D-MATH
Dr. Menny Akka Ginosar
Paula Truöl

HS 2020
ETH Zürich

Serie 5

Endliche Körper, Polynome

Hinweis: Punkte können Sie in den Aufgaben 1(a), (c) und (d), 5(a) und 7(c) bekommen. Wir erwarten, dass Sie nicht nur diese Aufgaben bearbeiten, sondern versuchen, die ganze Serie zu lösen. Eine Ausnahme bildet die mit einem $(*)$ deklarierte Aufgabe 7, von der wir manche Teilaufgaben als besonders schwierig einschätzen.

1. Sei p eine Primzahl. Zeigen Sie die folgenden Aussagen.
   (a) (Kleiner Satz von Fermat) Es gilt $a^{p-1} \equiv 1 \mod p$ für alle $a \in \mathbb{Z}$ mit $p \nmid a$, d.h. $[a]^{p-1} = [1]$ für alle $[a] \in \mathbb{F}_p^\times = \mathbb{F}_p \setminus \{0\}$. (2)
   (b) (Variante des Kleinen Satz von Fermat) Es gilt $a^p \equiv a \mod p$ für alle $a \in \mathbb{Z}$.
   (c) (Quadratwurzeln von 1 in $\mathbb{F}_p$) Zeigen Sie: Für $[m] \in \mathbb{F}_p^\times$ gilt $[m]^{-1} = [m]$ genau dann, wenn $[m] = [1]$ oder $[m] = -[1]$. (2)
   (d) (Satz von Wilson) Es gilt $(p-1)! \equiv -1 \mod p$. Dabei ist $n! := 1 \cdot 2 \cdot 3 \cdots n$ für $n \in \mathbb{N}$. (2)
   (e) (Quadratwurzel von -1 in $\mathbb{F}_p$) Es gelte $p \equiv 1 \mod 4$. Dann existiert ein $[m] \in \mathbb{F}_p$ mit $[m]^2 = [-1]$.

2. Sei K ein Körper. In der Vorlesung haben Sie die Abbildung $\mathrm{ev}_K \colon K[x] \to \mathrm{Abb}(K, K)$ kennen gelernt, welche durch $\mathrm{ev}_K(f)(\lambda) = f(\lambda)$ für $f \in K[x], \lambda \in K$ definiert ist.
   (a) Für diese Teilaufgabe sei $K = \mathbb{F}_p$ für eine Primzahl p. Finden Sie ein Polynom $0 \neq f \in \mathbb{F}_p[x]$, sodass $\mathrm{ev}_{\mathbb{F}_p}(f) = 0$ gilt. Die Abbildung $\mathrm{ev}_{\mathbb{F}_p}$ ist also nicht injektiv.
   Tipp: In der Vorlesung haben Sie gesehen, dass $f(x) = x^3 - x = (x-\overline{0})(x-\overline{1})(x-\overline{2}) \in \mathbb{F}_3[x]$ so ein Polynom ist für $p = 3$. Versuchen Sie dieses Beispiel zu verallgemeinern und benutzen Sie Aufgabe 1(a).
   (b) Seien $x_0, \ldots, x_n, y_0, \ldots, y_n \in K$ mit $x_i \neq x_j$ für alle $i \neq j$. Zeigen Sie, dass es genau ein Polynom $f \in K[x]$ vom Grad $\leq n$ gibt, sodass $f(x_i) = y_i$ für $i \in \{0, \ldots, n\}$.
   Tipp: Um die Existenz zu zeigen, konstruieren Sie zuerst Polynome $g_k \in K[x]$ vom Grad $\leq n$ mit
   $$g_k(x_i) = \begin{cases} 1 & \text{für } i = k \\ 0 & \text{für } i \neq k. \end{cases}$$
   Nehmen Sie für die Eindeutigkeit an, dass es ein Polynom $g \in K[x]$ gibt mit $g(x_i) = y_i$ für $i \in \{0, \ldots, n\}$ und betrachten Sie $f - g$.
   (c) Seien M und N endliche Mengen. Zeigen Sie, dass die Menge $\mathrm{Abb}(M, N)$ endlich ist, und bestimmen Sie die Anzahl ihrer Elemente.
   (d) Zeigen Sie, dass ev_K surjektiv, aber nicht injektiv ist, falls der Körper K endlich ist.
   Tipp: Zeigen Sie, dass $K[x]$ nicht endlich ist und benutzen Sie die Teilaufgaben (b) und (c).

