2 Gruppen

2.1 Definitionen

Gruppe G
G0 zweistellige Verknüpfung: $G \times G \to G$
G1 Assoziativgesetz $(x \cdot y) \cdot z = x \cdot (y \cdot z)$
G2 Einselement $ex = xe = x$
G3 Inverses $\forall x \in G \exists y \in G$ mit $xy = yx = e$

- Halbgruppe: $(A, \cdot)$: zweistellige assoziative Verknüpfung
  $G \times G \to G$, $(x, y) \mapsto x \cdot y$
  Assoziativgesetz: $(x \cdot y) \cdot z = x \cdot (y \cdot z)$
- Monoid: Halbgruppe mit Einselement e, $ex = xe = x$
- [2.4] Gruppe: Halbgruppe mit Einselement und Inversen
- (äußeres) kartesisches Produkt: $G_1 \times G_2$ mit komponentenweiser Verknüpfung
  $(g_1, g_2) \cdot (h_1, h_2) = (g_1 \cdot_1 h_1, g_2 \cdot_2 h_2)$
  Beispiel: Kleinsche Vierergruppe $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{\overline{0}, \overline{1}\} \times \{\overline{0}, \overline{1}\} = \{(\overline{0}, \overline{0}), (\overline{0}, \overline{1}), (\overline{1}, \overline{0}), (\overline{1}, \overline{1})\}$
- Kürzungsregeln gelten innerhalb einer Gruppe (lateinisches Quadrat)
  $a \cdot b = a \cdot c \Rightarrow b = c$
- $|m * n| = ggT(m, n) * kgV(m, n)$

2.2 Untergruppen und Zyklische Gruppen

Untergruppe U ($U \leq G$)
Eine nichtleere Teilmenge U einer Gruppe G heißt Untergruppe von G:
$a, b \in U \Rightarrow a \cdot b \in U$ und $a^{-1} \in U$ folgt.

- [2.7] Eine zyklische Gruppe ist eine von einem Element erzeugte Gruppe
- Eine unendliche Gruppe G ist zyklisch, wenn es in $a \in G$ gibt, so dass man alle von 0 verschiedenen Elemente von G durch Addition a bzw. von -a erhält.
  Für $\mathbb{Z}$ leistet dies $a = 1$.
- Ordnung einer Gruppe $|G| \in \mathbb{N} \cup \{\infty\}$
  Ordnung eines Elements ord(a) = $|<a>|$
- [2.9] $ord(a) = n \in \mathbb{N}$, dann ist n die kleinste natürliche Zahl m mit $a^m = e$
  Außerdem $<a> = \{e, a^0, a^1, ...a^{n-1}\}$ und $a^i = a^j$ ist äquivalent zu $i \equiv j(mod n)$
- Ein Element der Ordnung 2 nennt man Involution
- [2.11] G zyklisch $\Rightarrow$ jede Untergruppe von G zyklisch
  G hat endliche Ordnung n
  $\Rightarrow$ G hat für jeden Teiler r von n genau eine Untergruppe der Ordnung r
- Eulersche φ-Funktion
  Für $n \in \mathbb{N}$ bezeichne φ(n) die Anzahl der natürlichen Zahlen $1 \leq m \leq n$, die zu n teilerfremd sind
- zyklische Gruppe der Ordnung n hat $\varphi(n)$ Erzeuger
- (Üb 3.1c) $(\mathbb{Z}_m \times \mathbb{Z}_n, +)$ ist zyklisch $\Leftrightarrow$ m und n sind teilerfremd
  $\Rightarrow (\mathbb{Z}_m \times \mathbb{Z}_n, +) \cong (\mathbb{Z}_{mn}, +)$
- [2.13] $|a| = n$ und $ggT(n, m) = d \Rightarrow |a^m| = \frac{n}{d}$

2.3 Nebenklassen

Rechtsnebenklasse: $Ug = \{ug \mid u \in U\}$ (U\ G)
Linksnebenklasse: $gU = \{gu \mid u \in U\}$ (U/G)

- [2.16] Für zwei Nebenklassen Ug, Uh gilt entweder $Ug = Uh$ oder $Ug \cap Uh = \varnothing$
- **Index** von U in G: [G : U] = $|U\backslash G|$ (Anzahl der Nebeklassen)
- disjunkte Nebenklassenzerlegung = $G = \biguplus_i Ug_i$ für geeignete $g_i \in G$

  Partition von G

Lagrange
$U \leq G$. Dann gilt $|G| = |U||U\backslash G|$.
Insbesondere ist $|U|$ ein Teiler von $|G|$ (für $|G| < \infty$)

- Sei $|G| < \infty$. Für alle $g \in G$ ist ord(g) ein Teiler von $absG$
- [2.21] Gruppen von Primzahlordnung sind zyklisch

2.4 Normalteiler und Faktorgruppen

Normalteiler ($N \trianglelefteq G$)
$N \leq G$ heißt Normalteiler von G, wenn $Ng = gN$ für alle $g \in G$ gilt.

