Informationen zur mündlichen Prüfung Algebra/Geometrie

Der Prüfungsstoff umfasst die Vorlesungen, die Übungsaufgaben (exercices) und die Anwesenheitsaufgaben (exercices de présence).

Hier eine unvollständige Liste von DEFINITIONEN, *Beispielen* und **Theoremen** aus den Vorlesungen Algebra/Geometrie I:

Gruppentheorie

GRUPPEN, MONOIDE, ABELSCHER GRUPPEN, UNTERMONOIDE, UNTERGRUPPEN, ZYKLISCHE GRUPPEN

$(\mathbb{Z}, +)$, $\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$, *symmetrische Gruppe S_n und alternierende Gruppe A_n , Automorphismengruppen, Symmetriegruppen, Diedergruppe*
 $n\mathbb{Z} \subset \mathbb{Z}$, $\mathbb{Q}_{>0} \subset \mathbb{R}^*$, $SO(n) \subset GL_n(\mathbb{R})$, $A_n \subset S_n$

BESCHREIBUNG VON GRUPPEN DURCH ERZEUGER UND RELATIONEN, GRUPPENTAFEL

HOMOMORPHISMUS, EPI-, MONO-, ISOMORPHISMUS

det, sgn, Konjugation, Vektorraumhomomorphismen, Projektion $\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$, $SO(2) \cong S^1 \cong \mathbb{R}/\mathbb{Z}$

KARTESISCHES PRODUKT VON GRUPPEN

Ordnung einer Gruppe $ord(G)$, Ordnung eines Elements $ord(g)$

Links- und Rechtsnebenklassen, Index $(G : H)$ von H in G

G ist disjunkte Vereinigung der Nebenklassen gH .

Theorem von Lagrange

Die Ordnung eines Elements teilt die Gruppenordnung.
 $ord(G)$ Primzahl $\implies G$ zyklisch.

NORMALTEILER, FAKTORGRUPPEN

G/H Gruppe $\iff xH = Hx \forall x \iff H$ Normalteiler.

Universelle Eigenschaft der Faktorgruppe
Drei Isomorphiesätze und Korollare

GRUPPENOPERATIONEN $G \times M \rightarrow M$

Operation von $GL_n(K)$ auf K^n , Operation von S_n , Operation von G auf G durch Links-, Rechtsmultiplikation, oder durch Konjugation, Operation von $SL_2(\mathbb{R})$ auf der oberen Halbebene $\mathcal{H}$

ORBIT/BAHN, STABILISATOR/ISOTROPIEGRUPPE, FIXPUNKTE

Stabilisatoren sind Untergruppen, M ist disjunkte Vereinigung der Orbits

Operation von S^1 auf $\mathbb{C}$, Operation von $GL_n(\mathbb{C})$ auf $M(n \times n, \mathbb{C})$ durch Konjugation, Beziehung zur Jordan-Normalform, Operation von $O(n)$ auf den symmetrischen Matrizen

NORMALISATOR, ZENTRALISATOR, ZENTRUM

Bahngleichung und Klassengleichung

p -GRUPPEN

$ord(G) = p^n > 0 \implies$ Zentrum von G ist nicht trivial.

$ord(G) = p^n \implies |M| \equiv |M^G| \pmod{p}$.

Theorem von Cauchy

G endliche p -Gruppe $\iff ord(G) = p^n$.

p -SYLOWGRUPPEN

Sylowgruppen von S_3 , von $\mathbb{Z}/pq\mathbb{Z}$, von endlichen abelschen Gruppen und von p -Gruppen

G endl. Gruppe, U eine p -Untergruppe $\implies (N_G(U) : U) \equiv (G : U) \pmod{p}$.

Die drei Sylow-Sätze und Korollare

$ord(G) = pq$, $p > q$ Primzahlen und $q \nmid p - 1 \implies G$ zyklisch.

$ord(G) = 15$ oder $ord(G) = 33 \implies G$ ist zyklisch.

EINFACHE GRUPPEN

$ord(G) = p^2q$, $p \neq q$ Primzahlen $\implies G$ ist nicht einfach.

SYMMETRISCHE GRUPPE S_n , SIGNUM sgn , ALTERNIERENDE GRUPPE A_n ,
INVERSIONEN, TRANSPOSITIONEN, r -ZYKEL

Theorem von Cayley

Für $n \geq 3$ ist A_n die Menge aller Produkte von 3-Zykeln.

KOMMUTATOR $[a, b]$, KOMMUTATORGRUPPE $[G, G]$, PERFEKTE GRUPPEN,
NORMALREIHE VON G , FAKTOREN, AUFLÖSBARE GRUPPEN, G^k

$[G, G]$ ist normal in G und $G/[G, G]$ ist abelsch.