3. In der Vorlesung haben Sie die folgende Aussage gesehen (Lemma 1.54 im begleitenden Skript): Seien $f, g \neq 0 \in K[x]$ Polynome für einen Körper K. Dann existieren eindeutige Polynome $q, r \in K[x]$ mit $\deg(r) < \deg(g)$, sodass $f = q \cdot g + r$.
Finden Sie q, r in den folgenden Beispielen. Beachten Sie, dass in dieser Aufgabe und auch in Aufgabe 5 die Koeffizienten der Polynome immer als Elemente des jeweils betrachteten Körpers zu verstehen sind, insbesondere ist in Teilaufgabe (c) z.B. $2x^5$ als $\overline{2}x^5$ mit $\overline{2} \in \mathbb{F}_5$ zu verstehen.
   (a) $f = 2x^4 + x^3 + 4x^2 - 6, g = 2x + 1, K = \mathbb{Q}$.
   (b) $f = 3x^5 + 3x^4 + 2x^2 + 3x + 1\, g = x^2 + x + 1, K = \mathbb{Q}$.
   (c) $f = 2x^5 - x^3 - 2x^2 + 3, g = 2x^2 - 1, K = \mathbb{F}_5 = \mathbb{Z}/5\mathbb{Z}$.
   (d) $f = x^3 - x^2 - 4x + 4, g = x^2 - a, K = \mathbb{Q}$. Für welche $a \in \mathbb{R}$ ist der Rest 0? Was sagt dies über die Nullstellen des Polynoms $x^3 - x^2 - 4x + 4$?

4. Sei

$$f(x) = \sum_{i=0}^{n} a_i x^i = a_0 x^0 + a_1 x^1 + a_2 x^2 + \ldots + a_n x^n = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n \in \mathbb{Z}[x]$$

   mit $a_n \neq 0$. Zeigen Sie: Für jede Nullstelle $\frac{b}{c} \in \mathbb{Q}$ von f mit teilerfremden $b, c \in \mathbb{Z}$ gilt $b | a_0$ und $c | a_n$. Hierbei heißen zwei Zahlen $b, c \in \mathbb{Z}$ heißen *teilerfremd*, wenn es keine natürliche Zahl außer 1 gibt, die beide Zahlen teilt.

5. In dieser Aufgabe können sie 4 Punkte in Teilaufgabe (a) bekommen.
   (a) Faktorisieren Sie das Polynom (4)

$$f(x) = x^5 + 9x^4 + 31x^3 + 53x^2 + 48x + 18$$

   jeweils so weit wie möglich über den Körpern $\mathbb{R}, \mathbb{C}, \mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ und $\mathbb{F}_5 = \mathbb{Z}/5\mathbb{Z}$.
   Tipp: Finden Sie zuerst alle Nullstellen in $\mathbb{Q}$. Einige Nullstellen kann man "erraten", indem man kleine ganze Zahlen ausprobiert.
   (b) Faktorisieren Sie das Polynom

$$g(x) = x^4 + 2x^3 - 4x^2 - 5x - 6$$

   jeweils so weit wie möglich über den Körpern $\mathbb{R}, \mathbb{C}$ und $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$.

6. Seien $f, g \in \mathbb{C}[x]$ Polynome mit $\mu(f, \lambda) \leq \mu(g, \lambda)$ für alle $\lambda \in \mathbb{C}$. Zeigen Sie, dass dann f ein Teiler von g ist. Gilt die Aussage auch in $\mathbb{R}[x]$?

7. In dieser Aufgabe wollen wir zeigen, dass die Gruppe $\mathbb{F}_p^\times = \mathbb{F}_p \setminus \{\overline{0}\}$ für Primzahlen p zyklisch ist. (∗)

   Eine Gruppe $(G, \cdot)$ heißt *zyklisch*, falls es ein Element $g \in G$ gibt mit $G = \{g^n \mid n \in \mathbb{Z}\}$. Das Element g heißt dann ein *Erzeuger* von G. Man schreibt auch $\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$ für die *Untergruppe von G erzeugt von g*. Beispiele für zyklische Gruppen sind $(\mathbb{Z}, +) = \langle 1 \rangle = \langle -1 \rangle$ und $(\mathbb{Z}/n\mathbb{Z}, +) = \langle \overline{1} \rangle$ für $n \in \mathbb{N}$.
   (a) Zeigen Sie, dass eine zyklische Gruppe immer abelsch ist.

(b) Zeigen Sie: Sei G eine endliche zyklische Gruppe mit $|G| = n$. Dann ist G isomorph zur Gruppe $(\mathbb{Z}/n\mathbb{Z}, +)$.

In Aufgabe 4 von Serie 4 haben Sie gezeigt, dass $\mathbb{F}_5^\times$ isomorph zu $(\mathbb{Z}/4\mathbb{Z}, +)$ und damit zyklisch ist. (Überlegen Sie, was ein Erzeuger von $\mathbb{F}_5^\times$ ist.) Der folgende Beweis, dass $\mathbb{F}_p^\times$ zyklisch ist, ist nicht einfach, benutzt aber nur Aussagen aus der Vorlesung, u.a. über Nullstellen von Polynomen. Die folgende Proposition werden wir als "Blackbox" benutzen. Unten finden Sie eine Anleitung, wie man auch diese Proposition beweisen kann.

