Prüfungsstoff Algebra

(Algebra & Geometrie I, 2017)

Der Prüfungsstoff umfasst die Vorlesungen und die Übungsaufgaben.
Es folgt eine unvollständige Liste von Definitionen, *Beispielen* und Theoremen aus der Algebra Vorlesung:

Gruppentheorie

Gruppen, Monoide, abelsche Gruppen, Untergruppen, zyklische Gruppen

Beispiele von Gruppen: $(\mathbb{Z},+)$, $(\mathbb{Z}/n\mathbb{Z},+)$, $(\mathbb{R}^*,\cdot)$, $(\mathbb{C}^*,\cdot)$, $(\{z\in\mathbb{C}\mid z^n=1\},\cdot)$, $(V,+)$ *(wo V ein Vektorraum ist), die Automorphismengruppe $Aut(V)$, die symmetrische Gruppe S_n, die alternierende Gruppe A_n, Symmetriegruppen, zum Beispiel die Symmetriegruppe des Quadrats*

G zyklisch $\implies$ G abelsch.

Beispiele von Untergruppen: $n\mathbb{Z}\subset\mathbb{Z}$, $\mathbb{Q}_{>0}\subset\mathbb{R}^*$, $A_n\subset S_n$, $U(n)\subset Gl_n(\mathbb{C})$, $SO(n)\subset O(n)\subset GL_n(\mathbb{R})\subset GL_n(\mathbb{C})$

Beschreibung einer Gruppe durch Erzeuger und Relationen, Gruppentafel

Diedergruppe

Homomorphismus, Epimorphismus, Monomorphismus, Isomorphismus, Automorphismus

Beispiele: $det: GL_n(\mathbb{R})\to\mathbb{R}^*$, $sgn: S_n\to\{\pm1\}$, *Konjugation, lineare Abbildung von Vektorräumen, Projektion* $\mathbb{Z}\to\mathbb{Z}/n\mathbb{Z}$, $SO(2)\cong S^1\cong\mathbb{R}/\mathbb{Z}$

Sei $\Phi: G\to H$ ein Homomorphismus. Dann gilt: Φ injektiv $\iff$ $\ker\Phi=\{e\}$

Théorie des groupes

Groupes, monoïdes, groupes abéliens, sous-groupes, groupes cycliques

Exemples de groupes: $(\mathbb{Z},+)$, $(\mathbb{Z}/n\mathbb{Z},+)$, $(\mathbb{R}^*,\cdot)$, $(\mathbb{C}^*,\cdot)$, $(\{z\in\mathbb{C}\mid z^n=1\},\cdot)$, $(V,+)$ *(où V est un espace vectoriel), le groupe des automorphismes $Aut(V)$, le groupe symétrique S_n, le groupe alterné A_n, groupes des isométries, par exemple le groupe des isométries du carré*

G cyclique $\implies$ G abélien.

Exemples de sous-groupes: $n\mathbb{Z}\subset\mathbb{Z}$, $\mathbb{Q}_{>0}\subset\mathbb{R}^*$, $A_n\subset S_n$, $U(n)\subset Gl_n(\mathbb{C})$, $SO(n)\subset O(n)\subset GL_n(\mathbb{R})\subset GL_n(\mathbb{C})$

Présentation d'un groupe par générateurs et relations, table de multiplication

Groupe diédral

Homomorphisme, epimorphisme, monomorphisme, isomorphisme, automorphisme

Exemples: $det: GL_n(\mathbb{R})\to\mathbb{R}^*$, $sgn: S_n\to\{\pm1\}$, *conjugaison, application linéaire d'espaces vectoriels, projection* $\mathbb{Z}\to\mathbb{Z}/n\mathbb{Z}$, $SO(2)\cong S^1\cong\mathbb{R}/\mathbb{Z}$

Soit $\Phi: G\to H$ un homomorphisme. Alors: Φ injectif $\iff$ $\ker\Phi=\{e\}$

Kartesisches Produkt

Kleinsche Vierergruppe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

Ordnung eines Gruppe, $ord(G) = |G|$, *Ordnung eines Elements* $ord(g)$

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

G ist die disjunkte Vereinigung der Linksnebenklassen gH.

