Tutorium 4, Mittwoch, 24.09., 10^{30} – 12^{00}

(Teilbarkeit Teil I)

Wiederholung:

Def. (Teilbarkeit): Seien $a, b \in \mathbb{Z}$. Dann gilt:

$a \mid b \Leftrightarrow \exists r \in \mathbb{Z}$ mit $b = ra$

„a teilt b" oder „b ist ein Vielfaches von a"

5.3.1. Aufgabe: Hinweis: grundlegende Beweistechniken Implikation zeigen, durch Verwendung der Ann.

Beweisen oder widerlegen Sie die folgenden Aussagen für ganze Zahlen $a, b, c, \ldots \in \mathbb{Z}$:

1. $a \mid b \Rightarrow a \mid cb$.
2. $a \mid b \Rightarrow ca \mid b$.
3. $ca \mid b \Rightarrow a \mid b$.
4. $a \mid cb \Rightarrow a \mid b$.
5. $c \mid ab \Rightarrow c \mid a \vee c \mid b$.
6. $c \mid ab \Rightarrow c \mid a \wedge c \mid b$.
7. $c \mid a \vee c \mid b \Rightarrow c \mid ab$.
8. $c \mid a \wedge c \mid b \Rightarrow c \mid ab$
9. $a \mid (b+c) \wedge a \mid b \Rightarrow a \mid c$.
10. $d \mid a \Rightarrow (m \cdot d) \mid (m \cdot a)$.
11. $ab \mid c \Rightarrow a \mid c \vee b \mid c$.
12. $ab \mid c \Rightarrow a \mid c \wedge b \mid c$.
13. $(n \cdot d) \mid (n \cdot a) \Rightarrow d \mid a$
14. $a \mid c \vee b \mid c \Rightarrow ab \mid c$
15. $a \mid c \wedge b \mid c \Rightarrow ab \mid c$.

Welche Aussagen lassen sich leicht umformulieren, sodass sie allgemein gültig werden?

Lösung: 1. Beweis: $a \mid b \Leftrightarrow \exists r \in \mathbb{Z}: b = ra \Rightarrow \exists r \in \mathbb{Z}: cb = \underbrace{cr}_{=: r' \in \mathbb{Z}}a$
$\Leftrightarrow \exists r' \in \mathbb{Z}: cb = r'a \Leftrightarrow a \mid cb$.

2. Gegenbeispiel: $2 \mid 8$, aber $6 \nmid 8$.

3. Beweis: $ca \mid b \Leftrightarrow \exists r \in \mathbb{Z}: b = \underbrace{rc}_{=: r' \in \mathbb{Z}}a \Rightarrow \exists r' \in \mathbb{Z}: b = r'a \Leftrightarrow a \mid b$.

4. Gegenbeispiel: $15 \mid 5 \cdot 9 = 45$, aber $15 \nmid 9$.

5. Gegenbeispiel: $15 \mid 5 \cdot 9 = 45$, aber $15 \nmid 5$ und $15 \nmid 9$.

6. Gegenbeispiel: das Gleiche wie für 5.

7. Beweis: Es gelte $c \mid a \vee c \mid b$. oBdA: $c \mid a$.
Dann: $\exists r \in \mathbb{Z}: a = rc \Rightarrow ab = rcb \Leftrightarrow ab = \underbrace{rb}_{=: r' \in \mathbb{Z}}c$
$\Leftrightarrow \exists r' \in \mathbb{Z}: ab = r'c \Leftrightarrow c \mid ab$.

8. Beweis: analog zu 7.

9. Beweis: Es gilt: $\exists r \in \mathbb{Z}: \underbrace{b + c = ra}$ und $\exists s \in \mathbb{Z}: b = sa$.
$\Leftrightarrow c = ra - b$ einsetzen
$\Leftrightarrow c = ra - sa$
$\Leftrightarrow c = (r-s)a$
$\Leftrightarrow a \mid c$

10. ~~$d \mid a \Rightarrow (m \cdot d) \mid (m \cdot a)$~~
Beweis: Es gilt: $\exists r \in \mathbb{Z}: a = rd \Rightarrow ma = mrd \Leftrightarrow ma = rmd$
$\Leftrightarrow md \mid ma$.