Proposition: Sei G eine endliche Gruppe. Dann teilt die Ordnung jedes Elements die Gruppenordnung, d.h. $\mathrm{ord}(a)$ ist ein Teiler von $|G|$ für alle $a \in G$. (Erinnern Sie sich an die Definition der Ordnung in Aufgabe 2 von Serie 4.)

(c) Sei $\overline{b} \in \mathbb{F}_p^\times$. Zeigen Sie, dass $x^m - \overline{b} = 0$ höchstens m Lösungen in $\mathbb{F}_p^\times$ hat. (2)

(d) Sei I eine Untergruppe von $\mathbb{F}_p^\times$ mit $|I| = q^k$ für eine Primzahl q und $k \in \mathbb{N}$. Zeigen Sie, dass I dann zyklisch ist.

Tipp: Laut obiger Proposition teilt die Ordnung jedes Elements von I die Gruppenordnung q^k. Können Sie zeigen, dass es ein Element $a \in I$ mit $\mathrm{ord}(a) = q^k$ gibt? Benutzen Sie (c).

Betrachten Sie nun den Fall $p-1 = mq$ für teilerfremde $m, q \in \mathbb{N}$, q ist nun nicht mehr unbedingt eine Primzahl. Betrachten Sie weiter den Gruppenhomomorphismus $\varphi\colon \mathbb{F}_p \to \mathbb{F}_p^\times, a \mapsto a^m$, der jedes Element auf seine m-te Potenz schickt.

(e) Zeigen Sie, dass die Bildmenge $I := \varphi(\mathbb{F}_p^\times)$ eine Untergruppe von $\mathbb{F}_p^\times$ ist.

(f) Zeigen Sie

$$\mathbb{F}_p^\times = \bigcup_{b \in I} \{a \in \mathbb{F}_p^\times \mid \varphi(a) = b\}.$$

(g) Sei $U_b := \{a \in \mathbb{F}_p^\times \mid \varphi(a) = b\}$. Zeigen Sie $|U_b| \leq m$ für alle $b \in I$. Folgern Sie $|I| \geq q$.

(h) Benutzen Sie den kleinen Satz von Fermat (siehe Aufgabe 1 (a)), um zu zeigen, dass $b^q = \overline{1}$ gilt für alle $b \in I$.

(i) Folgern Sie jetzt, dass $|I| \leq q$ gilt. Zusammen mit Teilaufgabe (g) erhalten wir $|I| = q$. Es gibt also genau q viele m-te Potenzen in $\mathbb{F}_p^\times$.

Wir schreiben jetzt $p - 1 = q_1^{k_1} \dots q_n^{k_n}$ für $q_1, \dots, q_n$ paarweise verschiedene Primzahlen.

(j) Für $j \in \{1, \dots, n\}$, benutzen Sie die obigen Teilaufgaben mit $q = q_j^{k_j}$ und $m = m_j = \frac{p-1}{q_j^{k_j}}$, um eine Untergruppe I_j von $\mathbb{F}_p^\times$ der Ordnung $q_j^{k_j}$ zu definieren, welche aus den m_j-ten Potenzen der Elemente in $\mathbb{F}_p^\times$ besteht.

(k) Benutzen Sie Teilaufgabe (d), um zu zeigen, dass es $a_1, \dots, a_n \in \mathbb{F}_p^\times$ gibt mit $\mathrm{ord}(a_j) = q_j^{k_j}$ für $j \in \{1, \dots, n\}$.

(l) Zeigen Sie unter der Annahme, dass $q_1, \dots, q_n$ paarweise verschieden Primzahlen sind, dass

$$\mathrm{ord}(a_1 \cdot \ldots \cdot a_n) = q_1^{k_1} \dots q_n^{k_n} = p - 1.$$

Erläutern Sie, warum wir damit gezeigt haben, dass $\mathbb{F}_p^\times$ für Primzahlen p zyklisch ist.

Tipp: Sie können folgende Aussage benutzen, welche man mit Division mit Rest über $\mathbb{Z}$ beweisen kann: Seien $a, b \in \mathbb{Z}$ teilerfremd. Dann gibt es $k, l \in \mathbb{Z}$ mit $ka + lb = 1$.

Die Proposition folgt aus folgender allgemeinerer Aussage: Sei G eine endliche Gruppe und sei $H \subset G$ eine Untergruppe. Dann teilt die Ordnung von H die Ordnung von G.

Tipp: Für geeignete Elemente $g_1, \ldots, g_k \in G$ kann man G schreiben als disjunkte Vereinigung

$$g_1 H \cup g_2 H \ldots \cup g_k H \,,$$

und jede der Teilmengen $g_j H = \{g_j h \mid h \in H\}$ hat genau $|H|$ Elemente.