

Zur Vorbereitung der mündlichen Prüfung

BI: Beweisidee bzw. die wesentlichen Punkte des Beweises

Kap.	Definitionen & Begriffe	Beweise von Sätzen & Beziehungen zwischen Begriffen	Übungen
13	(i) irreduzible Elemente	(0) Beziehungen zwischen den Begriffen: Primelement, irreduzibles Element, Primideal [Lem. 13.1, Fkt. 13.2, Kor. 13.5] (1) BI: Jeder Hauptidealring ist faktoriell [Thm. 13.6] (2) BI: Lemma von Gauss [Lem 13.7] (3) Kriterium von Schönemann-Eisenstein [13.9]	75, 77, 79, 80
	(ii) Primelemente		
	(iii) assoziiert Elemente		
	(iv) eind. in irred. Fakt. zerlegbar		
	(v) faktorielle Ringe		
	(vi) grösster gemeinsamer Teiler		
	(vii) primitive Elemente		
14	(viii) Körpererweiterung	(4) $L : K$ Körpererw. und $s_0 \in L$, so ist $\alpha_{s_0} = (f)$ und $K[X]/(f) \cong K[s_0]$ [mit Kor. 12.4 & Thm. 12.8 aus Alg. I]	82–86
	(ix) Zwischenkörper	(5) Gradsatz für Körpererweiterungen [14.1]	
	(x) $K[A]$ und $K(A)$	(6) $a \in L$ alg. über K . Es gilt $K(a) = K[a]$, $K(a) \cong K[X]/(f)$ mit f Min.-Polynom von a , $[K(a) : K] = \deg(f) =: n$ und $1, \dots, a^{n-1}$ ist Basis vom K -Vektorraum $K(a)$ [Satz 14.3].	
	(xi) einfache Körpererweiterung	(7) $\varphi : K \xrightarrow{\sim} K'$, $a \in L$, $a' \in L'$, es ex. irred. $f \in K[X]$ mit $f(a) = 0$ und $\varphi f(a') = 0$. Dann gilt $\tilde{\varphi} : K(a) \xrightarrow{\sim} K'(a')$ mit $\tilde{\varphi}(a) = a'$ und $\tilde{\varphi} _K = \varphi$ [Satz 14.4.(b)].	
	(xii) primitives Element	(8) Adjunktion einer symbolischen Nullstelle [Satz 14.6.(a)], und Eindeutigkeit (falls f irred.) [Satz 14.6.(c)].	
	(xiii) Grad der Körpererweiterung	(9) $A \subseteq L$, $L = K(A)$, und jedes Element aus A ist alg. über K . Dann ist $L : K$ algebraisch [Satz 14.7.(a)]; Folgerungen und weitere Resultate [Kor. 14.8, Satz 14.9, und Übungen].	
	(xiv) endliche Körpererweiterung		
	(xv) alg. und transz. Körpererweiterung		
	(xvi) $a \in L$ alg./transz. über K		
	(xvii) Minimalpolynom		
15	(xviii) Zerfällungskörper	(10) BI: Existenz und Eindeutigkeit von Zerfällungskörpern [Kor. 15.1 und Satz 15.2].	88, 89
16	(xix) Frobeniusendomorphismus	(11) BI: Existenz von endlichen Körpern von Primzahlpotenzordnung [aus Grundstrukturen bzw. Skript]	91, 94–96, 99
		(12) Endliche Körper haben immer Primzahlpotenzordnung [Lem. 16.1]	
		(13) Nullstellen von $h \in \mathbb{F}_p[X]$ in einem Erweiterungskörper $L \supseteq \mathbb{F}_p$ [Prp. 16.4 und Satz 16.5]	
17	(xx) K algebraisch abgeschlossen	(14) Äquivalente Formulierungen von “algebraisch abgeschlossen” und eine Folgerung [Lem. 17.1 und Prp. 17.2].	100–102
	(xxi) algebraischer Abschluss von K	(15) BI: Existenz eines algebraischen Abschlusses aus dem Primidealtheorem [Satz 17.3 (ohne Eindeutigkeit)]	
18	(xxii) normale Körpererweiterungen (xxiii) formale Ableitung (xxiv) separable Polynome (xxv) perfekte Körper (xxvi) separable Körpererweiterungen	(16) BI: Charakterisierung von endlichen normalen Körpererweiterungen [Satz 18.1]	104, 105
		(17) Charakterisierung von separablen Polynomen [Prp. 18.1]	
		(18) Alle Körper $\mathbb{F}_p$ (p prim) und Körper mit Charakteristik 0 sind perfekt [Prp. 18.3 & 18.4].	
		(19) $L : K$ separabel und $K \subseteq M \subseteq L$, dann sind $L : M$ und $M : K$ separabel [Satz 18.5].	
		(20) Endliche Körper sind perfekt [Kor. 18.6].	