Der Index $(G : H)$

Theorem von Lagrange.
Die Ordnung einer Elements g teilt die Ordnung von G, $ord(g) \mid ord(G)$.
$ord(G)$ Primzahl $\implies$ G zyklisch.

Normalteiler, Faktorgruppe

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

Universelle Eigenschaft der Faktorgruppe. Die drei Isomorphiesätze und ihre Korollare.

Operation (oder Aktion) von G auf M, $G \times M \to M$

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

Orbit/Bahn Gm, Stabilisator/Isotropiegruppe G_m, Fixpunkte

G_m ist eine Untergruppe von G. M ist disjunkte Vereinigung der Orbiten. G endlich $\implies$ $|Gm| = (G : G_m)$

Produit cartésien

Groupe de Klein $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

L'ordre du groupe G, $ord(G) = |G|$, *l'ordre d'élément* $ord(g)$

Classe à gauche et à droite suivant H, *l'index* $(G : H)$ *de* H *dans* G

Les classes à gauche gH forment une partition de G.

L'indice $(G : H)$

Théorème de Lagrange.
L'ordre d'un élément g divise l'ordre de G, $ord(g) \mid ord(G)$.
$ord(G)$ premier $\implies$ G cyclique.

sous-groupe normal/distingué, groupe quotient

G/H groupe $\iff$ $xH = Hx \; \forall \; x \in G$ $\iff$ H sous-groupe normal.

Propriété universelle de groupe quotient. Les trois théorèmes d'isomorphisme et leurs corollaires.

Action de G sur M, $G \times M \to M$

Action de $GL_n(K)$ *sur* K^n, *action de* S_n, *action de* G *sur* G *par multiplication à gauche, ou par conjugaison, action de* $SL_2(\mathbb{R})$ *sur le demi-plan supérieur* $\mathcal{H}$

Orbite Gm, stabilisateur G_m, points fixes

G_m est un sous-groupe de G. Les orbites forment une partition de M. G fini $\implies$ $|Gm| = (G : G_m)$

Operation von S^1 auf $\mathbb{C}$ durch Multiplikation, 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, Operation von S_3 auf sich durch Konjugation

Action de S^1 sur $\mathbb{C}$ par multiplication, action de $GL_n(\mathbb{C})$ sur $M(n \times n, \mathbb{C})$ par conjugaison, relation avec la réduction de Jordan, action de $O(n)$ sur l'ensemble des matrices symétriques, action de S_3 sur lui-même par conjugaison

NORMALISATOR, ZENTRALISATOR, ZENTRUM

Bahnengleichung und Klassengleichung.

NORMALISATEUR, CENTRALISATEUR, CENTRE

Formule des orbites, formule des classes.

p-GRUPPEN

$ord(G) = p^n > 1 \implies$ das Zentrum $Z(G)$ ist nicht trivial.
$ord(G) = p^n \implies |M| \equiv |M^G| \bmod p$.

Theorem von Cauchy.
G endliche p-Gruppe $\Leftrightarrow$ $ord(G) = p^n$.

p-GROUPES

$ord(G) = p^n > 1 \implies$ le centre $Z(G)$ est non trivial.
$ord(G) = p^n \implies |M| \equiv |M^G| \bmod p$.

Théorème de Cauchy.
G un p-groupe fini $\iff$ $ord(G) = p^n$.

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 $\implies (N_G(U) : U) \equiv (G : U) \bmod p$.

Die drei Sylow-Sätze und ihre Korollare.

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

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

p-SOUS-GROUPE DE SYLOW

Sous-groupes de Sylow de S_3, de $\mathbb{Z}/pq\mathbb{Z}$, des groupes abéliens finis et des p-groupes

G groupe fini, U un p-sous-groupe $\implies (N_G(U) : U) \equiv (G : U) \bmod p$.

Les trois théorèmes de Sylow und leurs corollaires.

$ord(G) = pq$, $p > q$ deux nombres premiers et $q \nmid p - 1 \implies G$ cyclique.

$ord(G) = 15$ ou $ord(G) = 33 \implies G$ cyclique.

EINFACHE GRUPPEN

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

GROUPES SIMPLES

$ord(G) = p^2q$, $p \neq q$ deux nombres premiers $\implies G$ n'est pas simple.

Symmetrische Gruppe S_n, Signum sgn, altern. 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 $[G, G]$ (oder abgeleitete Gruppe), Normalreihe, 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 $\Longrightarrow$ $[G, G] \subset N$.