N normal in G und G/N abelsch $\implies [G, G] \subset N$.

G auflösbar $\iff G^k = \{e\}$ für ein k .

S_1, S_2, A_2, S_3, A_3 , Normalreihe für S_3 , $[A_4, A_4] = V_4$ (=Kleinsche Vierergruppe), Normalreihen für A_4 und für S_4 .

Weitere Beispiele auflösbarer Gruppen: abelsche Gruppen, p -Gruppen, $ord(G) = pq$, p, q Primzahlen.

Theorem von Burnside: (ohne Beweis) $ord(G) = p^a \cdot q^b \implies G$ auflösbar.

Theorem von Feit-Thompson: (ohne Bew.) $ord(G)$ ungerade $\implies G$ auflösbar.

Bilder und Untergruppen von auflösbaren Gruppen sind auflösbar.

S_n, A_n sind für $n \geq 5$ nicht auflösbar.

A_n ist für $n \neq 4$ einfach.

Ringtheorie

RINGE, KOMMUTATIVE RINGE, EINSELEMENT, RINGE MIT 1

*Körper, $\mathbb{Z}$, $2\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$, $M(n \times n, R)$, Produkt von zwei Ringen, $\text{Map}(X, R)$,
 $R := \{a + b \cdot \sqrt{2} \mid a, b \in \mathbb{Q}\}$*

GRUPPE DER EINHEITEN R^* , NULLTEILER, INTEGRITÄTSRING,
UNTERRING, RINGERWEITERUNG, CHARAKTERISTIK $\text{char}(R)$

Einheiten in $\mathbb{Z}/n\mathbb{Z}$ für $n < 9$

*R Integritätsring $\implies \text{char}(R) = 0$ oder $\text{char}(R) = p$, p Primzahl.
 $\text{char}(R) = p \implies (x + y)^p = x^p + y^p$ (Frobenius-Homomorphismus)*

Von nun an sind alle Ringe kommutativ mit 1!

POTENZREIHENRING $R^{\mathbb{N}}$, POLYNOMRING $R[x]$, GRAD EINES POLYNOMS,
NORMIERTES POLYNOM

Euklidischer Algorithmus

Euklidischer Algorithmus für $f = [2]x^3 + [3]x + [1]$, $g = [3]x^2 - x - [1] \in \mathbb{Z}/4\mathbb{Z}[x]$

RINGHOMOMORPHISMUS (BEACHTE $1 \mapsto 1$), IDEAL I , HAUPTIDEALE, SUMME,
SCHNITT UND PRODUKT VON IDEALEN, FAKTORRING R/I

Universelle Eigenschaft des Faktorrings

$\varphi : R \rightarrow R'$ Epimorphismus $\implies R' \cong R/\ker(\varphi)$.

Einheiten, Ideale, Hauptideale, Faktorringe in $\mathbb{Z}$, $\mathbb{Q}[x]$

m Primzahl $\iff \mathbb{Z}/m\mathbb{Z}$ ist Integritätsring $\iff \mathbb{Z}/m\mathbb{Z}$ ist Körper.

PRIMIDEALE, MAXIMALE IDEALE

$\mathfrak{p} \subset R$ Primideal $\iff R/\mathfrak{p}$ Integritätsring.

$\mathfrak{m} \subset R$ maximal $\iff 0 \subset R/\mathfrak{m}$ maximal $\iff R/\mathfrak{m}$ Körper.
 $\mathfrak{m}$ maximal $\implies \mathfrak{m}$ Primideal.

Primideale und max. Ideale in $R = \mathbb{Z}$, max. Ideale in $R = C([0, 1], \mathbb{R})$

HAUPTIDEALRINGE (HIR), EUKLIDISCHE RINGE, GRAD/NORMABB. *deg*

R euklidisch $\implies R$ HIR.

$\mathbb{Z}$ mit $\deg(a) = |a|$,

$K[x]$ mit $\deg(f) = \text{Grad des Polynoms}$,

$\mathbb{Z}[i]$ mit $\deg(a + ib) = a^2 + b^2$ (Ring der ganzen Gaussischen Zahlen)

ASSOZIIERTE ELEMENTE, GRÖSSTER GEMEINSAMER TEILER (GGT), KLEIN-
STES GEMEINSAMES VIELFACHES (KGV)

Bestimmung des ggT mit dem euklidischen Algorithmus

Bestimmung von $\text{ggT}(42, 642) \in \mathbb{Z}$ mit dem euklidischen Algorithmus.

