Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

Fachbereich Mathematik
Algebra und Zahlentheorie
Christian Curilla

Grundlagen der Mathematik (LPSI/LS-M1)

Lösungen Blatt 8 WiSe 2010/11 - Curilla/Koch/Ziegenhagen

Präsenzaufgaben

(P27) (a) Wir schauen uns als Beispiel $m = 6$ und die Äquivalenzklassen $[2]$ und $[4]$ an: Es ist $[2] = \{..., -10, -4, 2, 8, ...\}$ und $[4] = \{..., -8, -2, 4, 10, ...\}$. Es ist also unter anderem $[2] = [-10] = [8]$ und $[4] = [-8]$. Wir berechnen alle Möglichkeiten, $[2] \odot [4]$ mit diesen verschiedenen Darstellungen auszurechnen:

$$\begin{aligned}
[2] \odot [4] &= [8] = [2 + 1 \cdot 6] = [2]\,, \\
[2] \odot [-8] &= [-16] = [2 + (-3) \cdot 6] = [2]\,, \\
[-10] \odot [4] &= [-40] = [2 + (-7) \cdot 6] = [2]\,, \\
[-10] \odot [-8] &= [80] = [2 + 13 \cdot 6] = [2]\,, \\
[8] \odot [4] &= [32] = [2 + 5 \cdot 6] = [2]\,, \\
[8] \odot [-8] &= [-64] = [2 + (-11) \cdot 6] = [2]\,.
\end{aligned}$$

Für diese Beispielzahlen ist das Ergebnis also stets dasselbe, egal welche der obigen Repräsentaten wir zur Berechnung nutzen.

(b) Sei $m \in \mathbb{Z}$ fest und $a, a', b, b' \in \mathbb{Z}$ gegeben mit $[a] = [a']$ und $[b] = [b']$. Wir gehen wie folgt vor: Zunächst überlegen wir uns, was $[a] = [a']$ bedeutet. Dann überlegen wir uns, was zu zeigen ist und was dies bedeutet. Schließlich kombinieren wir unsere Erkenntnisse zu einem Beweis.
Was bedeutet also die Gleichheit $[a] = [a']$? Die Mengen $[a]$ und $[a']$ sind Äquivalenzklassen. Die beiden Mengen sind folglich genau dann gleich, wenn a und a' in derselben Äquivalenzklasse liegen, also äquivalent zueinander sind bezüglich der Relation R_m. Es ist also $a \equiv a' \mod m$, d.h. m teilt $a - a'$. Es gibt folglich ein $k \in \mathbb{Z}$ mit $mk = a - a'$. Mit derselben Argumentation gibt es ein $l \in \mathbb{Z}$ mit $ml = b - b'$, da wir $[b] = [b']$ vorausgesetzt hatten.
Was ist zu zeigen? Wir wollen zunächst $[a] \oplus [b] = [a'] \oplus [b']$ beweisen, also (nach Definition von $\oplus$) zeigen, dass $[a + b]$ und $[a' + b']$ dieselbe Äquivalenzklasse sind. Wie oben für $[a]$ und $[a']$ erwähnt bedeutet dies, dass die Zahlen $a + b$ und $a' + b'$ äquivalent zueinander sind bezüglich R_m. Es gäbe dann also, mit den gleichen Argumenten wie oben, ein $s \in \mathbb{Z}$ mit $ms = a + b - (a' + b')$.
Nun sind wir beinahe fertig, wir müssen nur die Informationen aus dem ersten Teil so kombinieren, dass wir das gesuchte s finden. Die rechte Seite von $ms = a + b - (a' + b')$ ist gleich $a - a' + b - b'$. Dies ist die Summe der rechten Seiten unserer nach Voraussetzung gültigen Gleichungen $mk = a - a'$ und $ml = b - b'$. Addieren wir diese Gleichungen also, so erhalten wir mit $s := k + l$

$$ms = m(k + l) = mk + ml = a - a' + b - b' = a + b - (a' + b').$$

Folglich liegen $a+b$ und $a'+b'$ in derselben Äquivalenzklasse und die Wohldefiniertheit von $\oplus$ ist bewiesen.

