Algebra und Diskrete Mathematik, PS3

Sommersemester 2017

Prüfungsfragen

- Erläutern Sie die Sätze über die Division mit Rest für ganze Zahlen und für Polynome (mit Koeffizienten in einem Körper). Wodurch unterscheiden sich die entsprechenden Divisionsalgorithmen? Warum ist dieser Unterschied notwendig?

- Was besagt der Satz über die Zifferndarstellung (zur Basis $b > 1$) einer ganzen Zahl? Wie kann man diese Ziffern berechnen? Erläutern Sie, wie man die Zifferndarstellung von Zahlen zur Basis $b > 1$ benutzen kann, um die Zifferndarstellung des ganzzahligen Quotienten und des Restes einer natürlichen Zahl nach Division mit Rest durch eine andere zu berechnen.

- Berechnet man die Zifferndarstellung zur Basis b des Produktes von zwei natürlichen Zahlen in Zifferndarstellung zur Basis b, muss zuerst das „kleine Einmaleins“eingeübt werden. Was muss analog bei der Addition, der Subtraktion, der Division mit Rest eingeübt werden?

- Was ist der Quotientenkörper des Ringes der ganzen Zahlen und des Polynomringes über einem Körper? Welche Eigenschaften muss ein Ring haben, damit die Konstruktion eines Quotientenkörpers möglich ist? Wie werden dann die Rechenoperationen definiert? Hat der kommutative Ring aller Funktionen von $\mathbb{R}$ nach $\mathbb{R}$ einen Quotientenkörper?

- Wie kann die Zifferndarstellung einer rationalen Zahl näherungsweise berechnet werden? Was ist eine rationale Zahl in Exponentialform zu einer Basis b? Was ist eine Maschinenzahl?

- Was ist der größte gemeinsame Teiler von zwei ganzen Zahlen bzw. von zwei Polynomen mit Koeffizienten in einem Körper? Wie kann dieser berechnet werden? Beweisen Sie, dass dieses Verfahren nach endlich vielen Schritten zum richtigen Ergebnis führt. Was bedeutet es, eine rationale Zahl oder eine rationale Funktion bestmöglich zu kürzen? Gibt es von zwei rationalen Zahlen einen größten gemeinsamen Teiler?

- Was sind Dezimalzahlen? Beweisen Sie, dass die Menge der Dezimalzahlen ein Unterring des Körpers der rationalen Zahlen ist. Ist der Quotient von Dezimalzahlen ($\neq 0$) wieder eine Dezimalzahl? Erklären Sie das Verfahren zur Multiplikation von zwei Dezimalzahlen in Zifferndarstellung.

- Was ist das kleinste gemeinsame Vielfache von zwei ganzen Zahlen bzw. zwei Polynomen mit Koeffizienten in einem Körper? Wie kann man es berechnen? Verwenden Sie den erweiterten euklidischen Algorithmus, um die Korrektheit dieses Verfahrens zu beweisen.

- Es seien drei ganze Zahlen a, b, c gegeben. Unter welchen Voraussetzungen an a, b, c gibt es ein Paar (x, y) von ganzen Zahlen mit $ax + by = c$? Beweisen Sie Ihre Behauptung. Erklären Sie, wie ein solches Paar berechnet werden kann. Welche „Strategie“ wird dafür verwendet?

- Was ist eine Primzahl, was ist ein irreduzibles Polynom in einem Polynomring mit Koeffizienten in einem Körper ? Beweisen Sie, dass die Zerlegung einer ganzen Zahl > 1 bzw. eines Polynoms vom Grad ≥ 1 in irreduzible Faktoren eindeutig ist. Brauchen Sie dazu den erweiterten euklidischen Algorithmus?

- Beweisen Sie: Der größte gemeinsame Teiler zweier positiver ganzer Zahlen > 1 ist das Produkt der gemeinsamen Primfaktoren. Warum soll man den ggT nur dann so berechnen, wenn die zwei Zahlen schon als Produkt von Primzahlen gegeben sind?

- Wie ist der Restklassenring $\mathbb{Z}_n$ für $n > 1$ definiert? Für welche Zahlen n ist dieser Ring ein Körper? Beweisen Sie Ihre Behauptung. Wie dividiert man in diesem Körper? Begründen Sie: Eine ganzen Zahl wird genau dann von 9 geteilt, wenn ihre Ziffernsumme von 9 geteilt wird.

- Formulieren und beweisen Sie den kleinen Satz von Fermat. Welche Bedeutung hat dieser für das RSA-Verfahren?

- Erläutern Sie das RSA-Verfahren. Welche Rolle spielt dabei der kleine Satz von Fermat?

