\Leftrightarrow \; Kern(\phi) = \{1\}$
- Jede unendliche zyklische Gruppe ist isomorph zu $\mathbb{Z}$
- Jede endliche Gruppe mit n Elementen ist isomorph zu $\mathbb{Z}/n\mathbb{Z}$
- **Homomorphiesatz für Gruppen**: G, H Gruppen, $\phi : G \to H$ Homomorphismus $\Rightarrow$ $\widetilde{\phi} : G/Kern(\phi) \to Bild(\phi), \; gKern(\phi) \mapsto \phi(g)$ Isomorphismus, $G/Kern(\phi) \cong Bild(\phi)$

1.2 Ringe und Ideale

Definitionen

- R **Ring** mit Verknüpfungen $+, \cdot \; \Leftrightarrow$
  - $(R, +)$ ablesche Gruppe
  - $(a \cdot b) \cdot c = a \cdot (b \cdot c) \, \forall \, a, b, c \in R$
  - $(a + b) \cdot c = a \cdot c + b \cdot c, a \cdot (b = c) = a \cdot b + a \cdot c \, \forall \, a, b, c \in R$

- R **kommutativer Ring** $\Leftrightarrow\ a \cdot b = b \cdot a\ \forall\ a,b \in R$
- R **Ring mit Eins** $\Leftrightarrow\ \exists\ 1 \in R : 1 \cdot r = r\ \forall\ r \in\ R$
- S **Unterring** von $R\ \Leftrightarrow\ S \subseteq R,\ S$ Ring bzgl. $+, \cdot$
- I **Ideal** von $R\ \Leftrightarrow\ (I,+) \leq (R,+),\ \ r \cdot i, i \cdot r \in I\ \ \forall\ i\ \in I, r \in R$
- **Hauptideal**: R komm. Ring, $a \in R : aR = \{a \cdot r : r\ \in\ R\}$
- $\phi : R \to S$ **Ringhomomorphismus** $\Leftrightarrow\ R, S$ Ringe, $\phi(r_1 + r_2) = \phi(r_1 + \phi(r_2),\ \phi(r_1 \cdot r_2) = \phi(r_1) \cdot \phi(r_2)\ \ \forall\ r_1, r_2 \in R$
  - ϕ inj., surj., bij.: **Mono-, Epi-, Isomorphismus**
  - **Kern**$(\phi) = \{r \in R : \phi(r) = 0\}$, **Bild**$(\phi) = \{\phi(r) : r \in R\}$
- **Summe** von $M_i \subseteq R,\ i = 1, .., s :\ M_1 + .. + M_s = \{m_1 + .. + m_s : m_i \in M_i\}$
- **Produkt** von den Idealen I, J von R: $I \cdot J = \{\sum_{i=1}^{s} a_i \cdot b_i : a_j \in I,\ b_j \in J\}$
- **Erzeugnis** von $M \subseteq R : < M >= \bigcup_{I\ Ideal\ von\ R, M \subseteq I} I$ (eindeutig bestimmtes, kleinstes Ideal von R, das M enthält)

Sätze

- $\emptyset \neq S \subseteq R$ Unterring $\Leftrightarrow\ r - s, r \cdot s\ \in S\ \ \forall\ r, s \in S$
- $\emptyset \neq I \subseteq R$ Ideal $\Leftrightarrow\ i - j, i \cdot r, r \cdot i\ \in I\ \ \forall\ i, j \in I,\ r \in R$
- $\phi : R \to S$ Ringhomomorphismus $\Rightarrow\ Kern(\phi)$ Ideal von R, $Bild(\phi)$ Unterring von S
- $I_1, .., I_s$ Ideale $\Rightarrow\ \sum_{i=1}^{s} I_i$ Ideal
- $I_j\ \forall\ j \in J$ Ideal $\Rightarrow\ \bigcup_{j \in J} I_j$ Ideal
- I, J Ideale $\Rightarrow\ I \cdot J \subseteq I \cap J$ Ideal
- $M, N \subseteq R$
  - $< M \cup N >=< M > \cup < N >$
  - $< M \cap N > \subseteq < M > \cap < N >$
  - $M \subseteq N \Rightarrow < M > \subseteq < N >$
- $a_1, .., a_s \in R$ komm. Ring mit Eins $\Rightarrow < a_1, .., a_s >= a_1 R + .. + a_s R$

1.3 Faktorringe

- I Ideal von $R :\ (r + I) \cdot (s + I) = (r \cdot s) + I$ (wohldefiniert)
- ν **natürlicher Epimorphismus** von R auf R/I: I Ideal von $R, \nu : R \to R/I, r \mapsto r + I$
- **Homomorphiesatz für Ringe**: $\phi : R \to S$ Ringhomomorphismus, $I = Kern(\phi) \Rightarrow R/I \cong Bild(\phi),\ \ \widetilde{\phi} : R/I \to Bild(\phi), r + I \mapsto \phi(r)$ Isomorphismus

1.4 Integritätsbereiche

Definitionen

- R kommutativer Ring mit Eins, $r, s, e \in R$:
  - r **Teiler** von $s \Leftrightarrow\ s$ **Vielfaches** von $r \Leftrightarrow\ \exists\ t \in R :\ s = r \cdot t \Leftrightarrow\ r \mid s$
  - e **Einheit** von $R \Leftrightarrow\ e \mid 1$
  - r, s **assoziiert** $\Leftrightarrow\ \exists$ Einheit $e :\ r = s \cdot e \Leftrightarrow\ r \sim s$
  - r **echter Teiler** von $s \Leftrightarrow\ r \mid s, r \not\sim s, r$ keine Einheit
  - R **nullteilerfrei** $\Leftrightarrow \nexists\ 0 \neq a \in R : \exists\ 0 \neq b \in\ R,\ a \cdot b = 0$
- R **Integritätsbereich** $\Leftrightarrow\ R$ kommutativer, nullteilerfreier Ring mit Eins
- R Integritätsbereich, $0 \neq p$ keine Einheit
  - p **unzerlegbar** $\Leftrightarrow\ [p = r \cdot s \Rightarrow r$ oder s Einheit$]$
  - p **Primelement** $\Leftrightarrow\ [p \mid (r \cdot s) \Rightarrow\ p \mid r$ oder $p \mid s]$
- R **ZPE-Ring** $\Leftrightarrow\ R$ Int.bereich, jedes $r \neq 0$ lässt sich eindeutig als Produkt von einer Einheit und Primelementen schreiben
  - d **ggT** von $r_1, .., r_n \in R \Leftrightarrow\ d \mid r_i\ \forall\ i,\ [t \mid r_i\ \forall\ i \Rightarrow t \mid d]$
  - v **kgV** von $r_1, .., r_n \in R \Leftrightarrow\ r_i \mid v\ \forall\ i, [r_i \mid \tilde{v}\ \forall\ i \Rightarrow\ v \mid \tilde{v}]$