Für die Wohldefiniertheit der Multiplikation sind die Voraussetzungen dieselben: Es gibt $k, l \in \mathbb{Z}$ mit $mk = a - a'$ und $ml = b - b'$.
Mit denselben Überlegungen wie eben erhalten wir, dass $[a] \odot [b] = [a'] \odot [b']$ bedeutet, dass es ein r mit $mr = ab - a'b'$ gibt.
Wir wollen also solch ein r finden. Da kein so unmittelbarer Zusammenhang zwischen Voraussetzungen und der zu beweisenden Gleichung zu sehen ist wie bei der Addition, formen wir die Voraussetzungen um, um sie in die zu zeigende Gleichung einzusetzen: Es ist

$$mk = a - a' \Leftrightarrow a = mk + a' \quad \text{und} \quad ml = b - b' \Leftrightarrow b = ml + b'.$$

Wir setzen dies in die rechte Seite der zu beweisenden Gleichung $mr = ab - a'b'$ ein:

$$\begin{aligned} ab - a'b' &= (mk + a')(ml + b') - a'b' \\ &= m^2kl + mkb' + mla' + a'b' - a'b' \\ &= m^2kl + mkb' + mla' = m(mkl + kb' + la'). \end{aligned}$$

Setzen wir also $r := mkl + kb' + la'$, so ist $mr = ab - a'b'$, und ab und $a'b'$ liegen in derselben Äquivalenzklasse. Damit ist auch die Multiplikation wohldefiniert.

(c) Wir schauen uns zunächst wieder die Beispielzahlen aus (P27a) an: Für $m = 6$ betrachten wir $[2] = [8]$ und $[4]$. Es ist $[2] * [4] = [|2 - 4|] = [2]$, aber $[8] * [4] = [|8 - 4|] = [4] \neq [2]$. Die Vorschrift $*$ liefert also keine wohldefinierte Verknüpfung.
Vorsicht: Man kann zwar durch ein Gegenbeispiel beweisen, dass eine Verknüpfung nicht wohldefiniert ist, aber nicht umgekehrt. Beispielsweise könnten wir Pech mit der Wahl unserer Beispiele haben: Es ist $[2] = [8] = [14] = [20] = ...$ und $[4] = [10] = [16] = [22]...$ und es gilt

$$[2] = [|2 - 4|] = [|8 - 10|] = [|14 - 16|] = [|20 - 22|] = ...$$

Man sieht also: Nur weil wir unendlich viele Beispiele finden, für die es keine Probleme gibt, heißt das nicht, dass eine Vorschrift wohldefiniert ist.

(P28) (a) Wir berechnen zwei Beispiele: Es ist $[2] \oplus [3] = [2+3] = [5] = [1+4] = [1]$ und $[2] \odot [3] = [2 \cdot 3] = [6] = [2+4] = [2]$. Es ist aber nicht nötig, alle Kombinationen einzeln auszurechnen. Drei Beobachtungen sparen Arbeit:
Erstens ist $[a] \oplus [b] = [a + b] = [b + a] = [b] \oplus [a]$ für alle $a, b \in \mathbb{Z}$, ebenso gilt $[a] \odot [b] = [a \cdot b] = [b \cdot a] = [b] \odot [a]$. Addition und Multiplikation sind also *kommutativ*.
Zweitens wissen wir, dass $[a] \oplus [0] = [a + 0] = [a]$ und $[a] \odot [1] = [a \cdot 1] = [a]$ ist für alle $a \in \mathbb{Z}$. Bezüglich der Addition ist also $[0]$, bezüglich der Multiplikation $[1]$ das *neutrale Element*.

Drittens hilft die Beobachtung, dass $[a] \odot [0] = [a \cdot 0] = [0]$ gilt für alle $a \in \mathbb{Z}$. Nutzt man dies, so muss man nur noch wenige Einträge per Hand ausrechnen und erhält schließlich:

$\oplus$	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

$\odot$	[0]	[1]	[2]	[3]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]
[2]	[0]	[2]	[0]	[2]
[3]	[0]	[3]	[2]	[1]

(b) Ein auffälliger Unterschied zu $\mathbb{Z}$ ist, dass das neutrale Element bezüglich der Addition, also [0], als Ergebnis der Multiplikation zweier Elemente ungleich [0] auftaucht: Es ist $[2] \odot [2] = [4] = [0]$. In $\mathbb{Z}$ ist stets $a \cdot b \neq 0$, falls $a, b \neq 0$ sind. *Anmerkung:* Ein Ring, in dem ein Produkt nur 0 ist, wenn ein Faktor des Produktes 0 ist, wird *nullteilerfrei* genannt. Dies ist wichtig, da man in einem solchen Ring Elemente ungleich 0 wegkürzen kann: Ist $ab = ac$ für Elemente a, b, c eines nullteilerfreien Rings, so können wir das zu $0 = ab - ac = a(b - c)$ umformen. Wegen der Nullteilerfreiheit lässt sich daraus $a = 0$ oder $b = c$ folgern.

