Algebra und Zahlentheorie

Ulrich Bunke

Institut für Reine Mathematik

SS 2004

Anmeldung

Die Anmeldung zur Übung erfolgt über das System StudIP

Inhalt

1. Gruppen und Symmetrien
2. Struktur von Gruppen
3. Lineare Darstellungen
4. Ganze Zahlen
5. Ringe und Körper
6. Körpererweiterungen

Färbungen

F - Menge

Definition

Eine durch F gefärbte Menge ist ein Paar (X, f) aus einer Menge X und einer Abbildung $f : X \to F$.

Färbungen

F - Menge

Definition

Eine durch F gefärbte Menge ist ein Paar (X, f) aus einer Menge X und einer Abbildung $f : X \to F$.

(X, f), (Y, g) - F-gefärbte Mengen

Färbungen

F - Menge

Definition

Eine durch F gefärbte Menge ist ein Paar (X, f) aus einer Menge X und einer Abbildung $f : X \to F$.

(X, f), (Y, g) - F-gefärbte Mengen

Definition

Eine Abbilddung $\phi : X \to Y$ ist färbungserhaltend, wenn $g \circ \phi = f$ gilt.

Relationen

Definition

Eine Relation auf einer Menge X ist eine Färbung R von $X \times X$ durch $\{wahr, falsch\}$.

Relationen

Definition

Eine Relation auf einer Menge X ist eine Färbung R von $X \times X$ durch $\{wahr, falsch\}$.

(X, R), (Y, S) - Mengen mit Relationen

Relationen

Definition

Eine Relation auf einer Menge X ist eine Färbung R von $X \times X$ durch $\{wahr, falsch\}$.

(X, R), (Y, S) - Mengen mit Relationen

Definition

Eine Abbildung $\phi : X \to Y$ ist verträglich mit den Relationen, falls $R = S \circ (\phi \times \phi)$ gilt.

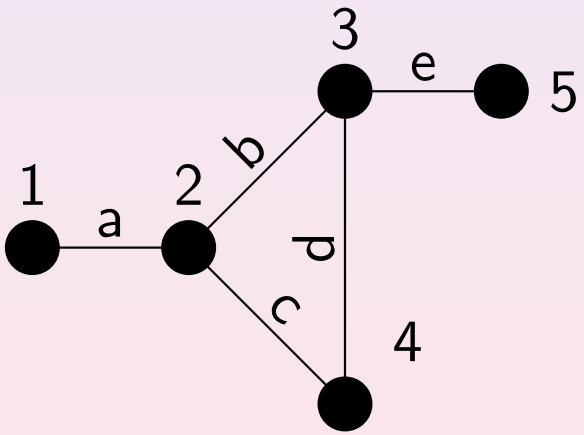
Graphen

Definition

Ein Graph ist Tripel (V, E, r), wobei V die Menge der Punkte, E die Menge der Seiten, und $r : E \to P^2(V)$ die Endpunkte der Seiten festlegt.

Graphen

$V = \{1, 2, 3, 4, 5\}$, $E = \{a, b, c, d, e\}$



$x \in E$	$r(x)$
a	$\{1, 2\}$
b	$\{2, 3\}$
c	$\{2, 4\}$
d	$\{3, 4\}$
e	$\{3, 5\}$

Graphen

Definition

Ein Graph ist Tripel (V, E, r), wobei V die Menge der Punkte, E die Menge der Seiten, und $r : E \to P^2(V)$ die Endpunkte der Seiten festlegt.

(V, E, r), (W, F, s) - Graphen.

Definition

Eine Morphismus $\phi : (V, E, r) \to (W, F, s)$ von Graphen ist durch zwei Abbildungen $\phi : V \to W$, $\psi : E \to F$ mit $P^2(\phi) \circ r = s \circ \psi$ gegeben

Isometrien

Definition

Ein metrischer Raum (X, d) ist eine Menge X mit einem ausgezeichneten Abstand d.

Isometrien

Definition

Ein metrischer Raum (X, d) ist eine Menge X mit einem ausgezeichneten Abstand d.

(X, d_X), (Y, d_Y) - metrische Räume

Isometrien

Definition

Ein metrischer Raum (X, d) ist eine Menge X mit einem ausgezeichneten Abstand d.

(X, d_X), (Y, d_Y) - metrische Räume

Definition

Eine Abbildung $\phi : X \to Y$ ist eine Isometrie, falls $d_Y \circ (\phi \times \phi) = d_X$ gilt.

Verknüpfungen

M - Menge

Verknüpfungen

M - Menge

Definition

Eine Verknüpfung auf M ist eine Abbildung $m : M \times M \longrightarrow M$.

Verknüpfungen

M - Menge

Definition

Eine Verknüpfung auf M ist eine Abbildung $m : M \times M \to M$.

(M, m), (N, n) - Mengen mit Verknüpfung

Verknüpfungen

M - Menge

Definition

Eine Verknüpfung auf M ist eine Abbildung $m : M \times M \to M$.

(M, m), (N, n) - Mengen mit Verknüpfung

Definition

Eine Morphismus $\phi : (M, m) \to (N, n)$ von Mengen mit Verknüpfung ist eine Abbildung $\phi : M \to N$ derart, daß $n \circ (\phi \times \phi) = \phi \circ m$ gilt.

Lineare Abbildungen

K - ein Körper

Lineare Abbildungen

K - ein Körper

Definition

Ein Vektorraum über K ist ein Tripel $(V, +, \bullet)$, wobei $+ : V \times V \to V$ die Vektoraddition und $\bullet : K \times V \to V$ die skalare Multiplikation ist. Diese Operationen erfüllen die Vektorraumaxiome.

Lineare Abbildungen

K - ein Körper

Definition

Ein Vektorraum über K ist ein Tripel $(V, +, \bullet)$, wobei $+ : V \times V \to V$ die Vektoraddition und $\bullet : K \times V \to V$ die skalare Multiplikation ist. Diese Operationen erfüllen die Vektorraumaxiome.

$(V, +_V, \bullet_V)$, $(W, +_W, \bullet_W)$ - Vektorräume

Lineare Abbildungen

K - ein Körper

Definition

Ein Vektorraum über K ist ein Tripel $(V, +, \bullet)$, wobei $+ : V \times V \to V$ die Vektoraddition und $\bullet : K \times V \to V$ die skalare Multiplikation ist. Diese Operationen erfüllen die Vektorraumaxiome.

$(V, +_V, \bullet_V)$, $(W, +_W, \bullet_W)$ - Vektorräume

Definition

Eine Abbildung $\phi : V \to W$ ist linear, falls $\phi \circ +_V = +_W \circ (\phi \times \phi)$ und $\phi \circ \bullet_V = \bullet_W \circ (\mathtt{id}_K \times \phi)$ gilt.

Objekte und Morphismen

Eine Kategorie beinhaltet :

1. die (Klasse der) Objekte $\mathtt{ob}(\mathcal{C})$
2. für je zwei Objekte $A, B \in \mathtt{ob}(\mathcal{C})$ eine Menge von Morphismen $\mathtt{Hom}_{\mathcal{C}}(A, B)$,
3. für jedes Objekt einen Identitätsmorphismus $\mathtt{id}_A \in \mathtt{Hom}_{\mathcal{C}}(A, A)$
4. für je drei Objekte eine Komposition

$$\mathtt{Hom}_{\mathcal{C}}(B, C) \circ \mathtt{Hom}_{\mathcal{C}}(A, B) \longrightarrow \mathtt{Hom}_{\mathcal{C}}(A, C) \ .$$

Objekte und Morphismen

Eine Kategorie beinhaltet :

1. die (Klasse der) Objekte $\mathtt{ob}(\mathcal{C})$
2. für je zwei Objekte $A, B \in \mathtt{ob}(\mathcal{C})$ eine Menge von Morphismen $\mathtt{Hom}_{\mathcal{C}}(A, B)$,
3. für jedes Objekt einen Identitätsmorphismus $\mathtt{id}_A \in \mathtt{Hom}_{\mathcal{C}}(A, A)$
4. für je drei Objekte eine Komposition

$$\mathtt{Hom}_{\mathcal{C}}(B, C) \circ \mathtt{Hom}_{\mathcal{C}}(A, B) \longrightarrow \mathtt{Hom}_{\mathcal{C}}(A, C) \ .$$

Objekte und Morphismen

Eine Kategorie beinhaltet :

1. die (Klasse der) Objekte $\mathtt{ob}(\mathcal{C})$
2. für je zwei Objekte $A, B \in \mathtt{ob}(\mathcal{C})$ eine Menge von Morphismen $\mathtt{Hom}_{\mathcal{C}}(A, B)$,
3. für jedes Objekt einen Identitätsmorphismus $\mathtt{id}_A \in \mathtt{Hom}_{\mathcal{C}}(A, A)$
4. für je drei Objekte eine Komposition

$$\mathtt{Hom}_{\mathcal{C}}(B, C) \circ \mathtt{Hom}_{\mathcal{C}}(A, B) \longrightarrow \mathtt{Hom}_{\mathcal{C}}(A, C) \ .$$