11. Beweis: Es gilt: $\exists r \in \mathbb{Z}: c = \underbrace{ra}_{=: r' \in \mathbb{Z}}b \Rightarrow \exists r' \in \mathbb{Z}: c = r'b$
$\Leftrightarrow b \mid c$.
$\Rightarrow a \mid c \vee b \mid c$.

12. Beweis: Analog zu 11: $\exists r \in \mathbb{Z}: c = \underbrace{ra}_{=: r' \in \mathbb{Z}}b \Rightarrow \exists r' \in \mathbb{Z}: c = r'b \Leftrightarrow b \mid c$
und $c = \underbrace{rb}_{=: r'' \in \mathbb{Z}}a \Rightarrow \exists r'' \in \mathbb{Z}: c = r''a \Leftrightarrow a \mid c$.

falls $n \neq 0$ nötig

13. Beweis: Es gilt: $\exists r \in \mathbb{Z}: na = rnd$
$\Leftrightarrow na = nrd \overset{n \neq 0,\ \text{Kürzungsregel}}{\Leftrightarrow} a = rd \Leftrightarrow d \mid a$

14. Gegenbeispiel: z.B. $2 \mid 16$, aber $2 \cdot 3 \nmid 16$. $(2 \mid 16 \vee \underbrace{3 \nmid 16}_{3 \nmid 16 \text{ wahr}}$ wahr)

15. Gegenbeispiel: $6 \mid 12$ und $4 \mid 12$, aber $24 \nmid 12$.

5.3.2. Aufgabe:

Zeigen Sie mit Hilfe der bisher erarbeiteten Regeln die folgenden Implikationen:

1. $4 \mid (2a + 3b) \Rightarrow 4 \mid (2a + 7b)$
2. $6 \mid (5x + 3y) \Rightarrow 2 \mid (5(x+1) + 5(y-3))$

Lösung:

1. Beweis: Es gelte: $4 \mid \underbrace{(2a + 3b)}_{= 2a + 7b - 4b}$.
Dann gilt: $4 \mid \underbrace{2a + 7b} + \underbrace{(-4b)}$ und $4 \mid 4b$.
teilt Summand + ganze Summe
Mit Regel 9: $4 \mid 2a + 7b$.

2. Es gelte: $6 \mid (5x + 3y)$. $2 \cdot 3 = 6 \mid \underbrace{(5x + 3y)}_{= 6} \overset{\text{Regel 3}}{\Rightarrow} 2 \mid (5x + 3y)$
Es gilt: $5(x+1) + 5(y-3) = 5x + 5y - 10 = (5x + 3y) + \underbrace{(2y - 10)}_{= 2(y-5)}$
Da $2 \mid 2(y-5)$, gilt: $2 \mid 5x + 3y + 2y - 10 = 5(x+1) + 5(y-3)$
mit Satz 5.1.5(2) $(a \mid x \wedge a \mid y \Rightarrow a \mid (x+y))$ aus der Vorlesung.

<u>Beweis</u> Satz 5.1.5 (2) aus der Vorlesung:

Es gelte $a \mid x \wedge a \mid y$. Dann $\exists r, r' \in \mathbb{Z}: x = ra \wedge y = r'a$.

Jetzt: $x + y = ra + r'a = \underbrace{(r + r')}_{=r'' \in \mathbb{Z}} a \Rightarrow \exists r'' \in \mathbb{Z}: x + y = r''a$

$\Leftrightarrow a \mid x + y$

Welche Aussagen lassen sich leicht umformen?:

z.B. 15.: $a \mid c \wedge b \mid c \Rightarrow ab \mid c$ ist richtig wenn $ggT(a,b) = 1$ ist

also: $a \mid c \wedge b \mid c \wedge ggT(a,b) = 1 \Rightarrow ab \mid c$.

(Beweis mit Hilfe von Lemma von Bézout)

Anmerkung machen: Zuerst Aufgabe 5.3.4. Lösen

5.3.3. Aufgabe:

~~z.B. Für $n \in \mathbb{Z}$ 1) n ist g~~

Zeigen Sie für $n \in \mathbb{Z}$:

1. n ist gerade $\Leftrightarrow$ n liefert bei Division ~~mit Rest~~ durch 2 den Rest 0.

