WS 2011/12

Zentralübung zur Vorlesung Diskrete Strukturen (Prof. Mayr)

Dr. Werner Meixner

Fakultät für Informatik
TU München

http://www14.in.tum.de/lehre/2011WS/ds/uebung/

11. Januar 2012

ZÜ XI

Übersicht:

1. Übungsbetrieb: Fragen, Probleme?
2. Tipps: Berechnung von $19^{29} \bmod 35$.
3. Thema: Rationale Funktionen.
4. Vorbereitung: auf TA Blatt 11

1. Übungsbetrieb

Fragen?

2. Tipps

In der Zusatzaufgabe von Blatt 10 musste man auf geschickte Weise den Wert von $19^{29} \bmod 35$ berechnen.
Taschenrechner können das nicht.
Wir wenden eine einfache Methode der Quadratbildung an.

$$
\begin{aligned}
19^{29} \bmod 35 &= [19 \cdot (19^2 \bmod 35)^{14}] \bmod 35 \\
&= [19 \cdot 11^{14}] \bmod 35 \\
&= [19 \cdot (11^2 \bmod 35)^{7}] \bmod 35 \\
&= [19 \cdot (16)^{7}] \bmod 35 \\
&= [19 \cdot 16 \cdot (11)^{3}] \bmod 35 \\
&= (-11) \bmod 35 \\
&= 24\,.
\end{aligned}
$$

Es gibt eine bessere Methode, die den ,,Satz von Euler“ verwendet:

$$n \in \mathbb{N}, a \in \mathbb{Z}_n^* \quad \Longrightarrow \quad a^{\varphi(n)} \equiv 1 \pmod{n}\,.$$

Wegen $19 \in \mathbb{Z}_{35}^*$ und $\varphi(35) = (5-1)(7-1) = 24$
rechnet man

$$19^{29} \equiv_{35} 19^5 \equiv_{35} (-16)^5 \equiv_{35} (-16) \cdot (16^2)^2 \equiv_{35} -11 \equiv_{35} 24\,.$$

Bemerkung: Die Eulersche φ-Funktion berechnet man allgemein für $n = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_k^{e_k}$ mit paarweise verschiedenen Primfaktoren p_i:

$$\varphi(n) = \prod_{i=1}^{k} (p_i - 1) p_i^{e_i - 1}\,.$$

3. Thema Rationale Funktionen

3.1 Rationale Ausdrücke

Addition, Subtraktion, Multiplikation, Division.

3.2 Rationale Funktionen

Ganze rationale Funktionen (Polynomfunktionen)

Gebrochene rationale Funktionen

Definitionsbereiche mit ,,endlich vielen Ausnahmen“.

Siehe Vorbereitungsaufgabe 3!

4. Vorbereitung auf TA's Blatt 11

4.1 VA 1

Sei F die Menge aller Abbildungen einer Menge M in die Menge $\mathbb{C}$ der komplexen Zahlen. Wir definieren für alle $f \in F$ und $g \in F$

die Summe, i. Z. $f + g$, bzw. das Produkt, i. Z. $f \cdot g$,

als diejenigen komplexwertigen Funktionen h bzw. k, für die für alle $x \in M$ gilt

$$\begin{aligned} h(x) = (f+g)(x) &= f(x) + g(x) \quad \text{bzw.} \\ k(x) = (f \cdot g)(x) &= f(x) \cdot g(x)\,. \end{aligned}$$

Entsprechend führen wir über der Menge $F \to F$ der Operatoren über F Addition und Multiplikation wie folgt ein.

Für alle $A, B : F \to F$ und $f \in F$ gilt

$$\begin{aligned} (A+B)(f) &= A(f)+B(f) \quad \text{bzw.} \\ (A \cdot B)(f) &= A(f) \cdot B(f)\,. \end{aligned}$$

Beispiele für Operatoren über F sind
sowohl der Translationsoperator E
als auch der Differenzenoperator Δ.

