Diskrete Mathematik Übungsstunde Zusammenfassung

Leon Kolmanić

27.11.2023

1 Besprechung Bonusaufgabe

Häufige Fehler waren:

- **G2** Axiom für Monoid verwendet
- Nicht korrekt begründet, wieso man auf beiden Seiten der Gleichung addieren darf
- Vergessen in die Begründung aufzunehmen, dass 1 Neutralelement bezüglich der Multiplikation ist
- Nicht genau mit den gegebenen Axiomen argumentiert

Die Axiome **G1**, **G2** und **G3** sind alles Gruppenaxione. Ihr könnt diese nur auf Gruppen verwenden. Die Algebra $\langle R; \cdot, 1\rangle$ war in dieser Aufgabe ein Monoid. Auf diesen könnt ihr diese Axiome nicht anwenden. Stattdessen konnte man zum Beispiel schreiben: 1 ist Neutralelement bezüglich $\cdot$, weil $\langle R; \cdot, 1\rangle$ ein Monoid ist. Viele von euch haben auf beiden Seiten der Glechung addiert, aber dann eine falsche Begründung angegeben, wie zum Beispiel "$-b$ ist das Inverse von b. Wenn wir auf beiden Seiten einer Gleichung addieren, notieren und begründen wir das wie folgt:

$$a = a \stackrel{\cdot}{\Longrightarrow} .a + b = a + b \qquad \text{(Addiere } b \text{ auf beiden Seiten von rechts)}$$

Den Pfeil in die andere Richtung schreiben wir nicht. Wenn wir das wollten, müssten wir als Begründung zusätzlich das Cancellation Law angeben. Man darf auf beiden Seiten einer Gleichung addieren, weil Operationen wie $+$ und $\cdot$ Funktionen sind. Bei Funktionen wissen wir schon, dass $x = y$ $f(x) = f(y)$ impliziert. Funktionen ordnen nämlich jedem Input den gleichen Output zu. Wenn wir wissen, dass $a = b$ gilt, können wir schliessen, dass $a + c = b + c$ ist, weil das nichts anderes ist als $\text{add}(a, c) = \text{add}(b, c)$. Und weil $a = b$ sind das zwei Funktionsauswertungen mit dem gleichen Input.
Weil die Rechengesetze von Ringen sehr verwandt mit denen der reellen Zahlen

sind, muss man besonders darauf aufpassen, dass man die Begründungen von offensichtlichen Schritten nicht vergisst. Die Umformung

$$(1+1)(a+b) = a+a+b+b$$

erfordert als Begründung zusätzlich zum Distributivgesetz, dass 1 Neutralelement bezüglich $\cdot$ ist.
Bei dieser Aufgabe war kein Ring gegeben, sondern eine Algebra mit drei Eigenschaften. In solchen Fällen ist es wichtig, dass man beim Begründen erwähnt, woraus man die verwenden Eigenschaften ableitet. Statt zum Beispiel einfach nur zu schreiben "+ ist kommutativ", sollte man schreiben, dass dies aus Axiom 1 aus der Aufgabenstellung folgt.

2 Polynomdivision

Polynomdivision über endlichen Körpern zu lernen ist im Kapitel 5 wichtig, weil man sie in den verschiedensten Aufgabentypen braucht. Sie funktioniert genau so wie die Polynomdivision über den reellen Zahlen. Zwei Dinge sind aber unterschiedlich: Das Subtrahieren von einer Zahl und die Division durch eine Zahl.

