

Prüfungsstoff Algebra

(Algebra & Geometrie I, 2011)

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

Es folgt eine unvollständige Liste von DEFINITIONEN, *Beispielen* und **Theoremen** aus der Algebra Vorlesung:

Gruppentheorie

GRUPPEN, MONOIDE, ABELSCHES GRUPPEN, UNTERGRUPPEN, ZYKLISCHE GRUPPEN

Beispiele von Gruppen: $(\mathbb{Z}, +)$, $(\mathbb{Z}/n\mathbb{Z}, +)$, (\mathbb{R}^*, \cdot) , $(V, +)$ (wo V ein Vektorraum ist), die Automorphismengruppe $\text{Aut}(V)$, 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

HOMOMORPHISMUS, EPIMORPHISMUS, MONOMORPHISMUS, ISOMORPHISMUS, AUTOMORPHISMUS

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

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

KARTESISCHES PRODUKT

Théorie des groupes

GROUPES, MONOÏDES, GROUPES ABÉLIENS, SOUS-GROUPES, GROUPES CYCLIQUES

Exemples de groupes: $(\mathbb{Z}, +)$, $(\mathbb{Z}/n\mathbb{Z}, +)$, (\mathbb{R}^*, \cdot) , $(V, +)$ (où V est un espace vectoriel), le groupe des automorphismes $\text{Aut}(V)$, 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

HOMOMORPHISME, EPIMORPHISME, MONOMORPHISME, ISOMORPHISME, AUTOMORPHISME

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

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

PRODUIT CARTÉSIEN

<i>Kleinsche Vierergruppe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$</i>	<i>Groupe de Klein $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$</i>
<i>Ordnung eines Gruppe, $ord(G) = G$, Ordnung eines Elements $ord(g)$</i>	<i>L'ordre du groupe G, $ord(G) = G$, l'ordre d'élément $ord(g)$</i>
<i>Links- und Rechtsnebenklassen von H, Index $(G : H)$ von H in G</i>	<i>Classe à gauche et à droite suivant H, l'index $(G : H)$ de H dans G</i>
<i>G ist die disjunkte Vereinigung der Linksnebenklassen gH.</i>	<i>Les classes à gauche gH forment une partition de G.</i>
<i>Theorem von Lagrange. Die Ordnung einer Elements g teilt die Ordnung von G, $ord(g) \mid ord(G)$. $ord(G)$ Primzahl $\implies G$ zyklisch.</i>	<i>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.</i>
NORMALTEILER, FAKTORGRUPPE	SOUS-GROUPE NORMAL/DISTINGUÉ, GROUPE QUOTIENT
<i>G/H Gruppe $\iff xH = Hx \forall x \in G$ $\iff H$ Normalteiler.</i>	<i>G/H groupe $\iff xH = Hx \forall x \in G$ $\iff H$ sous-groupe normal.</i>
<i>Universelle Eigenschaft der Faktor- gruppe. Die drei Isomorphiesätze und ihre Korollare.</i>	<i>Propriété universelle de grou- pe quotient. Les trois théorèmes d'isomorphisme et leurs corollaires.</i>
OPERATION (ODER AKTION) VON G AUF M, $G \times M \rightarrow M$	ACTION DE G SUR M, $G \times M \rightarrow M$
<i>Operation von $GL_n(K)$ auf K^n, Ope- ration 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}</i>	<i>Action de $GL_n(K)$ sur K^n, action de S_n, action de G sur G par mul- tiplication à gauche, ou par conjuga- ison, action de $SL_2(\mathbb{R})$ sur le demi-plan supérieur \mathcal{H}</i>
ORBIT/BAHN Gm, STABILISATOR/ISO- TROPIEGRUPPE G_m, FIXPUNKTE	ORBITE Gm, STABILISATEUR G_m, POINTS FIXES
<i>G_m ist eine Untergruppe von G. M ist disjunkte Vereinigung der Orbits.</i>	<i>G_m est un sous-groupe de G. Les orbi- tes forment une partition de M.</i>
<i>Operation von S^1 auf \mathbb{C} durch Mul- tiplikation, Operation von $GL_n(\mathbb{C})$ auf $M(n \times n, \mathbb{C})$ durch Konjugation, Beziehung zur Jordan-Normalform,</i>	<i>Action de S^1 sur \mathbb{C} par multi- plication, action de $GL_n(\mathbb{C})$ sur $M(n \times n, \mathbb{C})$ par conjugaison, rela- tion avec la réduction de Jordan,</i>

Operation von $O(n)$ auf den symmetrischen Matrizen, Operation von S_3 auf sich durch Konjugation

Action de $O(n)$ sur l'ensemble des matrices symétriques, action de S_3 sur lui-même par conjugaison

NORMALISATOR, ZENTRALISATOR, ZENTRUM

NORMALISATEUR, CENTRALISATEUR, CENTRE

Bahngleichung und Klassengleichung.

