Übungsstunde 8

Dan Philipp

Nachbesprechung Bonus

- Bei Gegenbeispiel konkretes Element angeben
- Mit Definition des lcm argumentieren

7.3 Properties of Greatest Common Divisors and Least Common Multiples ($\star$) ***(8 Points)***

Prove or disprove the following properties. Only use the definitions of ideals, gcd and lcm, and don't use the the results from Section 4.3.3 in the lecture.

a) For all positive integers a, b

$$(a) \cup (b) = (\gcd(a, b)).$$

b) For all positive integers a, b

$$(a) \cap (b) = (\operatorname{lcm}(a, b)).$$

Definition 4.5. The *least common multiple* l of two positive integers a and b, denoted $l = \operatorname{lcm}(a, b)$, is the common multiple of a and b which divides every common multiple of a and b, i.e.,

$$a \mid l \;\wedge\; b \mid l \;\wedge\; \forall m\big((a \mid m \wedge b \mid m) \rightarrow l \mid m\big).$$

Algebra

Algebra

Algebra: $\langle G, * \rangle$ für eine Menge G und eine abgeschlossene Operation $*: G^k \to G$

Monoid: $\langle M, *, e \rangle$

$*$ ist assoziativ: $a * (b * c) = (a * b) * c$ für alle $a, b, c \in M$

$e \in M$ ist neutrales Element: $a * e = e * a = a$ für alle $a \in M$

Gruppe: $\langle G, *, \hat{}, e \rangle$

G1: $*$ ist assoziativ $a * (b * c) = (a * b) * c$ für alle $a, b, c \in G$

G2: $e \in G$ ist neutrales Element: $a * e = e * a = a$ für alle $a \in G$

G3: Jedes $a \in G$ hat ein inverses Element: $a * \hat{a} = \hat{a} * a = e$

Eine Gruppe ist **abelsch**, wenn $*$ kommutativ: $a * b = b * a$ für alle $a, b \in G$

Aufgabe

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

Subgroups

Definition 5.11. A subset $H \subseteq G$ of a group $\langle G; *, \widehat{\ }, e \rangle$ is called a *subgroup* of G if $\langle H; *, \widehat{\ }, e \rangle$ is a group, i.e., if H is closed with respect to all operations:

(1) $a * b \in H$ for all $a, b \in H$,

(2) $e \in H$, and

(3) $\widehat{a} \in H$ for all $a \in H$.

Lagrange: Die Ordnung einer Subgroup teilt die Ordnung der Gruppe

Aufgabe: Finde alle Subgroups von $\langle \mathbb{Z}_8, \oplus_8 \rangle$ und von $\langle \mathbb{Z}_7, \oplus_7 \rangle$

Morphismen

Ein Homomorphismus ist eine Funktion $\psi: G \to H$ für zwei Gruppen $\langle G, *, \hat{}, e \rangle$ und $\langle H, \star, \tilde{}, e' \rangle$, die folgendes erfüllt:

$\psi(a * b) = \psi(a) \star \psi(b)$ für alle $a, b \in G$

Wenn diese Funktion zusätzlich bijektiv ist, ist es ein Isomorphismus. Man schreibt dann $G \simeq H$.

Isomorphismus beweisen

Zu beweisen: $G \simeq H$ für zwei Gruppen $\langle G, *, \hat{}, e \rangle$ und $\langle H, \star, \tilde{}, e' \rangle$:

- Funktion $\psi: G \to H$ finden
- Homomorphismus zeigen:

  $\psi(a * b) = \psi(a) \star \psi(b)$ für alle $a, b \in G$ zeigen
- Injektivität von ψ zeigen
- Surjektivität von ψ zeigen

Aufgabe

($\star$) Let $\langle G; +, \hat{}, e_G\rangle$ and $\langle H; \odot, \tilde{}, e_H\rangle$ be groups. Moreover, let $\varphi : G \to H$ be a bijective group homomorphism.
Prove that $\varphi^{-1} : H \to G$ is a group homomorphism. *(3 Points)*

Zyklische Gruppen

- Für eine Gruppe G und ein $a \in G$ ist die Gruppe generiert von a:

  $\langle a \rangle = \{a^i | i \in \mathbb{Z}\}$

  $\langle a \rangle$ ist eine Subgroup von G
- Eine Gruppe G ist **zyklisch,** wenn es ein $g \in G$ gibt mit $\langle g \rangle = G$

Generatoren finden

Wir wollen einen Generator einer zyklischen Gruppe G finden:

- Gruppenordnung |G| berechnen
- Die Ordnung jedes Elements muss nun ein Teiler der Gruppenordnung sein
- Wenn für ein $g \in G$ gilt $\mathrm{ord}(g) = |G|$, ist es ein Generator
- Somit finden wir die Generatoren durch Ausprobieren