- Was ist eine Polynomfunktion, was ist ein Polynom? Unter welcher Bedingung an den Koeffizientenkörper sind die Koeffizienten einer Polynomfunktion durch diese eindeutig bestimmt? Beweisen Sie Ihre Behauptung.

- Wie sind die Addition, die Multiplikation mit Elementen von K und die Multiplikation von Polynomen bzw. von Polynomfunktionen mit Koeffizienten in einem Körper K definiert? Welche Rechenregeln gelten dafür? Wie können diese in zwei Worten zusammengefasst werden?

- Unter welchen Bedingungen an den Koeffizientenkörper kann der Grad einer Polynomfunktion definiert werden? Wie verhält sich der Grad, wenn Polynome addiert oder multipliziert werden? Welche Polynome mit Koeffizienten in einem Körper sind invertierbar?

- Zeigen Sie: Die Familie $((x-1)^i)_{i\in\mathbb{N}}$ ist eine R-Basis des Polynomrings $R[x]$ mit Koeffizienten in einem Ring R.

- Was ist eine Nullstelle in einem Körper K eines Polynoms in $K[x]$? Beweisen Sie: Ein Element $a \in K$ ist genau dann eine Nullstelle eines Polynoms, wenn dieses von $x - a$ geteilt wird. Folgern Sie daraus: Jedes von 0 verschiedene Polynom f hat höchstens $gr(f)$ Nullstellen in K.

- Erläutern Sie die Methoden von Lagrange und von Newton zur Interpolation durch Polynomfunktionen. Welche Strategien werden dabei verfolgt?

- Was ist ein Ideal in einem kommutativen Ring? Welche Ideale gibt es in $\mathbb{Z}$, welche in $\mathbb{Q}[x]$? Beweisen Sie Ihre Behauptungen.

- Wie findet man die gemeinsamen Nullstellen von zwei Polynomen mit Koeffizienten in einem Körper? Wie bestimmt man die Anzahl der (paarweise verschiedenen) komplexen Nullstellen eines Polynoms mit komplexen Koeffizienten? Begründen Sie Ihre Behauptung.

- Zeigen Sie: In jedem Polynomring über einem Körper gibt es unendlich viele normierte irreduzible Polynome. Folgern Sie daraus: Wenn der Körper K endlich ist, gibt es zu jeder natürlichen Zahl n irreduzible Polynome in $K[x]$, deren Grad größer als n ist.

- Was ist eine irreduzibles Polynom? Welche Kriterien kennen Sie, um zu entscheiden, ob ein Polynom in $\mathbb{Z}[x]$, in $\mathbb{Q}[x]$, in $\mathbb{R}[x]$, in $\mathbb{C}[x]$ irreduzibel ist? Begründen Sie: Jedes reelle Polynom mit Grad 4 ist reduzibel.

- Es sei n eine positive ganze Zahl. Was ist eine lineare Differenzengleichung der Ordnung n mit Koeffizienten in K? Warum gibt es genau eine Lösung einer solchen Differenzengleichung, wenn die ersten n Folgenglieder vorgegeben sind? Erläutern Sie, wie man die Menge aller Folgen in K als $K[x]$-Modul betrachten kann und mit Hilfe der Division mit Rest eine Lösung bestimmen kann.

- Was ist eine homogene lineare Differenzengleichung der Ordnung 2 mit reellen Koeffizienten? Geben sie an, wie man die Lösungsmenge einer solchen Differenzengleichung bestimmt.

- Was ist die Partialbruchzerlegung von rationalen Funktionen? Beweisen Sie, dass sie existiert und eindeutig bestimmt ist.

- Es sei f ein irreduzibles Polynom in $K[x]$. Beschreiben Sie, wie man einen Körper konstruiert, in dem f eine Nullstelle hat. Wie stellt man die Elemente dieses Körpers am Computer dar? Wie berechnet man das zu einem von Null verschiedenen Element inverse Element? Was bedeutet das für das Polynome $x^2 + 1 \in \mathbb{C}[x]$ und $x^2 - 2 \in \mathbb{Q}[x]$?

- Was ist eine quadratische Funktion? Was ist die Scheitelform einer quadratischen Funktion, wie kann sie bestimmt werden? Wie können Nullstellen und Extremstellen einer quadratischen Funktion bestimmt werden, wie ihr Graph gezeichnet werden?

- Wir nehmen an, die reelle Zahl $\sqrt[3]{7}$ sei bekannt. Begründen Sie: Die Menge $\{a+b\sqrt[3]{7}+c\sqrt[3]{49} \mid a, b, c \in \mathbb{Q}\}$ ist eine $\mathbb{Q}$-Unteralgebra von $\mathbb{R}$ und $(1, \sqrt[3]{7}, \sqrt[3]{49})$ ist eine $\mathbb{Q}$-Basis davon. Bestimmen Sie das Minimalpolynom von $\sqrt[3]{7}$ und entscheiden Sie damit, ob dieser Ring ein Körper ist. Wie dividiert man in diesem Körper?

