6. Musterlösung zu Mathematik für Informatiker II, SS 2004

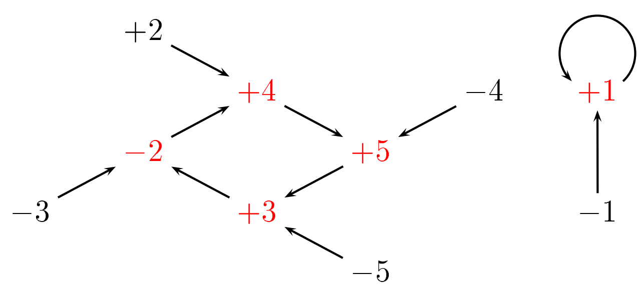
MARTIN LOTZ & MICHAEL NÜSKEN

Aufgabe 6.1 (Quadrismus). (7 Punkte)

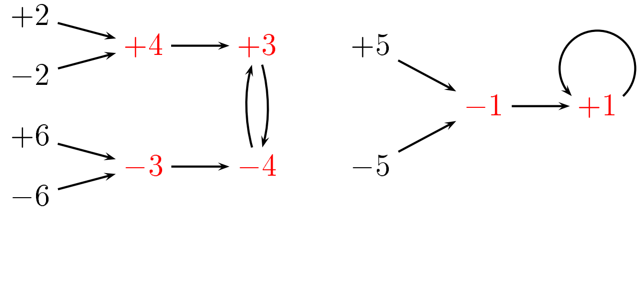
Wir wollen untersuchen, was Quadrieren in den multiplikativen Gruppen $\mathbb{Z}_p^\times$ mit p prim bewirkt.

(i) Zeichne für $p = 11, 13, 17$ je einen Graphen: Zeichne für jedes Element in $\mathbb{Z}_p^\times$ einen Punkt und von einem Element $x \in \mathbb{Z}_p^\times$ soll ein Pfeil zu dessen Quadrat x^2 zeigen. Ordne die Punkte dazu übersichtlich an.

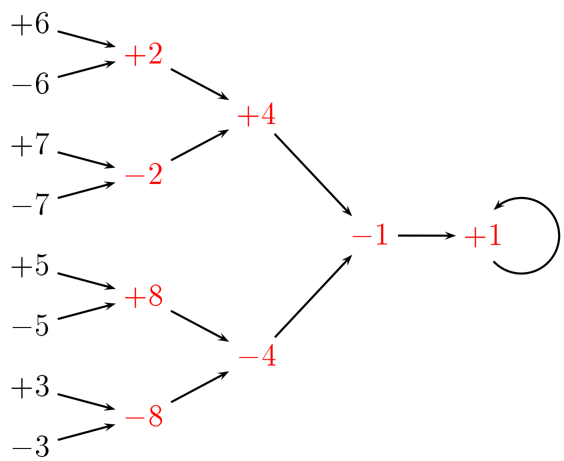
Lösung. Wir verwenden wie auch früher schon jeweils das symmetrische Restesystem $\{0, \pm 1, \pm 2, \ldots, \pm \frac{p-1}{2}\}$. Für $p = 11$ erhalten wir folgendes Bild:



Für $p = 13$ erhalten wir folgendes Bild:



Für $p = 17$ erhalten wir folgendes Bild:



$\bigcirc$

(ii) Markiere alle Punkte, an denen Pfeile enden. Zähle zu jedem Punkt, wieviele Pfeile dort ankommen.

Lösung. Die Punkte sind bereits oben in rot markiert. An jedem roten Punkt kommen zwei Pfeile an. $\bigcirc$

Betrachte nun allgemein die Quadrierungsabbildung

$$q\colon \begin{array}{rcl} \mathbb{Z}_p^\times & \longrightarrow & \mathbb{Z}_p^\times, \\ x & \longmapsto & x^2 \end{array}$$

für p prim.

(iii) Zeige, dass q ein Homomorphismus ist.

Lösung. Da die Gruppe $\mathbb{Z}_p^\times$ kommutativ ist, haben wir

$$q(xy) = (xy)^2 = xyxy = xxyy = x^2y^2 = q(x)q(y).$$

Daraus folgt dass q ein Homomorphismus ist. $\bigcirc$

(iv) Bestimme den Kern $\ker q$ von q und dessen Anzahl. [Ein Polynom vom Grad n hat in einem Körper — wie $\mathbb{Z}_p$ für p prim einer ist — höchstens n Nullstellen.]

