SKRIPTUM
Algebra I

Definitionen und Sätze

1 Einführung

2 Gruppen

2.1 Definitionen und Beispiele

Definition 2.1. Eine Menge G mit einer zweistelligen Verknüpfung $G \times G \to G$, $(x, y) \to x \cdot y$ heißt **Halbgruppe**, wenn das Assoziativgesetz gilt: $(x \cdot y) \cdot z = x \cdot (y \cdot z)$

Definition 2.2. Eien Halbgruppe G heißt **abelsch** oder **kommutativ**, falls $x \cdot y = y \cdot x \quad \forall x, y \in G$.

Definition 2.3. Eine Halbgruppe heißt **Monoid**, falls es $e \in G$ gibt mit $e \cdot x = x \cdot e = x \quad \forall x \in G$. e heißt dann **Einselement** oder **neutrales Element**.

Definition 2.4. Ein Monoid G heißt **Gruppe**, wenn es für alle $x \in G$ ein $y \in G$ gibt mit $xy = yx = e$.

2.2 Untergruppen und zyklische Gruppen

Definition 2.5. Eine nichtleere Teilmenge U einer Gruppe G heißt **Untergruppe**, wenn aus $a, b \in U$ schon $ab \in U$ und $a^{-1} \in U$ folgt. Man schreibt $U \leq G$.

Definition 2.6. Sei $M \subset G$ eine nicht leere Teilmenge der Gruppe G. Die von M **erzeugte Untergruppe** $< M >$ ist die kleinste Untergruppe von G, die M enthält. (d.h. der Schnitt aller Untergruppen die M enthalten)

Definition 2.7. Eine Gruppe, die von einem Element erzeugt wird, heißt **zyklisch**.

Definition 2.8. Ist G eine Gruppe, dann heißt $|G| = \mathbb{N} \cup \{\infty\}$ die **Ordnung** von G. Für $a \in G$ heißt $ord(a) = | < a > |$ die Ordnung von a.

Lemma 2.9. *Sei G eine Gruppe und $ord(a) = n \in \mathbb{N}$ die Ordnung von $a \in G$. Dann ist n die kleinste natürliche Zahl m mit $a^m = e$. Ferner gilt $< a >= \{a^0, a^1, \ldots, a^{n-1}\}$ und $a^i = a^j \Leftrightarrow n | i - j$.*

Definition 2.10. Elemente der Ordnung 2 heißen **Involutionen**.

Satz 2.11. *Die Gruppe G sei zyklisch. Dann ist jede Untergruppe von G zyklisch. Hat G zusätzlich endliche Ordnung, dann hat G für jeden Teiler r der Gruppenordnung $|G|$ genau eine Untergruppe der Ordnung r.*

Satz 2.12. *Sei d der größte gemeinsame Teiler der natürlichen Zahlen m und n. Dann gibt es $u, v \in \mathbb{Z}$ mit $d = u \cdot m + v \cdot n$.*

Satz 2.13. *Sei a ein Element der Ordnung $n \in \mathbb{N}$. Für $m \in \mathbb{Z}$ sei $d = ggT(n, m)$. Dann hat a^m die Ordnung $\frac{n}{d}$.*

Definition 2.14. Für $n \in \mathbb{N}$ sei $\varphi(n)$ die Anzahl der $m \in N$ mit $1 \leq m < n$ die zu n teilerfremd sind.

Korollar 2.15. *Eine zyklische Gruppe der Ordnung $n \in N$ hat genau $\varphi(n)$ Erzeuger.*

Lemma 2.16. *Sei $a, b \in G$ mit Teilerfremden und endlichen Ordnungen. Ferner gelte $ab = ba$. Dann gilt $ord(ab) = ord(a) \cdot ord(b)$.*

2.3 Nebenklassen

Zusatzdefinition. Für $g \in G$ nennt man $Ug := \{ug | u \in U\}$ eine **Rechtsnebenklasse**. Analog gU eine **Linksnebenklasse**.