	(xxvii) K-Automorphismus (xxviii) Galoisgruppe (xxix) Fixkörper L^H zur Untergruppe H (xxx) konjugierte Elemente (xxxi) Galoisgruppe eines Polynoms	(21) Ist $H \leq \text{Gal}(L : K)$, dann gilt $K \subseteq L^H \subseteq L$ und $H \leq \text{Gal}(L : L^H)$ [Satz 19.1]. (22) Ist $K \subseteq M \subseteq L$, dann ist $\text{Gal}(L : M) \leq \text{Gal}(L : K)$ [Satz 19.2]. (23) Ist $L : K$ algebraisch, $\alpha \in L$, und $\sigma \in \text{Gal}(L : K)$, so ist $\sigma(\alpha)$ in L zu α konjugiert [Kor. 19.3]. (24) Ist $f \in K[X]$ mit $\text{grad}(f) = n$, so ist $\text{Gal}(f)$ ein Teiler von $n!$ [Kor. 19.5] (25) BI: Ist $L : K$ eine endliche Körpererweiterung, so gilt $\text{Gal}(L : K) \leq [L : K]$ (Prp. 19.6, bzw. Satz 19.7). (26) BI: Ist L_f der Zerfällungskörper eines separablen Polynoms $f \in K[X]$, so gilt $\text{Gal}(L_f : K) = [L_f : K]$ (Prp. 19.8 bzw. Satz 19.9). (27) BI: Eine endliche Körpererweiterung $L : K$ mit $K = \infty$ ist einfach genau dann, wenn es nur endlich viele Zwischenkörper $K \subseteq M \subseteq L$ gibt [Satz 19.10].	110, 111
20	(xxxii) endl. Galoiserweiterungen bzw. galoische Körpererweiterungen (xxxiii) konjugierte Körper	(28) BI: Ist L_f der Zerfällungskörper des separablen Polynoms $f \in K[X]$, dann ist $L_f^{\text{Gal}(f)} = K$ [Lem. 20.1]. (29) Ist L_f der Zerfällungskörper des sep. Polynoms $f \in K[X]$, dann ist die Körpererweiterung $L_f : K$ normal und separabel [Kor. 20.2 mit Bem.]. (30) BI: Ist L ein Körper und $H \leq \text{Aut}(L)$ endlich, dann ist $[L : L^H] \leq H$ [Lem. 20.3]. (31) BI: Hauptsatz der Galoistheorie (auch Formulierung) [Satz 20.4]. (32) BI: Ist $L : K$ eine endliche, separable Körpererweiterung und $\text{char}(K) = 0$, dann ist $L : K$ einfach [Kor. 20.5]. (33) Für Zwischenkörper M mit $K \subseteq M \subseteq L$ und $L : K$ galoissch gilt: $[M : K] = [\text{Gal}(L : K) : \text{Gal}(L : M)]$ [Kor. 20.6]. (34) Aufsteigende Folge von Zwischenkörpern $K \subseteq M \subseteq L$ und absteigende Folge von Untergruppen $H \leq \text{Gal}(L : K)$ [Kor. 20.7]. (35) Für Zwischenkörper $K \subseteq M \subseteq L$ und $\sigma \in \text{Gal}(L : K)$ gilt: $\text{Gal}(L : \sigma[M]) = \sigma \text{Gal}(L : M) \sigma^{-1}$ [Kor. 20.8]. (36) BI: Für Zwischenkörper $K \subseteq M \subseteq L$ ist $M : K$ genau dann normal wenn $\text{Gal}(L : M) \trianglelefteq \text{Gal}(L : K)$ [Kor. 20.9]. (37) Ist $K \subseteq M \subseteq L$ und die Körpererweiterung $M : K$ normal, dann gilt: $\text{Gal}(L : K) / \text{Gal}(L : M) \cong \text{Gal}(M : K)$ [Kor. 20.10]. (38) Galoisgruppe und Zwischenkörper von Körpererweiterungen wie zum Beispiel $\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}$.	115, 116, 118, 126, 127