Objekte und Morphismen

Eine Kategorie beinhaltet :

1. die (Klasse der) Objekte $\mathtt{ob}(\mathcal{C})$
2. für je zwei Objekte $A, B \in \mathtt{ob}(\mathcal{C})$ eine Menge von Morphismen $\mathtt{Hom}_{\mathcal{C}}(A, B)$,
3. für jedes Objekt einen Identitätsmorphismus $\mathtt{id}_A \in \mathtt{Hom}_{\mathcal{C}}(A, A)$
4. für je drei Objekte eine Komposition

$$\mathtt{Hom}_{\mathcal{C}}(B, C) \circ \mathtt{Hom}_{\mathcal{C}}(A, B) \longrightarrow \mathtt{Hom}_{\mathcal{C}}(A, C) \ .$$

Objekte und Morphismen

Eine Kategorie beinhaltet :

1. die (Klasse der) Objekte $\mathtt{ob}(\mathcal{C})$
2. für je zwei Objekte $A, B \in \mathtt{ob}(\mathcal{C})$ eine Menge von Morphismen $\mathtt{Hom}_{\mathcal{C}}(A, B)$,
3. für jedes Objekt einen Identitätsmorphismus $\mathtt{id}_A \in \mathtt{Hom}_{\mathcal{C}}(A, A)$
4. für je drei Objekte eine Komposition

$$\mathtt{Hom}_{\mathcal{C}}(B, C) \circ \mathtt{Hom}_{\mathcal{C}}(A, B) \longrightarrow \mathtt{Hom}_{\mathcal{C}}(A, C) \ .$$

Eigenschaften

1. Die Komposition ist assoziativ, d.h. es gilt $(f \circ g) \circ h = f \circ (g \circ h)$ für komponierbare Morphismen.
2. Die Identitätsmorphismen erfüllen $\mathtt{id}_B \circ f = f$ und $f \circ \mathtt{id}_A = f$ für $f \in \mathtt{Hom}_{\mathcal{C}}(A, B)$.

Eigenschaften

1. Die Komposition ist assoziativ, d.h. es gilt $(f \circ g) \circ h = f \circ (g \circ h)$ für komponierbare Morphismen.
2. Die Identitätsmorphismen erfüllen $\mathtt{id}_B \circ f = f$ und $f \circ \mathtt{id}_A = f$ für $f \in \mathtt{Hom}_{\mathcal{C}}(A, B)$.

Eigenschaften

1. Die Komposition ist assoziativ, d.h. es gilt $(f \circ g) \circ h = f \circ (g \circ h)$ für komponierbare Morphismen.
2. Die Identitätsmorphismen erfüllen $\mathtt{id}_B \circ f = f$ und $f \circ \mathtt{id}_A = f$ für $f \in \mathtt{Hom}_{\mathcal{C}}(A, B)$.

Example

In allen Beispielen oben haben wir Kategorien beschrieben.

Automorphismen

$\mathcal{C}$ - Kategorie, $A \in \mathtt{ob}(\mathcal{C})$ Objekt

Automorphismen

$\mathcal{C}$ - Kategorie, $A \in \mathrm{ob}(\mathcal{C})$ Objekt

Definition

Ein $f \in \mathrm{Hom}_{\mathcal{C}}(A, A)$ heißt Automorphismus, falls es Morphismen $g_l, g_r \in \mathrm{Hom}_{\mathcal{C}}(A, A)$ (Links- und Rechtsinverses) mit $g_l \circ f = f \circ g_r = \mathrm{id}_A$ gibt.

Automorphismen

Lemma

Sei f ein Automorphismus. Dann gilt:

1. $g_l = g_r$.
2. *Das Rechtsinverse g_r eines Automorphismus f ist eindeutig bestimmt. Wir schreiben auch $f^{-1} := g_r$.*
3. *Die Komposition von Automorphismen ist ein Automorphismus.*
4. $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$.
5. id_A *ist ein Automorphismus.*

Automorphismen

Lemma

Sei f ein Automorphismus. Dann gilt:

1. $g_l = g_r$.
2. *Das Rechtsinverse g_r eines Automorphismus f ist eindeutig bestimmt. Wir schreiben auch $f^{-1} := g_r$.*
3. *Die Komposition von Automorphismen ist ein Automorphismus.*
4. $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$.
5. id_A *ist ein Automorphismus.*

Automorphismen

Lemma

Sei f ein Automorphismus. Dann gilt:

1. $g_l = g_r$.
2. *Das Rechtsinverse g_r eines Automorphismus f ist eindeutig bestimmt. Wir schreiben auch $f^{-1} := g_r$.*
3. *Die Komposition von Automorphismen ist ein Automorphismus.*
4. $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$.
5. id_A *ist ein Automorphismus.*

Automorphismen

Lemma

Sei f ein Automorphismus. Dann gilt:

1. $g_l = g_r$.
2. *Das Rechtsinverse g_r eines Automorphismus f ist eindeutig bestimmt. Wir schreiben auch $f^{-1} := g_r$.*
3. *Die Komposition von Automorphismen ist ein Automorphismus.*
4. $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$.
5. id_A *ist ein Automorphismus.*

Automorphismen

Lemma

Sei f ein Automorphismus. Dann gilt:

1. $g_l = g_r$.
2. *Das Rechtsinverse g_r eines Automorphismus f ist eindeutig bestimmt. Wir schreiben auch $f^{-1} := g_r$.*
3. *Die Komposition von Automorphismen ist ein Automorphismus.*
4. $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$.
5. id_A *ist ein Automorphismus.*

Automorphismen

Lemma

Sei f ein Automorphismus. Dann gilt:

1. $g_l = g_r$.
2. *Das Rechtsinverse g_r eines Automorphismus f ist eindeutig bestimmt. Wir schreiben auch $f^{-1} := g_r$.*
3. *Die Komposition von Automorphismen ist ein Automorphismus.*
4. $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$.
5. $\mathtt{id}_A$ *ist ein Automorphismus.*

Permutationen

$$S(A) := \mathtt{Aut}_{\mathtt{sets}}(A)$$

Permutationen

$A := \{a, b, c, d\}$.

$$f = \begin{array}{c|c|c|c|c} x & a & b & c & d \\ \hline f(x) & b & c & a & d \end{array} .$$

Permutationen

$A := \{a, b, c, d\}$.

$$f = \begin{array}{c|c|c|c|c} x & a & b & c & d \\ \hline f(x) & b & c & a & d \end{array} .$$

Zyklendarstellung

$$f = (abc) .$$

Permutationen

$h \in S_9$.

x	1	2	3	4	5	6	7	8	9
$h(x)$	2	4	6	5	1	7	3	8	9

.

Permutationen

$h \in S_9$.

x	1	2	3	4	5	6	7	8	9
$h(x)$	2	4	6	5	1	7	3	8	9

.

in Zyklen

$$h = (1, 2, 4, 5) \circ (3, 6, 7) \ .$$

Die Gruppe C_n

$$X_n := \{1, 2, \ldots, n\} \subset \mathbb{N}$$

Die Gruppe C_n

$$X_n := \{1, 2, \ldots, n\} \subset \mathbb{N}$$

Relation :

$$\{(1,2), (2,3), \ldots, (n-1, n), (n, 1)\} \subset X_n \times X_n$$

Die Gruppe C_n

$$X_n := \{1, 2, \ldots, n\} \subset \mathbb{N}$$

Relation :

$$\{(1,2), (2,3), \ldots, (n-1, n), (n, 1)\} \subset X_n \times X_n$$

Definition

Wir definieren die zyklische Gruppe C_n durch

$$C_n := \mathtt{Aut}_{\mathtt{set+rel}}(X_n) \ .$$

Die Gruppe C_n

$$r := (1, \ldots, n) \in C_n$$

Die Gruppe C_n

$r := (1, \ldots, n) \in C_n$

Lemma

Die Liste der Elemente von C_n ist $\{1, r, \ldots, r^{n-1}\}$.

Die Gruppe D_n

`met` - Kategorie der metrischen Räume und Isometrien

Die Gruppe D_n

$\mathtt{met}$ - Kategorie der metrischen Räume und Isometrien

Lemma

Ist $A \in \mathtt{ob}(\mathtt{met})$ *eine endliche Menge, so gilt* $\mathtt{Hom}_{\mathtt{met}}(A, A) = \mathtt{Aut}_{\mathtt{met}}(A, A)$.

