D-MATH
Dr. Menny Akka Ginosar
Paula Truöl

HS 2020
ETH Zürich

Lösungen zu 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)

   Lösung:

   Wir zeigen zunächst folgendes Lemma.

   Lemma: Sei p eine Primzahl und $a \in \mathbb{Z}$ mit $p \nmid a$. Dann lassen die ersten $(p-1)$ Vielfachen von a, d.h. die Zahlen $a, 2a, 3a, \ldots, (p-1)a$ beim Teilen durch p jeden der Reste $1, 2, 3, \ldots, p-1$ genau einmal.

   Beweis: Es genügt zu zeigen, dass es unter den Vielfachen $a, 2a, 3a, \ldots, (p-1)a$ von a keine zwei verschiedenen gibt, die beim Teilen durch p den gleichen Rest lassen. Angenommen, es gilt $ka \equiv la \mod p$ für $1 \leq k, l \leq p-1$. In $\mathbb{F}_p$ haben wir also die Gleichheit $[ka] = [la]$. Wegen $p \nmid a$ ist $[a] \in \mathbb{F}_p^\times$, also existiert ein mulitplikativ Inverses für $[a]$ und Multiplikation mit diesem liefert $[k] = [l] \in \mathbb{F}_p$. Wegen $1 \leq k, l \leq p-1$ folgt $k = l$, also die Behauptung. □

   Wir folgern nun den Kleinen Satz von Fermat aus diesem Lemma. Da die Multiplikation in $\mathbb{F}_p$ kommutativ ist, gilt dort

   $$[a][2a]\ldots[(p-1)a] = [1]\cdot[2]\cdot[3]\cdots[p-1] \qquad \Longleftrightarrow \qquad [(p-1)!][a]^{p-1} = [(p-1)!].$$

   Da jeder Term in $[(p-1)!] = [1]\cdot[2]\cdot[3]\cdots[p-1]$ ein Element von $\mathbb{F}_p^\times$ ist, ist auch das Produkt in $\mathbb{F}_p^\times$ und wir können die Gleichung mit dem Inversen von $[(p-1)!]$ multiplizieren, um $[a]^{p-1} = [1]$ zu erhalten wie behauptet.

   (b) (Variante des Kleinen Satz von Fermat) Es gilt $a^p \equiv a \mod p$ für alle $a \in \mathbb{Z}$.

   Lösung:

   Im Fall $p|a$ gilt $a^p \equiv 0 \equiv a \mod p$. Falls $p \nmid a$, so gilt für $a \in \mathbb{Z}$ wegen (a), dass

   $$a^{p-1} \equiv 1 \mod p \qquad \Rightarrow \qquad a^p \equiv a \mod p.$$

   Tatsächlich könnten wir hier "⇔" schreiben, da $[a] \in \mathbb{F}_p^\times$ eine multiplikative Inverse hat.

   (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)

Lösung:

Wir nehmen zuerst an, dass $[m] = [1]$ oder $[m] = -[1]$ gilt. Dann ist $[m] \cdot [m] = 1$, also $[m]^{-1} = [m]$, da das inverse Element eindeutig ist.
Für die andere Richtung nehmen wir an, dass $[m]^{-1} = [m]$ für $[m] \in \mathbb{F}_p \setminus \{0\}$ gilt. Also gilt $[m]^2 = [1]$. Dies können wir schreiben als

$$([m] - [1])([m] + [1]) = [m]^2 - [1] = 0.$$

Falls $[m] \neq [1]$ ist, dann erhalten wir durch Multiplikation mit dem multiplikativ Inversen von $([m] - [1])$ die Gleichung $[m] + [1] = 0$, also $[m] = -[1]$. Also gilt $[m] = [1]$ oder $[m] = -[1]$ wie behauptet.

(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)

Lösung:

Der Satz von Wilson taucht als Wilson's lemma in Lemma 4.45 im Buch `https://link.springer.com/book/10.1007/978-3-030-55233-6` auf. Dort finden Sie auch einen Beweis (auf Englisch). Das dort verwendete Korollar 4.39 ist die Aussage auf Teilaufgabe (c). Wenn Sie Fragen zu dem Beweis im Buch haben, stellen Sie diese im Forum oder im StudyCenter oder wenden sich an die Übungsleiterin.