1. F ist ein Ring bezüglich
   obiger Addition „+“ und Multiplikation „$\cdot$“.
   Beweis!

   Geben Sie die entsprechenden neutralen Elemente
   bezüglich $+$ und $\cdot$ an.

Lösung:

Da Addition und Multiplikation in $\mathbb{C}$
beides assoziativ und kommutativ sind,
gilt dies auch für die entsprechend induzierten Verknüpfungen
von komplexwertigen Funktionen.

Entsprechend folgt die Distributivität.

Dazu die folgende Rechnung für alle $x \in M$:

$$
\begin{aligned}
[f + (g + h)](x) &= f(x) + g(x) + h(x) &&= [(f + g) + h](x)\,,\\
[f \cdot (g \cdot h)](x) &= f(x) \cdot g(x) \cdot h(x) &&= [(f \cdot g) \cdot h](x)\,,\\
[f \cdot (g + h)](x) &= f(x) \cdot g(x) + f(x) \cdot h(x) &&= [(f \cdot g) + (f \cdot h)](x)\,.
\end{aligned}
$$

1. F ist eine Gruppe bezüglich „+“:

Es genügt, die Lösbarkeit der Gleichung $f + h = g$ für alle Funktionen $f, g \in F$ zu beweisen.

Seien $f, g \in F$.
Wir definieren $h \in F$ für alle $x \in M$ durch $h(x) = g(x) - f(x)$.

Dann folgt für alle $x \in M$

$$\begin{aligned} (f+h)(x) = f(x) + h(x) &= f(x) + (g(x) - f(x)) = g(x), \qquad \text{d. h.} \\ f + h &= g\,. \end{aligned}$$

Das neutrale Element bezgl. $+$ ist die konstante Funktion $e(x) = 0$.

2. F ist ein Monoid bezüglich „$\cdot$“:

Das neutrale Element bezgl. $\cdot$ ist die konstante Funktion $e(x) = 1$.

Die Assoziativität von $\cdot$ wurde schon gezeigt.

Bemerkung:

Wir haben auch über der Menge $F \to F$ der Operatoren über F eine Addition und eine Multiplikation durch Induzierung eingeführt.

Analog den Verknüpfungen über F begründen diese Verknüpfungen eine Ringstruktur über der Operatorenmenge $F \to F$.

2. Sei $\circ$ die Komposition von Operatoren. Man zeige für alle Operatoren A, B, C über F:

$$(A + B) \circ C = A \circ C + B \circ C \qquad \text{(Rechtsdistributivität)}\,.$$

Beispiel:

$$\Delta \circ E^{-1} = (E - I) \circ E^{-1} = E \circ E^{-1} - I \circ E^{-1} = \nabla\,.$$

Lösung:

Für alle $f \in F$ gilt

$$\begin{aligned}
[(A+B)\circ C](f) &= [A+B](C(f)) \\
&= A(C(f)) + B(C(f)) \\
&= [A\circ C](f) + [B\circ C](f) \\
&= [(A\circ C) + (B\circ C)](f)\,, \quad \text{q.e.d.}
\end{aligned}$$

3. Sowohl der Translationsoperator E als auch der Differenzenoperator Δ sind Beispiele für Operatoren über F (wobei $M = \mathbb{Z}$).
   Begründung!

Lösung:

Sei $M = \mathbb{Z}$.

Durch E wird jeder Funktion $f \in F$
die Funktion $g \in F$ zugeordnet mit

$$g : M \ni x \rightarrow g(x) = f(x+1) \in \mathbb{C}.$$

Durch Δ wird jeder Funktion $f \in F$
die Funktion $g \in F$ zugeordnet mit

$$g : M \ni x \rightarrow g(x) = f(x+1) - f(x) \in \mathbb{C}.$$

4.2 VA 2

Der Translationsoperator E und der Differenzenoperator Δ sind Beispiele für Operatoren, mit denen man wie in Ringen rechnen kann.

Seien M eine Menge und F die Menge aller Abbildungen von M in die Menge $\mathbb{C}$ der komplexen Zahlen, wie in VA 1.