- [2.23] $N \leq G$ ist Normalteiler $\Leftrightarrow g^{-1}Ng \subseteq N$ für alle $g \in G$
- Untergruppen vom Index 2 sind stets Normalteiler
- **Faktorgruppe** von G modulo N: G/N
  $N \trianglelefteq G$. Dann gilt $(Ng)(Nh) = Ngh$ für alle $g, h \in G$
- Gruppe $|G| > 1$ heißt **einfach**, wenn sie außer G und $\{e\}$ keine weiteren Normalteiler hat

$N \leq G$: $\exists \varphi : N = ker\varphi \Leftrightarrow N \trianglelefteq G$

2.5 Symmetrische und alternierende Gruppen

Symmetrische Gruppe S_n
die Gruppe der Permutationen von {1,2,...,n}
$\varphi \in S_n$: $\varphi(a)$ ist das Bild von a unter φ
Angabe durch Wertetabelle oder Zykelnotation

Zykelnotation
$\psi \in S_n$ heißt m-Zykel, falls es eine Folge $a_1, ..., a_m$ gibt mit $\psi(a_i) = a_{i+1}$

- Ist $\phi \in S_n$ so heißt die Menge der von ϕ bewegten Elemente den Träger von ϕ
- Jedes Element ϕ aus S_n ist ein **Produkt von Zykeln** ψ_i mit disjunkten Trägern

Konjugiertheit
Die Elemente $a, b \in G$ heißen konjugiert, wenn es ein $g \in G$ gibt mit $b = g^{-1}ag = a^g$

- [2.27] Sei $\varphi = (a_1 a_2 ...)(b_1 b_2 ...) \in S_n$ in Zykeln und $\psi \in S_n$
  Dann gilt $\varphi^\psi = (a_1^\psi a_2^\psi ...)(b_1^\psi b_2^\psi ...)$
  Konjugation in Zykelschreibweise
- Seien $\alpha, \beta \in S_n$ Permutationen mit gleichen Zykellängen
  Dann sind α und β in S_n konjugiert
- 2-Zykel heißen **Transpositionen** (ungerade)
- Jede Permutation $\phi \in S_n$ ist ein Produkt von Transpositionen und jeder Zykel der Länge m ist ein Produkt von m-1 Transpositionen
- Länge von ϕ: $l(\phi) = \sum_{i=1}^{r}(m_i - 1)$, wobei $m_1, ..., m_r$ die Zykellängen sind
- Permutationen ϕ mit $l(\phi) \equiv 0 \pmod 2$ heißen gerade,
  solche mit $l(\phi) \equiv 1 \pmod 2$ heißen ungerade

Alternierende Gruppe A_n
Die Menge der gerade Permutationen aus S_n bildet eine Gruppe A_n mit $[S_n : A_n] = 2$
A_n ist für $n \geq 5$ einfach

- [2.33] Jede gerade Permutation ist ein Produkt von 3-Zykeln.
  Insbesondere wird A_n von den 3-Zykeln aus S_n erzeugt

$n \geq 5$: Alle 3-Zykel aus A_n konjugiert
$n \geq 5$: A_n einfach

- Träger = supp(g) = $\{x \in X \mid g(x) \neq x\}$ (Elemente die von g bewegt werden)
- $S_n, n \geq 3$, $A_n, n \geq 4$ nicht kommutativ
  τ_1 = (12), τ_2 = (23) und es gilt: $\tau_1\tau_2$ = (132), $\tau_2\tau_1$ = (123)
  σ_1 = (123), σ_2 = (234) und es gilt: $\sigma_1\sigma_2$ = (13)(24), $\sigma_2\sigma_1$ = (12)(34)

2.6 Homomorphismen

Homomorphismen (Strukturerhaltende Abbildung)
$\phi : G \to H$ von der Gruppe G in die Gruppe H heißt Homomorphismus,
wenn $(xy)^\phi = x^\phi y^\phi$ für alle $x, y \in G$.

- Beispiel:
  G = ($\mathbb{C}$,+), H = ($\mathbb{C}\backslash\{0\}$, $\cdot$), $x^\phi = e^x$ ist Homomorphismus, da
  $(x+y)^\phi = e^{x+y} = e^x e^y = x^\phi y^\phi$
- Homomorphismus bildet das neutrale Element auf das neutrale Element ab
- Das **Bild** $U^\phi = \{u^\phi \mid u \in U\}$ einer Untergruppe $U \leq G$ ist Untergruppe von H
- Das **Urbild** $V^{\phi^{-1}} = \{g \in G \mid g^\phi \in V\}$ einer Untergruppe $V \leq H$ ist eine Untergruppe von G. Ist dabei V normal in H, dann ist $V^{\phi^{-1}}$ normal in G
- Sind $x, y \in G$ konjugiert, so sind x^ϕ, y^ϕ in H konjugiert

Monomorphismus	ϕ ist injektiv
Epimorphismus	ϕ ist surjektiv
Isomorphismus	ϕ ist bijektiv
Endomorphismus	G = H
Automorphismus	G = H und ϕ ist bijektiv