2.1 Subtraktion und Division in $\mathbb{Z}_n$

Im Folgendem sei n eine Primzahl. Dann ist $\mathbb{Z}_n$ ein Körper. Seien $a, b \in \mathbb{Z}_n$. Die Addition und Multiplikation funktionieren genau so, wie man das schon gewohnt ist. Man muss nur daran denken, dass man am Ende das Resultat modulo n rechnet. Um b von a zu subtrahieren, also um $a - b$ auszurechnen, bemerken wir, dass dieser Ausdruck gleich ist zu $a + (-b)$. Wir müssen also zuerst das Inverse zu b bezüglich $+$ finden. In dem Körper $\mathbb{Z}_n$ ist dies $n - b$. Ein Beispiel: Wenn $n = 11$ und $b = 3$, dann ist $-b = 8$, weil dann gilt:

$$b + (-b) = 3 + 8 = 11 \equiv_{11} 0$$

Für die Division in einem Körper muss man sich an an das Konzept von "multiplikativen Inversen modulo n" erinnern. Wenn $\gcd(a, n) = 1$, nennen wir die einzige Zahl $x \in \{1, 2, ..., n-1\}$ mit $a \cdot x \equiv_n 1$ das multiplikative Inverse von a modulo n. Man kann dieses durch Ausprobieren oder durch den erweiterten euklidischen Algorithmus finden. Wenn beispielsweise $n = 7$, ist das multiplikative Inverse von 5 modulo 7 3, weil

$$3 \cdot 5 = 15 \equiv_7 1$$

$\frac{a}{b}$ auszurechnen, beziehungsweise a durch b zu dividieren, bedeutet a mit dem multiplikativen Inversen von b zu multiplizieren. Das kennen wir schon von den reellen Zahlen: Um 5 durch 2 zu dividieren, multiplizieren wir 5 mit 0.5, also dem multiplikativen Inversen von 2. Wenn $n = 5$ gilt für die Division in $\mathbb{Z}_n$ $\frac{4}{3} = 3$. Das Inverse von 3 modulo 5 ist 2, weil $2 \cdot 3 = 6 \equiv_5 1$. Jetzt multiplizieren wir dies mit 4: $4 \cdot 2 = 8 \equiv_5 3$. Wie auch in den reellen Zahlen können wir auch in $\mathbb{Z}_n$ nicht durch 0 dividieren.

2.2 Polynomdivision am Beispiel

Wir wollen im Folgendem Polynome über dem endlichen Körper $\mathbb{Z}_7$ betrachten. Nun sollen wir

$$2x^5 + 4x^4 + x^3 + 3x^2 + 5x + 4 : 3x^3 + 2x^2 + 6x + 3$$

mit Rest bestimmen. Keine Panik! Polynomdivision ist nicht so kompliziert, wie sie aussieht. Sie besteht aus einer Abfolge von elementaren Schritten. Zunächst fokussieren wir uns auf die Monome des höchsten Grades der beiden Polynome, also auf $2x^5$ und $3x^3$. Für den ersten Schritt sollen wir nun ein c finden, sodass $c \cdot 3x^3 = 2x^5$ gilt. Zunächst mal ist klar, dass $x^3 \cdot x^2 = x^5$ gilt. Also muss c schonmal x^2 enthalten. Wie schaffen wir es nun, die 3 mit einer Zahl zu multiplizieren, sodass 2 rauskommt? Dafür berechnen wir $\frac{2}{3}$. Von den reellen Zahlen wissen wir schon, dass $b \cdot \frac{a}{b} = a$. Wie oben erklärt berechnen wir das multiplikative Inverse von 3 modulo 7 und multiplizieren dieses mit 2. Es ergibt sich

$$\frac{2}{3} = 2 \cdot 3^{-1} = 2 \cdot 5 = 10 \equiv_7 3$$

Wir bestätigen: $3 \cdot 3 = 9 \equiv_7 2$. Also $c = 3x^2$. Wir multiplizieren nun c mit dem rechten Polynom:

$$3x^2 \cdot (3x^3 + 2x^2 + 6x + 3) = 9x^5 + 6x^4 + 18x^3 + 9x^2 \equiv_7 2x^5 + 6x^4 + 4x^3 + 2x^2$$

Das war eine ganz normale Multiplikation, bis darauf dass man am Ende modulo 7 rechnet. Nun ziehen wir das Resultat dieses Produkts vom linken Polynom ab:

$$\begin{aligned} &2x^5 + 4x^4 + x^3 + 3x^2 + 5x + 4 - (2x^5 + 6x^4 + 4x^3 + 2x^2) \\ &= -2x^4 - 3x^3 + x^2 + 5x + 4 \\ &\equiv_7 5x^4 + 4x^3 + x^2 + 5x + 4 \end{aligned}$$