Lemma 2.17. *Für zwei Nebenklassen Ug und Uh gilt entweder $Ug = Uh$ oder $Ug \cap Uh = \emptyset$.*

Definition 2.18. Sei G endlich und U eine Untergruppe. Aus Lemma 2.17 erhält man eine disjunkte Zerlegung $G = \bigcup_i Ug_i$ für gewisse Menge von g_i's. Man nennt das eine **Nebenklassenzerlegung** von G bzgl. U. Die Menge der g_i nennt man eine **Rechtstransversale** oder ein **Vertretersystem** von $U\backslash G$

Satz 2.19 (Lagrange)**.** *Sei U eine Untergruppe einer endliche Gruppe G. Dann gilt $|G| = |U| \cdot |U\backslash G|$, also insbesondere $|U|$ teilt $|G|$.*

Korollar 2.20. *Sei G eine endliche Gruppe, dann ist $ord(g)$ ein Teiler von $|G|$ für alle $g \in G$.*

Korollar 2.21 (Kleiner Satz von Fermat)**.** *Sei $a \in \mathbb{Z}$ nicht durch die Primzahl p teilbar. Dann ist $p | a^{p-1} - 1$. Insbesondere ist $a^p \equiv a \mod p$.*

Korollar 2.22. *Gruppen von Primzahlordnung sind zyklisch.*

2.4 Normalteiler und Faktorgruppen

Definition 2.23. Eine Untergruppe U von G heißt **Normalteiler** von G, falls $gU = Ug$ für alle $g \in G$ gilt. In diesem Fall schreibt man $U \trianglelefteq G$.

Lemma 2.24. *$U \leq G$ ist genau dann normal in G, wenn $g^{-1}Ug \subseteq U \quad \forall g \in G$.*

Zusatzdefinition. $U \leq G$, dann heißt $[G : U] := |U\backslash G|$ der **Index** von U in G. Für $|G| < \infty$ gilt $[G : U] = \frac{|G|}{|U|}$.

Satz 2.25. *Sei $N \trianglelefteq G$. Dann gilt $NgNh = Ngh$ für alle g und h. Mit diesem Produkt wird G/N zu einer Gruppe, der **Faktorgruppe** von G modulo N.*

Definition 2.26. Eine Gruppe G mit $|G| > 1$ heißt **einfach**, falls sie außer $\{e\}$ und G keine Normalteiler hat.

2.5 Symmetrische Gruppe und alternierende Gruppen

Definition 2.27. $a, b \in G$ heißen **konjugiert**, falls es ein $g \in G$ gibt mit $b = g^{-1}ag$. Konjugiertheit liefert eine Äquivalenzrelation auf G. Statt $g^{-1}ag$ schreibt man auch a^g.

Satz 2.28. *Sei $\varphi = (a_1\ a_2\ \dots)(b_1\ b_2\ \dots) \cdots \in S_n$ und $\psi \in S_n$. Dann gilt $\varphi^\psi = (a_1^\psi\ a_2^\psi\ \dots)(b_1^\psi\ b_2^\psi\ \dots) \dots$.*

Satz 2.29. *Die Permutationen $\alpha, \beta \in S_n$ mögen die gleichen Zykellängen haben. Dann sind α und β konjugiert.*

Satz 2.30. *Jede Permutation aus S_n ist ein Produkt von Transpositionen, und jeder m-Zykel ist ein Produkt von $m - 1$ Transpositionen.*

Satz 2.31. *Für* $\varphi, \psi \in S_n$ *gilt* $l(\varphi\psi) \equiv l(\varphi) + l(\psi) \mod 2$.

Definition 2.32. Permutationen φ mit $l(\varphi) \equiv 0 \mod 2$ heißen **gerade**, solche mit $l(\varphi) \equiv 1 \mod 2$ heißen **ungerade**.

Satz 2.33. *Sei* $1 < m \in \mathbb{N}$. *Die Menge der geraden Permutationen aus* S_n *bildet eine Gruppe* A_n *mit* $[S_n : A_n] = 2$. *Man nennt* A_n *die* ***alternierende Gruppe*** *vom Grad* n.

Satz 2.34. *Jede gerade Permutation ist ein Produkt aus 3-Zykeln. Insbesondere wird* A_n *von den 3-Zykeln aus* S_n *erzaugt.*

Lemma 2.35. *Sei* $n \geq 5$ *Dann sind alle 3-Zykel aus* A_n *konjugiert.*

Satz 2.36. *Für* $n \geq 5$ *ist die Gruppe* A_n *einfach.*

2.6 Homomorphismen

Definition 2.37. Eine Abbildung $\varphi : G \to H$ von der Gruppe G in die Gruppe H heißt Homomorphismus, wenn $\varphi(xy) = \varphi(x) \cdot \varphi(y)$ für alle $x, y \in G$.

Zusatzdefinition. $Aut(G)$ bezeichnet die Menge aller Automorphismen von G und ist eine Gruppe. Besteht ein Isomorphismus zwischen G und H, so nennt man G und H **isomorph**.