- Die Menge der Automorphismen einer Gruppe G ist selbst eine Gruppe: Aut(G)
- $N \trianglelefteq G$, dann ist $\varphi : G \to G/N$ ein (**kanonischer**) Epimorphismus
- [2.37] Der **Kern** eines Hom. $\phi : G \to H$ ist die Menge der $g \in G$ mit $g^\phi = e_H$
  Kern(ϕ) $\trianglelefteq$ G
- **Bild**(ϕ) ist das Bild G^ϕ von G unter ϕ

Isomorphiesatz
Homomorphismus $\phi : G \to H$. Dann ψ: G/Kern(ϕ)$\to$ Bild(ϕ) (G mod Kern(ϕ))
Kern(ϕ)x $\mapsto x^\phi$ wohldefiniert und liefert Isomorphismus **G/Kern(ϕ)** $\cong$ **Bild(ϕ)**

- Bis auf Isomorphie gibt es nur die folgenden zyklischen Gruppen: ($\mathbb{Z}$,+) und ($\mathbb{Z}$/n$\mathbb{Z}$,+) für ein n $\in \mathbb{N}$
- (Cayley) Jede Gruppe G ist isomorph zu einer Untergruppe von Sym(G)
- Sei G eine Gruppe mit Untergruppe U und Normalteiler N.
  Dann gilt $U/_{U\cap N} \cong UN/_N$.
- Seien G eine Gruppe mit Normalteilern $N \subseteq M$.
  Dann gilt $(G/N)/_{(M/N)} \cong G/_M$.
- trivialer Homorphismus bildet auf das neutrale Element ab

2.7 Gruppenoperationen

Operation
Eine Operation einer Gruppe G auf einer Menge M ist eine Abbildung
$M \times G \to M\ (m, g) \mapsto m^g$, für die $m^e = m$ und $(m^g)^h = g^{gh}$ gilt für alle $m \in M, g \in G$

- $\phi : G \to Sym(M)$, dann ist ϕ ein Homomorphismus
  G operiert auf M $\Leftrightarrow$ Es gibt Hom: $\varphi : G \to S_M$
- Operation heißt **treu**, wenn es für alle $e \neq g \in G$ ein $m \in M$ gibt mit $m^g \neq m$
- Äquivalenzrelation auf M: zwei Elemente $m_1, m_2 \in M$ sind äquivalent genau dann, wenn es ein Element $g \in G$ gibt mit $m_2 = m_1^g$

Bahn
Die Äquivalenzklassen nennt man Bahnan (orbits)
$\{m^g \mid g \in G\} =: m^G$
Operation heißt **transitiv**, wenn M nur aus einer Bahn besteht
Die Bahnen bilden eine Partition von M

Stabilisator
$G_m = \{g \in G \mid m^g = m\}$ ist der Stabilisator von $m \in M$
$G_m \leq G$

- G operiert auf den Mengen M und N.
  $\phi : M \to N$ ist G-äquivariant, wenn $(m^g)^\phi = (m^\phi)^g$ gilt für alle $m \in M, g \in G$
- G operiere transitiv auf M. Sei U der Stabilisator eines Elements $m \in M$.
  Dann wird durch $\phi : U\backslash G \to M, Ux \mapsto m^x$ G-äquivariante Bijektion definiert.
- G operiere auf M.Die **Länge der Bahn** durch m berechnet sich durch
  $|m^G| = [G : G_m]$

Gruppe G operiere durch Konjugation auf sich selbst
Zentralisator
Stabilisator unter dieser Operation heißt Zentralisator von x in G: $C_G(x)$
besteht also aus allen $g \in G$ mit $gx = xg$
Konjugationsklasse
Bahn $x^G = \{g^{-1}xg \mid g \in G\}$ nennt man Konjugationsklasse von x in G
Zentralisator
$X \subseteq G$, so ist $C_G(X) = \{g \in G \mid x^g = x$ für alle $x \in X\}$ der Zentralisator von X in G
Zentrum
X = G, $Z(G) = C_G(G)$ das Zentrum von G
Normalisator
Stabilisator heißt Normalisator von X in G: $N_G(X) = \{g \in G \mid X^g = X\}$

$N_G(X), C_G(x), C_G(X)$ und Z(G) sind Untergruppen von G
$Z(G) \leq C_G(X) \leq C_G(x)$ und $C_G(X) \leq N_G(X)$

$C_G(H)$	$\subseteq$	$N_G(H)$	und $C_G(G) \subseteq C_G(X) \subseteq C_G(x)$
$\{g \in \mid gx = xg \forall x \in H\}$		$\{g \in G \mid H^g = H\}$	
stabilisert		stabilisiert	
punktweise		mengenweise	

Bahnengleichung
G operiere auf der endlichen Menge M; $m_1, ..., m_r$ sind Repräsentanten der Bahnen von G. Dann gilt
$|M| = \sum_{i=1}^{r} [G : G_{m_i}]$

Klassengleichung
Sind $x_1, ..., x_r$ Repräsentanten der Konjugationsklassen der endlichen Gruppe G, dann
$|G| = \sum_{i=1}^{r} [G : C_G(x_i)]$

- [2.50] $p \in \mathbb{P}$, $n \in \mathbb{N}$ und $|G| = p^n \Rightarrow |Z(G)| > 1$
- Konjugation ist ein Automorphismus, also insbesondere ordnungserhaltend!