(e) (Quadratwurzel von -1 in $\mathbb{F}_p$) Es gelte $p \equiv 1 \mod 4$. Dann existiert ein $[m] \in \mathbb{F}_p$ mit $[m]^2 = [-1]$.

Lösung:

Wegen der Voraussetzung $p \equiv 1 \mod 4$ gilt $2s = p - 1$ für $s = \frac{p-1}{2} \in \mathbb{N}$. Weiter gilt

$$\begin{aligned}(2s)! &= 1 \cdot 2 \cdot 3 \cdots (s) \underbrace{(s+1)}_{p-s} \underbrace{(s+2)}_{p-(s-1)} \cdots \underbrace{(2s-1)}_{p-2} \underbrace{(2s)}_{p-1} \\ &\equiv s!(-s)(-(s-1)) \cdots (-2)(-1) \mod p \\ &\equiv s!(-1)^s s! \equiv (s!)^2 \mod p,\end{aligned}$$

wobei wir im letzten Schritt benutzt haben, dass $s = \frac{p-1}{2}$ wegen $4|(p-1)$ (nach Voraussetzung) gerade ist. Wegen Teilaufgabe (d) gilt $(2s)! = (p-1)! \equiv -1 \mod p$, also folgt die Behauptung für $[m] = [(s!)]$.

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).

Lösung:

Betrachten Sie das Polynom $f(x) = x^p - x \in \mathbb{F}_p[x]$. Es gilt $f \neq 0 \in \mathbb{F}_p[x]$, aber $f(a) = a^p - a = [0]$ für alle $a \in \mathbb{F}_p$ wegen des kleinen Satzes von Fermat, also $\mathrm{ev}_{\mathbb{F}_p}(f) = 0$.

Bemerkung:

Weil jedes $a \in \mathbb{F}_p$ eine Nullstelle von $x^p - x$ ist, folgt $f(x) = x^p - x = (x-\overline{0})(x-\overline{1})\dots(x-\overline{p-1})$ aus der Gleichheit der Grade und der Normiertheit der beiden Polynome.

(b) Seien $x_0, \dots, x_n, y_0, \dots, y_n \in K$ mit $x_i \neq y_i$ 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 $i \in \{0, \dots, n\}$.

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 $i \in \{0, \dots, n\}$ und betrachten Sie $f - g$.

Lösung:

Eine Lösung zu dieser Aufgabe können Sie im „Übungsbuch zur Linearen Algebra, Aufgaben und Lösungen“ von Hannes Stoppel und Birgit Griese finden, siehe hier: `https://link.springer.com/book/10.1007%2F978-3-658-14522-4`. Dort ist dies Aufgabe 6 zum Abschnitt 1.3. Wenn Sie Fragen zu dem Beweis im Buch haben, stellen Sie diese im Forum oder im StudyCenter oder wenden sich an die Übungsleiterin.

(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.

Lösung:

Sei $M = \{x_1, \dots, x_m\}$, also $|M| = m$.

Behauptung 1: $|\mathrm{Abb}(M, N)| = |N^m| = |N \times \dots \times N|$**.**

Beweis von Behauptung 1:

Für $r = (r_1, \dots, r_m) \in N^m$ definieren wir eine Abbildung $\varphi_r \in \mathrm{Abb}(M, N)$ durch

$$\varphi_r(x_i) = r_i$$

für $i \in \{1, \dots, m\}$. Das induziert eine Abbildung $\varphi\colon N^m \to \mathrm{Abb}(M, N)$ durch $\varphi(r) := \varphi_r$ für $r \in N^m$.

Wir behaupten, dass die Abbildung φ injektiv ist. Seien dazu $r, r' \in N^m$ mit $\varphi_r = \varphi_{r'}$. Dann gilt $\varphi_r(x_i) = \varphi_{r'}(x_i)$ für $i \in \{1, \dots, m\}$ also per Definition $r_i = \varphi_r(x_i) = \varphi_{r'}(x_i) = r'_i$ für $i \in \{1, \dots, m\}$.