(c) Zu $\mathbb{Z}/4\mathbb{Z}$: Um sagen zu können, was ein inverses Element bezüglich der Multiplikation im Ring ist, müssen wir erst das neutrale Element bezüglich der Multiplikation bestimmen. An der Verknüpfungstafel aus (P28a) sehen wir, dass [1] dieses neutrale Element ist.
Wiederum an der Verknüpfungstafel sehen wir, dass [1] und [3] invers zu sich selber sind und dass es zu [0] und [2] kein inverses Element bezüglich der Multiplikation gibt.

Zu $\mathbb{Z}/3\mathbb{Z}$: Die Verknüpfungstafel von $\mathbb{Z}/3\mathbb{Z}$ bezüglich $\odot$ ist

$\odot$	[0]	[1]	[2]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]
[2]	[0]	[2]	[1]

Wir lesen an der Verknüpfungstafel ab, dass [1] das neutrale Element bezüglich der Multiplikation ist. Zu [0] gibt es also kein Inverses, aber [1] ist zu sich selbst invers, ebenso [2].

Hausaufgaben

(H29) (a) Die Gleichung $[a] \odot [b] = [1]$ ist äquivalent zu $a \cdot b \equiv 1 \mod 15$. Dies ist wiederum gleichbedeutend zu $15|a \cdot b - 1$. Wir müssen also für alle $a \in \mathbb{Z}$ mit $0 \leq a < 15$ überprüfen, ob es ein $b \in \mathbb{Z}$ mit $0 \leq b < 15$ gibt, sodass $a \cdot b - 1$ durch 15 teilbar ist. Durch Verifizierung der unterschiedlichen Kombinationen erhalten wir:

$[a]$	$[1]$	$[2]$	$[4]$	$[7]$	$[8]$	$[11]$	$[13]$	$[14]$
$[b]$	$[1]$	$[8]$	$[4]$	$[13]$	$[2]$	$[11]$	$[7]$	$[14]$

Zusatzbemerkung: Man kann zeigen, dass es für $[a] \in \mathbb{Z}/m\mathbb{Z}$ genau dann ein Inverses bezüglich der Multiplikation gibt, wenn $\mathrm{ggT}(a, m) = 1$ ist.

(b) Die Gleichung $[a] \odot [b] = [0]$ ist äquivalent zu $a \cdot b \equiv 0 \mod 15$. Dies ist wiederum gleichbedeutend zu $15|a \cdot b$. Wir müssen also für alle $a \in \mathbb{Z}$ mit $0 < a < 15$ überprüfen, ob es ein $b \in \mathbb{Z}$ mit $0 < b < 15$ gibt, sodass $a \cdot b$ durch 15 teilbar ist (nach Voraussetzung ist $[a], [b] \neq [0]$, daher betrachten wir nur a und b mit $0 < a$ und $0 < b$). Wenn 15 ein Teiler von $a \cdot b$ sein soll, so muss 3 und 5 in der Primfaktorzerlegung von $a \cdot b$ vorkommen (weil $3 \cdot 5$ die Primfaktorzerlegung von 15 ist). Genau genommen muss in a eine Primzahl und in b die andere Primzahlen vorkommen (es können nicht beide in a oder beide in b vorkommen, weil sonst a oder b größer oder gleich 15 wären). Bei den Zahlen $3, 6, 9$ und 12 kommt die 3 in der Primfaktorzerlegung vor. Bei den Zahlen 5 und 10 kommt die 5 vor. Die restlichen Zahlen sind nicht durch 3 oder 5 teilbar. Es folgt somit, dass

- $[5]$ mit $[3], [6], [9], [12]$ Null ergibt,
- $[10]$ mit $[3], [6], [9], [12]$ Null ergibt,
- $[3]$ mit $[5], [10]$ Null ergibt,
- $[6]$ mit $[5], [10]$ Null ergibt,
- $[9]$ mit $[5], [10]$ Null ergibt und
- $[12]$ mit $[5], [10]$ Null ergibt.