Lösung. Der Kern von q ist wie folgt gegeben:

$$\begin{aligned} \ker q &= \{x \in \mathbb{Z}_p^\times \mid x^2 = 1\} \\ &= \{x \in \mathbb{Z}_p^\times \mid x^2 - 1 = 0\} \end{aligned}$$

Das Polynom x^2-1 hat in $\mathbb{Z}_p$ höchstens zwei Nullstellen, also gilt $\#\ker q \leq 2$.

Die Zahlen 1 und -1 sind Nullstellen von x^2-1 und beide in $\mathbb{Z}_p^\times$, also beide im Kern von q. Für $p=2$ sind sie gleich und es gibt sonst nicht einmal andere Elemente, also hat $\ker q$ hier genau ein Element. Für $p>2$ ist $1 \neq -1$ in $\mathbb{Z}_p^\times$, also besitzt $\ker q$ in diesem Fall genau zwei Elemente. ○

(v) Bestimme die Größe $\#\operatorname{im} q$ des Bildes von q.

Lösung. Aus der Definition des Bildes haben wir:

$$\operatorname{im} q = \left\{ a \in \mathbb{Z}_p^\times \,\middle|\, \exists x \in \mathbb{Z}_p^\times \colon a = x^2 \right\}.$$

Für ein $a \in \mathbb{Z}_p^\times$ bedeutet $a \in \operatorname{im} q$, dass die Gleichung $x^2 - a = 0$ eine Lösung besitzt. Ist x_1 eine Lösung, so auch $x_2 = -x_1$. Ist $p > 2$, so gilt $1 \neq -1$ in $\mathbb{Z}_p^\times$ und folglich auch $x_1 \neq -x_1$. Da der Grad von x^2-1 zwei ist, gibt es keine weiteren Lösungen.

Wir folgern: Für $p>2$ entsprechen jedem $a \in \operatorname{im} q$ genau zwei verschiedene Elemente $x_1, x_2 \in \mathbb{Z}_p^\times$. Es gilt also (für $p>2$)

$$\#\operatorname{im} q = \frac{\#\mathbb{Z}_p^\times}{2} = \frac{p-1}{2}. \qquad ○$$

Lösung. Aus dem Homomorphiesatz folgt $\operatorname{im} q \cong \mathbb{Z}_p^\times / \ker q$. Daraus ergibt sich $\#\operatorname{im} q = (\#\mathbb{Z}_p^\times)/(\#\ker q) = (p-1)/2$. ○

Aufgabe 6.2 (Verschiedene Moduln). (6 Punkte)

Betrachte folgenden Versuch einer Definition:

> Sei $f \colon \mathbb{Z}_m \to \mathbb{Z}_n$ die Abbildung mit $f(a \bmod m) = a \bmod n$.

(i) Wann ist das in Ordnung, wann ist die Abbildung wohldefiniert? [Unterscheide gegebenenfalls Fälle und gib Gegenbeispiele bzw. Beweise.]

Lösung. Das Problem besteht darin, dass wir etwa $f(0 mod m)$ mehrfach angeben, denn $0 \bmod m = m \bmod m = (2m) \bmod m$ und so fort. Widersprechen sich die Werte, so haben wir keine sinnvolle Definition. Die Abbildung ist also wohldefiniert, wenn für verschiedene a, a' mit gleichen Argumenten, dh. $a \bmod m = a' \bmod m$ (d.h. $a \equiv a' \bmod m$) auch die gewünschten Werte gleich sind, also $a \bmod n = a' \bmod n$ (d.h. $a \equiv a' \bmod n$) gilt. Wir unterscheiden zwei Fälle:

n teilt m: $a \equiv a' \bmod m$ bedeutet $m \mid a - a'$, was wiederum $n \mid a - a'$ und somit $a \equiv a' \bmod n$ zur Folge hat. In dieser Situation ist f wohldefiniert.

n teilt m nicht: Nimm $a = 0$, $a' = m$. Dann hätten wir nach unserer „Definition“: $f(0 \bmod m) = 0 \bmod n$ und $f(m \bmod m) = m \bmod n$. Aber während $0 \bmod m = m \bmod m$ gilt, haben wir $0 \bmod n \neq m \bmod n$, da n die Zahl m nicht teilt. Also ist f hier nicht wohldefiniert. ◯

(ii) Wann ist f ein Homomorphismus?