Sei op die Menge aller Operatoren über M und $a \in op$. Dann definieren wir einen Operator A_a über F wie folgt für alle $f \in F$ und $x \in M$:

$$[A_a(f)](x) = f(a(x))\,.$$

Sei $OP = \{A_a\,;\, a \in op\}$.

1. Sei $M = \mathbb{Z}$. Zeigen Sie $E^n \in OP$ für alle $n \in \mathbb{Z}$.
2. Man zeige für alle $a \in op$ und Operatoren B, C über F die Linksdistributivität

$$A_a \circ (B + C) = A_a \circ B + A_a \circ C\,.$$

3. Seien $a_i, b_j \in op$ für alle $i, j \in \mathbb{N}$. Man zeige

$$\left(\sum_{i=1}^{m} A_{a_i}\right) \circ \left(\sum_{j=1}^{n} B_{b_j}\right) = \sum_{i=1}^{m}\sum_{j=1}^{n}(A_{a_i} \circ B_{b_j})\,.$$

1. Sei $M = \mathbb{Z}$. Zeigen Sie $E^n \in OP$ für alle $n \in \mathbb{Z}$.

Lösung:

Wir definieren den Operator $a \in op$ durch

$$a : \mathbb{Z} \ni x \to x + 1 \in \mathbb{Z}\,.$$

Dann gilt $E = A_a \in OP$.

A_a ist invertierbar: $(A_a)^{-1} = A_{a^{-1}}$ mit $a^{-1} : \mathbb{Z} \ni x \to x - 1 \in \mathbb{Z}$.

Es folgt für alle $n \in \mathbb{Z}$ die Gleichung

$$(A_a)^n = A_{a^n}\,.$$

Mithin $E^n \in OP$.

Bemerkung:

Wegen $a^n : \mathbb{Z} \ni x \to x + n \in \mathbb{Z}$ folgt für alle $n \in \mathbb{Z}$

$$E^n(f)(x) = f(x + n)\,,$$

in Erweiterung von Beispiel 199 der Vorlesung für $n \in \mathbb{N}_0$.

2. Man zeige für alle $a \in op$ und Operatoren B, C über F die Linksdistributivität

$$A_a \circ (B + C) = A_a \circ B + A_a \circ C\,.$$

Lösung:

Die Linksdistributivität von Operatoren steht in direktem Zusammenhang mit der Additivität von Operatoren.

Die Additivität von Operatoren geht in die Linearitätseigenschaft von Operatoren ein.

Die Linearität des Translationsoperators und des Differenzenoperatos wurden insbesondere in Satz 200 der Vorlesung benutzt.

Ein Operator A über F heißt linear, wenn für alle $f, g \in F, \alpha \in \mathbb{C}$ gilt

$$\begin{aligned} A(f+g) &= A(f) + A(g) && \text{(Additivität)}, \\ A(\alpha f) &= \alpha \cdot (A(f)) && \text{(Homogenität)}. \end{aligned}$$

Wir zeigen im Folgenden die Additivität aller $A_a \in OP$
und folgern daraus anschließend deren Linksdistributivität.

Additivität:

Um eine Gleichung $A(f+g) = A(f) + A(g)$ nachzuweisen, muss man für alle $x \in M$ die Gleichung

$$[A(f+g)](x) = [A(f) + A(g)](x)$$

beweisen.

Für alle $x \in M$ gilt nun

$$\begin{aligned}
[A_a(f+g)](x) &= (f+g)(a(x)) \\
&= f(a(x)) + g(a(x)) \\
&= [A_a(f)](x) + [A_a(g)](x) \\
&= [A_a(f) + A_a(g)](x)\,.
\end{aligned}$$

Linksdistributivität:

Um eine Gleichung $A_a \circ (B + C) = A_a \circ B + A_a \circ C$ nachzuweisen, muss man für alle $f \in F$ die Gleichung $[A_a \circ (B + C)](f) = [A_a \circ B + A_a \circ C](f)$ beweisen.