Sätze

- R komm. Ring mit Eins, $\ r, s, t \in R$
  - $t \mid r, r \mid s \Rightarrow\ t \mid s$
  - $t \mid r \Rightarrow\ t \mid (r \cdot s)\ \forall\ s \in R$
  - $t \mid r, t \mid s \Rightarrow\ t \mid (r + s)$
  - e_1, e_2 Einheiten $\Rightarrow\ e_1 \cdot e_2$ Einheit ($\Rightarrow$ **Einheitengruppe**)
  - e Einheit $\Rightarrow\ e \mid r\ \forall\ r \in R$
  - $r \sim s \Rightarrow r \mid s, s \mid r$
  - $\sim$ ist Äquivalenzrelation
- R Integritätsbereich
  - $0 \neq r = t \cdot s : t$ echter Teiler von $r \Leftrightarrow t, s$ keine Einheiten
  - $r \sim s \Leftrightarrow\ r \mid s, s \mid r$
  - Jedes Primelement ist unzerlegbar
  - p Primelement, $p \mid (s_1 \cdot .. \cdot s_n) \Rightarrow\ p \mid s_i$ für min. ein $i \in \{1, .., n\}$
  - e, f Einheiten, $p_1, .., p_r, q_1, .., q_s$ Primelemente, $e \cdot \prod_{i=1}^{r} p_i = f \cdot \prod_{i=1}^{s} q_i \Rightarrow$ $r = s,\ p_i \sim q_i, i = 1, .., r$ bei geeigneter Numerierung
- R ZPE-Ring: p unzerlegbar $\Leftrightarrow\ p$ Primelement
- R ZPE-Ring, $r_1, .., r_n, r \in R, r_i$ teilerfremd zu $r_j\ \forall\ r \neq j, r_i \mid r\ \forall\ i \Rightarrow \prod_{i=1}^{n} \mid r$
- R ZPE-Ring $\Rightarrow\ \exists$ ggT und kgV von $r_1, .., r_n \in R$

1.5 Hauptidealringe und euklidische Ringe

Definitionen

- R **Hauptidealring** $\Leftrightarrow$ R Int.bereich, $[I$ Ideal von $R \Rightarrow \exists\, a \in R : I = aR]$
- $\phi : R\backslash\{0\} \to \mathbb{N}_0$ **Gradfunktion** von $R \Leftrightarrow [a, b \in R,\ b \neq 0 \Rightarrow\ a = b \cdot t + r,\ r = 0$ oder $\phi(r) < \phi(b)]$ **Division mit Rest**
- R **euklidischer Ring** $\Leftrightarrow\ \exists\, \phi$ Gradfunktion

Sätze

- R Integritätsbereich: R/pR nullteilerfrei $\Leftrightarrow p$ Primelement
- R HIR, $0 \neq p \in R$ keine Einheit.
  p Primelement $\Leftrightarrow$ p unzerlegbar $\Leftrightarrow$ pR maximales Ideal $\Leftrightarrow$
  R/pR Körper $\Leftrightarrow$ R/pR nullteilerfrei $\Leftrightarrow$ p Primelement
- R euklidischer Ring $\Rightarrow$ R HIR $\Rightarrow$ R ZPE-Ring
- R HIR: d ggT von $r_1, .., r_n \in R\backslash\{0\} \Leftrightarrow sum_{i=1}^{n} r_i = dR$
- **Euklidischer Algorithmus**: Verfahren um zu $a, b \in R$ eukl. Ring, d ggT von a, b, x, y zu finden, so dass gilt: $a \cdot x + b \cdot y = d$
  Beispiel: $a = 1694,\ b = 490$

1694	$=$	$3 \cdot 490 + 224$	490	$=$	$2 \cdot 224 + 42$
224	$=$	$5 \cdot 42 + 14$	42	$=$	$3 \cdot 14 + 0$
$\Rightarrow$		ggT von a, b:	$\mathbf{14}$		
14	$=$	$1 \cdot 224 - 5 \cdot 42$		$=$	$1 \cdot 224 - 5 \cdot (490 - 2 \cdot 224)$
	$=$	$11 \cdot 224 - 5 \cdot 490$		$=$	$11 \cdot (1694 - 3 \cdot 490) - 5 \cdot 490$
	$=$	$\mathbf{11 \cdot 1694 - 38 \cdot 490}$			

1.6 Quotientenkörper

- R Integritätsbereich, $\sim$: $R \times (R\backslash\{0\}),\ (a, b) \sim (c, d) \Leftrightarrow\ a \cdot d = b \cdot c$ Äquivalenzrelation, Äquivalenzklassen: $\overline{(a, b)} = \frac{a}{b}$
- **Quotientenkörper** $Q(R)$: Menge aller Äquivalenzklassen mit den Verknüpfungen:
  $\frac{a}{b} + \frac{c}{d} = \frac{a \cdot d + b \cdot c}{b \cdot d}$ $\quad \frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d}$ (wohldefiniert)
- $Q(R)$ ist der kleinste Körper, der R enthält.