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

S_n und A_n sind für $n \leq 4$ auflösbar, Normalreihe für A_4 und für S_4.

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

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

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

Bilder und Untergruppen von auflösbaren Gruppen sind auflösbar.

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

A_n ist für $n \geq 5$ einfach (ohne Bew.).

Groupe symétrique S_n, signum sgn, groupe alterné A_n, inversions, transpositions, r-cycle
Théorème de Cayley.

Pour $n \geq 3$ A_n est l'ensemble des permutations qui sont des produits de 3-cycles.

Commutateur $[a, b]$, groupe des commutateurs (ou groupe dérivé) $[G, G]$, chaîne normale, facteurs, groupes résolubles, G^k

$[G, G]$ est normal dans G et $G/[G, G]$ est abélien.
N normal dans G et G/N abélien $\Longrightarrow$ $[G, G] \subset N$.

G résoluble $\Leftrightarrow G^k = \{e\}$ pour un k.

S_n et A_n sont résolubles pour $n \leq 4$, chaîne normale pour A_4 et pour S_4.

Autres exemples de groupes résolubles: groupes abéliens, p-groupes finis, $ord(G) = pq$ avec p, q premiers.

Théorème de Burnside (sans dém.): $ord(G) = p^a \cdot q^b \implies G$ résoluble.

Th. de Feit-Thompson (sans dém.): $ord(G)$ impair $\Longrightarrow$ G résoluble.

Tout sous-groupe et toute l'image d'un groupe résoluble est résoluble.

S_n est A_n ne sont pas résoluble pour $n \geq 5$.

A_n est simple pour $n \geq 5$ (sans dém.).

Ringtheorie

Ringe, kommutative Ringe, Einselement, Ringe mit 1

$\mathbb{Z}$, $2\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$, $M(n \times n, R)$, jeder Körper (zum Beispiel $\mathbb{Q}$, $\mathbb{R}$), Produkt von zwei Ringen, $\prod_{i \in I} R_i$, $Map(X, R)$, $\{a + b \cdot \sqrt{2} \mid a, b \in \mathbb{Q}\}$

Gruppe der Einheiten R^*, Nullteiler, Integritätsring, Unterring, Ringerweiterung, Charakteristik $char(R)$

Einheitengruppe R^* für $R = \mathbb{Z}$ und für $R = \mathbb{Z}/n\mathbb{Z}$, $n < 9$

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

Von nun an sind alle Ringe kommutativ mit 1!

Polynom von Grad n, Ring der Polynome $R[x]$, Grad-Funktion deg, normiertes Polynom

Euklidischer Algorithmus.

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

Ringhomomorphismus, Ideal I, Summe, Schnitt und Produkt von Idealen, Faktorring (oder Quotientenring) R/I

Universelle Eigenschaft des Faktorrings.

Théorie des anneaux

Anneaux, anneaux commutatifs, élément neutre, anneaux unitaires

$\mathbb{Z}$, $2\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$, $M(n \times n, R)$, chaque corps (par exemple $\mathbb{Q}$, $\mathbb{R}$), produit de deux anneaux, $\prod_{i \in I} R_i$, $Map(X, R)$, $\{a + b \cdot \sqrt{2} \mid a, b \in \mathbb{Q}\}$

groupe des unités (ou groupe des inversibles) R^*, diviseur de zéro, anneau intègre, sous-anneau, extension d'anneau, caractéristique $char(R)$

Groupe des unités R^* pour $R = \mathbb{Z}$ et pour $R = \mathbb{Z}/n\mathbb{Z}$, $n < 9$

R un anneau intègre $\implies$ $char(R) = 0$ ou $char(R) = p$, p premier.
$char(R) = p \implies (x + y)^p = x^p + y^p$ (homomorphisme de Frobenius).

À partir de maintenant, tous les anneaux sont commutatifs et unitaires!

Polynôme de degré n, anneau des polynômes $R[x]$, degré deg, polynôme unitaire

Algorithme d'Euclide.

Algorithme d'Euclide pour $f = [2]x^3 + [3]x + [1]$ et $g = [3]x^2 - x - [1] \in \mathbb{Z}/4\mathbb{Z}[x]$

Homomorphisme d'anneaux, idéal I, somme, intersection et produit des idéaux, anneau quotient R/I

Propriété universelle d'anneau quotient.