Zusatzbemerkung: Nullteiler können niemals Inverse bezüglich der Multiplikation haben. Angenommen $[a]$ ist ein Nullteiler und $[a']$ ist das Element mit $[a] \odot [a'] = [0]$ und $[a'] \neq [0]$. Wenn jetzt $[a]$ ein Inverses hat, es also ein $[b]$ mit $[a] \odot [b] = [1]$ gibt, so würde gelten: $[a'] \odot ([a] \odot [b]) = [a'] \odot [1]$. Hieraus folgt $([a'] \odot [a]) \odot [b] = [a']$ und somit $[0] \odot [b] = [a']$. Dies liefert allerdings $[0] = [a']$, was ein Widerspruch ist, denn es war $[a'] \neq [0]$ vorausgesetzt.

(H30) (a) Wir erhalten $\mathrm{ggT}(a, b) = 1$, denn der Euklidische Algorithmus liefert

$$\begin{aligned} a &= 8 \cdot b + 1529 \\ b &= 8 \cdot 1529 + 80 \\ 1529 &= 19 \cdot 80 + 9 \\ 80 &= 8 \cdot 9 + 8 \\ 9 &= 8 + 1 \end{aligned}$$

(b) Weil für Zahlen $a, b \in \mathbb{Z} \setminus \{0\}$ die Formel $\mathrm{ggT}(a,b) \cdot \mathrm{kgV}(a,b) = |a| \cdot |b|$ gilt, erhalten wir mit der ersten Aufgabe

$$\mathrm{kgV}(a,b) = a \cdot b = 1231507800\,.$$

(H31) (a) Wir prüfen die Gruppenaxiome nach:

- Wohldefiniertheit: Es ist zu zeigen, dass die Verkettung zweier Abbildungen aus S_n wieder eine Abbildung aus S_n ist. Sind $f, g \in S_n$, so ist offenbar auch $f \circ g$ eine Abbildung von $\{1, ..., n\}$ auf sich selbst ist. Dass mit f und g auch $f \circ g$ bijektiv ist, hatten wir in Aufgabe (H21) bewiesen. Folglich ist $f \circ g \in S_n$.
- Assoziativität: Die Verknüpfung ist assoziativ, da die Verkettung von Funktionen stets assoziativ ist.
- Existenz des neutralen Elementes: Wir müssen eine Abbildung $e \in S_n$ finden, für die $e \circ f = f = f \circ e$ gilt für alle $f \in S_n$. Dies gilt offensichtlich für die in S_n enthaltene Identitätsabbildung

$$\mathrm{id}_{\{1,\ldots,n\}} \colon \{1, ..., n\} \to \{1, ..., n\},\ x \mapsto x.$$

- Existenz von Inversen: Sei $f \in S_n$ beliebig. Da f bijektiv ist, gibt es eine Umkehrabbildung $\tilde{f} \colon \{1, ..., n\} \to \{1, ..., n\}$ zu f. Da Umkehrabbildungen selbst wieder bijektiv sind, liegt $\tilde{f}$ in S_n. Nach Definition von Umkehrabbildungen gilt

$$f \circ \tilde{f} = \mathrm{id}_{\{1,\ldots,n\}} = \tilde{f} \circ f,$$

$\tilde{f}$ ist also das inverse Element zu f.

Die Gruppe S_n ist nicht kommutativ: Für $n \geq 3$ definiere $g, h \in S_n$ durch

$$g(x) := \begin{cases} 2 & \text{falls } x = 1, \\ 1 & \text{falls } x = 2, \\ x & \text{falls } x \neq 1, 2 \end{cases} \qquad \text{und} \qquad h(x) := \begin{cases} 3 & \text{falls } x = 2, \\ 2 & \text{falls } x = 3, \\ x & \text{falls } x \neq 2, 3. \end{cases}$$

Dann ist $(g \circ h)(1) = g(h(1)) = g(1) = 2$, aber $(h \circ g)(1) = h(g(1)) = h(2) = 3$. Also ist $h \circ g \neq g \circ h$.