Weiter ist φ surjektiv. Sei dazu $f\colon M \to N$ beliebig und definiere $r_i := f(x_i) \in N$ für $i \in \{1, \dots, m\}$ dann gilt $r = (r_1, \dots, r_m) \in N^m$ und es gilt per Definition von φ_r die Gleichheit $\varphi_r(x_i) = r_i = f(x_i)$ für $i \in \{1, \dots, m\}$ also ist $\varphi_r = f$. Folglich ist φ eine Bijektion und es gilt $|\mathrm{Abb}(M, N)| = |N^m|$.

Behauptung 2: Für eine endliche Menge A gilt $|A \times A| = |A|^2$.

Beweis von Behauptung 2:

Wegen $|A| = n = |\{1, \dots, n\}|$ für ein geeignetes $n \in \mathbb{N}_0$ (der Fall $n = 0$ entspricht $A = \emptyset$ und ist trivial) genügt es $|\{1, \dots, n\} \times \{1, \dots, n\}| = |\{1, \dots, n^2\}$ zu zeigen. Für $n = 0$ ist nichts zu zeigen, sei also $n \geq 0$. Es gilt $\{1, \dots, n+1\} = \{1, \dots, n\} \cup \{n+1\}$ und folglich

auch

$$\begin{aligned}\{1,\dots,n+1\}^2 &= (\{1,\dots,n\}\cup\{n+1\})\times(\{1,\dots,n\}\cup\{n+1\})\\ &= \{1,\dots,n\}^2\cup\{n+1\}\times\{1,\dots,n\}\cup\{1,\dots,n\}\times\{n+1\}\cup\{n+1\}^2.\end{aligned}$$

Nach Induktionshypothese gibt es eine bijektive Abbildung $\psi\colon \{1,\dots,n\}^2\to\{1,\dots,n^2\}$. Definieren wir nun die Abbildung $\varphi\colon \{1,\dots,n+1\}^2\to\{1,\dots,(n+1)^2\}$ durch

$$\varphi(a,b)=\begin{cases}\psi(a,b), & \text{falls } (a,b)\in\{1,\dots,n\}^2\\ n^2+b, & \text{falls } a=n+1, b\le n\\ n^2+n+a, & \text{falls } a\le n, b=n+1\\ n^2+2n+1, & \text{falls } a=b=n+1.\end{cases}$$

Nun bildet nach Induktionshypothese ψ die Menge $\{1,\dots,n\}^2$ bijektiv auf $\{1,\dots,n^2\}$ ab. Man überzeugt sich leicht, dass es für die Bijektivität von φ dann genügt zu zeigen, dass die Abbildung

$$\psi|_{\{1,\dots,n+1\}^2\setminus\{1,\dots,n\}^2}\colon \{1,\dots,n+1\}^2\setminus\{1,\dots,n\}^2\to\{1,\dots,(n+1)^2\}\setminus\{1,\dots,n^2\}$$

bijektiv ist. Seien dazu $(a,b),(a',b')\in\{1,\dots,n+1\}^2\setminus\{1,\dots,n\}^2$ mit $\varphi(a,b)=\varphi(a',b')$. Falls $a=n+1, b\le n$ ist, dann gilt $\varphi(a,b)=n^2+b\le n^2+n$, also muss auch $a'=n+1, b'\le n$ sein. Dann ist aber $n^2+b=\varphi(a,b)=\varphi(a',b')=n^2+b'$, also auch $b=b'$. Analog zeigt man $(a,b)=(a',b')$ in den anderen Fällen. Folglich ist $\psi|_{\{1,\dots,n+1\}^2\setminus\{1,\dots,n\}^2}$ injektiv.
Für die Surjektivität sei $y\in\{1,\dots,(n+1)^2\}\setminus\{1,\dots,n^2\}$ beliebig. Falls $n^2<y\le n^2+n$ ist, dann gilt $\varphi(n+1,y-n^2)=$ y. Im anderen Fall ist $n^2+n<y\le n^2+2n+1$ und damit $\varphi(y-n^2-n,n+1)=y$.