$\varphi : R \to R'$ Epimorphismus $\Longrightarrow$ $R' \cong R/ker(\varphi)$.

Einheitengruppe, Ideale, Faktorringe für $\mathbb{Z}$ und $\mathbb{Q}[x]$

m Primzahl
$\Longleftrightarrow$ $\mathbb{Z}/m\mathbb{Z}$ ist Integritätsring $\neq 0$
$\Longleftrightarrow$ $\mathbb{Z}/m\mathbb{Z}$ ist Körper.

Primideale, maximale Ideale

$\mathfrak{p} \subset R$ Primideal $\Longleftrightarrow$ $R/\mathfrak{p}$ Integritätsring.
$\mathfrak{m} \subset R$ maximal $\Longleftrightarrow$ $0 \subset R/\mathfrak{m}$ maximal $\Longleftrightarrow$ $R/\mathfrak{m}$ Körper.
$\mathfrak{m}$ maximal $\Longrightarrow$ $\mathfrak{m}$ 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 $\Longrightarrow$ R HIR.

Beispiele von Euklidischen Ringen: $\mathbb{Z}$ *mit Grad* $deg(a) := |a|$,
$K[x]$ *mit Grad* $deg(f) :=$ *Grad des Polynoms,*
$\mathbb{Z}[i]$ *mit Grad* $deg(a + ib) := a^2 + b^2$ *(Ring der ganzen Gaussschen Zahlen)*

assoziierte Elemente, grösster gemeinsamer Teiler (ggT), kleinstes gemeinsames Vielfaches (kgV)

Lemma von Bézout.

Bestimmung des ggT mit dem euklidischen Algorithmus.

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

$\varphi : R \to R'$ epimorphisme $\Longrightarrow$ $R' \cong R/ker(\varphi)$.

Groupe des unités, idéaux, anneaux quotients pour $\mathbb{Z}$ et $\mathbb{Q}[x]$

m nombre premier
$\Longleftrightarrow$ $\mathbb{Z}/m\mathbb{Z}$ est un anneau intègre $\neq 0$
$\Longleftrightarrow$ $\mathbb{Z}/m\mathbb{Z}$ est un corps.

Idéaux premiers, idéaux maximaux

$\mathfrak{p} \subset R$ idéal premier $\Longleftrightarrow$ $R/\mathfrak{p}$ anneau intègre.
$\mathfrak{m} \subset R$ maximal $\Longleftrightarrow$ $0 \subset R/\mathfrak{m}$ maximal $\Longleftrightarrow$ $R/\mathfrak{m}$ corps.
$\mathfrak{m}$ maximal $\Longrightarrow$ $\mathfrak{m}$ idéal premier.

Idéaux premiers et max. dans $R = \mathbb{Z}$, idéaux max. dans $R = C([0,1], \mathbb{R})$

Anneaux pricipaux, anneaux euclidiens, degré/norme *deg*

R euclidien $\Longrightarrow$ R principal.

Exemples d'anneaux euclidiens: $\mathbb{Z}$ *muni du degré* $deg(a) := |a|$,
$K[x]$ *muni du degré* $deg(f) :=$ *degré de polynôme,*
$\mathbb{Z}[i]$ *muni du degré* $deg(a+ib) := a^2+b^2$ *(anneau des entiers de Gauss)*

Éléments associés, plus grand commun diviseur (PGCD), plus petit commun multiple (PPCM)

Identité de Bézout.

Determination du PGCD avec l'algorithme d'Euclide.

Determination du $PGCD(42, 642) \in \mathbb{Z}$ avec l'algorithme d'Euclide.

teilerfremde/koprime Elemente, koprime Ideale

Chinesischer Restsatz.

Lösungsmenge der Kongruenzen $x \equiv x_i \bmod a_i$, $i = 1, \ldots, n$, *in* $\mathbb{Z}$

irreduzible Elemente, Primelemente

R Integritätsring, $p \in R$, $p \neq 0$. Dann gilt: (p) maximales Ideal $\Longrightarrow$ p Primelement $\Longrightarrow$ p irreduzibel.

