Übung 9

Nachbesprechung

- $x = x * e = x * (y * \hat{y})$ x ist ein Element, keine Aussage
- $x \cdot y = u \cdot z$
  $\Rightarrow (x \cdot y) \cdot a = (u \cdot z) \cdot a$ oder $a \cdot (x \cdot y) = a \cdot (u \cdot z)$
  $\not\Rightarrow x \cdot a \cdot y = u \cdot z \cdot a$
- Beweist, dass $f([a]) = [\hat{a}]$ wohldefiniert ist

  Def.: $\forall a \in A \; \forall b, b' \in B \; (afb \wedge afb' \rightarrow b = b')$

  Lemma 5.2.: In a monoid, if a has a left and a right inv., then they are equal. In particular, a has at most one inverse.

Zyklische Gruppen

Def. Für Gruppe G und $a \in G$ ist Gruppe generiert von a $\langle a \rangle = \{a^i \mid i \in \mathbb{N}\}$.
$\langle a \rangle$ ist eine Untergruppe von G

Bsp. Gruppe $\langle \mathbb{Z}_8; \oplus \rangle$, $\langle 2 \rangle = \{0, 2, 4, 6\} = \langle 6 \rangle$, $\langle 1 \rangle = \mathbb{Z}_8$, $\langle 4 \rangle = \{0, 4\}$

Def. Eine Gruppe G heisst zyklisch, wenn ein $g \in G$ existiert, so dass $\langle g \rangle = G$. g ist ein Generator von G und es gilt $ord(g) = |G|$.

Bsp. Da $\langle 3 \rangle = \mathbb{Z}_8$ ist $\mathbb{Z}_8$ eine zyklische Gruppe und 3 ein Generator
($gcd(3,8) = 1$)

Aufg. Finde einen Generator von $\mathbb{Z}_{14}^*$

Es gilt $|\mathbb{Z}_{14}^*| = \varphi(14) = 6 = 2 \cdot 3$

Corollary 5.9 $ord(a) \mid G$ für alle $a \in G$

Also wissen wir, dass $ord(a) \in \{1, 2, 3, 6\}$ für alle $a \in \mathbb{Z}_{14}^*$ ist.

Es gilt also für jedes $a \in \mathbb{Z}_{14}^*$: $ord(a) \notin \{1, 2, 3\} \Rightarrow ord(a) = 6 \Rightarrow a$ ist Generator. Wir müssen also nur überprüfen, ob a^1, a^2 oder a^3 1 ergibt.

$\mathbb{Z}_{14}^* = \{1, 3, 5, 9, 11, 13\}$

$ord(1) = 1$, also kein Generator

Es gilt $3^1 \not\equiv_{14} 1$, $3^2 \not\equiv_{14} 1$ und $3^3 \equiv_{14} 13 \not\equiv_{14} 1$, also $\langle 3 \rangle = \mathbb{Z}_{14}^*$

Thm. Eine zyklische Gruppe G mit $|G| = n$ ist isomorph zu $\langle \mathbb{Z}_n; \oplus_n \rangle$ und abelsch (da Isomorphismus Strukturerhaltend ist)

- Jede zyklische Gruppe ist kommutativ
- Jede Gruppe G mit $|G| = p$ für Pz p ist zyklisch und jedes Element ausser dem NE ist ein Generator von G

Aufg. Ist jede kommutative Gruppe zyklisch?

Nein (Umkehrung gilt). z.B. $\langle \mathbb{Z}_2; \oplus \rangle \times \langle \mathbb{Z}_2; \oplus \rangle$ ist kommutativ, aber nicht zyklisch (jedes Element hat Ordnung 1 oder 2)

Isomorphe Gruppen

- $\mathbb{Z}_{n \cdot m} \simeq \mathbb{Z}_n \times \mathbb{Z}_m$ wenn $\gcd(n,m) = 1$