1.7 Polynomringe

Definitionen

- $\sum a_i \cdot x^i + \sum b_i \cdot x^i = \sum (a_i + b_i) \cdot x^i$
- $\sum a_i \cdot x^i \cdot \sum b_i \cdot x^i = \sum_{i,j} a_i \cdot b_j \cdot x^{i+j}$
- $\sum a_i \cdot x^i = \sum b_i \cdot x^i \Leftrightarrow\ a_i = bi\ \forall\, i$

- **Polynomring in n Variablen**: $R[x_1, .., x_n] = (R[x_1, .., x_{n-1}])[x_n]$
- **Körper der rationalen Funktionen**: Quotientenkörper $R(x)$ von $R[x]$
- $\phi : R \to S$ Ringisomorphismus $\Rightarrow R[x] \cong S[x],\ \overline{\phi} : R[x] \to S[x], \sum r_i \cdot x^i \mapsto \sum \phi(r_i) \cdot x^i$ Isomorphismus (**kanonische Fortsetzung** von ϕ)
- $0 \neq f \in R[x]$ **primitiv** $\Leftrightarrow$ R ZPE-Ring, die Koeffizienten von f haben nur Einheiten als gemeinsame Teiler
- $f \in R[x]$ **irreduzibel** $\Leftrightarrow$ f unzerlegbar
- $f = \sum a_i \cdot x^i, g \in R[x] :\ f(g) = \sum a_i \cdot g^i$
- $c \in R \subset R[x]$ **Nullstelle** von $f \in R[x] \Leftrightarrow\ f(c) = 0$

Sätze

- $f, g \in R[x], R$ Integritätsbereich
  - $Grad(f \cdot g) = Grad(f) + Grad(g)$
  - $Grad(f + g) \leq max\big(Grad(f), Grad(g)\big)$
  - $Grad(r \cdot f) = Grad(f)\ \ \forall\, r \in R\backslash\{0\}$
- R Integritätsbereich $\Rightarrow$ $R[x]$ Integritätsbereich
- R ZPE-Ring $\Rightarrow$ $R[x]$ ZPE-Ring
- R Integritätsbereich
  - p Primelement von $R \Rightarrow$ p Primelement von $R[x]$
  - e Einheit von $R \Leftrightarrow$ e Einheit von $R[x]$
  - $K = R(x), f \in K[x] \Rightarrow\ \exists\, r \in R :\ r \cdot f \in R[x]$
- R ZPE-Ring, $Q = Q(R),\ f, g \in R[x]$
  - f, g primitiv $\Rightarrow$ $f \cdot g$ primitiv
  - f unzerlegbar in $R[x] \Rightarrow$ f unzerlegbar in $Q[x]$
  - f primitiv, $f \big| g$ in $Q[x] \Rightarrow$ $f \big| g$ in $R[x]$
- **Eisensteinkriterium**: R Integritätsbereich, $0 \neq f = \sum_{i=0}^{n} a_i \cdot x^i \in R[x],\ n \geq 1$ primitiv $p \in R$ Primelement, $p \big| a_i, i = 0, .., n-1,\ p^2 \not| a_0 \Rightarrow$ f irreduzibel
- R Integritätsbereich, $g \in R[x]$: $\phi; R[x] \to R[x], f \mapsto f(g)$ Ringhomomorphismus $Grad(g) \geq 1 \Rightarrow$ ϕ injektiv (**Einsetzhomomorphismus**)
- R Integritätsbereich, $f \in R[x],\ c \in R :\ f(c) = 0 \Leftrightarrow\ (x - c) \big| f$
- R Integritätsbereich, $0 \neq f \in R[x] \Rightarrow$ f besitzt max. $Grad(f)$ verschiedene Nullstellen

2 Galoistheorie

2.1 Grundlagen

- K, L Körper, $\phi : K \to L, \phi \neq 0$ ein Ringhomomorphismus. $\Rightarrow \phi$ injektiv (**Körpermonomorphismus** von K nach L)
- Die Menge $Aut(K)$ aller Körperautomorphismen ist eine Gruppe bzgl. Hinereinanderausführung von Abbildungen.
- $K \subseteq L$ **Unterkörper** vom Körper L
  $\Leftrightarrow [0, 1 \in K,\ a, b \in K \Rightarrow a+b, a \cdot b \in K, -a, a^{-1} \in K]$
  $\Leftrightarrow [0, 1 \in K,\ a, b \in K, b \neq 0 \Rightarrow a - b,\ ab^{-1} \in K]$
- **Körpererweiterung** $L : K \Leftrightarrow K$ Unterkörper von $L \Leftrightarrow L$ Oberkörper von K.
- Z **Zwischenkörper** von $L : K \Leftrightarrow Z$ Unterkörper von L, Oberkörper von K
- $K_n \subseteq K$ alle Unterkörper von K $\Rightarrow \bigcap K_n$ kleinster Unterkörper von K (**Primkörper**)

2.2 Die Charakteristik eines Körpers

Definitionen

- K Körper, Einselement 1_K
  - $n \cdot 1_K = \sum_{i=1}^{n} 1_K,\ (-n) \cdot 1_K = -(n \cdot 1_K),\ 0 \cdot 1_K = 0_K$
  - $\Rightarrow (a+b) \cdot 1_K = a \cdot 1_K + b \cdot 1_K,\ (a \cdot b) \cdot 1_K = (a \cdot 1_K) \cdot (b \cdot 1_K)$
  - $n \cdot k = \sum_{i=1}^{[n} k \ \forall\ k \in K$
- **Charakteristik** $Char(K)$ vom Körper K
  - $Char(K) = n \in \mathbb{N} \Leftrightarrow n \cdot 1_K = 0_K,\ m \cdot 1_K \neq 0_K \ \forall\ m < n$
  - $Char(K) = 0 \Leftrightarrow n \cdot 1_K \neq 0 \ \forall\ n \in \mathbb{N}$
- K Körper, $Char(K) = p > 0 \Rightarrow F : K \to K, F(k) = k^p$ **Frobeniusabbildung**

Sätze

- K Körper, $Char(K) = 0 \Rightarrow$ Primkörper von $K \cong \mathbb{Q}$
- K Körper mit $Char(K) = p > 0$
  - p ist Primzahl
  - $\forall\ a, b \in \mathbb{Z} : a \cdot 1_K = b \cdot 1_K \Leftrightarrow p | (b - a)$
  - $P = \{n \cdot 1_K : n = 0, .., p-1\}$ Primkörper von K $\cong \mathbb{Z}_p$
- K Körper, $Char(K) = p > 0 \Rightarrow$ Frobeniusabb. Körpermonomorphismus
- K Körper, $|K| < \infty \Rightarrow Char(K) \neq 0$, Frobeniusabb. Körperautomorphismus