Lösung. Nimm an, m und n seien so, dass f wohldefiniert ist (sonst kann f kein Homomorphismus sein!). Nun ist f ein Homomorphismus, wenn $f(a \bmod m + b \bmod m) = f(a \bmod m) + f(b \bmod m)$ für alle $a, b \in \mathbb{Z}$. Wegen

$$\begin{aligned} f(a \bmod m + b \bmod m) &= f(a + b \bmod m) \\ &= a + b \bmod n \\ &= a \bmod n + b \bmod n \\ &= f(a \bmod m) + f(b \bmod m). \end{aligned}$$

ist dies immer der Fall. ◯

(iii) Wann ist f surjektiv?

Lösung. Die Abbildung f ist surjektiv, wenn f wohldefiniert ist und im $f = \mathbb{Z}_n$. Das ist immer der Fall, wenn f wohldefiniert ist. Denn für jedes $a \bmod n$ gibt es ein Element (nämlich $a \bmod m$), welches auf $a \bmod n$ abgebildet wird. ◯

(iv) Wann ist f injektiv?

Lösung. Die Abbildung f ist injektiv, wenn f wohldefiniert ist und es zu jedem $a \bmod n$ *höchstens* ein $a \bmod m$ gibt. Das ist genau dann der Fall, wenn $n = m$ gilt. Denn dann ist f die Identitätsabbildung. Ist $n \neq m$, dann sind $0 \bmod m$ und $n \bmod m$ zwei verschiedene Elemente im Urbild von $0 \bmod n$ und f ist nicht injektiv. ◯

(v) Wann ist f bijektiv?

Lösung. Die Abbildung f ist genau dann bijektiv, wenn f surjektiv und injektiv ist. Nach Teilaufgaben (iii) und (iv) ist dies genau dann der Fall, wenn $n = m$ gilt. ◯

Aufgabe 6.3 (Zyklisch?). (5 Punkte)

Untersuche jeweils, ob die angegebene Gruppe zyklisch ist und gib gegebenenfalls einen Erzeuger an.

(i) $\mathbb{Z}_7^\times$.

Lösung. Diese Gruppe ist zyklisch der Ordnung 6 und ein Erzeuger ist die 5. Denn in $\mathbb{Z}_7^\times$ gilt: $5^2 = 4$, $5^3 = 6$, $5^4 = 2$, $5^5 = 3$, $5^6 = 1$. ○

(ii) $\mathbb{Z}_8^\times$.

Lösung. Diese Gruppe ist nicht zyklisch. Um dies zu sehen, bestimmen wir die Ordnungen der Elemente von $\mathbb{Z}_8^\times = \{1, 3, 5, 7\}$. Wenn kein Element die Ordnung $\#\mathbb{Z}_8^\times = 4$ hat, kann die Gruppe nicht zyklisch sein. Wir haben $3^2 = 1$, $5^2 = 1$ und $7^2 = 1$ in $\mathbb{Z}_8^\times$, also hat jedes dieser Elemente Ordnung 2 und kann kein Erzeuger von $\mathbb{Z}_8^\times$ sein. ○

Tatsächlich ist $\mathbb{Z}_8^\times$ dieselbe Gruppe, wie H aus Aufgabe 6.4(iv), nämlich die sogenannte *Kleinsche Vierergruppe* $\mathbb{Z}_2 \times \mathbb{Z}_2$.

(iii) $\mathbb{Z}_9^\times$.

Lösung. Diese Gruppe ist zyklisch der Ordnung 6. Ein Erzeuger ist die 2. Denn in $\mathbb{Z}_9^\times$ gilt: $2^2 = 4$, $2^3 = 8$, $2^4 = 7$, $2^5 = 5$, $2^6 = 1$. ○

(iv) $\mathbb{Z}_{10}^\times$.

Lösung. Diese Gruppe ist zyklisch der Ordnung 4, und ein Erzeuger ist die 3. Denn: $3^2 = 9$, $3^3 = 7$ und $3^4 = 1$. ○

(v) $\mathbb{Z}_{11}^\times$.

Lösung. Diese Gruppe ist zyklisch der Ordnung 10 und hat als Erzeuger die 2. Da nach dem Satz von Lagrange die Ordnung eines Elementes die Ordnung der Gruppe teilt, wissen wir: Wenn $\operatorname{ord} 2 > 5$, dann $\operatorname{ord} 2 = 10$. Also reicht es die Potenzen der 2 bis 2^5 zu überprüfen. Wir haben $2^2 = 4 \neq 1$, $2^3 = 8 \neq 1$, $2^4 = 5 \neq 1$, $2^5 = 10 \neq 1$. Daraus folgt $\operatorname{ord} 2 = 10$ und wir schliessen, dass 2 die Gruppe $\mathbb{Z}_{11}^\times$ erzeugt. ○

Aufgabe 6.4 (Permutationen). (5 Punkte)

Wir betrachten die Menge A_5 aller Permutationen auf fünf Elementen, die sich als ein Produkt einer geraden Anzahl von Vertauschungen angeben lassen.