Beispiel: M = G : $\gamma : G \times G \to G$
Gm = G für jedes m $\in G \Rightarrow$ G operiert transitiv

Operation auf den Rechtsnebenklassen:
transitiv, da eine Bahn mit allen Nebenklassen erzeugt wird
($ker\varphi = G$ unmöglich, da Rechtsnebenklasse nicht festgelassen werden!)

2.8 Produkte (nach Üb. 11)

Seien $A, B \leq G$

Komplexprodukte
Dann ist $AB = \{a, b \mid a \in A, b \in B\}$

- $AB \subseteq G$
- $|AB| = \frac{|A| \cdot |B|}{|A \cap B|}$
- AB Gruppe $\Leftrightarrow$ AB = BA ($A \trianglelefteq G \vee B \trianglelefteq G$)

Komplexprodukte können **direkte Produkte** sein
Dies ist der Fall, wenn $A \trianglelefteq G, B \trianglelefteq G, A \cap B = 1$
Für $a, a' \in A, b, b' \in B$ gilt:
$[a, b] = a^{-1}b^{-1}ab \in A \cap B = \{1\} \Rightarrow ab = ba$
Also $(ab)(a'b') = (aa')(bb')$

Komplexprodukte können **semidirekte Produkte** sein
Dies ist der Fall, wenn $B \trianglelefteq G, A \cap B = 1$
Für $a, a' \in A, b, b' \in B$ gilt:
$(ab)(a'b') = aba'b' = aa'(a')^{-1}ba'b' = (aa')(b^{a'}b') \in AB$

Externes direktes Produkt
Seien A,B Gruppen. Sei $A \times B = \{(a, b) \mid a \in A, b \in B\}$ mit $(a, b)(a', b') = (aa', bb')$
Dann $A \times B$ ist Gruppe mit $A \hookrightarrow A \times B, B \hookrightarrow A \times B$
$A \trianglelefteq A \times B, B \trianglelefteq A \times B, A \cap B = 1$

Externes semidirektes Produkt
Seien A,B Gruppen. Sei $A \ltimes_\phi B = \{(a, b) \mid a \in A, b \in B\}$
$\phi : A \to Aut(B)$, $(a, b)(a', b') = (aa', b^{\phi(a')}b')$
Dann: $A \ltimes_\phi B$ ist Gruppe
$A, B \hookrightarrow A \ltimes_\phi B, B \trianglelefteq A \ltimes_\phi B, A \cap B = 1$

- [2.54] Gilt $A \trianglelefteq G, B \trianglelefteq G, A \cap B = 1$ und G = AB $\Rightarrow G \cong A \times B$
- A und B Untergruppen der endl. Gruppe G. Dann gilt $|AB| = \frac{|A||B|}{|A \cap B|}$

Beispiele (nach Üb 11):
$|G| = 3 \cdot 5$
$n_5 \in \{1, 3\} \cap \{1, 6, ...\} = \{1\}$
$\mathbb{Z}_5 \trianglelefteq G, \mathbb{Z}_3 \leq G$ mit $\mathbb{Z}_5 \cap \mathbb{Z}_3 = 1$
$\Rightarrow G = \mathbb{Z}_3\mathbb{Z}_5 \cong \mathbb{Z}_3 \ltimes_\phi \mathbb{Z}_5$
$\phi : \mathbb{Z}_3 \to Aut(\mathbb{Z}_5)$
$|\phi(\mathbb{Z}_3)| \mid ggT(|\mathbb{Z}_3|, |Aut(\mathbb{Z}_5)|) = ggT(3, 4) = 1$
$\Rightarrow \phi = 1$ und $G \cong \mathbb{Z}_3 \ltimes_\phi \mathbb{Z}_5 \cong \mathbb{Z}_3 \times \mathbb{Z}_5 = \mathbb{Z}_{15}$

2.9 Endliche abelsche Gruppen

- $a, b \in G$ mit teilerfremden Ordnungen und ab = ba. Dann ist ord(ab) = ord(a)ord(b)
- G endliche abelsche Gruppe und U zyklische Untergruppe maximaler Ordnung Dann ist ord(g) ein Teiler von $|U|$ für alle $g \in G$
- G endliche abelsche Gruppe und U zyklische Untergruppe maximaler Ordnung Dann hat U ein Komplement in G
- Jede abelsche Gruppe ist eine direkte Summe zyklischer Untergruppen
- Eine endliche abelsche Gruppe ist isomorph zu einer direkten Summe zyklischer Gruppen von Primpotenzordnung, und die Ordnungen dieser zyklischer Gruppen sind bis auf Reihenfolge eindeutig gegeben.
- $[U9.1]$ G/Z zyklisch $\Rightarrow$ G ablesch