Definition 2.38. Der **Kern** eines Homomorphismus ist die Menge der $g \in G$ mit $\varphi(x) = e$. Der Kern von φ ist ein Normalteiler von G.

Satz 2.39 (Homomorphiesatz)**.** *Sei* $\varphi : G \to H$ *ein Homomorphismus. Dann ist die Abbildung* $\psi : G/_{Kern(\varphi)} \to Bild(\varphi) \quad Kern\varphi \cdot x \to \varphi(x)$ *wohldefiniert und liefert einen Isomorphismus* $G/_{Kern(\varphi)} \cong Bild(\varphi)$.

Korollar 2.40. *Bis auf Isomorphie gibt es nur die folgenden zyklischen Gruppen:* $(\mathbb{Z}, +)$; $(\mathbb{Z}/_{n\mathbb{Z}}, +)$.

Satz 2.41 (Cayley)**.** *Jede Gruppe* G *ist isomorph zu einer Untergruppe von* $Sym(G)$.

Satz 2.42. *Es gilt:*

1. *Sei* $U \leq G$, $N \trianglelefteq G \Rightarrow U/_{U\cap N} \cong UN/_N$
2. *Sei* $N \subset M \subset G$, $N \trianglelefteq G$, $M \trianglelefteq G$, *dann gilt* $G/_M \cong (G/N)/(M/N)$

2.7 Gruppenoperationen

Definition 2.43. Eine **Operation** einer Gruppe G auf einer Menge M ist eine Abbildung $M \times G \to M$, $(m, g) \to m^g$ für die $m^e = m$ und $(m^g)^h = m^{gh}$ gilt für alle $m \in M$ $g, h \in G$.

Zusatzbemerkung. G operiere auf M. Sei $\Delta : G \to Sym(M)$ die Abbildung, die $g \in G$ auf die Permutation $M \to M$, $m \mapsto m^g$ abbildet. Dann ist Δ homomorph.

Zusatzdefinition. Eine Operation G von M heißt **treu**, wenn es für alle $1 \neq g \in G$ ein $m \in M$ gibt mit $m^g \neq m$. Das ist gleichbedeutend damit, dass der zugehörige Homomorphismus $G \to Sym(M)$ injektiv ist.

Zusatzdefinition. Die Bahn durch m besteht aus den Elementen $m^g, g \in G$ und wird daher mit m^G bezeichnet.

Zusatzdefinition. Eine Operation von G auf M heißt **transitiv**, wenn M nur aus einer Bahn besteht.

Zusatzdefinition. Operiert G auf M, so nennt man $G_m = \{g \in G : m^g = m\}$ den **Stabilisator** von $m \in M$. Der Stabilisator von ist eine Untergruppe von G.

Definition 2.44. G operiert auf Menge M und N. Eine Abbildung $\varphi : M \to N$ nennen wir G-äquivalent, wenn $\varphi(m^g) = (\varphi(m))^g$ gilt für alle $m \in M, g \in G$.

Satz 2.45. *Die Gruppe G operiere transitiv auf der Menge M. Sei $U := G_m$ der Stabilisator für ein $m \in M$. Dann wird durch $\varphi : U/G \to M \quad Ux \mapsto m^x$ eine G-äquivalente Bijektion definiert.*

Korollar 2.46. *G operiere auf M. Die Länge $|m^G|$ der Bahn von G durch $m \in M$ ist gegeben durch $|m^G| = [G : G_m] \overset{|G|\leq\infty}{=} \frac{|G|}{|G_m|}$.*
Insbesondere entspricht $|M|$ bei transitiver Operation dem Index einer Untergruppe in G; $|M| \mid |G|$.

Lemma 2.47. *G operiere auf M. Die Elemente $u, v \in M$ seien in einer gemeinsamen Bahn. Dann sind die Stabilisatoren G_u und G_v in G kongruent. Genauer: Ist $v = u^g$, dann gilt [$G_v = g^{-1}G_v g = G_u^g$] $G_{u^g} = G_u^g$.*

Definition 2.48. G operiere per Konjugation auf sich selbst. Den Stabilisator $x \in G$ unter dieser Operation nennt man **Zentralisator** von x in G. Men schreibt $C_G(x)$. Die Menge $C_G(x)$ besteht aus allen g mit $gx = xg$. Die Bahn $x^G := \{g^{-1}xg : g \in G\}$ nennt man **Konjugationsklasse**
Sei $X \subset G$ eine Teilmenge. $C_G(X) = \{g \in G : gx = xg \; \forall x \in X\} = \bigcap_{x \in X} C_G(x)$.
Ist $X = G$, so nennt man $Z(G) := C_G(G)$ **Zentrum** von G.