(b) Für alle $n \in \mathbb{N}$ ist $|S_n| = n!$: Die 1 kann von einer Abbildung f auf n verschiedene Elemente abgebildet werden. Die 2 kann dann in jedem der n Fälle noch auf $n-1$ verschiedene Elemente abgebildet werden (wegen der Bijektivität darf $f(2)$ nicht gleich $f(1)$ sein), und so weiter. Kombiniert man alle Möglichkeiten für $f(1)$ mit allen für $f(2)$ etc., so ergeben sich $n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 2 \cdot 1 = n!$ verschiedene Möglichkeiten.

(c) Wir stellen uns, um systematisch zählen zu können, die vier (verschiedenfarbigen) Ecken der Holzplatte und die vier Ecken der Auflagefläche jeweils als von 1 bis 4 durchnummeriert vor. Damit lässt sich jede Möglichkeit, die Platte aufzulegen, als Element der S_4 interpretieren: Liegt die x-te Ecke der Platte

auf der y-ten Ecke der Fläche, so setzen wir $f(x) := y$.
Nun überlegen wir uns, wieviele Möglichkeiten es gibt, die Platte aufzulegen: Für die erste Ecke hat man natürlich noch freie Wahl, dafür gibt es also vier Möglichkeiten. Die Lage der ersten Ecke diagonal gegenüberliegenden Ecke ist dadurch aber auch festgelegt: Die gegenüberliegende Ecke der Platte muss auf der gegenüberliegenden Ecke der Fläche liegen. Betrachtet man nun eine der beiden noch nicht fixierten Plattenecken, hat man wieder freie Wahl, auf welche der beiden noch nicht belegten Flächenecken man sie legen will. Für die vierte Plattenecke ist dann nur noch eine Flächenecke frei.
Insgesamt erhalten wir also $4 \cdot 2 = 8$ verschiedene Möglichkeiten die Platte hinzulegen.

Anmerkung: Die Menge der acht zugehörigen Abbildungen aus S_4 bildet als echte Teilmenge von S_4 selbst wieder eine Gruppe mit $\circ$. Bildet eine Teilmenge einer Gruppe mit der Einschränkung der Verknüpfung auf die Teilmenge wieder eine Gruppe, so nennt man diese Teilmenge eine Untergruppe der ursprünglichen Gruppe.
Die Verkettung zweier solcher Abbildungen in diesem Beispiel entspricht dem Vorgang, die Platte erst hinzulegen und anschließend nochmal umzulegen - insgesamt wird die Platte also wieder auf die vorgegebene Fläche gelegt! Die Menge dieser acht Abbildungen wird häufig mit D_4 bezeichnet und „Diedergruppe“ genannt.

(H32) Die beiden Abbildungen sind wohldefinierte Verknüpfungen. Wir prüfen die Ringaxiome nach und halten uns dabei an die Bezeichnungen der Axiome aus der Vorlesung.

($R1$): Seien $a, b, c, d, e, f \in \mathbb{R}$, dann ist wegen der Assoziativität der Addition in $\mathbb{R}$

$$\begin{aligned}(a,b) + ((c,d) + (e,f)) &= (a,b) + (c+e, d+f)\\ &= (a + (c+e), b + (d+f))\\ &= ((a+c) + e, (b+d) + f)\\ &= (a+c, b+d) + (e,f)\\ &= ((a,b) + (c,d)) + (e,f)\end{aligned}$$

und wegen der Assoziativität der Multiplikation sowie der Distributivgesetze in $\mathbb{R}$

$$\begin{aligned}(a,b) \cdot ((c,d) \cdot (e,f)) &= (a,b) \cdot (ce - df, cf + de)\\ &= (a(ce-df) - b(cf+de), a(cf+de) + b(ce-df))\\ &= (ace - adf - bcf - bde, acf + ade + bce - bdf)\\ &= ((ac-bd)e - (ad+bc)f, (ad+bc)e + (ac-bd)f)\\ &= (ac-bd, ad+bc) \cdot (e,f)\\ &= ((a,b) \cdot (c,d)) \cdot (e,f).\end{aligned}$$