R Integritätsring und HIR, $p \in R$, $p \neq 0$, $p \notin R^*$. Dann gilt:
p irreduzibel $\Longleftrightarrow$ p Primelement $\Longleftrightarrow$ (p) maximales Ideal.

Primelement und irreduzible Elemente in $R = \mathbb{C}[x]$ *und in* $R = \mathbb{Z}[\sqrt{-5}]$

noethersche Ringe

Jeder HIR ist noethersch.

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

faktorielle Ringe

Äquivalente Beschreibungen (Th. 2.57)

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

R Integritätsring und HIR $\Longrightarrow$ R faktoriell.

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

Éléments premiers entre eux/copremiers, idéaux copremiers

Théorème des restes chinois.

L'ensemble des solutions des congruences $x \equiv x_i \bmod a_i$, $i = 1, \ldots, n$, *dans* $\mathbb{Z}$

Éléments irréductibles, éléments premiers

R un anneau intègre, $p \in R$, $p \neq 0$. Alors: (p) idéal maximal $\Longrightarrow$ p élément premier $\Longrightarrow$ p irréductible.

R un anneau intègre principal, $p \in R$, $p \neq 0$, $p \notin R^*$. Alors:
p irréductible $\Longleftrightarrow$ p élément premier $\Longleftrightarrow$ (p) idéal maximal.

Les éléments premiers et irréductibles dans $R = \mathbb{C}[x]$ *et dans* $R = \mathbb{Z}[\sqrt{-5}]$

Anneaux noethériens

Tout anneau principal est noethérien.

R un anneau intègre principal et $a \in R - \{R^* \cup \{0\}) \Longrightarrow$ a est un produit d'éléments premiers.

anneaux factoriels

Caractérisations équivalentes (Th. 2.57)

R anneau factoriel, $r \in R$. Alors on a: r irréductible $\Longleftrightarrow$ r premier.

R un anneau intègre principal $\Longrightarrow$ R factoriel.

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

Hauptsatz der elementaren Zahlentheorie.

Théorème fondamental de l'arithmétique.

GgT und kgV in einem faktoriellen Ring.

PGCD et PPCM dans un anneau factoriel.

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

R factoriel $\Longrightarrow$ tout $f \in R[x]$, $f \neq 0$, $f \notin R[x]^*$, est un produit de polynômes irréductibles.

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

R anneau intègre, $p \in R$ premier $\Longrightarrow$ p premier dans $R[x]$.

Theorem von Gauss:
R faktoriell $\Longrightarrow$ $R[x]$ faktoriell.

Théorème de Gauss:
R factoriel $\Longrightarrow$ $R[x]$ factoriel.

R faktoriell (zum Beispiel $R = \mathbb{Z}$ oder R ein Körper) $\Rightarrow$ $R[x_1, \ldots, x_n]$ faktoriell.

R factoriel (par exemple $R = \mathbb{Z}$ ou R un corps) $\Rightarrow$ $R[x_1, \ldots, x_n]$ factoriel.

Integritätsringe, die faktoriell, aber nicht HIR sind.

Anneaux intègres factoriels, qui ne sont par principal.

Eisensteinsches Irreduzibilitätskriterium.

Critère d'Eisenstein.

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

$x^3 + 2$ est irréductible dans $\mathbb{Z}[x]$.

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

S PARTIE MULTIPLICATIVE S, LOCALISIERUNG DE L'ANNEAU R EN LA PARTIE S: $S^{-1}R$, ANNEAU LOCAL R_I, CORPS DES FRACTIONS $Q(R)$

R faktorieller Ring $\Longrightarrow$ $S^{-1}R$ faktorieller Ring (nur die Beweisidee).

R anneau factoriel $\Longrightarrow$ $S^{-1}R$ anneau factoriel (l'idée de la dém.).

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

R factoriel, $S \subset R$ partie multiplicative. Soit $f \in R[x]$ de degré ≥ 1. Alors: f irréductible in $R[x]$ $\Longrightarrow$ f irréductible in $(S^{-1}R)[x]$.

Für p eine Primzahl ist $x^n - p$ irreduzibel in $\mathbb{Q}[x]$. $x^2+y^3+z^n$ ist irreduzibel in $K(x, y)[z]$

Pour p un nombre premier est $x^n - p$ irréductible dans $\mathbb{Q}[x]$. $x^2+y^3+z^n$ est irréductible dans $K(x, y)[z]$

R-Modul, unitärer Modul, Modul-Homomorphismus, Untermodul, Faktormodul/Quotientenmodul, zyklischer/Hauptmodul

R-module, module unitaire, homomorphisme de modules, sous-module, module quotient, module principal/cyclique

Isomorphiesatz.