- Begründen Sie: Die Algebra der Polynome mit reellen Koeffizienten und die Algebra der reellwertigen Polynomfunktionen sind isomorph. Geben Sie einen Isomorphismus an.

- Erläutern Sie, was Binärzahlen, Dezimalzahlen und algebraische Zahlen sind. Geben Sie eine rationale Zahl, die nicht Dezimalzahl ist, eine reelle Zahl, die nicht algebraisch ist und eine algebraische Zahl, die nicht reell ist, an (jeweils mit Begründung). Was sind irrationale Zahlen?

- Erläutern Sie, wie man mit dem Kriterium von Eisenstein feststellen kann, dass ein primitives Polynom mit ganzzahligen Koeffizienten irreduzibel ist. Beweisen Sie den Satz über das Kriterium von Eisenstein.

- Geben Sie drei verschiedene Möglichkeiten zur Konstruktion des Körpers der komplexen Zahlen (wenn der Körper $\mathbb{R}$ bekannt ist) an. Zeigen Sie, dass alle drei als $\mathbb{R}$-Algebren isomorph sind.

- Was ist eine algebraische Zahl? Beweisen Sie, dass die Summe, das Produkt und der Quotient algebraischer Zahlen wieder algebraisch sind.

- Was ist ein Polynom in n Variablen? Was ist sein Totalgrad? Zeigen Sie: Ist der Koeffizientenring eines Polynomrings in n Variablen ein Integritätsbereich bzw. ein ZPE-Ring, dann auch dieser Polynomring.

- Was ist eine algebraische Menge? Zeigen Sie: Beliebige Durchschnitte und endliche Vereinigungen von algebraischen Mengen sind algebraisch.

- Was ist eine quadratische Funktion von $\mathbb{R}^2$ nach $\mathbb{R}$? Erläutern Sie, wie man die Nullstellenmenge einer solchen Funktion skizzieren kann.

- Was ist ein Binomialkoeffizient? Welche Bedeutung hat er für das Rechnen in einem kommutativen Ring? Beweisen Sie: Der Binomialkoeffizient $\binom{n}{k}$ ist die Anzahl der Teilmengen mit k Elementen einer Menge mit n Elementen. Erläutern Sie, wieviele Potenzprodukte in n Variablen vom Grad d es gibt.

- Was ist ein Graph? Wie kann ein Graph durch eine Matrix dargestellt werden? Was ist der Grad einer Ecke? Wie kann mit Hilfe der Grade aller Ecken die Anzahl der Kanten eines Graphen bestimmt werden? Wie kann entschieden werden, ob ein zusammenhängender Graph Eulersch ist? Falls ja, wie kann dann eine Eulersche Tour gefunden werden? Unter welcher Bedingung existiert in einem zusammenhängenden Graph ein Eulerscher Kantenzug?

- Was ist ein Weg in einem Graphen? Was ist ein Baum? Welcher Zusammenhang besteht in einem Baum zwischen der Anzahl seiner Kanten und der Anzahl seiner Ecken? Was ist ein Minimalgerüst in einem zusammenhängenden bewerteten Graphen? Erläutern Sie den Algorithmus von Prim zur Berechnung eines Minimalgerüstes. Erklären Sie, warum der dort ermittelte Baum ein Minimalgerüst ist.

- Was ist die Länge eines Weges ? Erläutern Sie den Algorithmus von Dijkstra zur Berechnung eines kürzesten Weges zwischen zwei Ecken in einem zusammenhängenden bewerteten Graphen.

- Erklären Sie, was das Problem des Briefträgers ist und geben Sie ein Verfahren zu seiner Lösung an. Setzen Sie dabei die Algorithmen von Hierholzer und von Dijkstra als bekannt voraus.

- Es sei $f : \mathbb{Z}_2^n \longrightarrow \mathbb{Z}_2$ eine Funktion. Was ist ihre disjunktive Normalform, wie kann diese bestimmt werden? Wie kann eine Schaltung bestimmt werden, deren Schaltfunktion f ist?

- Was ist ein Boole'scher Ring? Geben Sie ein Beispiel für einen Boole'schen Ring mit 32 Elementen an. Zeigen Sie, dass jeder Boole'sche Ring kommutativ ist und Charakteristik 2 hat. Wenn a die charakteristische Funktion einer Teilmenge A von M und b die einer Teilmenge von B von M, wie können mit Hilfe von a und b die charakteristischen Funktionen von $A \cup B$, $A \cap B$ und $M \setminus A$ dargestellt werden?