2.10 Der Satz von Jorden-Hölder

- N ist genau dann maximaler Normalteiler von G, wenn G/N einfach ist+
- Sei G eine Gruppe und $G = G_0 > G_1 > G_2 > ... > G_n = \{e\}$ eine Kette von Untergruppen, so dass G_{i+1} ein maximaler Normalteiler von G_i ist. Eine solche Kette heißt Kompositionsreihe und die einfachen Gruppen G_i/G_{i+1} heißen Kompositionsfaktoren
  ist G endlich existiert trivialerweise eine Kompositionsreihe

Jordan-Hölder
Sei G eine endliche Gruppe. Dann haben alle Kompositionsreihen von G die gleiche Länge, und die Kompositionsfaktoren stimmen bis auf Reihenfolge und Isomorphie überein

Kommutatoren
Elemente der Form $a^{-1}b^{-1}ab$ für $a, b \in G$ heißen Kommutatoren. Die von den Kommutatoren erzeugte Gruppe G' heißt die Kommutatoregruppe von G. Die höheren Kommuatorengruppen $G^{(i)}$ werden rekursiv durch $G^{(0)} = G, G^{(i+1)} = (G^{(i)})'$ definiert.
Die Gruppe G heißt **auflösbar**, wenn es ein $n \in \mathbb{N}$ gibt mit $G^{(n)} = \{e\}$

- G Gruppe. Dann ist G' der kleinste Normalteiler N von G für den G/N abelsch ist
- $N \trianglelefteq G$. Dann ist G genau dann auflösbar, wenn N und G/N auflösbar sind
- G endliche Gruppe. Dann ist G genau dann auflösbar, wenn alle Kompositionsfaktoren von G zyklisch (von Primzahlordnung) sind.

2.11 Die Sätze von Sylow

p-Gruppe
Gruppe heißt p-Gruppe, wenn die Ordnung der Gruppe eine Potenz von p ist, $p \in \mathbb{P}$

p-Sylowgruppe
G endliche Gruppe und $p \in \mathbb{P}$.
Eine Untergruppe U von G heißt p-Sylowgruppe von G, wenn $|U|$ eine p-Gruppe ist und [G : U] nicht durch p teilbar ist
Ist also p^r die höchste Potenz von p, die $|G|$ teilt, dann sind die p-Sylowgruppe gerade die Untergruppen der Ordnung p^r

Für abelsche Gruppe gibt es für jedes p genau eine p-Sylowgruppe

[2.76*a*] Jede p-Untergruppe von G liegt in einer p-Sylowgruppe von G

Sylow I
G endliche Gruppe und $p \in \mathbb{P}$. Dann besitzt G eine p-Sylowgruppe
Sylow II
Alle p-Sylow-Untergruppen sind konjugiert in G
Sylow III
Sei n die Anzahl der p-Sylow-Untergruppen. Dann:

(a) $n \equiv 1 \pmod{p}$

(b) $n = \frac{|G|}{|N_G(P)|}$
Da $P \leq N_G(P)$ gilt $n \mid \frac{|G|}{|P|}$

2.12 Gruppen kleiner Ordnung

2.12.1 Automorphismen zyklischer Gruppen

- R Ring, dann ist $R^x = \{r \in R \mid rs = sr = 1\}$ (**Einheitengruppe**)
- Für $n \in \mathbb{N}$ gilt $(\mathbb{Z}/n\mathbb{Z})^x = \{k + n\mathbb{Z} \mid ggT(k,n) = 1, 1 \leq k \leq n\}$
  Insbesondere $|(\mathbb{Z}/n\mathbb{Z})^x| = \phi(n)$
- G zyklisch mit $|G| = n$, dann ist $Aut(G) \cong (\mathbb{Z}/n\mathbb{Z})^x$

Suche nach Normalteilern von G mit $|G|$ hat wenige Teiler

- Man nimmt den größten Primteiler von $|G|$ oder die Primzahl p mit der größten p-Sylowgruppe P.
  Nun versucht man mittels der Teilbarkeitseigenschaften, dass P normal in G ist
- Ist P nicht normal, dann hat P mindestens $1 + p$ Konjugierte
- Kleine Permutationsoperationen: $G \to Sym(P\backslash G)$
  Wenn $N_G(P) > P$, dann $G \to Sym(N_G(P)\backslash G)$
- Klassengleichung

3 Ringe

3.1 Definitionen, Beispiele

Ein **Ring** ist eine Menge R mit zweistelligen Verknüpfungen + und $\cdot$ und Elemente $0, 1 \in R$, sodass die folgenden Ringaxiome gelten:

(a) (R,+) ist eine (additiv geschriebene) abelsche Gruppe mit neutralem Element 0

(b) (R,$\cdot$) ist ein Monoid mit neutralem Element 1

(c) Es gelten die beiden Distributivgesetze $x \cdot (y + z) = c \cdot y + x \cdot z$ und $(y + z) \cdot x = y \cdot x + z \cdot x$ für alle $x, y, z \in R$