($R2$): Das neutrale Element bezüglich der Addition ist offensichtlich $(0,0) \in \mathbb{R}^2$: Es ist für beliebige $a, b \in \mathbb{R}$

$$(a,b) + (0,0) = (a+0, b+0) = (a,b) = (0+a, 0+b) = (0,0) + (a,b).$$

Um das neutrale Element bezüglich der Multiplikation zu finden, schreibt man die Bedingung $(a,b) \cdot (x,y) = (a,b)$ aus: Ist (x,y) neutral, so muss $a = ax - by$ und $b = ay + bx$ sein. Nach einigem Nachdenken kommen wir auf die Idee, dass $(1,0)$ das neutrale Element bezüglich der Multiplikation sein könnte und rechnen dies nach:

$$(1,0)\cdot(a,b) = (1\cdot a - 0\cdot b, 1\cdot b + 0\cdot a) = (a,b) = (a\cdot 1 - b\cdot 0, a\cdot 0 + b\cdot 1) = (a,b)\cdot(1,0).$$

($R3$): Da unsere Addition auf $\mathbb{R}^2$ komponentenweise definiert ist, ist die Summe von $(a,b) \in \mathbb{R}^2$ mit dem Tupel $(-a,-b) \in \mathbb{R}^2$

$$(a,b)+(-a,-b) = (a+(-a), b+(-b)) = (0,0) = ((-a)+a, (-b)+b) = (-a,-b)+(a,b),$$

wir finden also ein additiv Inverses $-(a,b) := (-a,-b)$ zu (a,b).

($R4$): Weil die Addition in $\mathbb{R}$ kommutativ ist, erhalten wir

$$(a,b) + (c,d) = (a+c, b+d) = (c+a, d+b) = (c,d) + (a,b).$$

Ehe wir die Distributivgesetze nachrechnen, untersuchen wir die Multiplikation in $(\mathbb{R}^2, +, \cdot)$ auf Kommutativität: Wegen der Kommutativität von Addition und Multiplikation in $\mathbb{R}$ ist

$$(a,b) \cdot (c,d) = (ac - bd, ad + bc) = (ca - db, cb + da) = (c,d) \cdot (a,b).$$

Die Multiplikation in $\mathbb{R}^2$ ist also kommutativ.

($R5$): Damit genügt es, nur ein Distributivgesetz nachzurechnen, denn dann folgt für beliebige $x, y, z \in \mathbb{R}^2$ aus $x \cdot (y+z) = x \cdot y + x \cdot z$ auch $(y+z) \cdot x = x \cdot (y+z) = x \cdot y + x \cdot z = y \cdot x + z \cdot x$.
Seien $a, b, c, d, e, f \in \mathbb{R}$ beliebig. Dann ist wegen der Distributivgesetze in $\mathbb{R}$

$$\begin{aligned}
(a,b) \cdot ((c,d) + (e,f)) &= (a,b) \cdot (c+e, d+f) \\
&= (a(c+e) - b(d+f), a(d+f) + b(c+e)) \\
&= (ac + ae - bd - bf, ad + af + bc + be) \\
&= (ac - bd, ad + bc) + (ae - bf, af + be) \\
&= (a,b) \cdot (c,d) + (a,b) \cdot (e,f).
\end{aligned}$$

Damit ist bewiesen, dass $(\mathbb{R}^2, +, \cdot)$ ein kommutativer Ring ist.

(H33) Will man die Äquivalenz dreier Aussagen A, B und C zeigen, so genügt es, $A \Rightarrow B, B \Rightarrow C$ und $C \Rightarrow A$ zu beweisen. Wegen der Transitivität der Implikation folgen dann die gewünschten Äquivalenzen. Dies nutzen wir im Folgenden.