Die Gruppe D_n

$$\mu_n := \{\exp(2\pi i \frac{m}{n}) | m = 0, 1, \ldots, n-1\} \subset \mathbb{C}$$

Menge der n-ten Einheitswurzeln

Die Gruppe D_n

$$\mu_n := \{\exp(2\pi i \frac{m}{n}) | m = 0, 1, \ldots, n-1\} \subset \mathbb{C}$$

Menge der n-ten Einheitswurzeln

Definition

Die Diedergruppe D_n wird durch $D_n := \mathtt{Aut}_{\mathtt{met}}(\mu_n)$ definiert.

Die Gruppe D_n

$$\mu_n := \{\exp(2\pi i \frac{m}{n}) | m = 0, 1, \ldots, n-1\} \subset \mathbb{C}$$

Menge der n-ten Einheitswurzeln

Definition

Die Diedergruppe D_n wird durch $D_n := \mathtt{Aut}_{\mathtt{met}}(\mu_n)$ definiert.

Lemma

Die Liste der Elemente von D_n ist

$$\{1, r, \ldots, r^{n-1}, s, sr, \ldots, sr^{n-1}\} .$$

die Gruppen $GL(n, K)$

K - Körper,

die Gruppen $GL(n, K)$

K - Körper, $K - \mathtt{vect}$ - Kategorie der Vektorräume über K

die Gruppen $GL(n, K)$

K - Körper, $K - \mathtt{vect}$ - Kategorie der Vektorräume über K

Definition

Für $V \in K - \mathtt{vect}$ definieren wir

$$\mathtt{GL}(V) := \mathtt{Aut}_{K-\mathtt{vect}}(V) \ .$$

Insbesondere setzen wir

$$\mathtt{GL}(n, K) := \mathtt{GL}(K^n) \ .$$

die Gruppen $GL(n, K)$

Die Elemente von $GL(n, K)$ können als Matrizen dargestellt werden. Die Verknüpfung ist dann gerade die Matrixmultiplikation.

die Gruppen $GL(n, K)$

Die Elemente von $GL(n, K)$ können als Matrizen dargestellt werden. Die Verknüpfung ist dann gerade die Matrixmultiplikation.

Lemma

Die Liste der Elemente von $GL(2, F_2)$ *ist*

$$\{\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}\}.$$

Gruppenaxiome

Definition

Ein Monoid $(M, \circ, 1)$ ist eine Menge mit Verknüpfung $(M, \circ)$ mit einem ausgezeichneten 1-Element, so daß

1. $\circ$ associativ ist, d.h. $x \circ (y \circ z) = (x \circ y) \circ z$ gilt, und
2. $1 \circ x = x \circ 1 = x$ gilt.

Gruppenaxiome

Definition

Ein Monoid $(M, \circ, 1)$ ist eine Menge mit Verknüpfung $(M, \circ)$ mit einem ausgezeichneten 1-Element, so daß

1. $\circ$ associativ ist, d.h. $x \circ (y \circ z) = (x \circ y) \circ z$ gilt, und
2. $1 \circ x = x \circ 1 = x$ gilt.

Gruppenaxiome

Definition

Ein Monoid $(M, \circ, 1)$ ist eine Menge mit Verknüpfung $(M, \circ)$ mit einem ausgezeichneten 1-Element, so daß

1. $\circ$ associativ ist, d.h. $x \circ (y \circ z) = (x \circ y) \circ z$ gilt, und
2. $1 \circ x = x \circ 1 = x$ gilt.

Gruppenaxiome

Definition

Ein Monoid $(M, \circ, 1)$ ist eine Menge mit Verknüpfung $(M, \circ)$ mit einem ausgezeichneten 1-Element, so daß

1. $\circ$ associativ ist, d.h. $x \circ (y \circ z) = (x \circ y) \circ z$ gilt, und
2. $1 \circ x = x \circ 1 = x$ gilt.

Definition

Eine Gruppe ist ein Monoid $(G, \circ, 1)$, in welchem jedes Element invertierbar ist, d.h. zu jedem $x \in M$ Elemente $y_l, y_r \in M$ mit $x \circ y_r = y_l \circ x = 1$ existieren.

Einfache Eigenschaften

G - eine Gruppe

Einfache Eigenschaften

G - eine Gruppe

Lemma

In einer Gruppe besitzt jedes Element ein eindeutig bestimmtes Linksinverses. Dieses ist dann auch ein Rechtsinverses.

Einfache Eigenschaften

G - eine Gruppe

Lemma

In einer Gruppe besitzt jedes Element ein eindeutig bestimmtes Linksinverses. Dieses ist dann auch ein Rechtsinverses.

Es gibt also eine Bijektion $(\dots)^{-1} : G \to G$ welche jedem Element sein Inverses zuordnet.

groups

Definition

groups bezeichnen wir die Kategorie der Gruppen und Homomorphismen.

groups

Definition

groups bezeichnen wir die Kategorie der Gruppen und Homomorphismen.

Definition

Eine Untergruppe U einer Gruppe G ist eine Teilmenge, welche die 1 enthält und unter der Verknüpfung und der Bildung des Inversen abgeschlossen ist.

groups

Definition

Eine Untergruppe U einer Gruppe G ist eine Teilmenge, welche die 1 enthält und unter der Verknüpfung und der Bildung des Inversen abgeschlossen ist.

Lemma

Sei $f : H \to G$ ein Homomorphismus von Gruppen. Dann gilt:

1. $\mathtt{ker}(f) := \{h \in H | f(h) = 1\}$ *ist eine Untergruppe von H.*
2. $\mathtt{im}(f) := f(H)$ *ist eine Untergruppe von G.*

Innere Automorphismen

G - Gruppe , $h \in G$

Innere Automorphismen

G - Gruppe , $h \in G$

Lemma

Die Abbildung $\alpha_h : G \to G$, $g \mapsto \alpha_h(g) := g^h := hgh^{-1}$ *ist ein Automorphismus* $\alpha_g \in \mathtt{Aut}_{groups}(G)$.

Innere Automorphismen

Lemma

Ist $f \in Hom_{groups}(G, H)$ und $U \subset G$ eine Untergruppe, dann ist $f(U) := \{f(u) | u \in U\}$ eine Untergruppe von H.

Generatoren und Relationen

G - Gruppe, $S \subset G$ - Teilmenge

Generatoren und Relationen

G - Gruppe, $S \subset G$ - Teilmenge

Definition

S erzeugt die Gruppe G, wenn man jedes Element aus G durch eine endliche Verknüpfung von Elementen aus S dargestellt werden kann.

Generatoren und Relationen

Definition

Sei S eine Menge. Die Elemente von

$$W_n(S) := \underbrace{S \times \cdots \times S}_{n\times}$$

werden auch Worte der Länge n im Alphabet S genannt. Wir verabreden, daß $W_0 := \{1\}$ gilt und setzen $W(S) := \bigcup_{n\geq 0} W_n(S)$.

Generatoren und Relationen

Definition

Sei S eine Menge. Die Elemente von

$$W_n(S) := \underbrace{S \times \cdots \times S}_{n\times}$$

werden auch Worte der Länge n im Alphabet S genannt. Wir verabreden, daß $W_0 := \{1\}$ gilt und setzen $W(S) := \bigcup_{n\geq 0} W_n(S)$.

$S := \{a := (1,2)\circ(3,4), b := (2,3), c := (1,2,3)\} \subset S_4$. (a,a,b) und (a,b,c,a) sind Worte der Länge 3 und 4 im Alphabet S.

Generatoren und Relationen

$$m : W(S) \to G, (a_1, \ldots, a_n) \mapsto a_1 \circ \cdots \circ a_n \ .$$

Generatoren und Relationen

$$m : W(S) \to G, (a_1, \ldots, a_n) \mapsto a_1 \circ \cdots \circ a_n \ .$$

Definition

Die Menge der Relationen ist die Teilmenge

$$R(S) := \{w \in W(S) | m(w) = e\} \ .$$

Freie Gruppen

T - eine Menge

Freie Gruppen

T - eine Menge

$$\hat{T} := T \times \{1, -1\}$$

Freie Gruppen

T - eine Menge

$$\hat{T} := T \times \{1, -1\}$$

Wir schreiben $t := (t, 1)$ und $t^{-1} := (t, -1)$.

Reduzierte Worte

Definition

Ein Wort $w = (t_1^{\epsilon_1}, \ldots, t_n^{\epsilon_n})$, $\epsilon_i \in \{1, -1\}$, heißt reduziert, wenn aus $t_i = t_{i+1}$ die Relation $\epsilon_i = \epsilon_{i+1}$ folgt.

Reduzierte Worte

Definition

Ein Wort $w = (t_1^{\epsilon_1}, \ldots, t_n^{\epsilon_n})$, $\epsilon_i \in \{1, -1\}$, heißt reduziert, wenn aus $t_i = t_{i+1}$ die Relation $\epsilon_i = \epsilon_{i+1}$ folgt.