Das war ein Schritt der Polynomdivision. Wir fangen nun von vorne an und arbeiten mit dem erhaltenen Polynom und dem rechten Polynom weiter. Zunächst finden wir die Monome höchsten Grades: Diese sind $5x^4$ und $3x^3$. Dann finden wir wieder c, sodass $c \cdot 3x^3 = 5x^4$. Natürlich enthält c x^1. Ausserdem

$$\frac{5}{3} = 5 \cdot 3^{-1} = 5 \cdot 5 = 25 \equiv_7 4$$

Somit $c = 4x$. Tatsächlich $c \cdot 3x^3 = 12x^4 \equiv_7 5x^4$. Nun multiplizieren wir das rechte Polynom mit c:

$$4x \cdot (3x^3 + 2x^2 + 6x + 3) = 12x^4 + 8x^3 + 24x^2 + 12x \equiv_7 5x^4 + x^3 + 3x^2 + 5x$$

Dann subtrahieren wir das erhaltene Polynom von dem aus dem vorherigen Schritt:

$$\begin{aligned} 5x^4 + 4x^3 + x^2 + 5x + 4 - (5x^4 + x^3 + 3x^2 + 5x) &= 3x^3 - 2x^2 + 4 \\ &\equiv_7 3x^3 + 5x^2 + 4 \end{aligned}$$

Das war der zweite Schritt der Polynomdivision. Man führt dies so lange durch, bis das aus dem Schritt resultierende Polynom den gleichen Grad hat wie das Divisorpolynom. Das ist nun der Fall, beide Polynome haben Grad 3. Dann führt man noch einen letzten Schritt durch. Wir finden c sodass $c \cdot 3x^3 = 3x^3$ gilt. Das ist nun leicht, $c = 1$. Dann multiplizieren wir das Divisorpolynom mit 1 und ziehen das Produkt von dem Polynom ab, das aus dem letzten Schritt resultiert ist:

$$\begin{aligned} 3x^3 + 5x^2 + 4 - (3x^3 + 2x^2 + 6x + 3) &= 3x^2 - 6x + 1 \\ &\equiv_7 3x^2 + x + 1 \end{aligned}$$

Die Polynomdivision gibt uns zwei Resultate, und zwar den Quotient und den Rest. Der Quotient ergibt sich durch Addition aller c's:

$$3x^2 + 4x + 1$$

Der Rest ist das Resultatpolynom, das man im letzten Schritt erhält. In unserem Fall ist das

$$3x^2 + x + 1$$

Was bedeutet dieses Resultat? Es gilt

$$\begin{aligned} &2x^5 + 4x^4 + x^3 + 3x^2 + 5x + 4 \\ &= \underbrace{(3x^3 + 2x^2 + 6x + 3)}_{\text{Divisor}} \cdot \underbrace{(3x^2 + 4x + 1)}_{\text{Quotient}} + \underbrace{(3x^2 + x + 1)}_{\text{Rest}} \end{aligned}$$

3 Der Ring $F[x]_{m(x)}$

Für einen Körper F und ein Polynom $m(x)$ können wir den Ring $F[x]_m(x)$ betrachten. Das sind alle Polynome über F, die Grad kleiner als $m(x)$ haben. Im Folgendem sei $F = Z_5$ und $m(x) = x^2 + 1$.