G operiert auch durch Konjugation auf den Teilmengen von G. Ist $X \subseteq G$, so nennt man den Stabilisator von X in G den **Normalisator** $N_G(X)$. Es gilt: $N_G(X) = \{g \in G : X^g = X\}$.

Da Stabilisatoren Untergruppen von G sind, sind $C_G(x), C_G(X), N_G(X), Z(G)$ Untergruppen von G.

Satz 2.49 (Bahnengleichung)**.** *Die endliche Gruppe G operiere auf der endlichen Menge M. Seien $m_1, m_2, \ldots, m_r$ Repräsentanten der Bahnen. Dann gilt $|M| = \sum_{i=1}^r [G : G_{m_i}]$.*

Satz 2.50 (Klassengleichung)**.** *Sind $x_1, \ldots x_r$ die Repräsentanten der Konjugationsklassen der endlichen Gruppe G, dann gilt $|G| = \sum_{i=1}^r [G : C_G(x_i)]$.*

Korollar 2.51. *Sei p eine Primzahl, $n \in \mathbb{N}$ und G eine Gruppe der Ordnung p^n. Dann gilt $|Z(G)| > 1$.*

Satz 2.52 (Burnsidesche Bahnenformel, Cauchy - Frobenius Bahnenformel)**.** *Die endliche Gruppe G operiere auf der endlichen Menge M. Für $g \in G$ sei $\chi(g)$ die Anzahl der Fixpunkte von g, d.h. $\chi(g) := |\{m \in M | m^g = m\}|$. Dann hat G genau $\frac{1}{|G|} \sum_{g \in G} \chi(g)$ Bahnen auf M.*

Korollar 2.53. *Die Gruppe G operiere transitiv auf der endlichen Menge M mit $|M| > 1$. Dann enthält G ein fixpunktfreies Element.*

Korollar 2.54. *Die echte Untergruppe U von G habe* endlichen *Index. Dann ist G nicht die Vereinigung der Konjugierten von U.*

2.8 Produkte von Gruppen

Zusatzdefinition. Sei I eine Indexmenge und G_i eine Gruppe. Die Menge der Tupel wird mit komponentenweiser Multiplikation zu einer Gruppe. Man nennt diese Gruppe das **direkte Produkt** der Gruppen G_i.

Zusatzdefinition. Die **direkte Summe** ist der Normalteiler bestehend aus allen Tupeln $(g_i)_{i\in I}$ mit $g_i \in G_i$, in denen für alle bis auf endlich viele Indizes i das Element g_i das neutrale Element ist.

Lemma 2.55. *Seien A und B Normalteiler der Gruppe G mit $A\cap B = \{e\}$ und $G = AB$. Dann gilt $G \cong A \times B$.*

Satz 2.56. *Sei I eine Indexmenge mit einer Totalordnung „$<$“ und G_i seinen Untergruppen einer Gruppe G. Dann sind äquivalent:*

1. *$G_i \trianglelefteq G$ für alle i, die G_i erzeugen G und $G_i \cap \hat{G}_i = \{e\}$, wo $\hat{G}_i$ das Erzeugnis der Gruppen G_j mit $j \in I\backslash\{i\}$ ist.*

2. *$G_i \trianglelefteq G$ für alle i und für jeden $g \in G$ gibt es bis auf Faktoren e genau eine Darstellung $g = g_{i_1}g_{i_2}\cdot\dots\cdot g_{i_n}$.*

3. *Für alle $i \neq j$ gilt $g_ig_j = g_jg_i$ für $g_i \in G_i$ und $g_j \in G_j$ und für jedes $g \in G$ gibt es bis auf Faktoren e genau eine Darstellung $g = g_{i_1}g_{i_2}\cdot\dots\cdot g_{i_n}$.*

Gilt eine der Aussagen, dann ist G isomorph zur direkten Summe der G_i.

Zusatzdefinition. Sei $G = UN$ mit $N \trianglelefteq G$ und $U < G$ und $N \cap U = \{e\}$. In dieser Situation sagt man, dass G das **semidirekte Produkt** des Normalteilers N mit dem Komplement U ist.