2.3 Körpererweiterungen

Definitionen

- $L : K$ Körpererweiterung, L Vektorraum über $K \Rightarrow dim(L) = [L : K]$ **Grad der Körpererweiterung**
- $L : K$ Körpererweiterung,

$$M \subseteq L \Rightarrow K(M) = \bigcap_{Z\ Unterk.\ von\ L;\ M, K \subseteq Z} Z$$

  kleinster Zwischenkörper von $L : K$, der M enthält (K adjungiert M)

Sätze

- **Gradsatz** $L : F, F : K$ endliche Körpererweiterungen $\Rightarrow [L : K] = [L : F] \cdot [F : K]$
- $L : K$ Körpererweiterung, $M, N \subseteq L$
  - $M \subseteq N \Rightarrow K(M) \subseteq K(N)$
  - $Z = K(M) \Rightarrow Z(N) = K(M \cup N)$
- $f \in K[x]$ irreduzibel, $n = Grad(f), I = fK[x]$
  - $L = K[x]/I$ ist Körper
  - $\forall\ l \in L\ \exists\ !g \in K[x], Grad(g) < n\ : g + I = l$
  - $K' = \{k + I : k \in K\} \cong K,\ [L : K'] = n$

2.4 Algebraische und Transzendente Erweiterungen

Definitionen

- $L : K$ **einfach** $\Leftrightarrow \exists\ a \in L : L = K(a)$
- K Körper, L Erweiterungskörper von K, $a \in L$
  - a **algebraisch** über K $\Leftrightarrow \exists f \in K[x] : f(a) = 0, f \neq 0$
  - a **transzendent** über K $\Leftrightarrow [f \in K[x] : f(a) = 0 \Rightarrow f = 0]$
- $L : K$ **algebraisch** $\Leftrightarrow [a \in L \Rightarrow a$ algebraisch über $K]$
- $L : K$ **transzendent** $\Leftrightarrow \exists\ a \in L : a$ transzendent über K
- $L : K$ **reintranszendent** $\Leftrightarrow [a \in L \backslash K \Rightarrow a$ transzendent über K
- $L : K$ Körpererweiterung, $a \in L \Rightarrow K[a] = \{f(a) : f \in K[x]\} \subseteq K(a) \subseteq L$ Unterring von L
- f **Minimalpolynom** von $a \in L \Leftrightarrow f \in K[x]$ normiert, $f(a) = 0,\ g(a) \neq 0 \forall g \in K[x], Grad(g) < Grad(f)$

Sätze

- $a \in L$ algebraisch über K, f Minimalpolynom von a
  - $I = \{g \in K[x] : g(a) = 0\}$ Ideal von $K[x]$
  - $I = fK[x], \quad \forall\, g \in K[x]\colon\ g(a) = 0 \Leftrightarrow f|g$
  - $K(a) = K[a],\ K(a) \cong K[x]/I$
  - $\phi : K[x]/I \to K(a), \phi(g + I) = g(a)$ ist Körperisomorphismus
  - $n = Grad(f) \Rightarrow [K(a) : K] = n,\ \{1, a, a^2, .., a^{n-1}\}$ ist eine K-Basis von $K(a)$ über K
- $L : K$ Körpererweiterung, $a \in L$ transzendent über K
  - $K[x] \cong K[a]$
  - $K(a) = Q(K[a])$
  - $K(a) \cong K(x), \nu : K(x) \to K(a),\ \nu(\frac{f}{g}) = \frac{f(a)}{g(a)}$ ist Isomorphismus
- $L : K$ Körpererw.: $a \in L$ algebraisch über K $\Leftrightarrow [K(a) : K] < \infty$
- $L : K$ Körpererw., $a_1, .., a_s \in L$ algebraisch über K $\Rightarrow [K(a_1, .., a_s) : K] < \infty$
- $L : K$ Körpererw., F Zw.körper: $L : K$ algebraisch $\Leftrightarrow L : F, F : K$ algebraisch
- a transzendent über K $\Rightarrow K(a) : K$ rein transzendente Erweiterung
- $K(a) : K,\ K(a') : K$ einfache alg. Erweiterungen, $f_a = f_{a'} \Rightarrow \exists$! Isomorphismus $\phi : K(a) \to K(a'), \phi(k) = k\ \forall\, k \in K, \phi(a) = a'$

2.5 Zerfällungskörper

Definitionen

- K Körper, $f_i, i \in I \in K[x]$ $\quad L$ Erweiterungskörper von K **Zerfällungskörper** $\Leftrightarrow$
  - f_i zerfällt in $L[x]$ in Linearfaktoren $\forall\, i \in I$
  - $M = \{a \in L : f_i(a) = 0, i \in I\} \Rightarrow L = K(M)$
- $K[x] \ni f = a \cdot (x - c_1) \cdot .. \cdot (x - c_s),\ a, c_i \in K, \quad c = c_j$ für genau i versch. $j \Rightarrow c$ **i-fache Nullstelle** von f (i=1 einfache NS, i>1 mehrfache NS)
- **Galoisgruppe** $G(L : K) = \{\phi \in Aut(L) : \phi(k) = k\ \forall k \in K\}$

Sätze

- $f \in K[x],\ Grad(f) \geq 1 \Rightarrow \exists$ Erweiterungskörper L von K : $[L : K] \leq Grad(f),\ \exists\, a \in L$: $f(a) = 0$
- $f \in K[x], Grad(f) = n \geq 0 \Rightarrow \exists$ ZFK L von f über K, $[L : K] \leq n!$