Behauptung 3: Für M,N endliche Mengen gilt $|\operatorname{Abb}(M,N)|=|N|^{|M|}$.

Beweis von Behauptung 3:

Wegen Behauptung 1 gilt $|\operatorname{Abb}(M,N)|=|N^m|$ mit $m=|M|$. Induktiv zeigt man, dass aus Behauptung 2 für endliche Mengen N und $m\in\mathbb{N}$ die Identität $|N^m|=|N|^m$ folgt. Kombiniert man diese Aussagen folgt sofort $\operatorname{Abb}(M,N)=|N|^{|M|}$.

(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).

Lösung:

Eine Lösung zu dieser Aufgabe können Sie im „Übungsbuch zur Linearen Algebra, Aufgaben und Lösungen“ von Hannes Stoppel und Birgit Griese finden, siehe hier: `https://link.springer.com/book/10.1007%2F978-3-658-14522-4`. Dort ist dies Aufgabe 8 zum Abschnitt 1.3. Wenn Sie Fragen zu dem Beweis im Buch haben, stellen Sie diese im Forum oder im StudyCenter oder wenden sich an die Übungsleiterin.

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 $x^3 - x^2 - 4x + 4$?

Lösung:

Wir geben hier für einige Teilaufgaben nur die Endergebnisse der Polynomdivision an. In der Prüfung müssen Sie vollständige Rechenwege angeben.

(a) Es ist $f = 2x^4 + x^3 + 4x^2 - 6 = (x^3 + 2x - 1)(2x + 1) + (-5) = q \cdot g + r$ für $q = x^3 + 2x - 1$, $r = -5$. Eine ausführlichere Lösung zu dieser Teilaufgabe finden Sie in der Datei Polynomdivision3a.pdf.

(b) $3x^5+3x^4+2x^2+3x+1 = (x^2+x+1)(3x^3-3x+5)+(x-4)$, also $q = 3x^3-3x+5, r = x-4$.

(c) $2x^5 - x^3 - 2x^2 + 3 = (2x^2 - 1)(x^3 - 1) + 2$, also $q = x^3 - 1, r = 2$.

(d) $x^3 - x^2 - 4x + 4 = (x^2 - a)(x - 1) + (a - 4)(x - 1)$, also $q = x - 1, r = (a - 4)(x - 1)$. Für $a = 4$ verschwindet der Rest. Also sind $x = \pm 2$ Nullstellen des Polynoms. Ausserdem sieht man direkt, dass $x = 1$ die dritte Nullstelle ist.

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.

Lösung:

Durch Einsetzen der Nullstelle $\frac{b}{c}$ erhalten wir

$$0 = f\left(\frac{b}{c}\right) = \sum_{i=0}^{n} a_i \left(\frac{b}{c}\right)^i = a_0 + a_1 \left(\frac{b}{c}\right) + a_2 \left(\frac{b}{c}\right)^2 + \ldots + a_n \left(\frac{b}{c}\right)^n.$$

Wir multiplizieren die Gleichung mit c^n und erhalten eine Gleichung in $\mathbb{Z}$:

$$0 = \sum_{i=0}^{n} a_i c^{n-i} b^i = a_0 c^n b^0 + a_1 c^{n-1} b + a_2 c^{n-2} b^2 + \ldots + a_n c^0 b^n.$$

Wir subtrahieren den ersten Summanden und erhalten

$$-a_0 c^n = \sum_{i=1}^{n} a_i c^{n-i} b^i \qquad \left(= a_1 c^{n-1} b + a_2 c^{n-2} b^2 + \ldots + a_n c^0 b^n\right).$$

Alle Terme der Summe auf der rechten Seite und somit auch die Summe auf der rechten Seite sind durch b teilbar, also muss auch die linke Seite durch b teilbar sein. Weil b und c teilerfremd sind, folgt daraus $b|a_0$. Analog erhalten wir durch Subtraktion des letzten Summanden die Gleichung

$$-a_n b^n = \sum_{i=0}^{n-1} a_i c^{n-i} b^i \qquad \left(= a_0 c^n b^0 + a_1 c^{n-1} b + a_2 c^{n-2} b^2 + \dots a_{n-1} c b^{n-1}\right).$$

Alle Terme der Summe auf der rechten Seite sind durch c teilbar, also muss auch die linke Seite durch c teilbar sein. Aus der Teilerfremdheit von c und b folgt nun wiederum $c|a_n$, also die Behauptung.