3.1 Nullteiler finden

Nun sollen wir alle Nullteiler in diesem Ring finden. In einem endlichen Ring ist jedes Element entweder Nullteiler, Einheit (invertierbar) oder 0. Die invertierbaren Elemente in dem Ring $F[x]_m(x)$ sind genau diejenigen, die teilerfremd zu $m(x)$ sind (Lemma 5.36). Der Rest (ohne die 0) sind dann die Nullteiler. Um herauszufinden, welche Elemente zu $m(x)$ teilerfremd sind, müssen wir zunächst $m(x)$ faktorisieren. Wir sehen, dass $m(x)$ die Nullstellen 2 und 3 hat, weil

$$\begin{aligned} 2^2 + 1 = 5 &\equiv_5 0 \\ 3^2 + 1 = 10 &\equiv_5 0 \end{aligned}$$

Also sind zwei Faktoren von $m(x)$ $x-2 \equiv_5 x+3$ und $x-3 \equiv_5 x+2$ (Lemma 5.29). Weil

$$(x+3)\cdot(x+2) = x^2+5x+6 \equiv_5 x^2+1$$

sind das alle Faktoren. Wir müssen nun alle Elemente in $F[x]_m(x)$ finden, die einen Teiler[1] mit $m(x)$ gemeinsam haben, also einen dieser beiden Faktoren enthalten. Diese Elemente müssen mindestens Grad 1 haben, weil die beiden Faktoren Grad 1 haben. Sie können höchstens Grad 1 haben, weil alle Elemente in $F[x]_m(x)$ nach Definition Grad kleiner 2 haben. Also suchen wir jetzt alle Vielfachen der beiden Faktoren mit Grad 1. Dazu multiplizieren wir die beiden Faktoren jeweils mit allen $x \in \mathbb{Z}_5 \setminus \{0\}$. Wir lassen die 0 aus, weil ein Polynom mal 0 0 ergibt und 0 kein Nullteiler sein kann. Es ergibt sich:

$$\begin{aligned} 1\cdot(x+3) &= x+3 \\ 2\cdot(x+3) &\equiv_5 2x+1 \\ 3\cdot(x+3) &\equiv_5 3x+4 \\ 4\cdot(x+3) &\equiv_5 4x+2 \end{aligned}$$

Und:

$$\begin{aligned} 1\cdot(x+2) &= x+2 \\ 2\cdot(x+2) &\equiv_5 2x+4 \\ 3\cdot(x+2) &\equiv_5 3x+1 \\ 4\cdot(x+2) &\equiv_5 4x+3 \end{aligned}$$

Folglich sind die Nullteiler des Rings genau

$$x+2, x+3, 2x+1, 2x+4, 3x+1, 3x+4, 4x+2, 4x+3$$

3.2 Einheiten finden

Nun sollen wir noch die Elemente von $F[x]_m(x)^*$ finden. Das sind diejenigen Elemente aus $F[x]_m(x)$, die zu $m(x)$ teilerfremd sind (in dem gleichen Sinn wie oben, Konstanten zählen nicht als gemeinsame Teiler). Weil wir bereits alle Elemente aufgelistet haben, die nicht teilerfremd zu $m(x)$ sind, müssen wir für diese Aufgabe nur noch alle Elemente von $F[x]_m(x)$ aufzählen, die nicht in der vorherigen Aufzählung vorkommen (oder 0 sind). Da das ziemlich viele Elemente sind (genau 25 - 1 - 8 = 16), lasse ich die komplette Aufzählung als Übung:)

3.3 Multiplikative Inverse finden

Zuletzt wollen wir noch das multiplikative Inverse von $3x+2$ finden. Da alle Elemente $F[x]_m(x)$ Grad höchstens 1 haben, haben sie alle die Form $\alpha x+\beta$ für

[1] Ein gemeinsamer Teiler von zwei Polynomen ist ein Polynom mit Grad mindestens 1, das beide teilt. Konstanten zählen nicht.