Sei $T = \{a, b, c\}$. Dann sind (a, b) und (a, b, a^{-1}, c) reduziert, nicht aber (a, b^{-1}, b, a).

Reduzierte Worte

Definition

Ein Wort $w = (t_1^{\epsilon_1}, \ldots, t_n^{\epsilon_n})$, $\epsilon_i \in \{1, -1\}$, heißt reduziert, wenn aus $t_i = t_{i+1}$ die Relation $\epsilon_i = \epsilon_{i+1}$ folgt.

Sei $T = \{a, b, c\}$. Dann sind (a, b) und (a, b, a^{-1}, c) reduziert, nicht aber (a, b^{-1}, b, a). Ist T eine Teilmenge einer Gruppe, so ist klar, daß $m(a, b^{-1}, b, a) = m(a, a)$ gilt.

Reduktion

Definition

Wir definieren die Reduktionsabbidlung

$$\mathtt{Red} : W(\hat{T}) \to W(\hat{T})$$

durch folgende Vorschrift. Sei $w = (t_1^{\epsilon_1}, \ldots, t_n^{\epsilon_n}) \in W(\hat{T})$. Ist w reduziert, dann setzen wir $\mathtt{Red}(w) := w$. Ist w nicht reduziert, dann sei $j := \mathtt{min}\{i | t_i = t_{i+1} \text{ und } \epsilon_i \neq \epsilon_{i+1}\}$ und

$$\mathtt{Red}(w) := (t_1^{\epsilon_1}, t_{j-1}^{\epsilon_{j-1}}, t_{j+2}^{\epsilon_{j+2}} \ldots, t_n^{\epsilon_n}) \ .$$

Die Wirkung der Reduktion

$$w := (a, b^{-1}, b, a^{-1}, a, b, a, a^{-1}, b^{-1})$$

$$\Big| \, .$$

Die Wirkung der Reduktion

$$w := (a, b^{-1}, b, a^{-1}, a, b, a, a^{-1}, b^{-1})$$

n	$\mathtt{Red}(w)$

.

Die Wirkung der Reduktion

$$w := (a, b^{-1}, b, a^{-1}, a, b, a, a^{-1}, b^{-1})$$

n	$\mathrm{Red}(w)$
0	$(a, b^{-1}, b, a^{-1}, a, b, a, a^{-1}, b^{-1})$

.

Die Wirkung der Reduktion

$$w := (a, b^{-1}, b, a^{-1}, a, b, a, a^{-1}, b^{-1})$$

n	$\mathrm{Red}(w)$
0	$(a, b^{-1}, b, a^{-1}, a, b, a, a^{-1}, b^{-1})$
1	$(a, a^{-1}, a, b, a, a^{-1}, b^{-1})$

.

Die Wirkung der Reduktion

$$w := (a, b^{-1}, b, a^{-1}, a, b, a, a^{-1}, b^{-1})$$

n	$\mathrm{Red}(w)$
0	$(a, b^{-1}, b, a^{-1}, a, b, a, a^{-1}, b^{-1})$
1	$(a, a^{-1}, a, b, a, a^{-1}, b^{-1})$
2	$(a, b, a, a^{-1}, b^{-1})$

.

Die Wirkung der Reduktion

$$w := (a, b^{-1}, b, a^{-1}, a, b, a, a^{-1}, b^{-1})$$

n	$\mathrm{Red}(w)$
0	$(a, b^{-1}, b, a^{-1}, a, b, a, a^{-1}, b^{-1})$
1	$(a, a^{-1}, a, b, a, a^{-1}, b^{-1})$
2	$(a, b, a, a^{-1}, b^{-1})$
3	(a, b, b^{-1})

.

Die Wirkung der Reduktion

$w := (a, b^{-1}, b, a^{-1}, a, b, a, a^{-1}, b^{-1})$

n	$\mathrm{Red}(w)$
0	$(a, b^{-1}, b, a^{-1}, a, b, a, a^{-1}, b^{-1})$
1	$(a, a^{-1}, a, b, a, a^{-1}, b^{-1})$
2	$(a, b, a, a^{-1}, b^{-1})$
3	(a, b, b^{-1})
4	(a)

.

Die Wirkung der Reduktion

$w := (a, b^{-1}, b, a^{-1}, a, b, a, a^{-1}, b^{-1})$

n	$\mathrm{Red}(w)$
0	$(a, b^{-1}, b, a^{-1}, a, b, a, a^{-1}, b^{-1})$
1	$(a, a^{-1}, a, b, a, a^{-1}, b^{-1})$
2	$(a, b, a, a^{-1}, b^{-1})$
3	(a, b, b^{-1})
4	(a)
5	(a)

.

Die Wirkung der Reduktion

$w := (a, b^{-1}, b, a^{-1}, a, b, a, a^{-1}, b^{-1})$

n	$\mathrm{Red}(w)$
0	$(a, b^{-1}, b, a^{-1}, a, b, a, a^{-1}, b^{-1})$
1	$(a, a^{-1}, a, b, a, a^{-1}, b^{-1})$
2	$(a, b, a, a^{-1}, b^{-1})$
3	(a, b, b^{-1})
4	(a)
5	(a)
$\vdots$	$\vdots$

.

Die Wirkung der Reduktion

$w := (a, b^{-1}, b, a^{-1}, a, b, a, a^{-1}, b^{-1})$

n	$\mathrm{Red}(w)$
0	$(a, b^{-1}, b, a^{-1}, a, b, a, a^{-1}, b^{-1})$
1	$(a, a^{-1}, a, b, a, a^{-1}, b^{-1})$
2	$(a, b, a, a^{-1}, b^{-1})$
3	(a, b, b^{-1})
4	(a)
5	(a)
$\vdots$	$\vdots$

.

Lemma

Für jedes $w \in W(T)$ ist $\mathrm{Red}^n(w)$ für genügend große n reduziert.

Die freie Gruppe

$W^{red}(\hat{T}) \subset W(\hat{T})$ - die Menge der reduzierten Worte

Die freie Gruppe

$W^{red}(\hat{T}) \subset W(\hat{T})$ - die Menge der reduzierten Worte

Definition

Wir definieren das Monoid $F(T) := W(\hat{T})^{red}$ mit der Verknüpfung

$$(t_1^{\epsilon_1}, \ldots, t_n^{\epsilon_n}) \circ (s_1^{\delta_1}, \ldots, s_m^{\delta_m}) = (t_1^{\epsilon_1}, \ldots, t_n^{\epsilon_n}, s_1^{\delta_1}, \ldots, s_m^{\delta_m})^{red} \ .$$

Die freie Gruppe

$W^{red}(\hat{T}) \subset W(\hat{T})$ - die Menge der reduzierten Worte

Definition

Wir definieren das Monoid $F(T) := W(\hat{T})^{red}$ mit der Verknüpfung

$$(t_1^{\epsilon_1}, \ldots, t_n^{\epsilon_n}) \circ (s_1^{\delta_1}, \ldots, s_m^{\delta_m}) = (t_1^{\epsilon_1}, \ldots, t_n^{\epsilon_n}, s_1^{\delta_1}, \ldots, s_m^{\delta_m})^{red} \ .$$

Lemma

Das Monoid $(F(T), \circ)$ ist eine Gruppe.

Die freie Gruppe

Definition

$F(T)$ heißt die freie durch T erzeugte Gruppe. Ist $T_n = \{1, \ldots, n\} \subset \mathbb{N}$, so schreibt man auch $F_n := F(T_n)$ für die freie Gruppe in n Erzeugenden.

Die freie Gruppe

Definition

$F(T)$ heißt die freie durch T erzeugte Gruppe. Ist $T_n = \{1, \ldots, n\} \subset \mathbb{N}$, so schreibt man auch $F_n := F(T_n)$ für die freie Gruppe in n Erzeugenden.

Lemma

Ist G eine Gruppe und $T \subset G$, so induziert $m : F(T) \to G$ einen Gruppenhomomorphismus.

Die freie Gruppe

Definition

Eine Gruppe G heißt frei, wenn es eine Teilmenge $T \subset G$ gibt, für welche $m : F(T) \longrightarrow G$ ein Isomorphismus ist.

Funktoren

$\mathcal{C}, \mathcal{D}$ - Kategorien

Definition

Ein Funktor $F : \mathcal{C} \to \mathcal{D}$ besteht aus folgenden Strukturen:

1. einer Zuordnung $F : \mathtt{ob}(\mathcal{C}) \to \mathtt{ob}(\mathcal{D})$,
2. für je zwei Objekte $A, B \in \mathtt{ob}(\mathcal{C})$ einer Abbildung $F : \mathtt{Hom}_{\mathcal{C}}(A, B) \to \mathtt{Hom}_{\mathcal{D}}(F(A), F(B))$.