- $\phi : K_1 \to K_2$ Körperisomorphismus, $0 \neq f_1 \in K_1[x],\ \phi(f_1) = f_2, L_i$ ZFK von f_i über $K_i \Rightarrow \exists$ Isomorphismus $\bar{\phi}$ von L_1 auf $L_2, \bar{\phi}(k) = \phi(k)\ \forall k \in K_1;\ \ \exists$ max. $[L_1 : K_1]$ versch. $\bar{\phi}$, Gleichheit, wenn kein irred. Faktor on f_1 eine mehrfache NS besitzt.
- K Körper, $f \in K[x] \Rightarrow$ bis auf Isomorphie $\exists$! ZFK L von f über K
- $|G(L : K)| \leq [L : K]$, Gleichheit, wenn die irred. $g \in K[x]$ nur einfache Nullstellen besitzen.
- L ZFK von $f \in K[x]$ über K, Z Zw.körper von $L : K,\ \phi : Z \to L,\ \phi(k) = k\ \forall k \in K$ Körpermonomorphismus $\Rightarrow \exists \hat{\phi} \in Aut(L) : \hat{\phi}(z) = \phi(z)\ \forall z \in Z$

2.6 Mehrfache Nullstellen

Definitionen

- **Ableitung** von $K[x] \ni f = \sum_{i=0}^{n} a_i \cdot x^i :\ f' = \sum_{i=1}^{n} i \cdot a_i \cdot x^{i-1} \in K[x]$
- irred. $f \in K[x]$ **separabel** $\Leftrightarrow f$ besitzt keine mehrfachen Nullstellen
- $0 \neq f \in K[x]$ **separabel** $\Leftrightarrow$ irred. Faktoren von f sind separabel
- $L : K$ Körpererw.: $a \in L$ **separabel** über $K \Leftrightarrow \exists\, f \in K[x]$ separabel: $f(a) = 0$
- Körpererw. $L : K$ **separabel** $\Leftrightarrow [a \in L \Rightarrow a$ separabel über K]
- Körper K **vollkommen/perfekt** $\Leftrightarrow \big[[L : K]$ algebraisch $\Rightarrow L : K$ separabel$\big]$

Sätze

- $k \in K, f, g \in K[x] \Rightarrow (kf)' = kf',\ (f + g)' = f' + g',\ (fg)' = f'g + fg'$
- $f \in K[x]$: $a \in L$ mehrfache Nullstelle von $f \Leftrightarrow f'(a) = 0$
- $K[x] \ni f \neq 0$ besitzt keine mehrfachen NS im ZFK $\Leftrightarrow f, f'$ teilerfremd
- $a \in L$ separabel $\Leftrightarrow a$ algebraisch über K, Min.polynom $f \in K[x]$ von a separabel
- $L : K$ separabel $\Leftrightarrow L : K$ algebraisch, $[f \in K[x]$ irred., $\exists\, a \in L : f(a) = 0 \Rightarrow f$ hat nur einfache Nullstellen]
- $L : K$ Körpererw., Z Zw.körper: $L : K$ separabel $\Leftrightarrow L : Z,\ Z : K$ separabel
- $Char(K) = 0 \Rightarrow K$ vollkommen
- $Char(K) = p > 0 : K$ vollkommen $\Leftrightarrow$ Frobeniusabb. $F(c) = c^p$ von K ist surjektiv
- Jeder endliche Körper ist vollkommen.

2.7 Normale Erweiterungen

Definitionen

- Körpererw. $L : K$ **normal** $\Leftrightarrow\ \ L : K$ algebraisch, $[f \in K[x]$ irred., $\exists\, a \in L : f(a) = 0 \Rightarrow f$ zerfällt in L in Lin.faktoren]

Sätze

- $L:K$ endlich: $L:K$ normal $\Leftrightarrow$ L ZFK von $f \in K[x]$ über K
- $L:K$ Körpererw., $M \subseteq L$, $L = K(M) \Rightarrow \forall\, l \in L\ \exists\, N \subseteq M, |N| < \infty : l \in K(N)$
- $L:K$ algebraisch: $L:K$ normal $\Leftrightarrow$ L ZFK über K von Polynomen $f_i, i \in I$
- $L:K$ normal, Z Zwischenkörper
  - $L:Z$ normal
  - $[L:K] < \infty \Rightarrow \big[Z:K \text{ normal} \Leftrightarrow g(Z) = Z\ \forall\, g \in G(L:K)\big]$
- $[L:K] < \infty \Rightarrow \exists$ Körpererw. $M:L$ mit:
  1. $M:K$ normal und endlich
  2. Z Zw.körper von $M:L, Z \neq M \Rightarrow Z:K$ nicht normal
  3. $M':L$ Körpererw. mit den Eigenschaften 1.,2. $\Rightarrow\ \exists\, \phi : M \to M'$ Isomorphismus, $\phi(l) = l\ \forall\, l \in L$

  M heißt **normaler Abschluss** von $L:K$

2.8 Galoiserweiterungen und Galoiskorrespondenz

Definitionen

- L Körper, $G \leq Aut(L) \Rightarrow Fix(G) = \{l \in L : g(l) = l\ \forall\, g \in G\}$ **Fixkörper** von G
- $L:K$ **Galoiserweiterung** $\Leftrightarrow$ $L:K$ normal und separabel
- A Menge, G symm. Gruppe aller Permutationen von A: $U \leq G$ **transitiv** $\Leftrightarrow [a, a' \in A \Rightarrow\ \exists\, u \in U : u(a) = a'] \ \Rightarrow |U| \geq |A|$

Sätze

- **Lemma von Artin**: L Körper, $G \leq Aut(L)$, $|G| < \infty$, $K = Fix(G) \Rightarrow [L:K] \leq |G|$ (es gilt sogar Gleichheit)
- $G \leq Aut(L)$, $|G| < \infty$, $K = Fix(G)$, $l_1, .., l_s \in L$, $\{g(l_1), .., g(l_s)\} = \{l_1, .., l_s\}\ \forall\, g \in G \Rightarrow f = \prod_{i=1}^{s}(x - l_i) \in K[x]$
- Für eine Körpererw. $L:K$ sind äquivalent:
  - $K = Fix(G)$, $G \leq Aut(L)$, $|G| < \infty$
  - $L:K$ endlich, separabel, normal
  - L ZFK von einem separablen $f \in K[x]$
  - $[L:K] = |G(L:K)| < \infty$
  - $|G(L:K)| < \infty, K = Fix\big(G(L:K)\big)$
- L Körper, $G \leq Aut(L), |G| < \infty \Rightarrow L:K$ endliche Galoiserweiterung, $G = G(L:K)$