Satz 2.57. *Seinen N und U Gruppen und $\Phi : U \to Aut(N)$ ein Gruppenhomomorphismus. Auf der Menge der Paare $(u,n) \in U \times N$ definiert man ein Produkt durch $(u_1,n_1)\cdot(u_2,n_2) := (u_1\cdot u_2, n_1^{\Phi(u_2)}\cdot n_2)$. Mit diesem Produkt ist G eine Gruppe. Man schreibt auch $G = U \ltimes_\Phi N$.*

Satz 2.58. *Seien A und B Untergruppen der endlichen Gruppe. Dann gilt $|AB| = \frac{|A|\cdot|B|}{|A\cap B|}$.*

2.9 Endliche abelsche Gruppen

Satz 2.59. *Eine von höchstens n Elementen erzeugte abelsche Gruppe ist eine direkte Summen von höchstens n zyklischen Gruppen.*

Zusatzbemerkung. Sei G eine endlich erzeugte abelsche Gruppe und T die Menge der Elemente mit endlicher Ordnung. Dann ist T die Torsionsgruppe und eine Untergruppe von G. Ferner Gilt $G = TZ \cong T \otimes Z$ mit $Z \cong \mathbb{Z}^r$.

Zusatzbemerkung. Aus 2.59. folgt, dass es für jeden Teiler t einer endlichen abelschen Gruppe eine Untergruppe der Ordnung t gibt.

Lemma 2.60. *Sei $p \in \mathbb{P}$ und p^m die höchste Potenz von p, die die Ordnung einer endlichen abelschen Gruppe teilt. Dann gibt es genau eine Untergruppe der Ordnung p^m.*

Lemma 2.61. *Sei $n = \Pi p_i^{e_i}$ die Primfaktorzerlegung der Ordnung n einer Gruppe G. Sei G_{p_i} die Untergruppe von G mit $|G_{p_i}| = p_i^{e_i}$. Dann ist $G = G_{p_1} G_{p_2} \dots G_{p_k} \cong \bigoplus G_{p_i}$ eine direkte Summe der G_{p_i}.*

Lemma 2.62. *Sei G eine endliche abelsche Gruppe von Primpotenzordnung, und $G = G_1 G_2 \dots G_n \cong \bigoplus G_i$ eine direkte Summe mit zyklischen Gruppen G_i mit $|G_i| > 1$. Dann sind n und die Ordnungen der G_i (bis auf Reihenfolge) eindeutig.*

Satz 2.63. *Eine endliche abelsche Gruppe ist isomorph zu einer direkten Summe zyklischer Gruppen von Primpotenzordnung. Die Ordnungen sind bis auf Reihenfolge eindeutig.*

2.10 Satz von Jordan-Hölder

Zusatzdefinition. Wir nennen N einen **maximalen Normalteiler**, wenn $N \lhd G$ normal ist und kein Normalteiler M von G mit $N \lhd M \lhd G$ existiert. Damit ist $N \lhd G$ genau dann maximal, wenn $G/_N$ einfach ist.

Definition 2.64. Sei G eine Gruppe und $G = G_0 > G_1 > \dots G_n = \{e\}$ eine Kette von Untergruppen, so dass G_{i+1} ein maximaler Normalteiler von G_i ist. Eine solche Kette heißt **Kompositionsreihe** von G und die einfachen Gruppen $G_i/_{G_i+1}$ heißen **Kompositionsfaktoren** von G.

Satz 2.65 (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.*

Definition 2.66. Sei G eine Gruppe. Elemente der Form $a^{-1}b^{-1}ab$ heißen **Kommutatoren**. Die von den Komutatoren erzeugte Untergruppe G' heißt die **Kommutatorengruppe**. G heißt **auflösbar**, wenn es ein $n \in \mathbb{N}$ gibt mit $G^{(n)} = \{1\}$.

Zusatzbemerkung. Die Kommutatorengruppe G' und alle weiteren sind normal in G.

Satz 2.67. *Sei G eine Gruppe. Dann ist G' der kleinste Normalteiler N von G mit $G/_N$ abelsch.*

Lemma 2.68. *Sei $N \lhd G$. Dann ist G genau dann auflösbar, wenn N und $G/_N$ auflösbar sind.*

Satz 2.69. *Sei G eine endliche Gruppe. Dann ist G genau dann auflösbar, wenn alle Kompositonsfaktoren von G zyklisch (von Primzahlordnung als einfache Gruppen) sind.*

Zusatzbemerkung. Abelsche Gruppen, Gruppen von Primzahlordnung und Homomorphe Bilder und direkte Produkte (mit endlich vielen Faktoren) auflösbarer Gruppen sind auflösbar.

2.11 Sätze von Sylow

Definition 2.70. Sei G eine endliche Gruppe und $p \in \mathbb{P}$. Eine Untergruppe U von G heißt **p-Sylowgruppe** von G, wenn U eine p-Gruppe ist und $p \nmid [G : U]$.