Diese Abbildung soll dabei die Verknüpfung erhalten.

Funktoren

Die Konstruktion F der freien Gruppe ordnet jeder Menge eine Gruppe zu. Ist $\phi : T \to S$ eine Abbildung, dann erhalten wir eine induzierte Abbildung $\hat{\phi} : \hat{T} \to \hat{S}$ und schließlich einen Homomorphismus $F(\phi) : F(T) \to F(S)$, indem wir $\hat{\phi}$ auf die Einträge der Worte anwenden. Es gilt dabei $F(\phi) \circ F(\psi) = F(\phi \circ \psi)$. Dies ist ein Beispiel eines Funktors

$$F : \texttt{sets} \to \texttt{groups} \ .$$

Funktoren

Lemma

Ist G eine Gruppe und $f : T \to G$ eine Abbildung. Dann gibt es genau eine Fortsetzung von f zu einem Gruppenhomomorphismus $F(f) : F(T) \to G$.

Funktoren

Lemma

Ist G eine Gruppe und $f : T \to G$ eine Abbildung. Dann gibt es genau eine Fortsetzung von f zu einem Gruppenhomomorphismus $F(f) : F(T) \to G$.

$\mathcal{F} : \texttt{groups} \to \texttt{sets}$ - Vergißfunktor

Funktoren

$\mathcal{F} : \mathtt{groups} \longrightarrow \mathtt{sets}$ - Vergißfunktor

Lemma

$$\mathrm{Hom}_{\mathtt{groups}}(F(T), G) \cong \mathrm{Hom}_{\mathtt{sets}}(T, \mathcal{F}(G)) \ .$$

Man sagt, daß der Funktor F zu $\mathcal{F}$ linksadjungiert ist. In der Tat kann man F so definieren (bis auf Isomorphie).

Permutationsdarstellung

Lemma

Jede Gruppe kann als Untergruppe einer Permutationsgruppe dargestellt werden.

Permutationsdarstellung

Lemma

Jede Gruppe kann als Untergruppe einer Permutationsgruppe dargestellt werden.

G - Gruppe,

Permutationsdarstellung

Lemma

Jede Gruppe kann als Untergruppe einer Permutationsgruppe dargestellt werden.

G - Gruppe, $g \in G$,

Permutationsdarstellung

Lemma

Jede Gruppe kann als Untergruppe einer Permutationsgruppe dargestellt werden.

G - Gruppe, $g \in G$, $\phi(g) : G \to G$, $\phi(g)(h) := gh$.

Permutationsdarstellung

Lemma

Jede Gruppe kann als Untergruppe einer Permutationsgruppe dargestellt werden.

G - Gruppe, $g \in G$, $\phi(g) : G \to G$, $\phi(g)(h) := gh$.
Die Abbildung $\phi : G \to \mathtt{Aut}_{\mathtt{sets}}(G)$ ist ein injektiver Gruppenhomomorphismus.

Linearisierung

K - Körper,

Linearisierung

K - Körper, X - Menge.

Linearisierung

K - Körper, X - Menge.
$K(X)$ - der von X erzeugte K- Vektorraum

Linearisierung

K - Körper, X - Menge.
$K(X)$ - der von X erzeugte K- Vektorraum
$i_X : X \to K(X)$ - kanonische Einbettung

Linearisierung

K - Körper, X - Menge.
$K(X)$ - der von X erzeugte K- Vektorraum
$i_X : X \to K(X)$ - kanonische Einbettung

Lemma

Ist $f : X \to Y$ eine Abbildung, so erhalten wir eine eindeutige lineare Fortsetzung $K(f) : K(X) \to K(Y)$ derart daß $K(f) \circ i_X = i_Y \circ f$.

Linearisierung

Durch K wird ein Funktor $K : \mathtt{sets} \longrightarrow K - \mathtt{vect}$ beschrieben. In der Tat gilt für jeden K-Vektorraum V auf natürliche Weise

$$\mathrm{Hom}_{K-\mathtt{vect}}(K(X), V) \cong \mathrm{Hom}_{\mathtt{sets}}(X, \mathcal{F}(V)) \ ,$$

wobei hier $\mathcal{F} : K - \mathtt{vect} \longrightarrow \mathtt{sets}$ die Vektorraumstruktur vergißt.

Lineare Darstellung

Lemma

Jede Gruppe kann als Untergruppe von $GL(V)$ für einen geeigneten K-Vektorraum V dargestellt werden.

Lineare Darstellung

Lemma

Jede Gruppe kann als Untergruppe von $GL(V)$ für einen geeigneten K-Vektorraum V dargestellt werden.

$\phi : G \longrightarrow \mathtt{Hom}_{\mathtt{sets}}(G, G)$ - Permutationsdarstellung

Lineare Darstellung

Lemma

Jede Gruppe kann als Untergruppe von $GL(V)$ für einen geeigneten K-Vektorraum V dargestellt werden.

$\phi : G \to \mathtt{Hom}_{\mathtt{sets}}(G, G)$ - Permutationsdarstellung
definieren

$$\psi : G \to \mathtt{GL}(K(G))$$

Lineare Darstellung

Lemma

Jede Gruppe kann als Untergruppe von $GL(V)$ für einen geeigneten K-Vektorraum V dargestellt werden.

$\phi : G \to \mathtt{Hom}_{\mathtt{sets}}(G, G)$ - Permutationsdarstellung
definieren

$$\psi : G \to \mathtt{GL}(K(G))$$

durch

$$\psi(g) = K(\phi(g)), \quad g \in G$$

Untergruppen

G - Gruppe

1. Das Bild $f(H) \subset G$ eines Homomorphismus $f : H \to G$ ist eine Untergruppe.
2. Der Kern $\ker(f) \subset G$ eines Homomorphismus $f : G \to H$ ist eine Untergruppe.
3. Ist $S \subset G$ eine Teilmenge, dann ist $< S >:= m(F(S)) \subset G$ die von S erzeugte Untergruppe.
4. Der Durchschnitt $U := \bigcap_i U_i$ über eine Familie $(U_i)_i$ von Untergruppen ist eine Untergruppe.
5. Sei $G \to \mathrm{Aut}_{\mathrm{sets}}(A)$ eine Wirkung. Für $a \in A$ sei $G_a := \{g \in G | ga = a\}$ der Stabilisator. Dann ist $G_a \subset G$ eine Untergruppe.

Untergruppen

G - Gruppe

Definition

Eine Teilmenge $U \subset G$ heißt Untergruppe, wenn

1. U unter der Verknüpfung abgeschlossen ist,
2. $1 \in U$ gilt
3. für $u \in U$ auch $u^{-1} \in U$ gilt.

1. Das Bild $f(H) \subset G$ eines Homomorphismus $f : H \longrightarrow G$ ist eine Untergruppe.
2. Der Kern $\ker(f) \subset G$ eines Homomorphismus $f : G \longrightarrow H$ ist eine Untergruppe.
3. Ist $S \subset G$ eine Teilmenge, dann ist $< S > := Im(F(S)) \subset G$

Untergruppen

Untergruppen entstehen z.B. so:

1. Das Bild $f(H) \subset G$ eines Homomorphismus $f : H \to G$ ist eine Untergruppe.
2. Der Kern $\ker(f) \subset G$ eines Homomorphismus $f : G \to H$ ist eine Untergruppe.
3. Ist $S \subset G$ eine Teilmenge, dann ist $< S >:= m(F(S)) \subset G$ die von S erzeugte Untergruppe.
4. Der Durchschnitt $U := \bigcap_i U_i$ über eine Familie $(U_i)_i$ von Untergruppen ist eine Untergruppe.
5. Sei $G \to \mathrm{Aut}_{\mathrm{sets}}(A)$ eine Wirkung. Für $a \in A$ sei $G_a := \{g \in G | ga = a\}$ der Stabilisator. Dann ist $G_a \subset G$ eine Untergruppe.

Untergruppen

Untergruppen entstehen z.B. so:

1. Das Bild $f(H) \subset G$ eines Homomorphismus $f : H \to G$ ist eine Untergruppe.
2. Der Kern $\ker(f) \subset G$ eines Homomorphismus $f : G \to H$ ist eine Untergruppe.
3. Ist $S \subset G$ eine Teilmenge, dann ist $< S >:= m(F(S)) \subset G$ die von S erzeugte Untergruppe.
4. Der Durchschnitt $U := \bigcap_i U_i$ über eine Familie $(U_i)_i$ von Untergruppen ist eine Untergruppe.
5. Sei $G \to \mathrm{Aut}_{sets}(A)$ eine Wirkung. Für $a \in A$ sei $G_a := \{g \in G | ga = a\}$ der Stabilisator. Dann ist $G_a \subset G$ eine Untergruppe.