- $[L:K] < \infty \Rightarrow |G(L:K)| \leq [L:K]$
- $[L:K] < \infty \Rightarrow \big[|G(L:K)| = [L:K] \Leftrightarrow L:K \text{ Galoiserweiterung}\big]$
- $L:K$ Körpererw., Z Zw.körper, $g \in G(L:K)$, $Z' = g(Z) \Rightarrow g \cdot G(L:Z) \cdot g^{-1} = G(L:Z')$
- **Hauptsatz der Galoistheorie**: $L:K$ Körpererw., $[L:K] < \infty, \mathcal{M} = \{U \leq G(L:K)\}, \mathcal{Z} = \{Z \text{ Zw.körper von } L:K\}$
  1. $\mathcal{M} \to \mathcal{Z}, U \mapsto Fix(U)$ bijektiv
  2. $\mathcal{Z} \to \mathcal{M}, Z \mapsto G(L:Z)$ bijektiv
  3. $Z = Fix(U) \Leftrightarrow U = G(L:Z)$
  4. 1. und 2. sind invers zueinander
  5. Z Zw.körper $\Rightarrow L:Z$ Galoiserweiterung
  6. Z Zw.körper: $Z:K$ Galoiserweiterung $\Leftrightarrow G(L:Z) \trianglelefteq G(L:K) \quad \Rightarrow G(Z:K) \cong G(L:K)/G(L:Z)$
- L ZFK von $f \in K[x]$ über K, r Anzahl der versch. NS von f in L:
  - $G(L:K)$ isomorph zu einer UG von S_r, $|G(L:K)| \mid r!$
  - f irred. $\Rightarrow G(L:K)$ isomorph zu einer trans. UG von S_r, $|G(L:K)| \geq r$

2.9 Der algebraische Abschluss

Definitionen

- Körper L **algebraisch abgeschlossen** $\Leftrightarrow \nexists$ alg. Erweiterung $\neq L \Leftrightarrow$ jedes Polynom $f \in L[x]$ zerfällt in L in Lin.faktoren
- $L:K$ Körpererw.: L **algebraischer Abschluss** von $K \Leftrightarrow L:K$ algebraisch, L algebraisch abgeschlossen

Sätze

- Jeder Körper besitzt einen eindeutig bestimmten algebraischen Abschluss
- K Körper, $f_i \in K[x], i \in I \Rightarrow\ \exists\,!$ ZFK der f_i über K

3 Gruppen

3.1 Permutationsdarstellung von Gruppen

In diesem Abschnitt werden Abb. von links nach rechts abgearbeitet: $(fg)(x) = g(f(x))$

Definitionen

- Schreibweise $x^f = f(x),\ x^{(fg)} = (x^f)^g$
- **Operation bzw. Permutationsdarstellung** von der Gruppe G auf eine Menge X: Homomorphismus T von G in die symm. Gruppe S_X von X
- Operation T **treu** $\Leftrightarrow T$ injektiv und transitiv $(x, y \in X \Rightarrow\ \exists\, g \in G : x^{T(g)} = y)$
- **Operation auf der alg. Struktur** X: T Operation von G auf X, X hat alg. Struktur, $T(g),\ g \in G$ Automorphismus von X
- G Gruppe, $X = G : x^g = g^{-1}xg$ Operation auf sich selbst durch **Konjugation**
- G operiert auf X: **Äquivalenzrelation** $x \sim y \Leftrightarrow\ \exists\, g \in G : y = x^g$
- Äquivalenzklassen: **Bahnen** von G auf X
  - $x^G = B_x = \{x^g : g \in G\} \subseteq X$ **Bahn** zu $x \in X$
  - $|x^G| = |B_x|$ = **Länge der Bahn** zu $x \in X$
  - $G_x = \{g \in G : x^g = x\}$ = **Stabilisator** von $x \in X$ in G
- $Fix_G(X) = \{x \in X : x^g = x\ \forall\ g \in G\}$ Menge aller **Fixpunkte** von G $(\Rightarrow |B_x| = 1)$
- Spezialfall Konjugation:
  - Bahnen: **Konjungiertenklassen** von G
  - $x, y \in G$ **konjugiert** $\Leftrightarrow y \in B_x \Leftrightarrow\ \exists\, g \in G : y = x^g$
  - **Zentrum** von $G : Z(G) = Fix_G(X) = \{x \in G : xg = gx\}$
  - **Zentralisator** von $x \in G : C_G(x) = G_x = \{g \in G : xg = gx\}$
- G **p-Gruppe** $\Leftrightarrow p$ Primzahl, $|G| = p^m, m \in \mathbb{N}$

Sätze

- T Operation von G auf $X,\ x^{T(g)} = x^g \Leftrightarrow x^1 = 1\ \forall\, x \in X, x^{(gh)} = (x^g)^h\ \forall\, g, h \in G$
- G operiert auf X
  - $x \in X \Rightarrow G_x \leq G$
  - B Bahn, $x \in B \Rightarrow\ G_x g \mapsto x^g$ wohldef. Bijektion der Menge der Nebenklassen von G_x auf B
  - X endlich $\Rightarrow\ |B_x| = [G : G_x]$
  - G endlich, transitiv $\Rightarrow [G : G_x] = |X|\ \forall\, x \in X$

- **Bahnengleichung**: $|G|, |X| < \infty,\ B_1, .., B_s$ die versch. Bahnen mit $|B_i| \geq 2, x_i \in B_i \Rightarrow |X| = |Fix_G(X)| + \sum_{i=1}^{s} [G : G_{x_i}]$
- **Klassengleichung**: $|G| < \infty, K_1, ..., K_s$ die versch. Konjugiertenklassen mit $|K_i| \geq 2, x_i \in K_i \Rightarrow |G| = |Z(G)| + \sum_{i=1}^{s} [G : C_G(x_i)]$
- G p-Gruppe $\Rightarrow Z(G) \neq \{1\}$, insb. $|Z(G)| = p^k, k \in \mathbb{N}$

