# Aufgabenblatt 6

**(16)** **Interpolation** Seien $\langle\alpha\rangle, \langle\beta\rangle$ und $\langle\gamma\rangle$ drei paarweise bis auf 1 disjunkte endliche Untergruppen von $G(\mathbb{C})$ der Ordnungen $2, 3$ und 5. Bestimmen Sie ein Polynom $f$ aus $\mathbb{Q}[x]$ mit den Eigenschaften

$$f(\alpha) = 0,\ f(\beta) = 1,\ f(\gamma) = 2\ .$$

**(17)** **Zum RSA-Verfahren.** Auf der Grundlage des folgenden zur Vereinfachung verkürzten Alphabets werden Botschaften als Sequenzen von Dezimalzahlen (entsprechend der Positionen 0 bis 9 in der Liste $\mathfrak{A}$ ) gebildet.

$$\mathfrak{A} = [\ \mathsf{b}\ ,\ \mathsf{d}\ ,\ \mathsf{e}\ ,\ \mathsf{i}\ ,\ \mathsf{n}\ ,\ \mathsf{r}\ ,\ \mathsf{s}\ ,\ \mathsf{t}\ ,\ \mathsf{u}\ ,\ .\ \ ]$$

Um bei kleinen Zahlen zu bleiben, werde jede Ziffer der kompletten Botschaft z.B. [3,4,7] von rechts nach links einzeln verschlüsselt und versandt nach dem RSA-Verfahren. Eine auf diese Weise verschlüsselte Botschaft sei [(1)]

$$[1,\ 61,\ 41,\ 63,\ 31,\ 61,\ 0,\ 8,\ 63,\ 32,\ 1,\ 81,\ 23,\ 32,\ 63]\ .$$

Leider ist der bei der Verschlüsselung benutzte öffentliche Modul $q$ verloren gegangen und nur noch der bei der Verschlüsselung ebenfalls benutzte und ebenfalls öffentliche Exponent $s$ bekannt. Irgendwie gelingt es jemandem, an die nicht öffentliche Zahl $\phi(q)$ zu gelangen. Ermitteln Sie $q$ und die Botschaft, wenn $s = 17$ und wenn $\phi(q) = 72$.

**(18)** Sei $n \in \mathbb{N}_{\geq 2}$. Der Körper $K$ enthalte eine so genannte **primitive n-te Einheitswurzel** $w$. Das heißt nichts anderes als dass es in $G(K) = K\backslash\{0\}$ ein Element $w$ gibt, dessen Ordnung genau $n$ ist. Bekanntestes Beispiel ist. $K = \mathbb{C},\ w = e^{\frac{2\pi i}{n}}$. Betrachtet wird die Abbildung

$$P_w : K[x] \to K^n \text{ mit } P_w(f) = (f(1),\ f(w), \ldots, f(w^{n-1})) \text{ für } f \in K[x].$$

**(a)** Zeigen Sie: $P_w$ ist ein surjektiver $K$-linearer Ringmorphismus, wenn im $K$-Vektorraum $K^n$ komponentenweise multipliziert wird.

**(b)** Weisen Sie nach, dass $\quad x^n - 1 = (x-1)(x^{n-1} + \cdots + x + 1) = \prod_{i=0}^{n-1}(x - w^i)$ und bestimmen Sie den normierten Erzeuger $g$ des Hauptideals $\mathsf{Kern}\,(P_w)$.

Sei $V := (K[x])_n$ der $K$-Untervektorraum von $K[x]$ der Polynome vom Grad kleiner als $n$. Die Einschränkung $\Delta_w := P_w \mid_V$ der $K$-linearen Abbildung $P_w$ auf $V$ heißt **diskrete Fouriertransformation** [(2)].

**(c)** $\Delta_w$ ist ein $K$-linearer Ringisomorphismus, wenn innerhalb $V$ modulo Division mit Rest durch $g$ multipliziert wird (diese Multiplikation wurde in der Vorlesung mit $\odot$ bezeichnet) und in $K^n$ wie in (a).

**(d)** $\sum_{j=0}^{n-1} w^{kj} = 0$ für $1 \leq k \leq n-1$

**(e)** Sei $D_w$ die Matrix von $\Delta_w$ bezüglich der kanonischen Basen in $V$ und $K^n$. Bestimmen Sie $D_w$ und bestätigen Sie die Invertierbarkeit.

Bei Aufgabe (18) können zwei zusätzliche Punkte erworben werden.

.....

(1) Bei realistischeren Anwendungen würden u.A. die Ziffern 0 und 1 nicht zugelassen werden. Ihnen macht es die Aufgabe kürzer.

(2) Wenn $R = \mathbb{C}$ und $w = e^{\frac{2\pi i}{n}}$ entsteht die diskrete Fouriertransformation bei Abtastvorgängen kontinuierlicher Signale. Gute Algorithmen zur schnellen Berechnung der diskreten Fouriertransformation ($FFT$, $F$ für 'fast' bzw. 'schnell') gehören zu den praktisch bedeutsamsten Algorithmen überhaupt. Die Aufgabe ist größtenteils orientiert an dem Buch mit der Internetseite `http://www-math.uni-paderborn.de/~aggathen/mca.html`