Untergruppen

Untergruppen entstehen z.B. so:

1. Das Bild $f(H) \subset G$ eines Homomorphismus $f : H \to G$ ist eine Untergruppe.
2. Der Kern $\mathtt{ker}(f) \subset G$ eines Homomorphismus $f : G \to H$ ist eine Untergruppe.
3. Ist $S \subset G$ eine Teilmenge, dann ist $< S >:= m(F(S)) \subset G$ die von S erzeugte Untergruppe.
4. Der Durchschnitt $U := \bigcap_i U_i$ über eine Familie $(U_i)_i$ von Untergruppen ist eine Untergruppe.
5. Sei $G \to \mathtt{Aut}_{\mathtt{sets}}(A)$ eine Wirkung. Für $a \in A$ sei $G_a := \{g \in G | ga = a\}$ der Stabilisator. Dann ist $G_a \subset G$ eine Untergruppe.

Untergruppen

Untergruppen entstehen z.B. so:

1. Das Bild $f(H) \subset G$ eines Homomorphismus $f : H \to G$ ist eine Untergruppe.
2. Der Kern $\mathtt{ker}(f) \subset G$ eines Homomorphismus $f : G \to H$ ist eine Untergruppe.
3. Ist $S \subset G$ eine Teilmenge, dann ist $< S >:= m(F(S)) \subset G$ die von S erzeugte Untergruppe.
4. Der Durchschnitt $U := \bigcap_i U_i$ über eine Familie $(U_i)_i$ von Untergruppen ist eine Untergruppe.
5. Sei $G \to \mathtt{Aut}_{\mathtt{sets}}(A)$ eine Wirkung. Für $a \in A$ sei $G_a := \{g \in G | ga = a\}$ der Stabilisator. Dann ist $G_a \subset G$ eine Untergruppe.

Untergruppen

Untergruppen entstehen z.B. so:

1. Das Bild $f(H) \subset G$ eines Homomorphismus $f : H \to G$ ist eine Untergruppe.
2. Der Kern $\mathtt{ker}(f) \subset G$ eines Homomorphismus $f : G \to H$ ist eine Untergruppe.
3. Ist $S \subset G$ eine Teilmenge, dann ist $< S >:= m(F(S)) \subset G$ die von S erzeugte Untergruppe.
4. Der Durchschnitt $U := \bigcap_i U_i$ über eine Familie $(U_i)_i$ von Untergruppen ist eine Untergruppe.
5. Sei $G \to \mathtt{Aut}_{\mathtt{sets}}(A)$ eine Wirkung. Für $a \in A$ sei $G_a := \{g \in G | ga = a\}$ der Stabilisator. Dann ist $G_a \subset G$ eine Untergruppe.

Untergruppen

Untergruppen entstehen z.B. so:

1. Das Bild $f(H) \subset G$ eines Homomorphismus $f : H \to G$ ist eine Untergruppe.
2. Der Kern $\mathtt{ker}(f) \subset G$ eines Homomorphismus $f : G \to H$ ist eine Untergruppe.
3. Ist $S \subset G$ eine Teilmenge, dann ist $< S >:= m(F(S)) \subset G$ die von S erzeugte Untergruppe.
4. Der Durchschnitt $U := \bigcap_i U_i$ über eine Familie $(U_i)_i$ von Untergruppen ist eine Untergruppe.
5. Sei $G \to \mathtt{Aut}_{\mathtt{sets}}(A)$ eine Wirkung. Für $a \in A$ sei $G_a := \{g \in G | ga = a\}$ der Stabilisator. Dann ist $G_a \subset G$ eine Untergruppe.

Nebenklassen

$G \mapsto \mathtt{Aut}_{sets}(A)$

Nebenklassen

$G \mapsto \mathtt{Aut}_{sets}(A)$
Definieren Relation:

Nebenklassen

$G \mapsto \mathtt{Aut}_{sets}(A)$
Definieren Relation:

$$a \sim b \Leftrightarrow \exists g \in G | ga = b \ .$$

Nebenklassen

$G \mapsto \mathtt{Aut}_{sets}(A)$
Definieren Relation:

$$a \sim b \Leftrightarrow \exists g \in G | ga = b \ .$$

Lemma

Diese Relation ist eine Äquivalenzrelation.

Nebenklassen

$G \mapsto \mathtt{Aut}_{sets}(A)$
Definieren Relation:

$$a \sim b \Leftrightarrow \exists g \in G | ga = b \ .$$

Lemma

Diese Relation ist eine Äquivalenzrelation.

Definition

Mit $G\backslash A$ bezeichnen wir die Menge der Äquivalenzklassen bezüglich $\sim$.

Nebenklassen

$$p : A \to G\backslash A,\ p(a) := [a] = Ga$$

Nebenklassen

$p : A \to G\backslash A,\ p(a) := [a] = Ga$

Lemma

Für jede Menge B und Abbildung $f : A \to B$ mit der Eigenschaft, daß $f(ga) = a$ für alle $g \in G$, gibt es genau eine Abbildung $\bar{f} : G\backslash A \to B$ mit $\bar{f} \circ p = f$.

Nebenklassen

$p : A \to G\backslash A,\ p(a) := [a] = Ga$

Lemma

Für jede Menge B und Abbildung $f : A \to B$ mit der Eigenschaft, daß $f(ga) = a$ für alle $g \in G$, gibt es genau eine Abbildung $\bar{f} : G\backslash A \to B$ mit $\bar{f} \circ p = f$.

$p : A \to G\backslash A$ ist der Quotient einer G-Wirkung in der Kategorie `sets`. Die in Lemma gezeigte Eigenschaft wird benutzt, um Quotienten von G-Wirkungen in anderen Kategorien zu charakterisieren.

Normalteiler - 1

$U \subset G$ - Untergruppe.

Normalteiler - 1

$U \subset G$ - Untergruppe.
Die Gruppe U kann auf G durch links und durch Rechtsmultiplikation wirken:

Normalteiler - 1

$U \subset G$ - Untergruppe.
Die Gruppe U kann auf G durch links und durch Rechtsmultiplikation wirken:

$$(u, g) \mapsto ug,$$

Normalteiler - 1

$U \subset G$ - Untergruppe.
Die Gruppe U kann auf G durch links und durch Rechtsmultiplikation wirken:

$$(u, g) \mapsto ug, \quad (u, g) \mapsto gu^{-1} \ .$$

Normalteiler - 1

Wir fragen nun, unter welchen Umständen die durch die (Links)Wirkung von U induzierte Äquivalenzrelation mit der Gruppenmultiplikation verträglich ist. Verträglich bedeutet hier:

$$g \sim g', h \sim h' \Rightarrow gh \sim g'h' \ .$$

Diese Verträglichkeit ist von Bedeutung, weil sie die Definition einer Verknüpfung $\circ : U\backslash G \times U\backslash G \to U\backslash G$ durch $[g] \circ [h] := [g \circ h]$ erlaubt.

Normalteiler -2

Definition

Die Untergruppe $U \subset G$ heißt Normalteiler, wenn die durch die Linkswirkung auf G induzierte Relation mit der Verknüpfung von G verträglich ist.

1. Für jedes $g \in G$ ist $gU = Ug$.
2. $U = \alpha_g(U)$ für jeden inneren Automorphismus α_g von G.
3. Die durch die Links- und Rechtwirkungen indizierten Relationen auf G stimmen überein.
4. G/U ist mit der induzierten Wirkung eine Gruppe

Lemma

1. *Der Kern eines Homomorphismus ist ein Normalteiler.*

Normalteiler -2

Wenn U ein Normalteiler ist, dann gilt:

1. Für jedes $g \in G$ ist $gU = Ug$.
2. $U = \alpha_g(U)$ für jeden inneren Automorphismus α_g von G.
3. Die durch die Links- und Rechtwirkungen indizierten Relationen auf G stimmen überein.
4. G/U ist mit der induzierten Wirkung eine Gruppe

Lemma

1. *Der Kern eines Homomorphismus ist ein Normalteiler.*
2. *Jede Untergruppe einer abelschen Gruppe ist ein Normalteiler.*
3. *Ein Durchschnitt $\bigcap_i U_i$ einer Familie von Normalteilern (U_i) ist wieder ein Normalteiler.*

Normalteiler -2

Wenn U ein Normalteiler ist, dann gilt:

1. Für jedes $g \in G$ ist $gU = Ug$.
2. $U = \alpha_g(U)$ für jeden inneren Automorphismus α_g von G.
3. Die durch die Links- und Rechtwirkungen indizierten Relationen auf G stimmen überein.
4. G/U ist mit der induzierten Wirkung eine Gruppe