(a) (f injektiv $\Rightarrow$ F_1 injektiv): Wir nehmen an, dass f injektiv ist und es gelte $F_1(C) = F_1(D)$ für Teilmengen $C, D \subseteq A$. Das bedeutet gerade $f(C) = \{f(c) : c \in C\} = \{f(d) : d \in D\} = f(D)$, also existiert zu jedem $c \in C$ ein $d \in D$ mit $f(c) = f(d)$. Weil daraus $c = d$ folgt (Injektivität von f!), gilt somit $c \in C \Rightarrow c \in D$. Das beweist $C \subseteq D$. Ganz analog geht die andere Richtung: Zu jedem $d \in D$ existiert ein $c \in C$ mit $f(d) = f(c)$, daraus folgt aber $d = c \in C$, also gilt $D \subseteq C$. Insgesamt können wir also $C = D$ folgern, F_1 ist also injektiv.
(F_1 injektiv $\Rightarrow$ F_2 surjektiv): Wir nehmen an, dass F_1 injektiv ist, und betrachten ein beliebiges, aber festes Element $C \in \mathrm{Pot}(A)$. Gesucht ist also eine Teilmenge $K \subseteq B$ mit $F_2(K) = C$. Wir setzen $K := F_1(C)$, dann gilt offensichtlich $F_2(K) = f^{-1}(K) \supseteq C$. Existierte ein Element $x \in f^{-1}(K) \setminus C$, so wäre $K = F_1(C) = F_1(C \cup \{x\})$, im Widerspruch zur Injektivität von F_1. Es folgt also $F_2(K) = C$, d.h. F_2 ist surjekiv.
(F_2 surjektiv $\Rightarrow$ f injektiv): Wir nehmen an, dass F_2 surjektiv ist. Seien $x, y \in A$ mit $f(x) = f(y)$. Dann existiert zu $\{x\} \in \mathrm{Pot}(A)$ ein Urbild bzgl. F_2, da F_2 ja surjektiv ist: $\exists\, M \subseteq B : F_2(M) = f^{-1}(M) = \{x\}$. Folglich ist $f(x) = f(y) \in M$, d.h. es gilt $y \in F_2(M) = f^{-1}(M) = \{x\}$, also $x = y$. Somit ist f injektiv.

(b) (f surjektiv $\Rightarrow$ F_1 surjektiv): Wir nehmen an, dass f surjektiv ist, und betrachten ein beliebiges, aber festes $M \in \mathrm{Pot}(B)$. Da f surjektiv ist, folgt $\forall\, m \in M : \exists\, a_m \in A : f(a_m) = m$. Eingesetzt in F_1 erhalten wir $F_1(\{a_m \in A : m \in M\}) = \{f(a_m) \in B : m \in M\} = M$, F_1 ist also surjektiv.
(F_1 surjektiv $\Rightarrow$ F_2 injektiv): Wir nehmen an, dass F_1 surjektiv ist, und betrachten Elemente $C, D \in \mathrm{Pot}(B)$ mit $C \neq D$. Wir können annehmen, dass ein Element $x \in C \setminus D$ existiert (sonst vertausche die Rollen von C und D). Da F_1 surjektiv ist, existiert eine Menge $K \subseteq A$ mit $F_1(K) = \{f(k) : k \in K\} = C$, insbesondere existiert also ein $k_0 \in K$ mit $f(k_0) = x \in C \setminus D$. Es folgt direkt $k_0 \in \underbrace{f^{-1}(C)}_{F_2(C)} \setminus \underbrace{f^{-1}(D)}_{F_2(D)}$, also $F_2(C) \neq F_2(D)$, d.h. F_2 ist injektiv.
(F_2 injektiv $\Rightarrow$ f surjektiv): Wir nehmen an, dass F_2 injektiv ist. Sei nun ein Element $y \in B$ vorgegeben. Da F_2 injektiv ist, gilt $F_2(\{y\}) \neq F_2(\emptyset) = \emptyset$, d.h. es existiert ein Element $x \in F_2(\{y\}) = f^{-1}(\{y\})$. Also existiert ein $x \in A$ mit $f(x) = y$, insgesamt folgt die Surjektivität von f.

(c) Wenn f bijektiv ist, sind nach Teil (a) und (b) auch F_1 und F_2 bijektiv, insbesondere existiert die Abbildung $F_1^{-1} : \mathrm{Pot}(B) \to \mathrm{Pot}(A)$.
Sei nun $M \subseteq B$ eine beliebige Menge. Da f und f^{-1} bijektiv sind, folgt nun

$$(F_1 \circ F_2)(M) = F_1(F_2(M)) = F_1\left(f^{-1}(M)\right) = F_1\left(\left\{f^{-1}(m) : m \in M\right\}\right)$$
$$= f\left(\left\{f^{-1}(m) : m \in M\right\}\right) = \left\{f\left(f^{-1}(m)\right) : m \in M\right\} = \{m : m \in M\} = M\ .$$