Ist also p^r die höchste Potenz von p, die $|G|$ teilt, dann sind die p-Sylowgruppen gerade die Untergruppen der Ordnung p^r.

Satz 2.71 (Sylow). *Sei G eine endliche Gruppe und p eine Primzahl. Dann besitzt G eine p-Sylowgruppe.*

Lemma 2.72. *Der Binomialkoeffizient n über p^r ist nicht durch p teilbar.*

Lemma 2.73. *Sei U echte Untergruppe der p-Gruppe G. Dann gilt $N_G(U) > U$. Ferner hat G für jeden Teiler m von $|G|$ eine Untergruppe der Ordnung m. Untergruppen von G vom Index p sind normal.*

Satz 2.74 (Sylow). *Sei G eine endliche Gruppe, $p \in \mathbb{P}$. Dann gilt:*

1. *Jede p-Untergruppe von G liegt in einer p-Sylowgruppe*

2. *Die p-Sylowgruppen sind konjugiert (Insbesondere operiert G transitiv auf der Menge der p-Sylowgruppen durch Konjugation)*

3. *Die Anzahl der p-Sylowgruppen von G ist $[G : N_G(P)]$ und von der Form $1 + kp$ mit $k \in \mathbb{N}_0$.*

2.12 Gruppen kleiner Ordnung

Zusatzbemerkung. Ist $|G| = p \in \mathbb{P}$, dann ist G zyklisch.

Ist $|G| = p^2$, dann ist G abelsch und $G \cong C_{p^2}$ oder $G \cong C_p \times C_p$.

Es gilt insbesondere $1 + kp \mid [G : P] = \frac{|G|}{|P|}$.

2.12.1 Automorphismen zyklischer Gruppen

Satz 2.75. *Für $n \in \mathbb{N}$ gilt $(\mathbb{Z}/_{n\mathbb{Z}})^\times = \{k + n\mathbb{Z} | 1 \leq k \leq n, ggT(k, n) = 1\}$. Insbesondere gilt $|\,(\mathbb{Z}/_{n\mathbb{Z}})^\times\,| = \varphi(n)$.*

Korollar 2.76. *Sei G eine zyklische Gruppe der Ordnung n. Dann gilt $Aut(G) \cong (\mathbb{Z}/_{n\mathbb{Z}})^\times$.*

Zusatzbemerkung. $(\mathbb{Z}/_{p\mathbb{Z}})^\times$ ist eine abelsche Gruppe der Ordnung $p - 1$.

2.12.2 $|G| = p \cdot q, \quad p, q \in \mathbb{P}, \quad p < q$

2.12.3 $|G| = 1001 = 7 \cdot 11 \cdot 13$

2.12.4 $|G| = p \cdot q \cdot r, \quad p, q, r \in \mathbb{P}, \quad p < q < r$

2.12.5 $|G| = p^a \cdot q^b, \quad p, q \in \mathbb{P},\ p < q, \quad 0 \leq a, b \leq 2$

2.12.6 $|G| = 8$

2.12.7 Auflösbarkeit von G für $|G| < 60$

A_5 der Ordnung 60 ist die kleinste einfache und nicht abelsche Gruppe.

3 Ringe

3.1 Definitionen, Beispiele

Definition und Lemma 3.1. Definition von **Ring** und ein paar kleine Folgerungen.

Definition 3.2. Ein Elment $a \in R$ heißt **invertierbar** oder eine **Einheit**, falls es $b \in R$ gibt mit $ab = ba = 1$.

Die Menge der **Einheiten** bildet die **Einheitengruppe** $R^\times$.

Ein $0 \neq a \in R$ heißt **Nullteiler**, falls es ein $0 \neq b \in R$ gibt mit $ab = 0$ oder $ba = 0$.

Ein $a \in R$ heißt **nilpotent**, falls es ein $n \in \mathbb{N}$ gibt mit $a^n = 0$.

R heißt **kommutativ**, falls $ab = ba \quad \forall a, b \in R$ gilt.

Der Ring heißt **Integritätsbereich** oder **Integritätsring**, falls er kommutativ und nullteilerfrei ist.