  Isomorphismus $\psi: \mathbb{Z}_{n \cdot m} \to \mathbb{Z}_n \times \mathbb{Z}_m$, $\psi(a) = (R_n(a), R_m(a))$
- $\mathbb{Z}_{n \cdot m}^* \simeq \mathbb{Z}_n^* \times \mathbb{Z}_m^*$ wenn $\gcd(n,m) = 1$

	Anz. Elemente	zyklisch?
$\langle \mathbb{Z}_n; \oplus \rangle$	n	für alle $n \in \mathbb{N}$
$\langle \mathbb{Z}_n; \oplus \rangle \times \langle \mathbb{Z}_m; \oplus \rangle$	$n \cdot m$	wenn $\gcd(n,m) = 1$
$\langle \mathbb{Z}_n^*; \odot \rangle$	$\varphi(n)$	wenn $n \in \{2, 4, p^e, 2 \cdot p^e\}$ für $p > 2$ Pz und $e \geq 1$
$\langle \mathbb{Z}_n^*; \odot \rangle \times \langle \mathbb{Z}_m^*; \odot \rangle$	$\varphi(n) \cdot \varphi(m)$	wenn $\gcd(n,m) = 1$ und $\mathbb{Z}_{n \cdot m}^*$ zyklisch

Aufg. Finde Gruppe Isomorph zu $\langle \mathbb{Z}_{12}; \oplus \rangle$

- $\langle \mathbb{Z}_3; \oplus \rangle \times \langle \mathbb{Z}_4; \oplus \rangle$
- $\langle \mathbb{Z}_{13}^*; \odot \rangle$ (13 is Pz, also ist $\mathbb{Z}_{13}^*$ zyklisch und $\varphi(13) = 12$)

Aufg. Wie viele nicht isomorphe Gruppen von Ordnung 23 gibt es?

Nur eine. 23 ist eine Primzahl. Also gilt für jede Gruppe G von Ordnung 23: $G \simeq \langle \mathbb{Z}_{23}; \oplus \rangle$

Satz von Euler

Aufg. Berechne $R_{21}(16^{12})$ $\quad R_a(b^c) \neq R_a(b^{R_a(c)})$

Wir können Korollar 5.10. verwenden: Sei G eine Gruppe mit $|G| = n$ und Operation $\circ_n$, dann gilt $a^n = 1$ (NE) für alle $a \in G$.

Hier sind wir in $\mathbb{Z}_{21}^*$. Da $\gcd(16, 21) = 1$ ist $16 \in \mathbb{Z}_{21}^*$. Es gilt $|\mathbb{Z}_{21}^*| = 2 \cdot 6 = 12$. Aus dem Korollar folgt $R_{21}(16^{12}) = R_{21}(16^{|\mathbb{Z}_{21}^*|}) = 1$

Allgemein: Nehmen wir an $\gcd(x, n) = 1$ und $x < n$, so gilt $x \in \mathbb{Z}_n^*$.

Sei $m = k \cdot \varphi(n) + r$ für $k, r \in \mathbb{N}$

$R_n(x^m) = R_n(x^{k \cdot \varphi(n) + r}) = R_n((x^{\varphi(n)})^k \cdot x^r) = R_n(1^k \cdot x^r) = R_n(x^r)$

RSA Verschlüsslung

Alice		Bob
$p, q \leftarrow$ sehr grosse Pz		
$n = p \cdot q$		$m \in \{1, \dots, n-1\}$
$f = (p-1)(q-1)$		
$e \leftarrow \mathbb{Z}_f^*$	$\xrightarrow{n, e}$	
		$y = R_n(m^e)$
	$\xleftarrow{y}$	
$d \equiv_f e^{-1}$		
$m = R_n(y^d)$		

es gilt $|\mathbb{Z}_n^*| = (p-1)(q-1) = f$ und $d \cdot e = k \cdot f + 1$ für ein $k \in \mathbb{N}$

Also ist $R_n(y^d) = R_n(m^{d \cdot e}) = R_n(m^{k \cdot f + 1}) = R_n(\underbrace{(m^f)^k}_{=1} \cdot m) = m$

Ringe $\langle R; +, -, 0, \cdot, 1\rangle$

$\langle R; +, -, 0\rangle$ abelsche Gruppe

$\langle R; \cdot, 1\rangle$ Monoid (muss nicht kommutativ sein)

R ist kommutativ, wenn $\cdot$ es ist

Bsp. nicht kommutativer Ring: Matrizen über $\mathbb{R}^{2\times 2}$

$A = \begin{bmatrix} 1 & -1 \\ 0 & 0 \end{bmatrix}$, $B = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$, dann ist $AB \neq BA$

Nie Kommutativität annehmen!