$\alpha, \beta \in \mathbb{Z}_5$. Wir suchen nun $\alpha x + \beta$ mit

$$(\alpha x + \beta) \cdot (3x + 2) \equiv_{m(x)} 1$$

Wir können den obigen Ausdruck umformen:

$$3\alpha x^2 + (2\alpha + 3\beta)x + 2\beta \equiv_{m(x)} 1$$

Wir können einen Trick der modularen Arithmetik benutzen: Wir dürfen auf einer Seite einer Kongruenz Vielfache vom Modulo $m(x) = x^2 + 1$ subtrahieren:

$$\begin{aligned} & 3\alpha x^2 + (2\alpha + 3\beta)x + 2\beta \equiv_{m(x)} 1 \\ \iff & (3\alpha x^2 + (2\alpha + 3\beta)x + 2\beta) - 3\alpha(x^2 + 1) \equiv_{m(x)} 1 \\ \stackrel{\cdot}{\iff} & (2\alpha + 3\beta)x + 2\beta - 3\alpha \equiv_{m(x)} 1 \end{aligned}$$

Die letzte Kongruenz ist erfüllt, wenn:

$$\begin{aligned} 2\alpha + 3\beta &\equiv_5 0 \\ 2\beta - 3\alpha &\equiv_5 1 \end{aligned} \tag{1}$$

Das ist ein lineares Gleichungssystem. Wenn wir die beiden Gleichungen addieren, erhalten wir:

$$\begin{aligned} & -\alpha + 5\beta \equiv_5 1 \\ \stackrel{\cdot}{\iff} & -\alpha \equiv_5 1 \\ \stackrel{\cdot}{\iff} & 4\alpha \equiv_5 1 \end{aligned}$$

Die letzte Kongruenz wird durch das multiplikative Inverse von 4 modulo 5 erfüllt, dieses ist 4. Also $\alpha = 4$. Wenn wir dies nun in 1 einsetzen, erhalten wir:

$$\begin{aligned} & 2 \cdot 4 + 3\beta \equiv_5 0 \\ \iff & 3\beta \equiv_5 -8 \\ \stackrel{\cdot}{\iff} & 3\beta \equiv_5 2 \end{aligned}$$

Also $\beta = 4$.

4 Erweiterungskörper

Sei $F = \mathbb{Z}_3[x]_{x^2+x+2}$. Wir sollen folgende Aufgaben lösen:

1. F ist ein Körper
2. $\langle x \rangle = F^*$
3. Schreibe $y^2 + 1 \in F[y]$ als Produkt von irreduziblen Polynomen. **Tipp:** $(x + 2)^2 \equiv_{x^2+x+2} 2$ in F.

Für den ersten Beweis müssen wir zeigen, dass $\mathbb{Z}_3$ ein Körper ist und dass $x^2 + x + 2$ irreduzibel ist. Bei Polynomen vom Grad 2 kann man einfach überprüfen, ob diese irreduzibel sind: Wenn das Polynom eine Nullstelle hat ist es reduzibel, andernfalls nicht. Also müssen wir alle Elemente im Körper $\mathbb{Z}_3$ einsetzen und zeigen, dass sie keine Nullstellen sind.

Beweis.

$$\begin{aligned} &3 \text{ ist Primzahl} \\ \overset{\cdot}{\Longrightarrow} &\ \mathbb{Z}_3 \text{ ist ein Körper} \end{aligned} \tag{2}$$

Es gilt $\mathbb{Z}_3 = \{0, 1, 2\}$. Wir setzen alle Elemente in das Polynom ein:

$$\begin{aligned} 0^2 + 0 + 2 = 2 &\not\equiv_3 0 \\ 1^2 + 1 + 2 = 4 &\equiv_3 1 \not\equiv_3 0 \\ 2^2 + 2 + 2 = 8 &\equiv_3 2 \not\equiv_3 0 \end{aligned}$$

Wir sehen, dass $x^2 + x + 2$ keine Nullstellen in $\mathbb{Z}_3$ hat. Mit Korollar 5.30 folgt, dass $x^2 + x + 2$ irreduzibel ist. Daraus folgt mit Fakt 2 und Theorem 5.37, dass $\mathbb{Z}_3[x]_{x^2+x+2}$ ein Körper ist. □

Um den zweiten Fakt zu zeigen, müssen wir beweisen, dass x ein Generator der multiplikativen Gruppe von F ist. Wir zeigen das genau wie es in der Zusammenfassung der letzten Woche erklärt wurde: Wir finden die Gruppenordnung, dann alle Teiler der Gruppenordnung und betrachten schliesslich x hoch alle Teiler. In einem Körper gilt per Definition $F^* = F \setminus \{0\}$, also $|F^*| = |F| - 1$. Die Anzahl der Elemente von F finden wir mit einem Lemma. Dann müssen wir nur noch Potenzen von x ausrechnen.