Gilt $R^\times = R \backslash \{0\}$, dann heißt R **Schiefkörper** oder **Integritätsring**. Ist R zusätzlich kommutativ, dann heißt R **Körper**

Lemma 3.3. *Ein* endlicher *Ring ohne Nullteiler ist ein Schiefkörper.*

Korollar 3.4. *Sei $n \in \mathbb{N}$. Dann ist $\mathbb{Z}/_{n\mathbb{Z}}$ genau dann ein Körper, wenn $n \in \mathbb{P}$.*

Zusatzdefinition. Ein **Teilring** eines Ringes R ist eine Teilmenge S von R, die unter Ringoperationen von R abgeschlossen ist.

3.2 Homomorphismen und Ideale

Definition 3.5. Eine Abbildung $\varphi : R \to S$ zwischen Ringen R und S heißt **Ringhomomorphismus**, wenn $\varphi(1) = 1$ und $\varphi(a + b) = \varphi(a) + \varphi(b)$, $\varphi(ab) = \varphi(a) \cdot \varphi(b)$.

Definition 3.6. Eine Untergruppe I von $(R, +)$ heißt **Ideal**, falls aus $r \in R$, $i \in I$ schon $ri \in I$, $ir \in I$ folgt. Man schreibt dann $I \trianglelefteq R$.

Zusatzbemerkung. Es gilt $1 \in I \Leftrightarrow I = R$.

Zusatzdefinition. Ein **Hauptideal** ist ein von einem Element erzeugtes Ideal.

Ist jedes Ideal eines Ringes ein Hauptideal, dann nennt man den Ring einen **Hauptidealring**

Satz 3.7. *Sei $I \neq R$ ein Ideal des Ringes R. Dann ist $R \to R/_I$; $x \to x + I$ ein Epimorphismus von Ringen mit Kern I.*

Satz 3.8 (Homomorphiesatz)**.** *Sei $\varphi : R \to S$ ein Homomorphismus von Ringen mit Kern I, dann gilt: $R/_I \cong \varphi(R) = Bild(\varphi)$.*

Satz 3.9 (Isomorphiesätze)**.** *Es gilt:*

1. *Sei R ein Ring mit Teilring S und Ideal I. Dann gilt $S/_{I \cap S} \cong (I + S)/_I$*

2. *Seien I, J Ideale von R mit $J \subset I$. Dann ist $I/_J$ ein Ideal von $R/_J$ mit $R/_I \cong (R/_J)/(I/_J)$.*

3.3 Maximale Ideale und Primideale

Zusatzdefinition. Sei R ein Ring. Ein **maximales Ideal** von R ist ein Ideal $I \neq R$, so dass es kein Ideal J gibt mit $I \subsetneq J \subsetneq R$.

Satz 3.10. *Sei I ein Ideal des kommutativen Ringes R. Dann ist I genau dann maximal, wenn $R/_I$ ein Körper ist.*

Satz 3.11 (Krull)**.** *Sei $I \subsetneq R$ ein Ideal, dann ist I in einem maximalen Ideal von R enthalten.*

Zusatzdefinition. Sei R kommutativ. Ein Ideal I von R heißt **Primideal**, wenn $R/_I$ ein Integritätsring ist. Ist $ab \in I$, so ist $a \in I$ oder $b \in I$. Umgekehrt ist I ein Primideal, wenn aus $ab \in I$ schon $a \in I$ oder $b \in I$ folgt.

Da Körper Integritätsringe sind, sind maximale Ideale automatisch Primideale.

3.4 Polynome, Teil 1

Zusatzdefinition. Definition von **Polynom, Grad und normiert**.

Lemma 3.12. *Seien $f, g \in R[X]$ Polynome. Dann gilt:*
$grad(f + g) \leq max(grad(f), grad(g))$ und $grad(fg) \leq grad(f) \cdot grad(g)$ mit Gleichheit im Zweiten, falls R ein Integritätsbereich ist.

Satz 3.13. *Sei $g \in R[X]$ ein Polynom mit invertierbarem Leitkoeffizienten. Dann gibt es eindeutige Polynome $q, r \in R[X]$ mit $f = q \cdot g + r$ und $grad(r) < grad(g)$.*

3.5 Euklidische Ringe

Definition 3.14. Ein Ring R heißt **euklidisch**, wenn er ein Integritätsbereich ist und es eine Abbildung $\nu : R\backslash\{0\} \to \mathbb{N}_0$ gibt mit der folgenden Eigenschaft. Für $a, b \in \mathbb{R}$ mit $b \neq 0$ gibt es $q, r \in R$ mit $a = qb + r$, so dass entweder $r = 0$ oder $\nu(r) < \nu(b)$ gilt.

Satz 3.15. *Jeder euklidische Ring ist ein Hauptidealring.*

3.6 Quotientenkörper

3.7 Teilbarkeit

Im folgenden sei R wieder ein Integritätsbereich.