3.2 Die Sylow-Sätze

Definitionen

- $|G| = p^n \cdot q < \infty, p$ Primzahl, $p \not| q \Rightarrow S \leq G, |S| = p^n$ **p-Sylowgruppe** von g
- $|G| = p^n \cdot q < \infty, p$ Primzahl, $q \in \mathbb{N}, p \not| q \Rightarrow Syl_p(G) = \{S \leq G : |S| = p^n\}$
- $U \leq G, g \in G \Rightarrow U^g = \{u^g : u \in U\} = \{g^{-1}ug : u \in U\}$ zu U **konjugierte Untergruppen** $(x \mapsto x^g$ Automorphismus von $G,\ |U^g| = |U|)$
- $U \leq G \Rightarrow$ **Normalisator** von U in $G :\ N_G(U) = \{g \in G : U^g = U\} = \{g \in G : gU = Ug\}$

Sätze

- $|G| = p^n \cdot q < \infty, p$ Primzahl, $q \in \mathbb{N}, p \not| q,\ 1 \leq m \leq n \Rightarrow\ \exists\, U \leq G : |U| = p^m$
- **Erster Sylow-Satz**: $|G| < \infty \Rightarrow\ \forall p$ Primzahl, $p||G|\ \exists\, S \leq G$ p-Sylowgruppe
- $|G| < \infty, p||G|$ Primzahl, P p-Sylowgruppe von G, U p-Untergruppe von $G (|U| \in p^{\mathbb{N}}) \Rightarrow \exists\, g \in G : U^g \subseteq P$
- **Zweiter Sylow-Satz**: $|G| < \infty, p||G|$ Primzahl , $P, P' \in Syl_p(G) \Rightarrow\ \exists\, g \in G : P^g = P'$
- $|G| < \infty, P \in Syl_p(G) \Rightarrow [G : N_G(P)] = |Syl_p(G)|$
- $|G| < \infty, P \in Syl_p(G), g \in G, P^g = P, Ord(g) = p^k, k \in \mathbb{N} \Rightarrow g \in P$
- **Dritter Sylow-Satz**: $|G| < \infty, p||G|$ Primzahl $\Rightarrow p|(|Syl_p(G)| - 1)$
- $|Syl_p(G)| = 1 \Leftrightarrow Syl_p(G) = \{P\} \Leftrightarrow G = N_G(P) \Leftrightarrow Syl_p(G) \ni P \trianglelefteq G$

3.3 Auflösbare Gruppen

Definitionen

- $g, h \in G$ **vertauschen** $\Leftrightarrow gh = hg$
- **Kommutator** von $g, h \in G : [g, h] = g^{-1}h^{-1}gh$
- **Kommutatorgruppe** $G' =< [g, h] : g, h \in G >$
- $G^{(0)} = G, G^{(i+1)} = (G^i)'$
- G **auflösbar** $\Leftrightarrow\ \exists\, n \in \mathbb{N} : G^{(n)} = 1$

Sätze

- $g,h \in G : gh = hg \Leftrightarrow [g,h] = 1$
- $G' = 1 \Leftrightarrow G$ abelsch
- $G' \trianglelefteq G$
- $N \trianglelefteq G : G/N$ abelsch $\Leftrightarrow G' \subseteq N$
- $U \leq G \Rightarrow U^{(i)} \subseteq G^{(i)};\ \ N \trianglelefteq G \Rightarrow (G/N)^{(i)} = G^{(i)}N/N$
- G auflösbar $\Rightarrow U \leq G$ auflösbar
- G auflösbar $\Leftrightarrow N \trianglelefteq G,\ G/N, N$ auflösbar
- $|G| < \infty, G \neq \{1\}$ abelsch $\Rightarrow\ \exists\, N \trianglelefteq G : G/N$ zyklische Gruppe von Primzahlordnung
- $|G| < \infty \Rightarrow$ Es sind äquivalent:
  - G auflösbar
  - $\exists\, G = N_0 \supset N_1 \supset .. \supset N_s = 1,\ N_i \leq G,\ N_i \trianglelefteq N_{i-1},\ N_{i-1}/N_i$ abelsch
  - $\exists\, G = N_0 \supset N_1 \supset .. \supset N_s = 1,\ N_i \trianglelefteq N_{i-1},\ N_{i-1}/N_i$ zyklisch von Primzahlordnung
- $A_n = \{\pi \in S_n : sgn(\pi) = 1\}$
  - $n \geq 3 \Rightarrow S_n' = A_n$
  - $n \geq 4 \Rightarrow A_n$ nicht abelsch
  - $n \geq 5 \Rightarrow A_n$ einfach, $A_n' = A_n,\ A_n, S_n$ nicht auflösbar

4 Anwendungen der Galoistheorie

4.1 Endliche Körper

Definitionen

- α **primitives Element** von $K \Leftrightarrow |K| = q < \infty, \alpha \in K^* = K\backslash\{0\}, K^* = \{\alpha^i : i = 0,1,..,q-2\}$
- α **primitives Element** von $L : K \Leftrightarrow L = K(\alpha)$

Sätze

- $|K| < \infty, P = Char(K) \Rightarrow |K| = p^n, n \in \mathbb{N}$
- p Primzahl, $n \in \mathbb{N} \Rightarrow\ \exists\, !K : |K| = p^n$ bis auf Isomorphie, K ZFK von $x^{(p^n)} - x$ über $\mathbb{Z}_p$
- $|L| = p^n < \infty, p = Char(L) \phi : L \to L, l \mapsto l^p$ Frobeniusautomorphismus von $L \Rightarrow Aut(L)$ zyklische Gruppe der Ordnung $n,\ Aut(L) = \{1, \phi, .., \phi^{n-1}\}$
- $L : K$ Körpererw., $|L| = p^n, |K| = p^m, Char(K) = p$