Für alle $f \in F$ gilt nun

$$\begin{aligned}
[A_a \circ (B + C)](f) &= A_a([B + C](f)) \\
&= A_a(B(f) + C(f)) \\
&= A_a(B(f)) + A_a(C(f)) \\
&= [A_a \circ B](f) + [A_a \circ C](f) \\
&= [A_a \circ B + A_a \circ C](f)\,.
\end{aligned}$$

3. Seien $a_i, b_j \in op$ für alle $i, j \in \mathbb{N}$. Man zeige

$$\left(\sum_{i=1}^{m} A_{a_i}\right) \circ \left(\sum_{j=1}^{n} B_{b_j}\right) = \sum_{i=1}^{m} \sum_{j=1}^{n} (A_{a_i} \circ B_{b_j}) .$$

Lösung:

Da nun die volle Distributivität (links und rechts) gilt, folgt die gewünschte Gleichung, indem
alle Summanden der linken Klammer mit allen Summanden der rechten Klammer „multipliziert“, d. h. hier ,

über die Komposition verknüpft und die Produkte aufsummiert.

4.3 VA 3

Man zeige:

1. Für alle $n \in \mathbb{Z}$ gilt $\Delta x^{\overline{n}} = n(x+1)^{\overline{n-1}}$.

   Beweis!

Lösung:

Für die steigende Fakultät gelten für alle ganzen Zahlen $g \in \mathbb{Z}$ die beiden fundamentalen Gleichungen

$$x^{\overline{g}} \cdot (x+g) = x^{\overline{g+1}} \qquad \text{und} \qquad x \cdot (x+1)^{\overline{g}} = x^{\overline{g+1}}\,.$$

Für die fallende Fakultät gelten für alle ganzen Zahlen $g \in \mathbb{Z}$ entsprechend die beiden fundamentalen Gleichungen

$$x^{\underline{g}} \cdot (x-g) = x^{\underline{g+1}} \qquad \text{und} \qquad x \cdot (x-1)^{\underline{g}} = x^{\underline{g+1}}\,.$$

Die Ausdrücke auf den Gleichungsseiten sind i. A.

Quotienten von polynomiellen Ausdrücken,

und stellen Elemente dar (sog. Brüche von Polynomen) aus dem

Quotientenkörper $\mathbb{C}(x)$ über dem Polynomring $\mathbb{C}[x]$

Diese Ausdrücke definieren gleichzeitig

rationale Funktionen aus $\mathbb{C} \rightarrow \mathbb{C}$,

die man durch Einsetzen in x und Auswertung der Ausdrücke erhält.

Übersicht:

Steigende Fakultät:

$$
\begin{aligned}
n > 0: \qquad & x^{\overline{n}} &&= x \cdot (x+1) \cdot (x+2) \cdot \ \ldots \ \cdot (x+n-1)\,, \\
n = 0: \qquad & x^{\overline{n}} &&= 1\,, \\
n < 0: \qquad & x^{\overline{n}} &&= \frac{1}{(x+n)\cdot(x+(n+1))\cdot \ \ldots \ \cdot(x-2)\cdot(x-1)}\,.
\end{aligned}
$$

Fallende Fakultät:

$$
\begin{aligned}
n > 0: \qquad & x^{\underline{n}} &&= x \cdot (x-1) \cdot (x-2) \cdot \ \ldots \ \cdot (x-(n-1))\,, \\
n = 0: \qquad & x^{\underline{n}} &&= 1\,, \\
n < 0: \qquad & x^{\underline{n}} &&= \frac{1}{(x-n)\cdot(x-(n+1))\cdot \ \ldots \ \cdot(x+2)\cdot(x+1)}\,.
\end{aligned}
$$

