Übung 8

Nachbesprechung

- $a = \prod_i p_i^{e_i}$ schreibt hin was p_i, e_i sind
  - ↪ Primfaktorenzerlegung
- Direkter Beweis von $S \Rightarrow T$:

  S

  $\Rightarrow S_1 \quad \dots \quad \Rightarrow S_n$

  $\Rightarrow T$

  sehr of wurden die Beweise umgekehrt gemacht

Algebra

$\langle G; * \rangle$ ist eine Algebra, wenn G eine Menge ist und $*: G^k \to G$. Das heisst alle Algebren sind abgeschlossen unter der Operation $*$ $(a,b \in G \Rightarrow a*b \in G)$

Monoid $\langle G; *, e \rangle$ $(*: G^2 \to G)$

- Assoziativität von $*$ $a*(b*c) = (a*b)*c$ für alle $a,b,c \in G$ (G1)
- Neutrales Element $e \in G$ $e*a = a*e = a$ für alle $a \in G$ (G2)

Gruppe $\langle G; *, \wedge, e \rangle$ Jede Gruppe ist auch ein Monoid, zusätzlich:

- Inverses Element für jedes $a \in G$ existiert $\hat{a} \in G$, so dass $a*\hat{a} = \hat{a}*a = e$ (G3)

Abelsche Gruppe $\langle G; *, \wedge, e \rangle$ Ist eine Gruppe, zusätzlich:

- Kommutativität $a*b = b*a$ für alle $a,b \in G$

(nicht jede Gruppe erfüllt Kommutativität)

Beispiele

- $\mathbb{Z}$, operation: $+$ Abelsche Gruppe
- $\mathbb{Z}$, operation: $a * b := a^b$ Nichts (nicht assoz.)
- $\{0,1,2\}$, operation: $a * b := a + b$ Nichts (nicht abgeschlossen)
- $\mathbb{Q} \setminus \{0\}$, operation: $a * b := \frac{1}{2}ab$ Abelsche Gruppe
- Menge der bijektiven Fn $f: A \to A$, operation: composition Gruppe
- $\mathcal{P}(\mathbb{N})$, $\cap$ Monoid (keine Inverse)
- $\mathbb{Z}_n$, $\oplus_n$ Abelsche Gruppe

  z.B. $\mathbb{Z}_5 = \{0,1,2,3,4\}$ und $2 \oplus_5 4 = 1$, $2 \oplus_5 3 = 0$ $R_5(\cdot)$

Aufg. Sei $\langle G; *, \hat{}, e \rangle$ eine Gruppe. Beweise $\hat{\hat{a}} = a$ für alle $a \in G$

Wir dürfen verwenden:
- G1 assoz.
- G2 NE
- G3 inverse

Sei $a \in G$ beliebig.

$$
\begin{aligned}
a &= a * e && (G2)\\
&= a * (\hat{a} * \hat{\hat{a}}) && (G3)\\
&= (a * \hat{a}) * \hat{\hat{a}} && (G1)\\
&= e * \hat{\hat{a}} && (G3)\\
&= \hat{\hat{a}} && (G2)
\end{aligned}
$$

Eine Definition pro Schritt!

Group Homomorphism

Funktion $\psi: G \to H$ von einer Gruppe $\langle G; *, \sim, e \rangle$ zu einer Gruppe $\langle H; \cdot, \sim, e' \rangle$, so dass $\psi(a * b) = \psi(a) \cdot \psi(b)$ für alle $a, b \in G$.

kein Isomorphismus

Bsp. $\psi: G \to H$, $\psi(a) = e'$ für alle $a \in G$

da $\psi(a * b) = e' = e' \cdot e' = \psi(a) \cdot \psi(b)$ für alle $a, b \in G$

Isomorphismus, wenn $\psi: G \to H$ eine Bijektion ist

Gruppe $\mathbb{Z}_n^*$

mult. Inv. existiert

$\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \mid \gcd(a,n) = 1\}$

Primfaktorenzerlegung

$\varphi(n) = |\mathbb{Z}_n^*| = \prod_{i=1}^{r} (p_i - 1) p_i^{e_i - 1}$ wenn $n = \prod_{i=1}^{r} p_i^{e_i}$

Bsp. $\mathbb{Z}_{10}^* = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\} = \{1, 3, 7, 9\}$

↳ da $2 \mid 10$ und $5 \mid 10$ müssen alle Zahlen, die durch 2 oder 5 teilbar sind weg

In $\langle \mathbb{Z}_{10}^*; \odot_{10} \rangle$: $3 \cdot 7 \equiv_{10} 21 \equiv_{10} 1$, also ist 7 die Inverse von 3.

$\varphi(10) = (2-1) \cdot (5-1) = 4$, da $10 = 2 \cdot 5$

$\varphi(40) = (2-1) \cdot 2^{3-1} \cdot (5-1) = 16$, da $40 = 2^3 \cdot 5$

Aufg. Finde einen Isomorphismus zwischen $\langle \mathbb{Z}_9^*; * \rangle$ und $\langle \mathbb{Z}_6; + \rangle$.