- Die ganzen Zahlen $\mathbb{Z}$ bilden einen Ring
- $n \in \mathbb{N}$, so ist die Menge $\mathbb{Z}/n\mathbb{Z}$ mit $(a + n\mathbb{Z}) + (b + n\mathbb{Z}) = (a + b) + n\mathbb{Z}$ und $(a + n\mathbb{Z}) \cdot (b + n\mathbb{Z}) = (ab) + n\mathbb{Z}$ einen Ring mit n Elemente

Einheit
Ein Element $a \in R$ heißt invertierbar oder Einheit, wenn es $b, c \in R$ gibt mit $ab = ca = 1$
(dann: $c = c1 = cab = 1b = b$)
R^x ist die Einheitengruppe von R
$R^* = E(R) = \{a \in R \mid \exists b \text{ mit } ab = ba = 1\}$

Im folgenden sei stets $0 \neq 1$

Nullteiler
$0 \neq a \in R$ heißt Nullteiler, wenn es ein $b \neq 0$ gibt mit ab = 0
0 ist kein Nullteiler!
nilpotent
$a \in R$ heißt nilpotent, wenn es ein $n \in \mathbb{N}$ gibt mit $a^n = 0$
R heißt kommuntativ, wenn ab = ba für alle $a, b \in R$ gilt
Integritätsbereich oder Integritätsring
R ist nullteilerfrei und kommutativ

Sind alle Elemente $\neq 0$ in R Einheiten, so heißt der Ring ein *Schiefkörper*
Kommutative Schiefkörper heißen Körper

- Ein endlicher Integritätsbereich ist ein Körper
- Sei $n \in \mathbb{N}$. Dann ist $\mathbb{Z}/n\mathbb{Z}$ genau dann ein Körper, wenn n eine Primzahl ist
- $[vorU11]$ nullteilerfrei $\Leftrightarrow$ in R kann man kürzen
- Ein Nullteiler ist niemals eine Einheit (Körper besitzen also keine Nullteiler)
  $0 \neq a \in R$ Nullteiler und es gibt $b \neq 0$ mit 0 = ab.
  Wäre a Einheit, so gäbe es $c \in R$ mit ca = 1.
  c0 = 0 = c(ab) = (ca)b = b, Widerspruch

- R endlich. Jedes Element $a \in R \backslash \{0\}$ ist Einheit oder Nullteiler
  Sei a kein Nullteiler. $\{a^n : n \in \mathbb{N}\}$ ist endlich.
  Somit gibt es $m, n \in \mathbb{N}$ mit $m < n$ und $a^m = a^n$.
  Dann ist $a^m(1 - a^{n-m}) = 0$. Da a kein Nullteiler ist, muss $1 - a^{n-m} = 0$ sein.
  Daher ist $aa^{n-m-1} = 1$, a ist eine Einheit.

3.2 Homomorphismen und Ideale

Ringhomomorphismus
$\phi : R \to S$ zwischen Ringen R und S heißt Ringhomomorphismus, wenn
- $1_R^\phi = 1_S$
- $(x+y)^\phi = x^\phi + y^\phi$
- $(xy)^\phi = x^\phi y^\phi$ gelten für alle $x, y \in R$

Ideal
Eine Untergruppe I von (R,+) heißt Ideal von R, wenn für alle $r \in R, i \in I$ gilt: $ri, ir \in I$.
Man schreibt dann auch $I \trianglelefteq R$

- Der Kern eines Ringhomomorphismus ist ein Ideal
- *Hauptideal* ist ein von einem einzigen Element erzeugtes Ideal
- Sei I ein Ideal des Rings R. Dann ist $R \to R/I$, $x \mapsto x + I$ ein Epimorphismus von Ringen mit Kern I

Homomorphiesatz
$\phi : R \to S$ mit Kern I. Dann gilt $R/I \cong Bild(\phi)$
Isomorphiesätze

(a) Sei R ein Ring mit Teilring S und Ideal I.
Dann gilt $S/S \cap I \cong S + I/I$

(b) Seien I und J Ideale des Rings R mit $J \subseteq I$.
Dann ist I/J ein Ideal von R/J und es gilt $R/I \cong (R/J)/(I/J)$

- [3.10] Die Ideale I und J von R heißen teilerfremd, wenn $I + J = R$
- **Chinesischer Restsatz**
Seien $I_1, I_2, ..., I_n$ paarweise teilerfremde Ideale eines Rings R. Sei I der Schnitt der Ideale I_i. Dann ist die Abbildung
$R \to R/I_1 \times R/I_2 \times ... \times R/I_n$
$r \mapsto (r + I_1, r + I_2, ..., r + I_n)$
eine Epimorphismus mit Kern I
Insbesondere gilt $R/I \cong R/I_1 \times R/I_2 \times .... \times R/I_n$
- Sei n = $\prod p_i^{e_i}$ die natürliche Primfaktorzerlegung von $n \in \mathbb{N}$
Dann ist der Ring $\mathbb{Z}/n\mathbb{Z}$ isomorphi zum direkten Produkt der Ring $\mathbb{Z}/p_i^{e_i}\mathbb{Z}$