Zusatzdefinition. Ist s keine Einheit, und hat s keine nichttrivialen Teiler, dann heißt s **irreduziebel** oder **unzerlegbar**.

Beispiel. Beispiel einer uneindeutigen Primfaktorzerlegung.

Zusatzdefinition. Eine Nichteinheit r heißt **prim**, wenn aus $r \mid ab$ stets $r \mid a$ oder $r \mid b$ folgt.

Diese Bedingung ist äquivalent dazu, das das Hauptideal (r) ein Primideal von R ist.

Satz 3.16. *Jedes Primelement eines Integritätsringes ist irreduziebel.*

Satz 3.17. *Jedes irreduzieble Element eines Hauptidealrings ist ein Primelement.*

Korollar 3.18. *In einem Hauptidealring ist jedes Primelement* $\neq 0$ *ein Maximales Ideal.*

Definition 3.19. Ein Integritätsbereich R heißt **faktoriell**, wenn jedes Element $\neq 0$ entweder eine Einheit oder ein Produkt endlich vieler Primelemente ist.

Satz 3.20. *Sei R ein faktorieller Ring. Dann ist jede Primfaktorzerlegung bis auf Reihenfolge und Einheiten eindeutig.*

Zusatzdefinition. Man nennt a und b **teilerfremd**, wenn $ggT(a, b) = 1$ ist, d.h. wenn $(a, b) = R$ ist.

Satz 3.21. *Ein Hauptidealring ist faktoriell.*

3.8 Euklidischer Algorithmus

3.9 Chinesischer Restsatz

Satz 3.22 (Chinesischer Restsatz)**.** *Seien $n_1, \ldots, n_r$ paarweise teilerfremde natürliche Zahlen, und $a_1, \ldots, a_r \in \mathbb{Z}$. Dann ist das System der Kongruenzen $x \equiv a_i \mod n_i$ lösbar.*

Korollar 3.23. *Sei $n = n_1 \cdot n_2 \cdot \cdots \cdot n_r$ eine Zerlegung von n in paarweise teilerfremde natürliche Zahlen n_i. Dann ist der Ring $\mathbb{Z}/_{n\mathbb{Z}}$ isomorph zum direkten Produkt der Ringe $\mathbb{Z}/_{n_i\mathbb{Z}}$*

3.10 Anwendung der Kongruenzrechnung

4 Aus Übungen

Satz 4.1. *Ist $g^2 = 1$ für alle $g \in G$, dann ist die Gruppe G abelsch.*

Satz 4.2. *Eine endliche Gruppe G ist genau dann zyklisch, wenn sie zu jedem Teiler ihrer Ordnung genau eine Untergruppe hat.*

Satz 4.3. *In einer endlichen Gruppe gerader Ordnung existiert eine Involution.*

Satz 4.4. *Sei N ein Normalteiler von G vom Index $r > 1$, dann erzeugen die Elemente von G mit einer zu r teilerfremden Ordung eine echte Untergruppe.*

Satz 4.5. *Sei $1 < u \in \mathbb{N}$ eine ungerade Zahl und G eine Gruppe der Ordnung $2u$, dann besitzt G einen nicht tivialen Normalteiler.*

Satz 4.6. *Sei G eine endliche Gruppe und $p \in \mathbb{P}$ die kleinste Primzahl, die $|G|$ teilt, dann ist jede Untergruppe $U \leq G$ vom Index p normal in G.*

Satz 4.7. *Sei G eine Gruppe, die treu und transitiv auf der Menge Ω operiere mit $|\Omega| = p \in \mathbb{P}$. Sei N ein Normalteiler von G.*

1. *Ist $1 < N$, so ist p ein Teiler von $|N|$.*

2. *Eine normale p-Sylowuntergruppe $P \trianglelefteq G$ ist zyklisch von Ordnung p.*

3. *Es gilt $|G/_P| \mid p - 1$.*

Satz 4.8. *Gilt $n = a \cdot b$ mit $ggT(a, b) = 1$, so ist $\varphi(n) = \varphi(a) \cdot \varphi(b)$.*

Satz 4.9. *Sei $p \in \mathbb{P}$, $k \in \mathbb{N}$. Dann ist $\varphi(p^k) = p^{k-1}(p - 1) = p^k - p^{k-1}$.*

Satz 4.10. *Eine einfache und abelsche Gruppe ist isomorph zu einer zyklischen Gruppe von Primzahlordnung.*