

Aufgaben zur Vorlesung Algebra

Blatt 11

Abgabe am Freitag, den 24.01.2014 vor der Vorlesung

Aufgabe 45: Abspalten von Linearfaktoren

(4 Punkte)

Wir betrachten die folgende Aussage:

Sei R ein kommutativer Ring und f ein Polynom aus $R[X]$. Ist $a \in R$ eine Nullstelle von f , so existiert eine Zerlegung $f = (X - a) \cdot g$ mit einem Polynom $g \in R[X]$.

Geben Sie für diese Aussage einen elementaren Beweis, der ohne Polynomdivision auskommt, indem Sie folgendermaßen vorgehen:

- (i) Behandeln Sie zunächst den Fall $a = 0$.
- (ii) Führen Sie den allgemeinen Fall auf den obigen zurück, indem Sie das Polynom $h(X) = f(X + a)$ betrachten.

Hinweis für Lehramtsstudierende: Im Fall $R = \mathbb{R}$ eignet sich diese elementare Argumentation auch für den Unterricht in der Oberstufe.

Aufgabe 46: Substitutionshomomorphismen

(4 Punkte)

Sei K ein Körper und $g \in K[X] \setminus \{0\}$. Zeigen Sie: $\varphi_g : K[X] \rightarrow K[X]$, $f \mapsto f(g)$ ist genau dann ein Ringisomorphismus, wenn $g = aX + b$ für $a, b \in K$ mit $a \neq 0$ gilt.

Aufgabe 47: Lokale Ringe

(4 Punkte)

Sei R ein kommutativer Ring. R heißt lokaler Ring, falls R genau ein maximales Ideal besitzt. Zeigen Sie:

- (i) R ist ein lokaler Ring genau dann, wenn die Nichteinheiten von R ein Ideal bilden.

Hinweis: Sie dürfen die aus dem Zornschen Lemma folgende Aussage, dass jedes echte Ideal in einem maximalen Ideal enthalten ist, ohne Beweis verwenden.

- (ii) Ist R ein lokaler Ring und ist $I \neq R$ ein Ideal in R , so ist auch R/I ein lokaler Ring.

Aufgabe 48: Eulersche φ -Funktion

(4 Punkte)

Es seien p und q zwei verschiedene Primzahlen sowie $n := pq$. Zeigen Sie:

- (i) Für alle $a \in \mathbb{Z}$ mit $a \not\equiv_p 0$ gilt stets $a^{p-1} \equiv_p 1$.

Hinweis: Verwenden Sie die multiplikative Gruppe $\mathbb{Z}_p^*$.

- (ii) Für alle $k \in \mathbb{N}_0$ und $a \in \mathbb{Z}$ gilt $a^{k \cdot \varphi(n) + 1} \equiv_n a$.

Hinweis: Zeigen Sie, dass $a^{k \cdot \varphi(n) + 1} \equiv_p a$ und $a^{k \cdot \varphi(n) + 1} \equiv_q a$ gilt.

- (iii) Zu teilerfremden Zahlen $a, b \in \mathbb{N}$ gibt es ganze Zahlen $s > 0$ und $t < 0$ mit $1 = sa + tb$.

- (iv) Für jedes $e \in \mathbb{N}$ mit $\text{ggT}(e, \varphi(n)) = 1$ ist die Abbildung $\mathbb{Z}_n \rightarrow \mathbb{Z}_n$, welche durch $\bar{a} \mapsto \bar{a}^e$ gegeben wird, eine Bijektion.

Hinweis: Nutzen Sie (ii) und (iii) um eine Umkehrabbildung zu konstruieren.

Der RSA-Algorithmus

Eine (beispielsweise bei der Kommunikation im Internet) weit verbreitete Klasse von Verschlüsselungsverfahren stellen die *asymmetrischen Verfahren* dar. Dabei möchte Alice auf sichere Weise eine Nachricht $g \in \mathbb{N}$ über einen unsicheren Kommunikationsweg an Bob übermitteln.