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.

   Lösung:
   Nach Aufgabe 4 sind alle Nullstellen in $\mathbb{Q}$ schon ganze Zahlen und Teiler von 18. (Ueberprüfen Sie das.) Probieren liefert die Nullstellen -1 und -3 und Polynomdivision mit Rest zeigt

   $$f(x) = (x+1)(x+3)(x^3 + 5x^2 + 8x + 6).$$

   Details zu dieser Rechnung finden Sie in der Datei Polynomdivision5a.pdf.
   Der Faktor $x^3 + 5x^2 + 8x + 6$ hat nochmal die Nullstelle -3 (wir proieren wiederum kleine ganze Zahlen aus; nach Aufgabe 4 sind alle Nullstellen in $\mathbb{Q}$ dieses Polynoms schon in $\mathbb{Z}$ und Teiler von 6) und ist gleich $(x+3)(x^2+2x+2)$. Der letzte Faktor x^2+2x+2 hat keine reelle Nullstelle, denn nach der p-q-Formel oder der "Mitternachtsformel" (siehe auch Nullstellen5a.pdf) sind die Nullstellen über $\mathbb{C}$ gerade $x_{1,2} = -1 \pm i$ für die imaginäre Einheit i (vgl. Analysis I-Vorlesung).
   Für die Faktorisierung über $\mathbb{F}_5[x]$ bemerken wir, dass wiederum $-\overline{1} = \overline{4}$ und $-\overline{3} = \overline{2}$ Nullstellen sind; $\overline{2}$ sogar dreifach, da es auch eine Nullstelle von x^2+2x+2 ist. Es gilt $x^2+2x+2 = (x+3)(x+4)$ über $\mathbb{F}_5$. Über $\mathbb{F}_2$ gilt $x^2+2x+2 = x^2$. Somit lautet die Faktorisierung

   $$f(x) = \begin{cases} (x+1)(x+3)^2(x^2+2x+2) & \text{in } \mathbb{R}[x] \\ (x+1)(x+3)^2(x+1-i)(x+1+i) & \text{in } \mathbb{C}[x] \\ (x+1)(x+3)^3(x+4) & \text{in } \mathbb{F}_5[x] \\ (x+1)^3x^2 & \text{in } \mathbb{F}_2[x]\,. \end{cases}$$

   (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 $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$.

Lösung:

Wir nutzen Aufgabe 4 um rationale Nullstellen zu erraten. Hier ist $a_0 = -6$ und $a_n = 1$. Wir erhalten also als Kandidaten für mögliche Nullstellen $\pm 1, \pm 2, \pm 3, \pm 6$. Ausprobieren zeigt, dass 2 eine Nullstelle ist, Polynomdivision ergibt

$$g(x) = (x-2)(x^3 + 4x^2 + 4x + 3)\,.$$

Wir setzen weiter die rationalen Nullstellenkandidaten ein und finden die Nullstelle -3. Wiederum durch Polynomdivision erhalten wir

$$x^3 + 4x^2 + 4x + 3 = (x+3)(x^2 + x + 1)\,.$$

Durch Anwenden der Lösungsformel für Nullstellen quadratischer Polynome (p-q-Formel oder "Mitternachtsformel") erhalten wir die verbleibenden zwei Nullstellen:

$$\omega = \frac{1}{2}(-1 + i\sqrt{3})\,, \qquad \omega^2 = \bar{\omega} = \frac{1}{2}(-1 - i\sqrt{3})\,.$$

Bemerkung:

Wir berechnen

$$\omega^3 = \omega \cdot \omega^2 = \omega \cdot (-\omega - 1) = \omega + 1 - \omega = 1\,,$$

das heißt ω ist eine (primitive) dritte Einheitswurzel.