TEILERFREMDE/KOPRIME ELEMENTE, KOPRIME IDEALE

Theorem von Bézout

Chinesischer Restsatz

Lösungsmenge der Kongruenzen $x \equiv x_i \pmod{a_i}$, $i = 1, \dots, n$, in $\mathbb{Z}$

IRREDUZIBLE ELEMENTE, PRIMELEMENTE

R Integritätsring, $p \in R$, $p \neq 0$. Dann gilt:

(p) maximales Ideal $\implies p$ Primelement.

p Primelement $\implies p$ irreduzibel.

Ist R ein Integritätsring und HIR und ist $p \in R$, $p \neq 0$, $p \notin R^*$, so gilt:
 p irreduzibel $\iff p$ Primelement $\iff (p)$ maximales Ideal.

$R = \mathbb{C}[x]$, $R = \mathbb{Z}[\sqrt{-5}]$

NOETHERSCHE RINGE

Jeder HIR ist noethersch.

R ein Integritätsring und HIR und $a \in R - \{R^* \cup \{0\}\} \implies a$ lässt sich als Produkt von Primelementen schreiben.

FAKTORIELLE RINGE, ÄQUIVALENTE BESCHREIBUNGEN (SIEHE SATZ 2.57)

R faktorieller Ring, $r \in R$. Dann gilt: r irreduzibel $\iff r$ Primelement.

R Integritätsring und HIR $\implies R$ faktoriell.

$\mathbb{Z}$, $\mathbb{Z}[i]$, $K[x]$

Hauptsatz der elementaren Zahlentheorie

Beschreibung des ggT und kgV in faktoriellen Ringen.

POLYNOMRING $R[x_1, \dots, x_n]$, HOMOGENE POLYNOME, TOTALGRAD

R Integritätsring $\implies R[x_1, \dots, x_n]$ Integritätsring und es gilt für die Einheiten $R[x_1, \dots, x_n]^* = R^*$.

$f, g \in R[x_1, \dots, x_n] \implies \deg(f + g) \leq \max(\deg(f), \deg(g))$ und $\deg(f \cdot g) \leq \deg(f) + \deg(g)$.

R Integritätsring $\implies \deg(f \cdot g) = \deg(f) + \deg(g)$

R faktoriell $\implies$ jedes $f \in R[x]$, $f \neq 0$, $f \notin R[x]^*$, ist Produkt von irreduziblen Polynomen.

R Integritätsring, $p \in R$ Primelement $\implies p$ Primelement in $R[x]$.

Theorem von Gauss

$R = \mathbb{Z}$ oder R ein Körper $\implies R[x_1, \dots, x_n]$ ist ein faktorieller Ring.
Sei R ein Integritätsring. Ist R HIR, so ist R faktoriell.

Es gibt Integritätsringe, die faktoriell, aber keine HIR sind.

Eisensteinsches Irreduzibilitätskriterium

$x^3 - 2$ irreduzibel in $\mathbb{Z}[x]$.

S MULTIPLIKATIVE MENGE, $S^{-1}R$ LOKALISIERUNG VON R BZGL. S , QUOTIENTENKÖRPER $Q(R)$

lokaler Ring an einer Primzahl bzw. an einem Ideal: $\mathbb{Z}_{(p)}$, R_I

R faktorieller Ring $\implies S^{-1}R$ faktorieller Ring.

R faktoriell, $S \subset R$ multiplikative Menge. Sei $f \in R[x]$ vom Grad ≥ 1 .
Dann gilt: f irreduzibel in $R[x] \implies f$ irreduzibel in $(S^{-1}R)[x]$.

$X^2 + Y^3 + Z^n$ irreduzibel in $K(X, Y)[Z]$

Körpertheorie

CHARAKTERISTIK EINES KÖRPERS, HOMOMORPHISMEN, ISOMORPHISMEN, UNTERKÖRPER, KÖRPERERWEITERUNGEN, PRIMKÖRPER

Beziehung zwischen Charakteristik und Primkörper

GRAD $[L : K]$ EINER KÖRPERERWEITERUNG, $K \subset L$ ENDLICHE KÖRPERERWEITERUNG, ALGEBRAISCHE ELEMENTE, ALG. ERWEITERUNG, TRANSCENDENTE ELEMENTE, TRANSZ. ERWEITERUNG, ALG. UND TRANSZ. ZAHLEN

Die Menge aller algebraischen Zahlen ist abzählbar.
Jedes nicht-leere Intervall besitzt überabzählbar viele transzendente Zahlen.
 π und e sind transzendente Zahlen (ohne Beweis).

MINIMALPOLYNOM EINES ALGEBRAISCHEN ELEMENTS $\alpha \in L$ ÜBER K .

Minimalpolynom $f \in K[x]$ ist prim.
 $K[x]/(f)$ ist ein Körper isomorph zu $K[\alpha]$.
 $[K[\alpha] : K] = \deg(f)$.