Formule des orbites, formule des classes.

p -GRUPPEN

p -GROUPES

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

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

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

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

p -SYLOWGRUPPEN

p -SOUS-GROUPE DE SYLOW

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

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

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

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

Die drei Sylow-Sätze und ihre Korollare.

Les trois théorèmes de Sylow und leurs corollaires.

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

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

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

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

EINFACHE GRUPPEN

GROUPES SIMPLES

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

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

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

GROUPE SYMÉTRIQUE S_n , SIGNUM $sign$, GROUPE ALTERNÉ A_n , INVERSIONS, TRANSPOSITIONS, r -CYCLE

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 $\implies [G, G] \subset N$.

G auflösbar $\iff G^k = \{e\}$ 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, $\text{ord}(G) = pq$ mit p, q Primzahlen.

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

Th. von Feit-Thompson (ohne Bew.): $\text{ord}(G)$ ungerade $\implies G$ 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.).

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 $\implies [G, G] \subset N$.

G résoluble $\iff G^k = \{e\}$ 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, $\text{ord}(G) = pq$ avec p, q premiers.

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

Th. de Feit-Thompson (sans dém.): $\text{ord}(G)$ impair $\implies G$ résoluble.

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

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

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

Ringtheorie

RINGE, KOMMUTATIVE RINGE, EINS-ELEMENT, 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, $\prod_{i \in I} R_i$, $\text{Map}(X, R)$, $\{a + b \cdot \sqrt{2} \mid a, b \in \mathbb{Q}\}$

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

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

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!

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 Faktoringes.

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, $\prod_{i \in I} R_i$, $\text{Map}(X, R)$, $\{a + b \cdot \sqrt{2} \mid a, b \in \mathbb{Q}\}$

GROUPE DES UNITÉS (OU GROUPE DES INVERSIBLES) R^* , DIVISEUR DE ZÉRO, ANNEAU INTÈGRE, SOUS-ANNEAU, EXTENSION D'ANNEAU, CARACTÉRISTIQUE $\text{char}(R)$

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

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

A 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.

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

Einheitengruppe, Ideale, Faktorringe für \mathbb{Z} und $\mathbb{Q}[x]$ *Groupe des unités, idéaux, anneaux quotients pour \mathbb{Z} et $\mathbb{Q}[x]$*

m Primzahl $\iff \mathbb{Z}/m\mathbb{Z}$ ist Integritätsring $\neq 0$
 $\iff \mathbb{Z}/m\mathbb{Z}$ ist Körper. m nombre premier
 $\iff \mathbb{Z}/m\mathbb{Z}$ est un anneau intègre $\neq 0$
 $\iff \mathbb{Z}/m\mathbb{Z}$ est un corps.

PRIMIDEALE, MAXIMALE IDEALE IDÉAUX PREMIERS, IDÉAUX MAXIMAUX

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

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

HAUPTIDEALRINGE (HIR), EUKLIDISCHE RINGE, GRAD/NORMABB. deg ANNEAUX PRINCIPAUX, ANNEAUX EUCLIDIENS, DEGRÉ/NORME deg

R euklidisch $\implies R$ HIR. R euclidien $\implies R$ principal.

Beispiele von Euklidischen Ringen: \mathbb{Z} mit Grad $\deg(a) := |a|$,
 $K[x]$ mit Grad $\deg(f) := \text{Grad des Polynoms}$,
 $\mathbb{Z}[i]$ mit Grad $\deg(a + ib) := a^2 + b^2$ (Ring der ganzen Gauss'schen Zahlen) Exemples d'anneaux euclidiens: \mathbb{Z} muni du degré $\deg(a) := |a|$,
 $K[x]$ muni du degré $\deg(f) := \text{degré de polynôme}$,
 $\mathbb{Z}[i]$ muni du degré $\deg(a+ib) := a^2+b^2$ (anneau des entiers de Gauss)

ASSOZIIERTE ELEMENTE, GRÖSSTER GEMEINSAMER TEILER (GGT), KLEINSTES GEMEINSAMES VIELFACHES (KGV) ÉLÉMENTS ASSOCIÉS, PLUS GRAND COMMUN DIVISEUR (PGCD), PLUS PETIT COMMUN MULTIPLE (PPCM)

Lemma von Bézout. Identité de Bézout.

Bestimmung des ggT mit dem euklidischen Algorithmus. Dtermination du PGCD avec l'algorithme d'Euclide.

Bestimmung von $\text{ggT}(42, 642) \in \mathbb{Z}$ mit dem euklidischen Algorithmus. *Determination du PGCD(42, 642) $\in \mathbb{Z}$ avec l'algorithme d'Euclide.*

TEILERFREMDE/KOPRIME TE, KOPRIME IDEALE	ELEMENTE	ÉLÉMENTS EUX/COPREMIERS, IDÉAUX COPREMIERS	PREMIERS ENTRE COPREMIERS
--	----------	--	---------------------------------

Chinesischer Restsatz.

Théorème des restes chinois.