Lemma

1. *Der Kern eines Homomorphismus ist ein Normalteiler.*
2. *Jede Untergruppe einer abelschen Gruppe ist ein Normalteiler.*
3. *Ein Durchschnitt $\cap_i U_i$ einer Familie von Normalteilern (U_i) ist wieder ein Normalteiler.*

Normalteiler -2

Wenn U ein Normalteiler ist, dann gilt:

1. Für jedes $g \in G$ ist $gU = Ug$.
2. $U = \alpha_g(U)$ für jeden inneren Automorphismus α_g von G.
3. Die durch die Links- und Rechtwirkungen indizierten Relationen auf G stimmen überein.
4. G/U ist mit der induzierten Wirkung eine Gruppe

Lemma

1. *Der Kern eines Homomorphismus ist ein Normalteiler.*
2. *Jede Untergruppe einer abelschen Gruppe ist ein Normalteiler.*
3. *Ein Durchschnitt $\cap_i U_i$ einer Familie von Normalteilern (U_i) ist wieder ein Normalteiler.*

Normalteiler -2

Wenn U ein Normalteiler ist, dann gilt:

1. Für jedes $g \in G$ ist $gU = Ug$.
2. $U = \alpha_g(U)$ für jeden inneren Automorphismus α_g von G.
3. Die durch die Links- und Rechtwirkungen indizierten Relationen auf G stimmen überein.
4. G/U ist mit der induzierten Wirkung eine Gruppe

Lemma

1. *Der Kern eines Homomorphismus ist ein Normalteiler.*
2. *Jede Untergruppe einer abelschen Gruppe ist ein Normalteiler.*
3. *Ein Durchschnitt $\cap_i U_i$ einer Familie von Normalteilern (U_i) ist wieder ein Normalteiler.*

Normalteiler -2

Wenn U ein Normalteiler ist, dann gilt:

1. Für jedes $g \in G$ ist $gU = Ug$.
2. $U = \alpha_g(U)$ für jeden inneren Automorphismus α_g von G.
3. Die durch die Links- und Rechtwirkungen indizierten Relationen auf G stimmen überein.
4. G/U ist mit der induzierten Wirkung eine Gruppe

Lemma

1. *Der Kern eines Homomorphismus ist ein Normalteiler.*
2. *Jede Untergruppe einer abelschen Gruppe ist ein Normalteiler.*
3. *Ein Durchschnitt $\cap_i U_i$ einer Familie von Normalteilern (U_i) ist wieder ein Normalteiler.*

Normalteiler -2

1. Für jedes $g \in G$ ist $gU = Ug$.
2. $U = \alpha_g(U)$ für jeden inneren Automorphismus α_g von G.
3. Die durch die Links- und Rechtwirkungen indizierten Relationen auf G stimmen überein.
4. G/U ist mit der induzierten Wirkung eine Gruppe

Lemma

1. *Der Kern eines Homomorphismus ist ein Normalteiler.*
2. *Jede Untergruppe einer abelschen Gruppe ist ein Normalteiler.*
3. *Ein Durchschnitt $\cap_i U_i$ einer Familie von Normalteilern (U_i) ist wieder ein Normalteiler.*

Normalteiler -2

1. Für jedes $g \in G$ ist $gU = Ug$.
2. $U = \alpha_g(U)$ für jeden inneren Automorphismus α_g von G.
3. Die durch die Links- und Rechtwirkungen indizierten Relationen auf G stimmen überein.
4. G/U ist mit der induzierten Wirkung eine Gruppe

Lemma

1. *Der Kern eines Homomorphismus ist ein Normalteiler.*
2. *Jede Untergruppe einer abelschen Gruppe ist ein Normalteiler.*
3. *Ein Durchschnitt $\cap_i U_i$ einer Familie von Normalteilern (U_i) ist wieder ein Normalteiler.*

Normalteiler -2

1. Für jedes $g \in G$ ist $gU = Ug$.
2. $U = \alpha_g(U)$ für jeden inneren Automorphismus α_g von G.
3. Die durch die Links- und Rechtwirkungen indizierten Relationen auf G stimmen überein.
4. G/U ist mit der induzierten Wirkung eine Gruppe

Lemma

1. *Der Kern eines Homomorphismus ist ein Normalteiler.*
2. *Jede Untergruppe einer abelschen Gruppe ist ein Normalteiler.*
3. *Ein Durchschnitt $\cap_i U_i$ einer Familie von Normalteilern (U_i) ist wieder ein Normalteiler.*

Die Alternierende Gruppe

A - endliche Menge

Die Alternierende Gruppe

A - endliche Menge
konstruieren Homomorphismus $\sigma : S(A) \to \mathbb{Z}/2\mathbb{Z}$:

Die Alternierende Gruppe

A - endliche Menge
konstruieren Homomorphismus $\sigma : S(A) \to \mathbb{Z}/2\mathbb{Z}$:
$\rho : S(A) \to GL(\mathbb{Q}(A))$ - lineare Darstellung

Die Alternierende Gruppe

A - endliche Menge
konstruieren Homomorphismus $\sigma : S(A) \to \mathbb{Z}/2\mathbb{Z}$:
$\rho : S(A) \to GL(\mathbb{Q}(A))$ - lineare Darstellung
$d : S(A) \to \mathbb{Q}^*$, $g \mapsto \det(\rho(g))$

Die Alternierende Gruppe

A - endliche Menge
konstruieren Homomorphismus $\sigma : S(A) \to \mathbb{Z}/2\mathbb{Z}$:
$\rho : S(A) \to GL(\mathbb{Q}(A))$ - lineare Darstellung
$d : S(A) \to \mathbb{Q}^*$, $g \mapsto \det(\rho(g))$
$d(S(A)) \subset \{1, -1\}$

Die Alternierende Gruppe

A - endliche Menge
konstruieren Homomorphismus $\sigma : S(A) \to \mathbb{Z}/2\mathbb{Z}$:
$\rho : S(A) \to GL(\mathbb{Q}(A))$ - lineare Darstellung
$d : S(A) \to \mathbb{Q}^*$, $g \mapsto \det(\rho(g))$
$d(S(A)) \subset \{1, -1\}$

Definition

Wir definieren

$$\sigma(g) := \begin{cases} 0 & \det(\rho(g)) = 1 \\ 1 & \det(\rho(g)) = -1 \end{cases} \in \mathbb{Z}/2\mathbb{Z}.$$

Die Alternierende Gruppe

Definition

Wir definieren die alternierende Gruppe $Alt(A) \subset S(A)$ als den Kern von $\sigma : S(A) \to \mathbb{Z}/2\mathbb{Z}$.

Die Alternierende Gruppe

Definition

Wir definieren die alternierende Gruppe $Alt(A) \subset S(A)$ als den Kern von $\sigma : S(A) \to \mathbb{Z}/2\mathbb{Z}$.

Wir schreiben Alt_n für $Alt(\{1, \ldots, n\})$.

Erzeugte Normalteiler

G - eine Gruppe,

Erzeugte Normalteiler

G - eine Gruppe, $R \subset G$ - eine Teilmenge,

Erzeugte Normalteiler

G - eine Gruppe, $R \subset G$ - eine Teilmenge, $< R > \subset G$ - die von R erzeugt Untergruppe

Erzeugte Normalteiler

G - eine Gruppe, $R \subset G$ - eine Teilmenge, $< R > \subset G$ - die von R erzeugt Untergruppe

Lemma

Die Gruppe $< R >$ ist der Durchschnitt

$$< R > = \cap_{R \subset U} U$$

aller R enthaltenden Untergruppen von G.

Erzeugte Normalteiler

Lemma

Die Gruppe $< R >$ *ist der Durchschnitt*

$$< R >= \cap_{R \subset U} U$$

aller R *enthaltenden Untergruppen von* G.

Im allgemeinen ist $< R >$ kein Normalteiler.

Erzeugte Normalteiler

Lemma

Die Gruppe $< R >$ *ist der Durchschnitt*

$$< R >= \cap_{R \subset U} U$$

aller R *enthaltenden Untergruppen von* G*.*

Definition

Der von R erzeugte Normalteiler $<< R >>$ ist der Durchschnitt

$$<< R >>= \cap_{R \subset N} N$$

aller R-enthaltenden Normalteiler von G.

Erzeuger und Relationen

T - eine Menge,

Erzeuger und Relationen

T - eine Menge, $F(T)$ -freie Gruppe über T,

Erzeuger und Relationen

T - eine Menge, $F(T)$ -freie Gruppe über T, $F(T) := W^{red}(\hat{T})$,

Erzeuger und Relationen

T - eine Menge, $F(T)$ -freie Gruppe über T, $F(T) := W^{red}(\hat{T})$,
$R \subset W^{red}(\hat{T})$ - eine Menge von reduzierten Worten

Erzeuger und Relationen

T - eine Menge, $F(T)$ -freie Gruppe über T, $F(T) := W^{red}(\hat{T})$, $R \subset W^{red}(\hat{T})$ - eine Menge von reduzierten Worten

Definition

Die durch T mit den Relationen R erzeugte Gruppe $< T|R >$ ist durch $F(T)/ << R >>$ definiert.