$\mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8\}$ und $\langle 2 \rangle = \{1, 2, 4, 8, 7, 5\} = \mathbb{Z}_9^*$, also ist 2 ein Generator von $\mathbb{Z}_9^*$. Somit ist $\mathbb{Z}_9^*$ eine zyklische Gruppe und jedes $a \in \mathbb{Z}_9^*$ kann geschrieben werden als $a = 2^x$ für $x \in \{0, \dots, 5\}$. 1 ist ein Generator von $\mathbb{Z}_6$. Es gilt $1^1 = 1$, $1^2 = 2$, $1^3 = 3$, ... Jede $a \in \mathbb{Z}_6$ kann eindeutig als 1^x geschrieben werden für ein $x \in \{0, \dots, 5\}$.

Wir definieren $\psi: \mathbb{Z}_9^* \to \mathbb{Z}_6$, $\psi(2^a) = 1^a$.

zu zeigen: ψ ist ein homomorphismus

Seien $a, b \in \mathbb{Z}_9^*$ beliebig. Es gilt $a = 2^x$, $b = 2^y$ für x, y

$$\begin{aligned}
&\psi(a) \oplus_6 \psi(b) \\
&= \psi(2^x) \oplus_6 \psi(2^y) \\
&= 1^x \oplus_6 1^y && \text{(def } \psi\text{)} \\
&= 1^{x+y} \\
&= \psi(2^{x+y}) && \text{(def } \psi\text{)} \\
&= \psi(2^x \odot_9 2^y)
\end{aligned}$$

ψ ist bijektiv, da alle $a \in \mathbb{Z}_9^*$ bzw. alle $b \in \mathbb{Z}_6$ eindeutig in der Form 2^x bzw. 1^y geschrieben werden können.

Untergruppe $\langle H; *, \wedge, e\rangle$ von $\langle G; *, \wedge, e\rangle$
(gleiche Operation, Inverse und Neutrales Element)
Muss folgende Eigenschaften erfüllen:

- Abgeschlossenheit: Wenn $a, b \in H$, dann $a * b \in H$
- $e \in H$
- Inverse: Wenn $a \in H$, dann auch $\hat{a} \in H$
- Assoziativität: trivial, $\langle H; * \rangle$ hat gleiche Operation wie $\langle G; * \rangle$

Zwei triviale Untergruppen jeder Gruppe G: $\{e\}$, G
Lagrange: die Ordnung jeder Untergruppe teilt die Gruppenordnung

Bsp. $\langle \mathbb{Z}_8; \oplus_8 \rangle$ hat Untergruppen $\{0\}$, $\mathbb{Z}_8$, $\{0,4\}$, $\{0,2,4,6\}$ Ordnung 1, 8, 2 und 4

Bsp. $\langle \mathbb{Z}_7; \oplus_7 \rangle$ hat Ordnung 7. Da 7 eine Pz ist, folgt aus Lagrange, dass $\mathbb{Z}_7$ nur die beiden trivialen Untergruppen $\{0\}$ und $\mathbb{Z}_7$ hat.

Aufg. Sei $\langle G; *, \wedge, e\rangle$ eine Gruppe. Zeige, dass $H = \{a \in G \mid a * b = b * a \text{ für alle } b \in G\}$ eine Untergruppe von G ist.

i.) Zeige Abgeschlossenheit: Für alle $c, d \in H$ gilt $c * d \in H$
Nehmen wir an $c, d \in H$. Also erfüllen sie $c * a = a * c$ und $d * a = a * d$ für alle $a \in G$. Zu zeigen $(c * d) * a = a * (c * d)$ für alle $a \in G$. Sei $a \in G$ beliebig

$(c * d) * a$
$= c * (d * a)$ (G1)
$= c * (a * d)$ ($d \in H$)
$= (c * a) * d$ (G1)
$= (a * c) * d$ ($c \in H$)
$= a * (c * d)$ (G1)
$\Rightarrow (c * d) \in H$

ii.) Zeige $e \in H$

Für alle $b \in G$ gilt $b * e = b = e * b$, wobei 2 Mal G2 angewendet wurde

$\Rightarrow e \in H$

iii.) Zeige $c \in H \Rightarrow \hat{c} \in H$ für alle $c \in H$

Zu zeigen: $\hat{c} * a = a * \hat{c}$ für alle $a \in G$.