3.4 Anwendungen der Kongruenzrechnung

Primzahlen: 2,3,5,7,11,13,17,19,23,29
$a^{p-1} \equiv 1(\text{mod p})$, falls $p \in \mathbb{P}$ und $a \in \mathbb{Z}$ kein Vielfaches von p
x^2 mod $3 \in \{0,1\}$
x^4 mod $3 \in \{0,1\}$
x^4 mod $4 \in \{0,1\}$
x^4 mod $5 \in \{0,1\}$
2^x mod $7 \in \{1,2,4\}$
x^2 mod $7 \in \{0,1,2,4\}$

3.5 Maximale Ideale

Sei R ein kommutativer Ring.
Ein maximales Ideal ist ein Ideal I von R mit $I \neq R$, so dass kein Ideal J von R existiert mit $I \subsetneq J \subsetneq R$

Sei I ein Ideal eines kommutative Rings R.
Dann ist I genau dann maximal wenn R/I ein Körper ist.

Körper: R Integritätsbereich und $R^* = R \backslash \{0\}$

3.6 Primideale

Sei R wieder ein kommutativer Ring
Ein Ideal I von R heißt Primideal, wenn R/I ein Integritätsring ist.
Ist also $ab \in I$, dann ist $(a+I)(b+I) \subseteq ab + I$ in R/I

Maximale Ideale sind automatisch Primideale

Sei R ein kommutativer Ring (mit $0 \neq 1$)

- S multiplikativ abgeschlossene Teilmenge von S mit $0 \neq S$.
  Dann hat R ein Primideal mit $S \cap I = \varnothing$
- Die Menge der nilpotenten Elte. besteht aus dem Durchschnitt der Primideale
- I Hauptideal, falls es von einem Element erzeugt wird
  Jedes Ideal Hauptideal $\Rightarrow$ Hauptidealring

3.7 Polynome

R sei stets kommutativ

Ein *Polynom* in der Variablen X ist eine formale Summe $r_0 + r_1X + r_2X^2 + \cdots + r_nX^n$
Die Menge der Polynome bildet einen Ring: R[X]

$r_0, r_1, ...$ heißen die Koeffizienten des Polynoms $f := \sum r_i X^i$
$n \in \mathbb{N}_0$ maximal mit $r_n \neq 0$ heißt *Leitkoeffizient* (n = grad f)
f *normiert*, wenn $r_n = 1$ und r_0 ist konstanter Term

- Seien $f, g \in R[X]$ Polynome. Dann gilt
  $grad(f + g) \leq max(grad\ \text{f}, grad\ \text{g})$
  $grad(f \cdot g) \leq grad$ f+$grad$ g
  R Integritätsbereich: $graf(f \cdot g) = grad$ f+$grad$ g
- Sei $g \in R[X]$ ein Polynome mit invertierbaren Leitkoeffizienten und $f \in R[X]$ beliebig
  Dann gibt es eindeutige $q, r \in R[X]$ mit $f = q \cdot g + r$ und grad r $<$ grad g.
- $a \in R$ und $f = \sum r_i X^i \in R[X]$, dann ist
  $R[X] \to R$, $f \mapsto f(a)$ ein **Ringhomorphismus**
- a Nullstelle (f(a) = 0) von f, dann gibt es $g \in R[X]$ mit $f = (X - a)g$
  $f = (X - a)^e g$ e maximal: Vielfachheit der Nullstelle a
- R Integritätsring und $0 \neq f \in R[X]$.
  Dann hat f höchstens grad f Nullstellen
- $p \in \mathbb{P}$. $(\mathbb{Z}/p\mathbb{Z})^X$ ist zyklisch
- *Ableitung* auf Polynomring: $(rX^i)' = riX^{i-1}$ eine additive Abbildung
- R Integritätsbereich und a Nullstalle. Dann ist a einfache Nst, g.d.w. $f'(a) \neq 0$

3.8 Einheitengruppe von $\mathbb{Z}/n\mathbb{Z}$

$n = \prod P_e^{e_i}$ Primfaktorzerlegung von $n \in \mathbb{N}$
$\mathbb{Z}/n\mathbb{Z} \cong \bigoplus \mathbb{Z}/p_i^{e_i}\mathbb{Z}$ und $(\mathbb{Z}/n\mathbb{Z})^x \cong \bigoplus(\mathbb{Z}/p_i^{e_i}\mathbb{Z})^x$

(a) p ungerade Primzahl und $l \in \mathbb{N}$. Dann ist $(\mathbb{Z}/p^l\mathbb{Z})^x$ zyklisch
Sei $w \in \mathbb{Z}$, so dass $w + p\mathbb{Z}$ ein Erzeuger von $(\mathbb{Z}/p\mathbb{Z})^x$ ist:
Dann ist $w^{p^{l-1}}(1+p) + p^l\mathbb{Z}$ Erzeuger von $(\mathbb{Z}/p^l\mathbb{Z})^x$