Fakt.
- *Jede Permutation σ lässt sich tatsächlich als ein Produkt von Vertauschungen schreiben, und zwar sogar auf beliebig viele Arten.*
- *Wenn eine Permutation σ sich als Produkt einer geraden Anzahl von Vertauschungen schreiben lässt, dann lässt sie sich nicht als Produkt einer ungeraden Anzahl von Vertauschungen schreiben und umgekehrt.*

(i) Bestimme die Zykelschreibweise der Elemente $(12)(23)$, $(12)(23)(31)(41)$, $(12)(23)(31)(45)$ und $(12)(23)(34)(45)$. [Achtung: Die Verknüpfung von Zykeln steht für die Hintereinanderausführung von rechts nach links.]

Lösung.

$$\begin{aligned} (12)(23) &= (123), \\ (12)(23)(31)(41) &= (14)(23), \\ (12)(23)(31)(45) &= (23)(45), \\ (12)(23)(34)(45) &= (12345). \end{aligned}$$

○

(ii) Welche der Elemente (123), (1342), (13425) sind in A_5 enthalten?

Lösung.
- $(123) = (12)(23)$, also ist (123) in A_5 enthalten.
- (1342) ist nicht in A_5 enthalten, denn $(1342) = (24)(12)(13)$.
- (13425) ist in A_5 enthalten, denn $(13425) = (51)(24)(12)(13)$ oder $(13425) = (13)(34)(42)(25)$.

○

(iii) Ist A_5 eine Gruppe? Ist A_5 kommutativ?

Lösung. A_5 ist eine Gruppe:

- Die identische Abbildung () liegt in A_5.
- Sind σ_1, σ_2 Elemente aus A_5, so lassen sich nach Definition σ_1 und σ_2 jeweils als Verknüpfung einer geraden Anzahl von Vertauschungen schreiben. Also besteht auch $\sigma_1\sigma_2$ aus einer geraden Zahl von Vertauschungen und A_5 ist abgeschlossen unter der Verknüpfung.

- Jede Vertauschung (i,j) ist zu sich selber invers: $(i,j)(i,j) = e$. Ist

$$\sigma = (i_1, j_1) \cdots (i_{2s}, j_{2s})$$

ein Element aus A_5, so ist das inverse Element $\sigma^{-1} = (i_{2s}, j_{2s}) \cdots (i_1, j_1)$. Dieses ist offenbar wieder in A_5, da die Anzahl an Vertauschungen gerade ist.

Die Gruppe A_5 ist nicht kommutativ: $(123)(234) = (12)(23)(23)(34) = (12)(34)$, aber $(234)(123) = (23)(34)(12)(23) = (13)(24) \neq (12)(34)$. ◯

(iv) Ist $H = \{(), (12)(34), (13)(24), (14)(23)\}$ eine Untergruppe von A_5? [Der Zykel $()$ steht für die identische Permutation.]

Lösung. Ja, H ist eine Untergruppe von A_5. Denn:

$$\begin{aligned}
(12)(34) \cdot (13)(24) &= (14)(23) = (13)(24) \cdot (12)(34) \\
(13)(24) \cdot (14)(23) &= (12)(34) = (14)(23) \cdot (13)(24) \\
(14)(23) \cdot (12)(34) &= (13)(24) = (12)(34) \cdot (14)(23).
\end{aligned}$$

Das zeigt, dass H in A_5 abgeschlossen ist, dh. das Produkt von je zwei Elementen aus H ist wieder in H. Das neutrale Element ist nach Definition auch in H. ◯

Wir beobachten hier übrigens, dass H sogar kommutativ ist.

Es ist ferner nützlich festzustellen, dass H genau die Elemente σ von A_4 (eine echte Teilmenge von A_5) enthält, deren Quadrat die identische Permutation ist, für die also $\sigma^2 = ()$ gilt.

Tatsächlich ist H die sogenannte *Kleinsche Vierergruppe* $\mathbb{Z}_2 \times \mathbb{Z}_2$.

(v) Ist H ein Normalteiler in A_5?