Wegen

$$x^{\overline{g}} \cdot (x+g) = x^{\overline{g+1}} \qquad \text{und} \qquad x \cdot (x+1)^{\overline{g}} = x^{\overline{g+1}}$$

gilt für alle $n \in \mathbb{Z}$

$$\begin{aligned}
\Delta x^{\overline{n}} &= (x+1)^{\overline{n}} - x^{\overline{n}} \\
&= (x+1)^{\overline{n-1}} \cdot (x+1+n-1) \; - \; x \cdot (x+1)^{\overline{n-1}} \\
&= (x+n)(x+1)^{\overline{n-1}} - x \cdot (x+1)^{\overline{n-1}} \\
&= n(x+1)^{\overline{n-1}} \, .
\end{aligned}$$

Man zeige:

2. Für alle $n \in \mathbb{Z}$ gilt $\nabla x^{\underline{n}} = n(x-1)^{\underline{n-1}}$.

   Benutzen Sie die Gleichung $E \cdot \nabla = \Delta$
   zusammen mit Lemma 203 für den Beweis!

Lösung:

In Lemma 203 wurde die Gleichung

$$\Delta x^{\underline{n}} = n x^{\underline{n-1}}$$

bewiesen.

Es folgt mit Operatorenrechnung

$$\begin{aligned} \nabla x^{\underline{n}} &= (E^{-1}\Delta) x^{\underline{n}} \\ &= E^{-1}(\Delta x^{\underline{n}}) \\ &= E^{-1}(n x^{\underline{n-1}}) \\ &= n(x-1)^{\underline{n-1}}. \end{aligned}$$

Man zeige:

3. Es gilt $\nabla\Delta = \Delta\nabla$.

   Beweis!

Lösung:

Es gilt

$$
\begin{aligned}
[[\nabla\Delta](f)](x) &= [\nabla(\Delta(f))](x) \\
&= [\Delta(f)](x) - [\Delta(f)](x-1) \\
&= (f(x+1) - f(x)) - (f((x-1)+1) - f(x-1)) \\
&= (f(x+1) - f((x+1)-1)) - (f(x) - f(x-1)) \\
&= [\nabla(f)](x+1) - [\nabla(f)](x) \\
&= [\Delta(\nabla(f))](x) \\
&= [[\Delta\nabla](f)](x)\,.
\end{aligned}
$$

4.4 VA 4

Berechnen Sie mit Hilfe der Partiellen Summation für $n \in \mathbb{N}$

$$\sum_{k=1}^{n} k \cdot 2^k \, .$$

Lösung:

Wir spezialisieren die Formel der Partiellen Summation wie folgt.

$$\sum_{k=1}^{n} f(k) \cdot \Delta g(k) = [f(k) \cdot g(k)]_1^{n+1} - \sum_{k=1}^{n} \Delta f(k) \cdot g(k+1)$$

Man setzt nun $f(k) = k$, $\Delta g(k) = 2^k$.
Damit gilt $\Delta f(k) = 1$, $g(k) = 2^k$ und es ergibt sich:

$$\begin{aligned}
\sum_{k=1}^{n} k \cdot 2^k &= \Big[k \cdot 2^k\Big]_1^{n+1} - \sum_{k=1}^{n} 1 \cdot 2^{k+1} \\
&= \big[(n+1) \cdot 2^{n+1} - 2\big] - 4 \cdot (2^n - 1) \\
&= (n+1) \cdot 2^{n+1} - 2 \cdot 2^{n+1} + 2 \\
&= (n-1) \cdot 2^{n+1} + 2\,.
\end{aligned}$$

4.5 VA 5

Beweisen Sie die folgende Identität für alle $n, i \geq 0$ mit Binomialinversion:

$$\sum_{k=0}^{n} \binom{n}{k} \binom{k}{i} (-1)^{k-i} = \delta_{n,i} \qquad .$$

Hierbei ist $\delta_{n,i} = 1$, falls $n = i$, und $\delta_{n,i} = 0$, falls $n \neq i$.

Lösung:

Wir machen den Ansatz

$$\sum_{k=0}^{n} \binom{n}{k} b_{k,i} = \delta_{n,i}$$

mit noch zu bestimmenden $b_{k,i}$.

Binomialinversion (siehe Vorlesung) liefert

$$b_{n,i} = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} \delta_{k,i} = (-1)^{n-i} \binom{n}{i}.$$