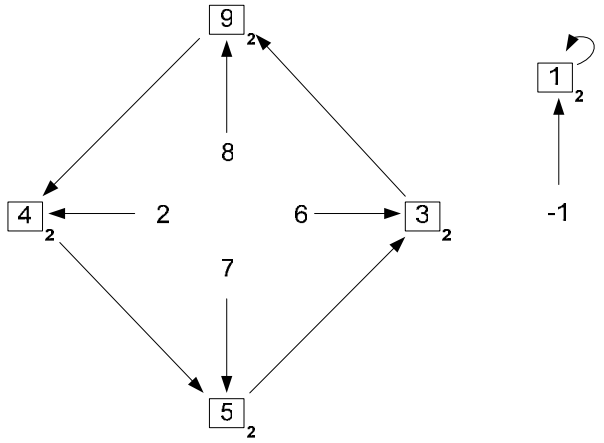
Bernhard Dietrich

[b|d] bernhard dietrich

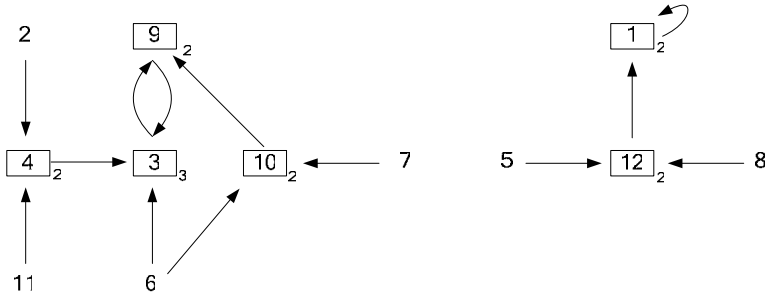
Mathematik für Informatiker II
Übungsblatt 6
Matrikel-Nr.: 6256800 · Übungsgruppe 2

Aufgabe 6.1

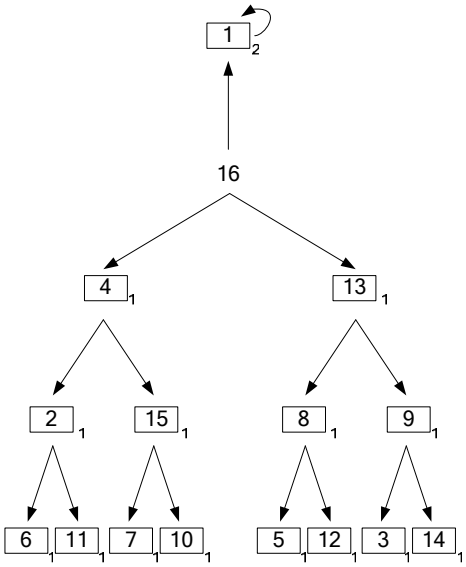
(i/ii) $\mathbb{Z}_{11}^{\times}$



$\mathbb{Z}_{13}^{\times}$



$\mathbb{Z}_{17}^{\times}$



(iii) Unter der Voraussetzung, dass die Operation „Mal“ in $\mathbb{Z}_p^\times$ kommutativ ist, gilt:

$$\begin{aligned} q(ab) &= (ab)^2 \\ &= abab \\ &= aabb \\ &= a^2b^2 \\ &= q(a)q(b) \end{aligned}$$

(iv) $$\begin{aligned} \ker q &= \left\{ x \in \mathbb{Z}_p^x \mid q(x) = 1 \right\} \\ &= \left\{ x \in \mathbb{Z}_p^x \mid x^2 \equiv 1 \bmod p \right\} \\ &= \left\{ x \in \mathbb{Z}_p^x \mid x^{2k} \equiv 1 \bmod p \right\} \end{aligned}$$

Da $\mathbb{Z}_p^x$ eine zyklische Gruppe ist, folgt

$\exists a \in \mathbb{Z}_p^x$ mit

$\mathbb{Z}_p^x = \left\{ a, a^2, ..., a^{p-1} \right\}$ und es gilt

$a^k \not\equiv 1 \mod p$ für alle $1 \le k < p-1$ sowie nach dem kleinen Satz von Fermat $a \equiv 1 \mod p$.

Es muss somit unterschieden werden zwischen $2 \mid p-1$ und $2 \nmid p-1$.