Zu diesem Zweck erzeugt Bob ein Schlüsselpaar, bestehend aus einem öffentlichen Schlüssel A und einem privaten Schlüssel B . Asymmetrische Verfahren sind so konstruiert, dass Nachrichten, die mit A verschlüsselt wurden, *nur* mit B entschlüsselt werden können.

Bob schickt also den Schlüssel A auf dem unsicheren Kommunikationsweg an Alice. Alice verschlüsselt ihre Nachricht g nun mit A und schickt das Ergebnis auf dem unsicheren Kommunikationsweg an Bob, welcher mittels B die ursprüngliche Nachricht g entschlüsseln kann. Da jedoch nur Bob im Besitz des privaten Schlüssels B ist, kann niemand sonst die Nachricht entschlüsseln, auch wenn die gesamte Kommunikation zwischen Alice und Bob abgehört wurde.

Ein in der Praxis häufig eingesetztes asymmetrisches Verfahren ist das RSA-Verfahren, benannt nach seinen Entwicklern Rivest, Shamir und Adleman. Die Vorgehensweise innerhalb des oben beschriebenen Szenarios ist folgende:

- (1) Bob erzeugt ein Schlüsselpaar.
 - (i) Dazu wählt Bob zwei sehr große Primzahlen p und q und setzt $n := pq$. Es muss hierbei $g < n$ gelten, was in der Praxis dadurch gewährleistet wird, dass Alice ihre Nachricht auf mehrere kleine Teilnachrichten $g_1, \dots, g_k$ aufspaltet und diese einzeln übermittelt, sodass Bob die Größe von g also tatsächlich nicht zu kennen braucht.
 - (ii) Nun wählt Bob eine Zahl $e \in \mathbb{N}$ mit $\text{ggT}(e, \varphi(n)) = 1$. Beispielsweise kann Bob hierfür eine Primzahl wählen, welche größer als p und q ist.
 - (iii) Schließlich berechnet Bob mit dem euklidischen Algorithmus Zahlen $d \in \mathbb{N}$ und $m \in \mathbb{Z}_{<0}$, sodass $1 = de + m\varphi(n)$ gilt. Er wählt nun $A = (n, e)$ als öffentlichen und $B = (n, d)$ als privaten Schlüssel.
- (2) Bob schickt den öffentlichen Schlüssel A an Alice.
- (3) Alice kodiert ihre Nachricht g , indem sie die eindeutig bestimmte Zahl $c \in \mathbb{Z}$ mit $0 \leq c < n$ und $c \equiv_n g^e$ berechnet.
- (4) Alice schickt diese Zahl c an Bob.
- (5) Bob dekodiert c . Dazu berechnet er die eindeutig bestimmte Zahl $g' \in \mathbb{Z}$ mit $0 \leq g' < n$ und $g' \equiv_n c^d$. Die Lösung von Aufgabe 48 (iv) garantiert nun die Gültigkeit der Gleichung $g' = g$.

Um dieses Verfahren zu brechen, muss ein Angreifer die Zahl d aus den Zahlen n und e berechnen. Verfolgen wir jedoch aufmerksam die Erzeugung des Schlüsselpaares, so stellen wir fest, dass hierfür $\varphi(n)$ berechnet werden muss. Die einzige (praktikable) Möglichkeit, $\varphi(n)$ zu berechnen, besteht jedoch darin, die Primfaktorzerlegung von n auszurechnen. Bob ist nach Konstruktion im Besitz dieser Primfaktorzerlegung, sodass er d leicht berechnen kann, aber ein Angreifer muss n tatsächlich faktorisieren.

Es ist selbst mit modernen Hochleistungsrechnern bislang unmöglich, in akzeptabler Zeit die Primfaktorzerlegung einer Zahl zu berechnen, deren Primfaktoren sehr groß sind (beispielsweise mit 200 stelligen Dezimaldarstellungen).