Beweis. Nach Lemma 5.34 gilt $|F| = 3^2 = 9$, weil $|\mathbb{Z}_3| = 3$ und weil $x^2 + x + 2$ Grad 2 hat. Weil F Körper ist gilt $F^* = F \setminus \{0\}$. Also auch $|F^*| = |F| - 1 = 8$. Wegen Korollar 5.9 ist die Ordnung jedes Elements von F^* in $\{1, 2, 4, 8\}$. Wenn ein Element Ordnung 8 hat, ist es ein Generator. Wir zeigen also, dass $\text{ord}(x) \notin \{1, 2, 4\}$.

$$\begin{aligned} &x^1 = x \neq 1 \\ &x^2 \equiv_{x^2+x+2} x^2 - (x^2 + x + 2) = -x - 2 = 2x + 1 \neq 1 \\ &x^4 = (x^2)^2 \equiv_{x^2+x+2} (2x + 1)^2 = 4x^2 + 4x + 1 \\ &\equiv_{x^2+x+2} 4x^2 + 4x + 1 - 4 \cdot (x^2 + x + 2) = -7 = 2 \neq 1 \end{aligned}$$

Also ist x ein Generator von F^*, das bedeutet $\langle x \rangle = F^*$. □

Statt bei x^4 mit der modularen Arithmetik zu tricken, indem man die vorherige Kongruenz wiederverwendet, hätte man auch mit Polynomdivision $R_{x^2+x+2}(x^4)$ bestimmen können.
Vielleicht ist es etwas verwirrend, dass ich im Beweis $=$ statt $\equiv_3$ verwendet habe. Weil wir im Körper $\mathbb{Z}_3$ rechnen, gilt zum Beispiel $-1 = 2$. Wenn man nicht

den Kontext eines konkreten Körpers hat, würde man aber auf jeden Fall $\equiv_3$ schreiben.
Um die letzte Aufgabe zu lösen müssen wir in die Trickkiste greifen. Es kann sehr hilfreich sein daran zu denken, dass viele algebraische Umformungen, die man schon aus der Schule kennt, in kommutativen Ringen anwendbar sind, weil sie sich ausschliesslich durch die Axiome beweisen lassen.
Man darf sich hier nicht davon beirren lassen, dass wir Polynome mit Polynomen als Koeffizienten betrachten. Das bedeutet einfach, dass vor der Variable des Polynoms (in diesem Fall y) anstatt Zahlen Polynome stehen. Aber meistens sind solche Aufgaben gut machbar, wenn man im Hinterkopf behält, dass die Variable y ist und das x in die Koeffizienten gehört und keine besondere Bedeutung hat. Wir könnten auch zum Beispiel Polynome über der Menge $\{\heartsuit, \square, \preceq\}$ betrachten (wenn Operationen $+$ und $\cdot$ auf dieser definiert sind, die die Ringaxiome erfüllen). Ein Polynom wäre zum Beispiel $\heartsuit y^2 + \square y + \preceq$. Bei dieser Aufgabe ist es nicht einmal so wichtig, viel mit den Polynomen zu rechnen. Zunächst mal überlegen wir uns, dass $1 \equiv_3 -2$, damit wir den Tipp verwenden können. So bekommen wir:

$$y^2 + 1 = y^2 - 2 \equiv_{x^2+x+2} y^2 - (x+2)^2$$

Jetzt kommt der Trick: Wir können die dritte binomische Formel verwenden:

$$a^2 - b^2 = (a+b)(a-b)$$

In unserem Fall:

$$y^2 - (x+2)^2 = (y + (x+2))(y - (x+2)) = (y + (x+2))(y + (2x+1))$$

Polynome vom Grad 1 sind irreduzibel. Also sind wir fertig.