Lösung. Die Untergruppe H ist kein Normalteiler in A_5. Wäre H ein Normalteiler, müsste für jedes $\sigma \in A_5$ gelten: $\sigma H = H\sigma$. Nimm $\sigma = (345)$. Wegen $(345) = (34)(45)$ liegt σ in A_5 (im allgemeinen sind Dreierzykel immer Produkt von zwei Vertauschungen). Wir berechnen nun $H\sigma$:

$$\begin{aligned}
(12)(34)(345) &= (12)(45) \\
(13)(24)(345) &= (13245) \\
(23)(14)(345) &= (14523).
\end{aligned}$$

Nun ist aber $\sigma(12)(34) = (345)(12)(34) = (12)(345)(34) = (12)(35) \notin H\sigma$, also ist H kein Normalteiler. ◯

Lösung. Die Untergruppe H ist kein Normalteiler in A_5. Wäre H ein Normalteiler, müsste für jedes $\sigma \in A_5$ gelten: $\sigma H = H\sigma$. Insbesondere muss für alle $\sigma \in A_5$ und $h \in H$ also $h\sigma \in \sigma H$ oder $\sigma^{-1}h\sigma \in H$ gelten. Nimm $\sigma = (345) \in A_5$ und $h = (12)(34) \in H$. Dann ist $\sigma^{-1} = (354)$ und $\sigma^{-1}h\sigma = (12)(35)$. Aber das ist nicht in H und damit ist H kein Normalteiler. ◯

(vi) Ist A_5 ein Normalteiler in S_5?

Lösung. Ja, A_5 ist ein Normalteiler von S_5. Wir wollen zeigen: Für jede Permutation $\sigma \in S_5$ gilt $\sigma A_5 = A_5\sigma$. Für $\sigma \in A_5$ ist dies klar, denn da A_5 eine Gruppe ist, gilt $\sigma A_5 = A_5$. Sei also $\sigma \in S_5 \backslash A_5$. Wir behaupten: $\sigma A_5 = A_5\sigma = S_5 \backslash A_5$, d.h., *jede* ungerade Permutation ensteht durch Zusammensetzung von σ mit einer geraden Permutation von rechts oder links. In der Tat, sei σ' eine beliebige ungerade Permutation. Dann ist $\sigma^{-1}\sigma' \in A_5$ (da ungerade und ungerade gerade gibt) und $\sigma' = \sigma(\sigma^{-1}\sigma') \in \sigma A_5$. Analog zeigt man $\sigma' \in A_5\sigma$. ◯

Lösung. Ja, A_5 ist ein Normalteiler von S_5. Wir beweisen die Aussage, indem wir A_5 als Kern eines Homomorphismus identifizieren, denn nach einem Satz aus der Vorlesung folgt, dass der Kern eines Homomorphismus ein Normalteiler ist. Betrachte die Abbildung

$$\operatorname{sgn}\colon \begin{array}{ccl} S_5 & \longrightarrow & \{+1,-1\}\,, \\ \sigma & \longmapsto & \begin{cases} -1, & \text{falls } \sigma \in S_5 \setminus A_5, \\ +1, & \text{falls } \sigma \in A_5. \end{cases} \end{array}$$

Betrachte $\{+1,-1\}$ als multiplikative Gruppe mit $+1$ als neutralem Element. Die Abbildung sgn ist ein Gruppenhomomorphismus: $\operatorname{sgn}(\sigma_1\sigma_2) = \operatorname{sgn}(\sigma_1)\operatorname{sgn}(\sigma_2)$. Dies lässt sich einfach überprüfen, indem die möglichen Fälle (z.B. σ_1, σ_2 beide gerade/ungerade) untersucht werden. Der Kern dieses Homomorphismus ist aber genau A_5, woraus insbesondere folgt dass A_5 ein Normalteiler in S_5 ist. ◯

Bemerkung: Man kann die Elemente der S_5 auch als Permutationsmatrizen darstellen: zu einer Permutation σ gehört dabei die Matrix S_σ mit Einträgen 0 und 1, wo genau an den Positionen $(\sigma(i), i)$ eine Eins steht, der i-te Einheitsvektor e_i im $\mathbb{R}^5$ wird also auf $e_{\sigma(i)}$ abgebildet. Die Abbildung $S_5 \to \mathrm{GL}_5(\mathbb{R}),\ \sigma \mapsto S_\sigma$ ist ein Gruppenhomomorphismus. (Prüfe das!)

Wenn man nun hier die Determinante, die ein Gruppenhomomorphismus von $\mathrm{GL}_5(\mathbb{R})$ nach $\mathbb{R}^\times$ ist (es gilt also $\det(AB) = \det A \cdot \det B$), anschließt, so erhält man die obige Funktion sgn, die nun als Komposition zweier Gruppenhomorphismen ein ebensolcher sein muss.