Théorème d'isomorphisme.

endlich erzeugter Modul, Basis, freier Modul, Dimension

module de type fini, base, module libre, dimension

Von nun an sind alle Ringe Integritätsringe und HIR!

À partir de maintenant, tous les anneaux sont intègre et principal!

F freier endlich erzeugter R-Modul, M Untermodul $\Longrightarrow$ M ist frei und $\dim M \leq \dim F$.

F R-module libre de type fin, M sous-module $\Longrightarrow$ M est libre et $\dim M \leq \dim F$.

M endlich erzeugter R-Modul, $\tilde{M}$ Untermodul $\Longrightarrow$ $\tilde{M}$ endlich erzeugt.

M un R-module de type fini, $\tilde{M}$ sous-module $\Longrightarrow$ $\tilde{M}$ de type fini.

Torsionselement, Torsionsmodul, torsionsfreier Modul, Rang, unabhängige Elemente

Élément de torsion, module de torsion, module sans torsion, rang, éléments indépendants

Jeder endlich erzeugte R-Modul E ist die direkte Summe des Torsionsuntermoduls E_{tor} und eines freien Untermoduls F.

Tout R-module E de type fini est la somme directe de sous-module de torsion E_{tor} et d'un sous-module libre F.

Klassifikation von endlich erzeugten abelschen Gruppen.

Classification des groupes abéliens de type fini.

Klassifikation von endlich erzeugten unitären R-Moduln (nur Beweisidee).

Classification des R-modules unitaires de type fini (l'idée de la dém.).

Körpertheorie

Charakteristik eines Körpers, Homomorphismen, Isomorphismen, Unterkörper, Körpererweiterung

Endliche Körpererweiterung $K \subset L$, Grad $[L : K]$

$\mathbb{R} \subset \mathbb{C}$, $\mathbb{Q} \subset \mathbb{R}$

Gradsatz.

algebraische Elemente, algebraische Erweiterung, transzendente Elemente, transzendente Erweiterung, algebraische und transzendente Zahlen

Die Menge aller algebraischen Zahlen ist abzählbar.
Jedes nicht-leere Intervall besitzt überabzählbar viele transzendente Zahlen.

π und e sind transzendente Zahlen (ohne Bew.).

Minimalpolynom eines algebraischen Elements $\alpha \in L$ über K.

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

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

Endliche Körpererweiterungen sind algebraisch.

$K(\alpha_1, \ldots, \alpha_n)$, endlich erzeugte Erweiterungen

Théorie de corps

Caractéristique d'un corps, homomorphisme, isomorphisme, sous-corps, extension de corps

Extension finie $K \subset L$, degré $[L : K]$

$\mathbb{R} \subset \mathbb{C}$, $\mathbb{Q} \subset \mathbb{R}$

Théorème du degré.

élément algébrique, extension algébrique, élément transcendant, extension transcendant, nombre algébrique, nombre transcendant

L'ensemble des nombres algébriques est dénombrable.
Dans tout intervalle non vide l'ensemble des nombres transcendant est indénombrable.

π und e sont transcendants (sans dém.).

Polynôme minimal d'un élément algébrique $\alpha \in L$ sur K.

Polynôme minimal $f \in K[x]$ est premier. $K[x]/(f)$ est un corps $\cong K[\alpha]$ et $[K[\alpha] : K] = deg(f)$.

$\mathbb{R}[x]/(x^2 + 1)$, $\mathbb{Q}[\sqrt[n]{p}]$, *p un nombre premier.*

Toute extension de corps finie est algébrique.

$K(\alpha_1, \ldots, \alpha_n)$, extension de type fini

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

$L = K(\alpha_1, \ldots, \alpha_n)$, tous α_i sont algébriques sur $K \implies$
$L = K[\alpha_1, \ldots, \alpha_n]$ et $[L : K] < \infty$.

$(17 + \sqrt[3]{5})^5 - 4 \cdot \sqrt{7}$ *ist algebraisch über* $\mathbb{Q}$.