1. Fall: $2 \mid p-1$, und somit $p-1 = 2 \cdot d$ mit $d \in \mathbb{Z}$.

Es folgt $\mathbb{Z}_p^x = \left\{ a, a^2, ..., a^d, ..., a^{2d}, ..., a^{p-1} \right\}$

und daraus:

$a^{2d} = a^{p-1} \equiv 1 \bmod p$, $a^{2 \cdot 1 \cdot d} = a^{1(p-1)} \equiv a^{p-1} \bmod p$

Daraus folgt $\#\ker q = 2$, da gemäß dem zweiten Fall alle anderen Fälle $a^k \not\equiv 1 \mod p$.

2. Fall: $2 \nmid p-1$

Es gelte $a^n \in \mathbb{Z}_p^x$ mit $1 \le n \le p-1$.

Aus $\left.\begin{aligned} a^{2n} &\equiv 1 \bmod p \\ a^{2n} &\equiv a^{p-1} \bmod p \end{aligned}\right\}$ folgt $p-1 \mid 2n$.

Da wir voraussetzen, dass $2 \nmid p-1$, muss gelten $p-1 \mid n$ und wegen $1 \le n \le p-1$ folgt schließlich $n = p-1$ und somit $\ker q = \{1\}$ und $\#\ker q = 1$, wenn $2 \nmid p-1$.

(v) Die Größe des Bildes $\mathrm{im}q$ von q berechnet sich durch

$$\#\mathrm{im}q = \frac{\#\mathbb{Z}_p^x}{\#\ker q}.$$

Nach Definition ist $\#\mathbb{Z}_p^x = p-1$ und $\#\ker q$ wurde in iv für $2 \mid p-1$ mit $\#\ker q = 2$ be-

stimmt, so dass sich $\#\mathrm{im}q = \frac{\#\mathbb{Z}_p^x}{\#\ker q} = \frac{p-1}{2}$ ergibt. Für $2 \nmid p-1$ wurde $\#\ker q = 1$ bestimmt, so dass sich in diesem Fall $\#\mathrm{im}q = \frac{\#\mathbb{Z}_p^x}{\#\ker q} = \frac{p-1}{1} = p-1$ ergibt.

Aufgabe 6.2

i) 1. Fall: Sei $ggT(m,n) = 1$ und $m \neq n$, so folgt

$f(0 \bmod m) = 0 \bmod n$.

Da $f(0 \bmod m) \equiv f(m \bmod m)$ muss nun, damit die Abbildung wohldefiniert ist, folgen, dass $f(m \bmod m) = 0 \bmod n$.

Als Gegenbeispiel sei hier $k : \mathbb{Z}_7 \to \mathbb{Z}_3$ mit $f(a \bmod 7) = a \bmod 3$ genannt, für das gilt:

$f(0 \bmod 7) = 0 \bmod 3 \neq 1 \bmod 3 \equiv 7 \bmod 3 = f(7 \bmod 7)$.

2. Fall: Es gelte $n \mid m$, so dass folgt

Sei $a \in \mathbb{Z}_m$ und $a' = a + m \cdot k$ mit $k \in \mathbb{N}$.

$f(a \bmod m) = a \bmod n$

$f(a' \bmod m) = a' \bmod n = a \bmod n + m \cdot k \bmod n$

Da $n \mid m$ gilt, folgt $m \cdot k \bmod n \equiv 0$ und daraus

$a \bmod n + m \cdot k \bmod n = a \bmod n + 0 = a \bmod n$. Die Abbildung ist somit wohldefiniert.

ii) Gemäß Definition des Homorphismus muss für eine Abbildung $f : (G_1, \circ) \to (G_2, \bullet)$

$f(a \circ b) = f(a) \bullet f(b)$ gelten.

Es folgt somit

$$f(a \bmod m + a' \bmod m) = f(a \bmod m) + f(a' \bmod m)$$

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

Somit ist f ein Homorphismus.

iii) f ist surjektiv, wenn jedem Element aus $\mathbb{Z}_n$ mindestens ein Element aus $\mathbb{Z}_m$ zugeordnet wird.

iv) f ist injektiv, wenn jedem Element aus $\mathbb{Z}_n$ maximal ein Element aus $\mathbb{Z}_m$ zugeordnet wird.

v) f ist bijektiv, wenn f injektiv und surjektiv ist.