Über $\mathbb{F}_3$ gilt $x^2 + x + 1 = (x+2)^2$, somit erhalten wir die Faktorisierung

$$g(x) = \begin{cases} (x-2)(x+3)(x^2+x+1) & \text{in } \mathbb{R}[x] \\ (x-2)(x+3)\left(x + \frac{1}{2} - \frac{i\sqrt{3}}{2}\right)\left(x + \frac{1}{2} + \frac{i\sqrt{3}}{2}\right) & \text{in } \mathbb{C}[x] \\ x(x+1)(x+2)^2 & \text{in } \mathbb{F}_3[x]\,. \end{cases}$$

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 $\mathbb{R}[x]$?

   Lösung:

   Eine Lösung zu dieser Aufgabe können Sie im „Übungsbuch zur Linearen Algebra, Aufgaben und Lösungen" von Hannes Stoppel und Birgit Griese finden, siehe hier: `https://link.springer.com/book/10.1007%2F978-3-658-14522-4`. Dort ist dies Aufgabe 7 zum Abschnitt 1.3. Wenn Sie Fragen zu dem Beweis im Buch haben, stellen Sie diese im Forum oder im StudyCenter oder wenden sich an die Übungsleiterin.

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.

Lösung:

Seien $a = g^n, b = g^m \in G$. Dann gilt $a \cdot b = g^n \cdot g^m = g^{n+m} = g^{m+n} = g^m \cdot g^n = b \cdot a$, weil Addition in $\mathbb{Z}$ 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 $a_1, \ldots, a_n \in \mathbb{F}_p^\times$ gibt mit $\mathrm{ord}(a_j) = q_j^{k_j}$ für $j \in \{1, \ldots, n\}$.

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

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

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.

Lösung:

Für die Lösungen der Teilaufgaben (b)-(l) verweisen wir auf Abschnitt 7.2 im Buch `https://link.springer.com/book/10.1007/978-3-030-55233-6`. Bei Fragen dazu können Sie sich gerne an den Dozenten wenden.

Wir zeigen hier noch die folgende oben genannte Aussage: Sei G eine endliche Gruppe und sei $H \subset G$ eine Untergruppe. Dann teilt die Ordnung von H die Ordnung von G.

Beweis: Sei $g \in G$. Wir betrachten die Linksnebenklassen

$$gH = \{gh | h \in H\} \,.$$

Wegen $e \in H$ folgt

$$G = \bigcup_{g \in G} gH \tag{1}$$

Wir zeigen, dass für $g, g' \in G$ die Linksnebenklassen gH bzw. $g'H$ entweder gleich oder disjunkt sind. Wir nehmen an, es gibt ein $x \in gH \cap g'H$. Dann ist x von der Form

$$x = gh = g'h' \,,$$

für gewisse $h, h' \in H$. Sei $\tilde{h} \in H$ beliebig, dann ist

$$g\tilde{h} = g'h'h^{-1}\tilde{h} \in g'H \,,$$

wobei $h'h^{-1}\tilde{h} \in H$ da H eine Untergruppe ist. Folglich gilt $gH \subset g'H$. Die gleiche Argumentation zeigt auch die umgekehrte Inklusion, also gilt

$$gH = g'H \,.$$

Somit kann die Vereinigung (1) tatsächlich nach Wahl gewisser Elemente $g_1, \ldots, g_k \in G$ als disjunkte Vereinigung geschrieben werden, also

$$G = g_1 H \cup g_2 H \ldots \cup g_k H \,.$$

Wir zeigen nun, dass die Linksnebenklassen gH alle die gleiche Größe haben. Für $g \in G$ ist die Abbildung

$$\begin{aligned} H &\to gH \\ h &\mapsto gh \,, \end{aligned}$$

stets injektiv, da aus $gh = gh'$ durch Multiplikation mit dem Inversen von g direkt $h = h'$ folgt. Da $|H|$ endlich ist, ist die Abbildung also bijektiv (vgl. Übung 1.73 im Analysis-Skript.)

Insgesamt folgt daher $|G| = k \cdot |H|$. □