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

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

IRREDUZIBLE ELEMENTE, PRIMELEMENTE

ÉLÉMENTS IRRÉDUCTIBLES, ÉLÉMENTS PREMIERS

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

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

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

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

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

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

NOETHERSCHE RINGE

ANNEAUX NOETHÉRIENS

Jeder HIR ist noethersch.

Tout anneau principal est noethérien.

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

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

FAKTORIELLE RINGE

ANNEAUX FACTORIELS

Äquivalente Beschreibungen (Th. 2.57)

Caractérisations équivalentes (Th. 2.57)

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

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

R Integritätsring und HIR $\implies R$ faktoriell.

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

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

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

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

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

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

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

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

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

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

Integritätsringe, die faktoriell, aber nicht HIR sind.

Anneaux intègres factoriels, qui ne sont pas 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 $\implies S^{-1}R$ faktorieller Ring (nur die Beweisidee).

R anneau factoriel $\implies S^{-1}R$ 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 $R[x] \implies f$ irreduzibel in $(S^{-1}R)[x]$.

R factoriel, $S \subset R$ partie multiplikative. Soit $f \in R[x]$ de degré ≥ 1 . Alors: f irréductible in $R[x] \implies f$ 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, R -MODULE, MODULE UNITAIRE, HOMOMORPHISMUS, UNTERMODUL, FAKTORMODUL/QUOTIENTENMODUL, ZYKLISCHER/HAUPTMODUL, 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 R Integritätsringe und HIR!

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

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

F R -module libre, M sous-module $\implies M$ est libre et $\dim M \leq \dim F$.

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

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

TORSIONSELEMENT, TORSIONSMODUL, TORSIONSFREIER MODUL

ÉLÉMENT DE TORSION, MODULE DE TORSION, MODULE SANS TORSION

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 und endlich erzeugten unitären R -Moduln.

Classification des groupes abéliens de type fini et de R -modules unitaires de type fini.

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, TRANSCENDENTE ELEMENTE, TRANSCENDENTE ERWEITERUNG, ALGEBRAISCHE UND TRANSCENDENTE 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 $[K[\alpha] : K] = \deg(f)$.

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

Endliche Körpererweiterungen sind algebraisch.

$K(\alpha_1, \dots, \alpha_n)$, EINFACHE ERWEITERUNGEN, 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 ALGÈBRE, EXTENSION ALGÈBRE, ÉLÉMENT TRANSCENDANT, EXTENSION TRANSCENDANT, NOMBRE ALGÈBRE, NOMBRE TRANSCENDANT

L'ensemble des nombres algébriques est dénombrable.

Dans tout intervalle non vide l'ensemble des nombres transcendants est indénombrable.

π und e sont transcendants (sans dém.).

POLYNÔME MINIMAL D'UN ÉLÉMENT ALGÈBRE $\alpha \in L$ SUR K .

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

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

Toute extension de corps finie est algébrique.

$K(\alpha_1, \dots, \alpha_n)$, EXTENSION SIMPLE, EXTENSION DE TYPE FINI

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

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

$17 + \sqrt[3]{5} + 4 \cdot (\sqrt[3]{5})^2$ ist algebraisch über \mathbb{Q} .

$17 + \sqrt[3]{5} + 4 \cdot (\sqrt[3]{5})^2$ 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.

$K \subset L$ 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.

$K \subset L$ algebraische Körpererweiterung $\iff L$ wird über K von algebraischen Elementen erzeugt.

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

$K \subset L$ 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 VON K IN L , ALGEBRAISCHER ABSCHLUSS \overline{K} VON K

CORPS ALGÈBRIQUEMENT CLOS, CLÔTURE ALGÈBRIQUE DE K DANS L , CLÔTURE ALGÈBRIQUE \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

$M \subset \mathbb{C}, 0, 1 \in M \implies$ 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 $L_0 \subset L_1 \subset \dots \subset L_n \subset \mathbb{C}$ 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 $L_0 \subset L_1 \subset \dots \subset L_n \subset \mathbb{C}$ 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.

Il n'est pas possible de partager un angle quelconque en trois parties égales.

Konstruktion von $e^{2\pi i/p}$.

Construction de $e^{2\pi i/p}$.

RADIKALERWEITERUNGEN, AUFLÖSEN DURCH RADIKALE

EXTENSION PAR RADICAUX, RÉOLUTION PAR RADICAUX

Auflösen der allgemeinen Gleichung vom Grad 2 durch Radikale, Cardanische Formeln für Grad 3

Résolution d'équation générale de degré 2 par radicaux, formules de Cardan pour degré 3

AUTOMORPHISMEN EINER KÖRPERERWEITERUNG, GALOISGRUPPE EINES POLYNOMS.

AUTOMORPHISMES D'EXTENSION DE CORPS, GROUPE DE GALOIS D'UN POLYNÔME.

Ausblick: Galoisgruppe auflösbar versus Gleichung auflösbar.

Perspective: groupe de Galois résoluble versus équation générale résoluble.