21 (xxxiv) Radikalerweiterung (xxxv) f auflösbar durch Radikale (xxxvi) normale Hülle (xxxvii) auflösbare Gruppen	(39) BI: Definition von Radikalerweiterungen mit Primzahlpotenzen [Lem. 21.1]. (40) BI: Ist $M \subseteq \mathbb{C}$ ein Zerfällungskörper von $X^p - 1$, $a \in M$, und $L \supseteq M$ ein Zerfällungskörper von $X^p - a$ über M, dann ist $\text{Gal}(L : M)$ abelsch [Lem. 21.3]. (41) BI: Sei $a \in K$, $M \supseteq K$ ein Zerfällungskörper von $X^p - 1$ über K, und $L \supseteq K$ ein Zerfällungskörper von $X^p - a$ über K. Für $G := \text{Gal}(L : K)$ und $N := \text{Gal}(L : M)$ ist $N \trianglelefteq G$, und N und G/N sind abelsch [Kor. 21.4]. (42) BI: Sei $\mathbb{Q} \subseteq K \subseteq L \subseteq \mathbb{C}$ und sei $L : K$ eine normale Radikalerweiterung. Dann ist $\text{Gal}(L : K)$ auflösbar [Lem. 21.6]. (43) Sei f ein Polynom über K ($\mathbb{Q} \subseteq K \subseteq L \subseteq \mathbb{C}$). Ist f auflösbar durch Radikale, so ist auch $\text{Gal}(f)$ auflösbar [Satz 21.7]. (44) BI: Sei p prim, $f \in \mathbb{Q}[X]$ ein über $\mathbb{Q}$ irred. Polynom mit $\text{grad}(f) = p$ welches über $\mathbb{C}$ genau zwei Nullstellen in $\mathbb{C} \setminus \mathbb{R}$ hat. Dann ist $\text{Gal}(f) \cong S_p$ [Lem. 21.8]. (45) BI: Lösungsformeln für cubische und quartische Gleichungen 120, 121, BI: 124
22 (xxxviii) Konstruierbarkeit von Punkten, Geraden, und Kreisen (xxxix) konstruierbare Körper	(46) BI: Konstruierbare Zwischenkörper K (mit $\mathbb{Q} \subseteq K$) und konstruierbare Erweiterungskörper von K [Lemmata 22.1, 22.2, 22.3, und Kor. 22.4]. (47) Ist $L : \mathbb{Q}$ eine normale Körpererweiterung mit $L \subseteq \mathbb{Q}$ und $[L : \mathbb{Q}] = 2^k$ (für $k \in \mathbb{N}$), dann ist L konstruierbar [Satz 22.5]. (48) BI: Das reguläre n-Eck ist genau dann konstruierbar wenn $\varphi(n) = 2^l$ (für $l \in \mathbb{N}$) [Satz 22.6, inkl. BI von Thm. 22.7]. (49) Galoisgruppen von Kreisteilungspolynomen wie zum Beispiel $X^{15} - 1$. (50) Charakterisierung der konstruierbaren regulären n-Ecke [Kor. 22.9]. (51) BI: Konstruktion des regelmässigen 5- und 17-Ecks. —