$\mathbb{R}[x]/(x^2 + 1)$, $\mathbb{Q}[\sqrt[n]{p}]$, p eine Primzahl.

Endliche Körpererweiterungen sind algebraisch.

$K(\alpha_1, \dots, \alpha_n)$, EINFACHE KÖRPERERWEITERUNGEN, ENDLICH ERZEUGTE KÖRPERERWEITERUNGEN

$L = K(\alpha_1, \dots, \alpha_n)$, alle α_i alg. über $K \implies L = K[\alpha_1, \dots, \alpha_n]$ und $[L : K] < \infty$.

$\sqrt[3]{5} + 4 \cdot (\sqrt[3]{5})^2 + 1/3$ ist algebraisch über $\mathbb{Q}$.

$K \subset L$ endlich $\iff L$ wird über K von endlich vielen algebraischen Elementen erzeugt $\iff K \subset L$ ist eine endlich erzeugte algebraische Körpererweiterung.

$K \subset L$ algebraische Körpererweiterung $\iff L$ wird über K von algebrai-

schen Elementen erzeugt.

$K \subset L$ algebraische Körpererweiterung, $L \subset M$ Körpererweiterung und $\alpha \in M$ algebraisch über L . Dann ist α auch algebraisch über K .

$K \subset L \subset M$ Körpererweiterungen. Dann gilt: M über K algebraisch $\iff$ M über L und L über K algebraisch.

ALGEBRAISCH ABGESCHLOSSENE KÖRPER, ALGEBRAISCHER ABSCHLUSS VON K IN L , ALGEBRAISCHER ABSCHLUSS $\overline{K}$ VON K

$\mathbb{C}$ ist algebraisch abgeschlossen.

Jeder Körper besitzt einen algebraischen Abschluss.

$\overline{\mathbb{R}} = \mathbb{C}$, $\overline{\mathbb{Q}} \subset \mathbb{C}$ ist der Körper der algebraischen Zahlen, $\overline{\mathbb{F}_p}$

KONSTRUKTION MIT ZIRKEL UND LINEAL, ERLAUBTE OPERATIONEN, KONSTRUIERBARE ZAHLEN

$M \subset \mathbb{C}$, $0, 1 \in M \implies$ die Menge der aus M konstruierbaren Zahlen $\hat{M}$ ist ein Unterkörper von $\mathbb{C}$.

$M \subset \mathbb{C}$, $0, 1 \in M \implies \mathbb{Q} \subset \hat{M}$.

$z \in \hat{M} \iff$ es gibt eine Kette von Körpererweiterungen

$$\mathbb{Q}(M \cup c(M)) =: L_0 \subset L_1 \subset \dots \subset L_n \subset \mathbb{C}$$

mit $z \in L_n$, $c(L_n) = L_n$ und $[L_{i+1} : L_i] \leq 2$ für alle i .

$\hat{M}$ ist quadratisch abgeschlossen, d.h. $\omega \in \hat{M} \implies \sqrt{\omega} \in \hat{M}$.

z aus M konstruierbar $\implies [\mathbb{Q}(M \cup c(M))(z) : \mathbb{Q}(M \cup c(M))] = 2^l$.

Würfel mit doppeltem Volumen nicht konstruierbar.

Quadratur des Kreises nicht möglich.

Dreiteilung des Winkels im Allgemeinen nicht möglich.

FORMALE ABLEITUNG f' , SEPARABLE POLYNOME, $a \in L \supset K$ SEPARABEL

$x^5 - 1 \in \mathbb{Q}[x]$ ist separabel.

$f \in K[x]$ irreduzibel. Dann gilt:

f inseparabel $\iff f' = 0 \iff \text{char}(K) = p$ und

$\exists g \in K[x]$ irreduzibel separabel, $m \geq 1$, mit $f(x) = g(x^{p^m})$.

VOLLKOMMENE/PERFEKTE KÖRPER

NORMALE KÖRPERERWEITERUNG, GALOISCHE KÖRPERERWEITERUNG, GALOISGRUPPE, FIXKÖRPER

Hauptsatz der Galoistheorie (ohne Beweis)

RADIKALERWEITERUNGEN, AUFLÖSEN DURCH RADIKALE

Polynome vom Grad ≤ 4 lassen sich durch Radikale auflösen (für $n = 4$ ohne Details)

GALOISGRUPPE $Gal(f)$ EINES POLYNOMS f

K ein Körper der Charakteristik Null, $f \in K[x]$ irreduzibel durch Radikale auflösbar. Dann ist $Gal(f)$ auflösbar. (ohne Beweis)

Galoisgruppe des allgemeinen Polynoms von Grad n ist S_n . (ohne Beweis)

Für $n \geq 5$ ist die allgemeine Gleichung n ten Grades $f = 0$ nicht durch Radikale auflösbar.