  - $m|n, [L : K] = \frac{n}{m}$
  - $L : K$ galoissch
  - $G(L : K)$ zyklisch von der Ordnung $\frac{n}{m}$
  - $G(L : K) =< \phi^m >,\ \phi^m(l) = l^{p^m}$
- $|L| = p^n < \infty, Char(L) = p \Rightarrow\ \forall\, m \in \mathbb{N}, m|n\ \exists\, !$ Unterkörper $K, |K| = p^m$ und es gibt keine weiteren Unterkörper von L
- $|G| < \infty$ abelsche Gruppe $\Rightarrow\ \exists\, e \in \mathbb{N} : g^e = 1\ \forall g \in G, \exists\, h \in G : Ord(h) = e$ (e heißt **Exponent von G**)
- Die mult. Gruppe endlicher Körper ist zyklisch
- **Satz vom primitiven Element**: $L : K$ Körpererw., $L = K(a,b), a$ separabel, b algebraisch über $K \Rightarrow L : K$ einfach ($|K| = \infty$ erlaubt!)
- $L = K(a, a_1, .., a_s), a$ algebraisch, a_i separabel über $K \Rightarrow \exists\, c \in L : L = K(c)$
- Jede endliche separable Körpererweiterung ist einfach
- $[L : K] < \infty, Char(K) = 0 \Rightarrow L : K$ einfach

4.2 Konstruktion mit Zirkel und Lineal

Im Folgenden sei E=$\mathbb{R}^2$, M eine Menge von Punkten aus E, oBdA $|M| \geq 2, (0,0), (0,1) \in$ M

Definitionen

- Eine **Gerade von M** ist eine Gerade durch 2 Punkte von M.
- Ein **Kreis von M** ist ein Kreis mit Mittelpunkt in M und Radius r, wobei r=—AB— für zwei Punkte A, B aus M.
- Ein Punkt P heißt **direkt konstruierbar aus M**, wenn P der Schnittpunkt von zwei Geraden aus M, einer Gerade und einem Kreis aus M oder zwei Kreisen aus M ist oder falls P in M ist.
- Ein Punkt P heißt **konstruierbar aus M**, falls es Punkte $P_1, .., P_n$ gibt, so dass P_i aus $M \cup \{P_j : j < i\}$ direkt konstruierbar ist und $P_n = P$.
- Die reelle Zahl r heißt **kostruierbar aus M**, falls der Punkt (r,0) aus M konstruierbar ist.
- $L = \{r \in \mathbb{R} : r$ konstruierbar aus M$\}$
- $\mathbb{Q}(M) = K = \mathbb{Q}(\{p,q : (p,q) \in M\}) =$ kleinster Unterkörper von $\mathbb{R}$, der die Koordinaten aller Punkte aus M enthält.
- Körpererweiterung $L : K$ **Radikalerweiterung** $\Leftrightarrow \exists$ Zwischenkörper $K_i : K = K_0 \subset .. \subset K_s = L,\ K_i = K_{i-1}(\sqrt[n]{b}), n \in \mathbb{N}, b \in K_{i-1}$

- $K[x] \ni f, f(x) = 0$ **durch Radikale lösbar** $\Leftrightarrow [f(a) = 0 \Rightarrow a$ liegt in einer Radikalerweiterung]
- $GL(L:K) = GL(f,K)$ **Galoisgruppe** von f über $K \Leftrightarrow L$ ZFK von $f \in K[x]$ über K
- $Char(K) = 0$: e **n-te Einheitswurzel**$\Leftrightarrow$ e Lösung von $x^n - 1 = 0$
- e **primitive n-te Einheitswurzel** $\Leftrightarrow$ e n-te Einheitswurzel, $Ord(e) = n$

Sätze

- (r,s) ist aus M konstruierbar $\Leftrightarrow$ r und s sind konstruierbar
- $r, s \in \mathbb{R}$ konstruierbar aus M $\Rightarrow$ $r - s$, $\frac{r}{s}, s \neq 0$ konstruierbar aus M
- $r \in \mathbb{R}, r^2$ konstruierbar aus M $\Rightarrow r$ konstruierbar aus M
- $K_0 = \mathbb{Q}, K_0 \subset K_1 \subset .. \subset K_n$ Körperturm, $[K_i : K_{i-1}] = 2, i = 1, .., n \Rightarrow K_n \subseteq L$
- $P = (p,q)$ direkt aus M konstruierbar $\Rightarrow K(p,q) = K$ oder $[K(p,q) : K] = 2$
- $c \in \mathbb{R}$ konstruierbar aus M $\Leftrightarrow$ $\exists$ Körperturm $\mathbb{Q}(M) = K_0 \subset K_1 \subset .. \subset K_n$, $c \in K_n, [K_i : K_{i-1}] = 2, i = 1, .., n$
- Die Quadratur des Kreises ist unmöglich.
- Die Verdoppelung des Würfels ist unm"glich.
- $\mathbb{N} \ni n = 2^s \cdot \prod_{i+1}^{t} p_i$, $\exists\, m \in \mathbb{N} : p_i - 1 = 2^m$ (Fermatsche Pirmzahlen) $\Leftrightarrow$ regelmäßiges n-Eck kontruierbar
- $Char(K) = 0$, $L : K$ Radikalerweiterung $\Rightarrow \exists\, M : [M : K] < \infty$, $M : K$ galoissche Radikalerweiterung
- $Char(K) = 0, L = K(e), e$ primitive n-te Einheitswurzel $\Rightarrow L : K$ galoissch, $G(L : K)$ abelsch
- $Char(K) = 0, [e^n = 1 \Rightarrow e \in K], L : K$ Körpererweiterung
  - $L = K(a), a^n \in K \Rightarrow L : K$ galoissch, $G(L : K)$ zyklisch
  - $L : K$ galoissch, $G(L : K)$ zyklisch, $[L : K] < \infty \Rightarrow \exists\, a \in L : L = K(a), a^n \in K, n \in \mathbb{N}$
- $L : K$ galoissche Radikalerweiterung $\Rightarrow$ $G(L : K)$ auflösbar
- $L : K$ endliche Galoiserweiterung, $Char(K) = 0, G(L : K)$ zyklisch, e n-te Einheitswurzel $\Rightarrow L(e) : K(e)$ endliche Galoiserweiterung, $G\big(L(e) : K(e)\big)$ zyklisch, $\big|G\big(L(e) : K(e)\big)\big| \,\big|\, [L : K]$
- $Char(K) = 0, K[x] \ni f \neq 0 : f(x)$ durch Radikale lösbar $\Leftrightarrow$ $G(f,K)$ auflösbar