Nullteiler und Einheiten

Ring R

$a \in R \setminus \{0\}$ ist Nullteiler, wenn $a \cdot b = 0$ für ein $b \in R \setminus \{0\}$

$a \in R \setminus \{0\}$ ist Einheit, wenn $a \cdot b = 1$ für ein $b \in R$

(multiplikative Inverse von a existiert)

Aufg. Finde alle Nullteiler und Einheiten aus $\mathbb{Z}_{12}$

Alle $a \in \mathbb{Z}_{12} \setminus \{0\}$ mit $\gcd(a,12) \neq 1$ sind Nullteiler. Sei $\gcd(a,12) = k > 1$.

Dann gilt $a \cdot \frac{12}{k} = 0$. Da $\gcd(a,12) \mid 12$, ist $\frac{12}{k}$ eine ganze Zahl.

und es gilt $\frac{12}{k} \in \mathbb{Z}_{12}$.

Alle Elemente, die Inverse haben ($\gcd(a,12) = 1$) sind Einheiten.

$$\mathbb{Z}_{12} = \underbrace{\mathbb{Z}_{12}^*}_{\text{Einheiten}} \cup \underbrace{\overline{\mathbb{Z}_{12}^*} \setminus \{0\}}_{\text{Nullteiler}} \cup \{0\}$$

Aufg. Gilt in jedem Ring $a \cdot c = b \cdot c \Rightarrow a = b$ für alle $a, b, c \in R, c \neq 0$

Nein. Sei $R = \mathbb{Z}_8$. $a = 2$, $b = 6$, $c = 2$

$a \cdot c \equiv_8 4 \equiv_8 12 \equiv_8 b \cdot c$, aber $a \not\equiv_8 b$

↖ Nullteiler

Aufg. Beweise oder widerlege: Für jeden Ring R und bel. $a,b \in R$ gilt $a^2b = aba \Rightarrow ab = ba$

Gilt nicht. Idee: nicht kommutativen Ring wählen und $a \in R$ ein Element, dass keine mult. Inv. in R besitzt. Wir wählen $a,b \in R$ so, dass $ab = 0$ und $ba \neq 0$. Dann ist $a^2b = a \cdot 0 = 0 \cdot a = aba$, aber $ab = 0 \neq ba$

Gegenbsp.: R ist Ring der 2×2 Matrizen über $\mathbb{Z}$

$a = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$, $b = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$, dann ist $ab = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ und $ba = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$

Aufg. Sei R ein Ring und $a,b \in R$ so dass $a \cdot b = 1$. Sei $S \overset{\text{def}}{=} \{x \in R \mid ax = 1\}$. Beweise, dass $1 + b - za \in S$ für alle $z \in S$.

$1 + b - za \in S \Leftrightarrow a(1 + b - za) = 1$ $\quad \Rightarrow az = 1$

$$
\begin{aligned}
a(1+b-za) &= a1 + ab + a(-za) && \text{(left. dist)} \\
&= a + 1 + a(-za) && \text{(NE 1, } ab = 1\text{)} \\
&= a + 1 - aza && (u(-v) = -uv) \\
&= a + 1 - 1a && (az = 1) \\
&= a + 1 - a && \text{(NE 1)} \\
&= a - a + 1 && \text{(comm. +)} \\
&= 0 + 1 && (u - u = 0) \\
&= 1 && \text{(NE 0)}
\end{aligned}
$$

Es ist okay Klammern auszulassen und mit G1 von + begründen