Aufgabe 6.3

(i) $\mathbb{Z}_7^\times = \{1,2,3,4,5,6\} = \langle 3 \rangle$

$3^0 = 1$

$3^2 = 2 \bmod 7$

$3^1 = 3$

$3^4 = 4 \bmod 7$

$3^5 = 5 \bmod 7$

$3^3 = 6$

(ii) $\mathbb{Z}_8^\times = \{1,3,5,7\}$ nicht zyklisch, da kein Erzeuger:

$3^1 = 3$	$5^1 = 5$	$7^1 = 7$
$3^2 = 1$	$5^2 = 1$	$7^2 = 1$
$3^3 = 3$	$5^3 = 5$	$7^3 = 7$
$3^4 = 1$	$5^4 = 1$	$7^4 = 1$
$3^5 = 3$	$5^5 = 5$	$7^5 = 7$
$3^6 = 1$	$5^6 = 1$	$7^6 = 1$
$3^7 = 3$	$5^7 = 5$	$7^7 = 7$

(iii) $\mathbb{Z}_9^\times = \{1,2,4,5,7,8\} = \langle 2 \rangle$

$2^0 = 1$

$2^1 = 2$

$2^2 = 4$

$2^5 = 5 \bmod 9$

$2^4 = 7 \bmod 9$

$2^3 = 8$

(iv) $\mathbb{Z}_{10}^\times = \{1,3,7,9\} = \langle 3 \rangle$

$3^0 = 1$

$3^1 = 3$

$3^3 = 7 \bmod 10$

$3^2 = 9$

(v) $\mathbb{Z}_{11}^{\times} = \{1,2,3,4,5,6,7,8,9\} = \langle 2 \rangle$

$2^0 = 1$

$2^1 = 2$

$2^8 = 3 \bmod 11$

$2^2 = 4$

$2^4 = 5 \bmod 11$

$2^9 = 6 \bmod 11$

$2^7 = 7 \bmod 11$

$2^3 = 8$

$2^6 = 9 \bmod 11$

$2^5 = 10 \bmod 11$

Aufgabe 6.4

(i) $(12)(23) = (123)$

$(12)(23)(31)(41) = (14)(23)$

$(12)(23)(31)(45) = (23)(45)$

$(12)(23)(34)(45) = (12345)$

(ii) Enthalten, sind $(123) = (12)(23)$ und $(13425) = (12)(14)(25)(13)$

Nicht enthalten ist (1342), da $(1342) = (24)(21)(13)$

(iii) Ist die Gruppenverknüpfung assoziativ, ein Neutralelement existiert und zu jedem Element existiert ein Inverses, dann ist die Definition der Gruppe erfüllt.
Assoziativität:
$\sigma_1, \sigma_2 \in A_5 \Rightarrow \sigma_1 \circ \sigma_2 \in A_5$
Neutralelement:
Das neutrale Element ist die identische Abbildung $(\ )$.
Inverse:
$\sigma, \sigma^{-1} \in A_5$
$(i, j) \circ (j, i) = e$
Somit ist A_5 eine Gruppe.
Kommutativität:
$(34)(45) = (345) \neq (354) = (45)(34)$
A_5 ist nicht kommutativ.

(iv) H ist Teilmenge von A_5.
H enthält mit $(\ )$ das neutrale Element.
Die Gruppe ist abgeschlossen und sogar kommutativ:
$(12)(34)(13)(24) = (14)(23) \in H = (13)(24)(12)(34)$
$(13)(24)(14)(23) = (12)(34) \in H = (14)(23)(13)(24)$

$(12)(34)(14)(23) = (24)(31) \in H = (14)(23)(12)(34)$

Also ist H eine kommutative Gruppe mit $\sigma \in H \Rightarrow \sigma^{-1} \in H$ mit $\sigma = \sigma^{-1}$.Somit ist H Untergruppe von A_5.

(v) Eine Untergruppe von A_5 ist ein Normalteiler wenn gilt:
$\sigma H = H\sigma$ mit $\sigma \in A_5$

(vi) Zu zeigen: $\sigma A_5 = A_5\sigma$ bzw. $\sigma x\sigma^{-1} \in A_5$ mit $\sigma \in S_5$