2. n ist ungerade $\Leftrightarrow$ es gibt ein $k \in \mathbb{Z}$, sodass $n = 2 \cdot k + 1$.

<u>Lösung:</u>

<u>Wiederholung:</u> (Division mit Rest)

5.2.1. Satz (Satz von der Division mit Rest)

Für alle $a, b \in \mathbb{Z}$ mit $b \neq 0$, gibt es eindeutige $q, r \in \mathbb{Z}$, sodass: $a = q \cdot b + r \quad (0 \leq r < |b|)$.

q wird Quotient und r Rest genannt.

Wir lösen Aufgabe 5.3.3. indem wir zuerst 5.3.4 zeigen:

5.3.4. Aufgabe:

Es seien $a, b, d \in \mathbb{Z}$. Zeigen Sie, dass a und b genau dann denselben Rest bei Division durch d liefern, wenn $d \mid (a - b)$ gilt.

<u>Beweis:</u> Formalisiert: z.z.: $r_1 = r_2 \Leftrightarrow d \mid (a - b)$ für $a = qd + r_1$, $b = pd + r_2$ mit $0 \leq r_1 < d$, $0 \leq r_2 < d$.

„$\Rightarrow$": $r_1 = r_2$. Dann: $a - b = (qd + r_1) - (pd + r_2)$

$= qd + r_1 - pd - r_2$

$= (q - p)d + \underbrace{(r_1 - r_2)}_{=0 \text{ wegen } r_1 = r_2}$ Ann.

$= \underbrace{(q - p)}_{\in \mathbb{Z}} d$

$\Leftrightarrow d \mid (a - b)$

„$\Leftarrow$": Es gelte: $d \mid (a - b) \Leftrightarrow \exists k \in \mathbb{Z}: a - b = kd \Leftrightarrow a = kd + b$

~~(bei $b = pd + r_2$ mit $0 \leq r_2 < d$)~~: $a = kd + (pd + r_2) = (k + p)d + r_2$ mit $0 \leq r_2 < d$

$\Rightarrow$ a hat den ~~gleichen~~ selben Rest wie b bei Division durch d

BRUNNEN

Jetzt zu Aufgabe 5.3.3.:

2. n ungerade $\Leftrightarrow$ n und 1 liefern Rest 1 bei Div. durch 2

$\overset{5.3.4.}{\Leftrightarrow} 2 \mid (n-1)$

$\Leftrightarrow \exists k \in \mathbb{Z} : n-1 = 2k \Leftrightarrow n = 2k+1$

1. n ungerade $\Leftrightarrow$ n hat Rest 0 bei Div. durch 2

$\Leftrightarrow 2 \mid n \Leftrightarrow \exists k : n = 2k$

„$\Rightarrow$": $2 \mid (n-2) = (2k-2) = 2(k-1) \overset{5.3.4.}{\Leftrightarrow}$ n und 2 haben gleichen Rest bei Div. durch 2

„$\Leftarrow$": n und 2 haben Rest 0 bei Div. durch 2

$\overset{5.3.4.}{\Leftrightarrow} 2 \mid (n-2) \overset{9.}{\Rightarrow} 2 \mid n \Leftrightarrow \exists k \in \mathbb{N} : n = 2k.$

5.3.5. Aufgabe:

Es seien $a, b, d \in \mathbb{Z}$. r_a sei Rest von a bei Div. durch d,
r_b sei " " b " "

Zeigen Sie, dass $a+b$ bei Div. durch d den selben Rest liefert wie $r_a + r_b$.

Beweis: Satz von Div. mit Rest: oBdA $b \neq 0$

$\exists\, q_a, r_a \in \mathbb{Z} : a = q_a d + r_a$, ~~$b = q_b d + r_b$~~
& $q_b, r_b \in \mathbb{Z} : b = q_b d + r$
& $q, r \in \mathbb{Z} \quad r_a + r_b = qd + r$
} mit $0 \leq r_a, r_b, r < |d|$

Wir setzen ein: $a+b = (q_a d + r_a) + (q_b d + r_b)$

$= (q_a + q_b)d + \underbrace{(r_a + r_b)}_{= qd + r}$

$= (q_a + q_b + q)d + r$. □