

Beispiele von Gruppen und kurze Wiederholung von W7.

Kurze Wiederholung von Buch Seiten 130-132 (schon in den Folien betrachtet)

Buch Seiten 133-136: insbesondere: $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ ist ein Ring

Für p Primzahl $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ ist ein Körper.

Besonders wichtig

Lemma 5.62 und Bemerkung 5.65. Davon folgt dass das multiplicative Inverse von a in $\mathbb{Z}/n\mathbb{Z}$ wird durch Euklidische Algorithmus als x Lösung von $ax+ny=1$ bestimmt.

Definition von eulersche ϕ Funktion, Beispiele und Bestimmung von $\phi(p)$ und $\phi(p^r)$ für p Primzahl.