$(17 + \sqrt[3]{5})^5 - 4 \cdot \sqrt{7}$ *est algébrique sur* $\mathbb{Q}$.

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

$K \subset L$ finie $\iff$ L est une extension sur K engendrée par un nombre fini des éléments algébriques $\iff$ $K \subset L$ est une extension algébrique engendrée par un nombre fini des éléments (sans dém.).

$K \subset L$ algebraische Körpererweiterung $\iff$ L wird über K von algebraischen Elementen erzeugt (ohne Beweis).

$K \subset L$ une extension algébrique $\iff$ L est une extension engendrée sur K par des éléments algébriques (sans dém.).

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

$K \subset L$ une extension algébrique, $L \subset M$ une extension et $\alpha \in M$ algébrique sur L. Alors, α est aussi algébrique sur K.

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

$K \subset L \subset M$ extensions de corps. Alors on a: M est algébrique sur K $\iff$ M est algébrique sur L et L est algébrique sur K.

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

CORPS ALGÉBRIQUEMENT CLOS, CLÔTURE ALGÉBRIQUE $\overline{K}$ DE K

$\mathbb{C}$ *ist algebraisch abgeschlossen.*

$\mathbb{C}$ *est algébriquement clos.*

Jeder Körper besitzt einen algebraischen Abschluss (ohne Beweis).

Tout corps a une clôture algébrique (sans dém.).

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

$\overline{\mathbb{R}} = \mathbb{C}$, $\overline{\mathbb{Q}} \subset \mathbb{C}$ *est le corps des nombres algébriques,* $\overline{\mathbb{F}}_p$

Konstruktion mit Zirkel und Lineal, erlaubte Operationen, konstruierbare Zahlen	Construction à la règle et au compas, opérations permettent, nombres constructibles
$\hat{M}$, $c(M)$	$\hat{M}$, $c(M)$
$M \subset \mathbb{C}$, $0,1 \in M \implies$ die Menge $\hat{M}$ der aus M konstruierbaren Zahlen ist ein Unterkörper von $\mathbb{C}$.	$M \subset \mathbb{C}$, $0,1 \in M \implies$ l'ensemble $\hat{M}$ de nombres qu'on peut construire à partir de M est un sous-corps de $\mathbb{C}$.
$M \subset \mathbb{C}$, $0,1 \in M \implies \mathbb{Q} \subset \hat{M}$.	$M \subset \mathbb{C}$, $0,1 \in M \implies \mathbb{Q} \subset \hat{M}$.
$z \in \hat{M} \iff$ es gibt eine Kette von Körpererweiterungen $L_0 \subset L_1 \subset \ldots \subset L_n \subset \mathbb{C}$ mit $L_0 := \mathbb{Q}(M \cup c(M))$, $z \in L_n$, $c(L_i) = L_i$ und $[L_{i+1} : L_i] \leq 2$ für alle i.	$z \in \hat{M} \iff$ il existe une chaîne des extensions de corps $L_0 \subset L_1 \subset \ldots \subset L_n \subset \mathbb{C}$ avec $L_0 := \mathbb{Q}(M \cup c(M))$, $z \in L_n$, $c(L_i) = L_i$ et $[L_{i+1} : L_i] \leq 2$ pour tout i.
$\hat{M}$ ist quadratisch abgeschlossen, d.h. $\omega \in \hat{M} \implies \sqrt{\omega} \in \hat{M}$.	$\hat{M}$ est clos par l'extension quadratique, c.-à-d. $\omega \in \hat{M} \implies \sqrt{\omega} \in \hat{M}$.
z aus M konstruierbar $\implies$ $[\mathbb{Q}(M \cup c(M))(z) : \mathbb{Q}(M \cup c(M))] = 2^l$.	z constructible à partir de $M \implies$ $[\mathbb{Q}(M \cup c(M))(z) : \mathbb{Q}(M \cup c(M))] = 2^l$.
Würfel mit doppeltem Volumen ist nicht konstruierbar.	Il n'est pas possible de construire un cube de volume double.
Quadratur des Kreises ist nicht möglich.	Il n'est pas possible de construire la quadrature du cercle.
Dreiteilung des Winkels ist im Allgemeinen nicht möglich (ohne Beweis).	Il n'est pas possible de partager un angle quelconque en trois parties égales (sans dém.).