Sei $a \in G$ beliebig

$$
\begin{aligned}
&(\hat{c} * b) * c \\
=\ &\hat{c} * (b * c) && (G1) \\
=\ &\hat{c} * (c * b) && (c \in H) \\
=\ &(\hat{c} * c) * b && (G1) \\
=\ &e * b && (G3) \\
=\ &b = b * e && (2 \times G2) \\
=\ &b * (\hat{c} * c) && (G2) \\
=\ &(b * \hat{c}) * c
\end{aligned}
$$

$(\hat{c} * b) * c = (b * \hat{c}) * c$

$\Rightarrow \hat{c} * b = b * \hat{c}$ (Right cancellation)

Aufg. Sei $\langle G; *, \hat{}, e \rangle$ eine Gruppe und $f, g: G \to G$ zwei group homomorphismen. Sei $H \overset{\text{def}}{=} \{x \in G \mid f(x) = g(x)\}$ Beweise, dass $\langle H; *, \hat{}, e \rangle$ eine Untergruppe ist. (Abgeschlossenheit Beweis ausgelassen)

G1: Folgt direkt aus der Assoz. von G.

G2: Aus Lemma 5.5.i folgt $f(e) = e = g(e)$. Also gilt $e \in H$

G3: Sei $x \in H$ beliebig. Aus Lemma 5.5.ii. folgt $f(\hat{x}) = \hat{f(x)}$ und $g(\hat{x}) = \hat{g(x)}$.

$g(\hat{x}) = \hat{g(x)}$ (5.5.ii.)

$= \hat{f(x)}$ ($x \in H \Rightarrow g(x) = f(x)$)

$= f(\hat{x})$ (5.5.ii.)

$\Rightarrow \hat{x} \in H$

Aufg. Sei $\langle G; *, \hat{}, e\rangle$ eine Gruppe, S eine Menge und $\theta: G \times S \to S$ eine Funktion, sodass

(i) $\theta(e,s) = s$ für alle $s \in S$

(ii) $\theta(a*b, s) = \theta(a, \theta(b,s))$ für alle $a,b \in G$, $s \in S$

Beweise, dass $\psi_a: S \to S$ mit $\psi_a(s) = \theta(a,s)$ eine bijektive Funktion ist für alle $a \in G$.

Injektivität: $\psi_a(s) = \psi_a(t) \Rightarrow s = t$ für alle $s,t \in S$

Seien $s,t \in S$ beliebig

$\psi_a(s) = \psi_a(t)$

$\Rightarrow \theta(a,s) = \theta(a,t)$ (def ψ_a)

$\Rightarrow \theta(\hat{a}, \theta(a,s)) = \theta(\hat{a}, \theta(a,t))$ ($b = c \Rightarrow \theta(\hat{a},b) = \theta(\hat{a},c)$)

$\Rightarrow \theta(\hat{a}*a, s) = \theta(\hat{a}*a, t)$ (ii)

$\Rightarrow \theta(e,s) = \theta(e,t)$ (G3)

$\Rightarrow s = t$ (i)

Surjektivität: für jedes $s \in S$ gibt es ein $t \in S$, so dass $\psi_a(t) = s$

Sei $s \in S$ beliebig.

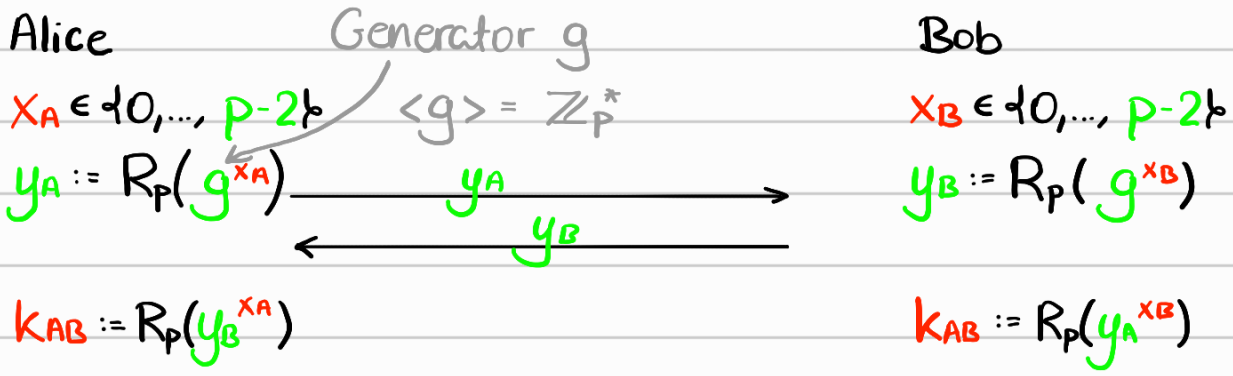
Wählen wir $t = \theta(\hat{a}, s)$, so gilt

$\psi_a(t) = \psi_a(\theta(\hat{a},s)) = \theta(a, \theta(\hat{a},s))$

$\overset{(ii)}{=} \theta(a*\hat{a}, s) \overset{(G3)}{=} \theta(e,s) \overset{(i)}{=} s$

Diffie-Hellman

Gruppe $\langle \mathbb{Z}_p^*; * \rangle$



Theorem 5.15. (vereinfacht)

Wenn p eine Pz ist, dann existiert Generator $g \in \mathbb{Z}_p^*$