(b) $l \geq 2$ ist $(\mathbb{Z}/2^l\mathbb{Z})^x$ isomorph zu einem direkten Produkt zweier zyklischer Gruppen der Ordnungen 2 und 2^{l-2} mit Erzeugern -1 und 5

3.9 Quotientenkörper

Sei R ein Integritätsbereich
Auf der Menge der Paare (r,s) mit $r, s \in R, s \neq 0$ führen wir eine Äquivalenrelation ein
(r,s) und (r',s') sind äquivalent, wenn rs' = r's
Wir konstruieren zu R einen kleinsten Körper K in dem R enthalten ist:
$\frac{r}{s} + \frac{r'}{s'} = \frac{rs'+r's}{ss'}$ und $\frac{r}{s} \cdot \frac{r'}{s'} = \frac{rr'}{ss'}$
Somit erhält man wohldefinierte Addition und Multiplikation.
Ferner ist via $r \mapsto \frac{r}{1}$ R ein Teilring von K.

K ist ein Körper: **Quotientenkörper** von R,
da R wegen $\frac{r}{s}\frac{s}{r} = 1$, $\frac{r}{s}$ multiplikativ invertierbar ist.

3.10 Teilbarkeit

Teilbarkeit
r teilt s, wenn es $x \in R$ gibt mit s = rx
Ist $K \supseteq R$ der Quotientenkörper von R und $s \neq 0$, dann ist s ein Teiler von r, genau dann wenn $\frac{r}{s} \in R$

- $0 \neq s \in R$ besitzt gewisse triviale Teiler:
  jede Einheit s = u(u's) mit uu' = 1 (u und su Teiler von s)
- s ist Eineheit und besitzt außer diesen trivialen Teilern keine weitern:
  s unzerlegbar oder irreduzibel
- Eine Nichteinheit heißt prim wenn aus $r \mid ab$ stets $r \mid a$ oder $r \mid b$ folgt
- [3.3.5] Jedes Primelement ist irreduzibel
- Jedes irreduzible Element eines Hauptidealrings ist Primelement

Integritätsbereich R heißt **faktoriell**, wenn jedes Element $\neq 0$ entweder eine Einheit oder ein Produkt endlich vieler Primelemente ist.
Natürlich ist in einem faktoriellen Ring jedes irreduzible Element Primelement.
Eindeutige Primfaktorzerlegung von Nicht-Einheiten in faktoriellem Ring

Ist R = $\mathbb{Z}$ oder R der Polynomring K[X] für Körper K. Dann stimmen in R irreduzible Elemente und prime Elemente überein. Insbesondere ist R faktoriell

3.11 Inhalt von Polynomen, Lemma von Gauß

R faktorieller Integritätsbereich, K Quotientenkörper von R

$0 \neq a \in K$ und $p \in R$(prim) $\Rightarrow a = p^m \frac{u}{v}$ mit $m \in \mathbb{Z}, u \in R, 0 \neq v \in R$, so dass p weder u noch v teilt. Dabei ist m unhabängig von der Wahl des Paares u,v. $v_p(a) = m$ mit $v_p(0) = \infty$.
Es gilt $v_p(ab) = v_p(a) = v_p(b)$
$0 \neq f = a_0 + a_1X + ...a_nX^n \in K[X]$, dann $v_p(f) := min_i v_p(a_i)$
Inhalt von f: I(f) := $\prod_{p \in \mathbb{P}} p^{v_p(f)}$

Für R = $\mathbb{Z}$ und $f \in \mathbb{Z}[X]$ ist der Inhalt I(f) gerade der größte gemeinsame Teiler der Koeffizienten von f

Gauß-Lemma
Seien $0 \neq f, g \in K[X]$. Dann gilt I(fg) = I(f)I(g)

$f \in R[X]$ heißt **reduzibel**, falls f = gh exisitiert mit $g, h \in R[X]$
Gibt es keine solche Zerlegung, dann heißt f **irreduzibel**

Sei R ein faktorieller Ring. Dann ist R[X] faktoriell. Die Primelemente von R[X] bestehen aus den Primelementen von R, zusammen mit den irreduziblen und primitiven Polynomen aus R[X]

3.12 Das Irreduziblitätkriterium von Eisenstein

Eisenstein
Sei R ein Integritätsbreich mit Quot. K, $p \in R$ ein Primelement und f(X) = $a_0a_1X + \cdots + a_nX^n$ ein Polynom mit

(i) für $0 \leq i \leq n-1$ ist a_i durch p teilbar

(ii) a_n ist nicht durch p teilbar

(iii) a_0 ist nicht durch p^2 teilbar

Dann ist f irreduzibel in R[X].
Ist R faktoriell, dann ist f auch irreduzibel in K[X]

Sei p eine Primzahl. Dann ist das Polynom $1 + X + X^2 + \cdots + X^{p-1}$ über $\mathbb{Q}$ irreduzibel