Erzeuger und Relationen

T - eine Menge, $F(T)$ -freie Gruppe über T, $F(T) := W^{red}(\hat{T})$, $R \subset W^{red}(\hat{T})$ - eine Menge von reduzierten Worten

Definition

Die durch T mit den Relationen R erzeugte Gruppe $< T|R >$ ist durch $F(T)/ << R >>$ definiert.

Das Paar (T, R) heißt auch Präsentation der Gruppe.

Der Satz von Lagrange

Definition

Die Ordnung $|G| \in$ einer endlichen Gruppe ist die Anzahl ihrer Elemente.

Der Satz von Lagrange

Definition

Die Ordnung $|G| \in$ einer endlichen Gruppe ist die Anzahl ihrer Elemente.

$|S_n| = n!$,

Der Satz von Lagrange

Definition

Die Ordnung $|G| \in$ einer endlichen Gruppe ist die Anzahl ihrer Elemente.

$|S_n| = n!, |Alt_n| = \frac{n!}{2},$

Der Satz von Lagrange

Definition

Die Ordnung $|G| \in$ einer endlichen Gruppe ist die Anzahl ihrer Elemente.

$|S_n| = n!, |Alt_n| = \frac{n!}{2}$, $|D_n| = 2n$,

Der Satz von Lagrange

Definition

Die Ordnung $|G| \in$ einer endlichen Gruppe ist die Anzahl ihrer Elemente.

$|S_n| = n!, |Alt_n| = \frac{n!}{2}$, $|D_n| = 2n$, $|C_n| = n$

Der Satz von Lagrange

Definition

Die Ordnung $|G| \in$ einer endlichen Gruppe ist die Anzahl ihrer Elemente.

$|S_n| = n!, |Alt_n| = \frac{n!}{2}$, $|D_n| = 2n$, $|C_n| = n$ und $|GL(2, F_2)| = 6$.

Der Satz von Lagrange

Definition

Die Ordnung $|G| \in$ einer endlichen Gruppe ist die Anzahl ihrer Elemente.

$|S_n| = n!, |Alt_n| = \frac{n!}{2}$, $|D_n| = 2n$, $|C_n| = n$ und $|GL(2, F_2)| = 6$.

Theorem

Ist $U \subset G$ eine Untergruppe, so gilt $|G| = |U||G/U|$.

Der Satz von Lagrange

Definition

Die Ordnung $|G| \in$ einer endlichen Gruppe ist die Anzahl ihrer Elemente.

$|S_n| = n!, |Alt_n| = \frac{n!}{2}$, $|D_n| = 2n$, $|C_n| = n$ und $|GL(2, F_2)| = 6$.

Theorem

Ist $U \subset G$ eine Untergruppe, so gilt $|G| = |U||G/U|$.

Corollary

Ist $U \subset G$ eine Untergruppe, so teilt $|U|$ die Gruppenordnung.

Einfache Gruppen

Definition

Ein maximaler Normalteiler von G ist ein echter Normalteiler $N \subset G$ derart, daß der einzige N enthaltende Normalteiler die Gruppe G selbst ist.

Einfache Gruppen

Definition

Ein maximaler Normalteiler von G ist ein echter Normalteiler $N \subset G$ derart, daß der einzige N enthaltende Normalteiler die Gruppe G selbst ist.

Definition

Eine Gruppe heißt einfach, wenn die triviale Untergruppe ein maximaler Normalteiler ist.

Kompositionsreihe

Definition

Eine aufsteigende Folge von Untergruppen

$$1 = U_0 \subset U_1 \subset \cdots \subset U_{a-1} \subset U_a = G$$

heißt Kompositionsreihe, wenn U_{i-1} für alle i ein maximaler Normalteiler in U_i ist.

Kompositionsreihe

Definition

Eine aufsteigende Folge von Untergruppen

$$1 = U_0 \subset U_1 \subset \cdots \subset U_{a-1} \subset U_a = G$$

heißt Kompositionsreihe, wenn U_{i-1} für alle i ein maximaler Normalteiler in U_i ist.

Die Kompositionsfaktoren U_i/U_{i-1} sind einfache Gruppen.

Der Satz von Jordan Hölder

Theorem

Seien

$$1 = U_0 \subset U_1 \subset \cdots \subset U_{a-1} \subset U_a = G$$

und

$$1 = V_0 \subset V_1 \subset \cdots \subset V_{b-1} \subset V_b = G$$

zwei Kompositionsreihen von G. Dann gilt $a = b$ und es gibt eine Permutation $\sigma \in S_a$ derart, daß $U_{\sigma(i)}/U_{\sigma(i)-1} \cong V_i/V_{i-1}$.

Alt_n ist einfach für $n \geq 5$

Theorem

Ist $n \geq 5$, so ist Alt_n einfach.

Alt_n ist einfach für $n \geq 5$

Theorem

Ist $n \geq 5$, so ist Alt_n einfach.

Also sind die Kompositionsfaktoren von S_n durch

$$\{\mathbb{Z}/2\mathbb{Z}, Alt_n\}$$

gegeben.

Direkte Produkte

G, H - Gruppen

Direkte Produkte

G, H - Gruppen

Definition

Die Gruppe $G \times H$ ist die Menge $G \times H$ mit Verknüpfung $(g_0, h_0) \circ (g_1, h_1) = (g_0 \circ h_0, g_1 \circ h_1)$ und dem Einselement $1 = (1, 1)$.

Direkte Produkte

G, H - Gruppen

Definition

Die Gruppe $G \times H$ ist die Menge $G \times H$ mit Verknüpfung $(g_0, h_0) \circ (g_1, h_1) = (g_0 \circ h_0, g_1 \circ h_1)$ und dem Einselement $1 = (1, 1)$.

Lemma

Das Produkt $G \times H$ ist wohldefiniert.

Eigenschaften des direkten Produktes

1. Die Einbettungen $G \longrightarrow G \times H$, $g \mapsto (g, 1)$, und $H \longrightarrow G \times H$, $h \mapsto (1, h)$ sind Einbettungen von Normalteilern.
2. $G \cong G \times H/H$ und $H \cong G \times H/G$
3. Die Bilder von G und H in $G \times H$ kommutieren.

Eigenschaften des direkten Produktes

1. Die Einbettungen $G \longrightarrow G \times H$, $g \mapsto (g, 1)$, und $H \longrightarrow G \times H$, $h \mapsto (1, h)$ sind Einbettungen von Normalteilern.
2. $G \cong G \times H/H$ und $H \cong G \times H/G$
3. Die Bilder von G und H in $G \times H$ kommutieren.

Eigenschaften des direkten Produktes

1. Die Einbettungen $G \longrightarrow G \times H$, $g \mapsto (g, 1)$, und $H \longrightarrow G \times H$, $h \mapsto (1, h)$ sind Einbettungen von Normalteilern.
2. $G \cong G \times H/H$ und $H \cong G \times H/G$
3. Die Bilder von G und H in $G \times H$ kommutieren.

Semidirekte Produkte - 1

$\rho : H \to \mathtt{Aut}(G)$ - ein Homomorphismus, $(h, g) \mapsto g^h$

Semidirekte Produkte - 1

$\rho : H \to \mathtt{Aut}(G)$ - ein Homomorphismus, $(h, g) \mapsto g^h$
auf $G \times H$ definieren wir die folgende Verknüpfung:

Semidirekte Produkte - 1

$\rho : H \longrightarrow \mathtt{Aut}(G)$ - ein Homomorphismus, $(h, g) \mapsto g^h$
auf $G \times H$ definieren wir die folgende Verknüpfung:

$$(g_0, h_0) \circ_\rho (g_1, h_1) = (g_0 \circ g_1^{h_0}, h_0 \circ h_1) \ .$$

Semidirekte Produkte - 1

Lemma

1. $G \times| H := (G \times H, \circ_\rho, (1,1))$ *ist eine Gruppe.*
2. $G \longrightarrow G \times| H$ *ist eine Einbettung eines Normalteilers.*
3. $H \longrightarrow G \times| H$ *ist eine Einbettung einer Untergruppe.*
4. $G \times| H \longrightarrow H$ *ist ein Homomorphismus.*

Semidirekte Produkte - 1

Lemma

1. $G \times | H := (G \times H, \circ_\rho, (1,1))$ *ist eine Gruppe.*
2. $G \longrightarrow G \times | H$ *ist eine Einbettung eines Normalteilers.*
3. $H \longrightarrow G \times | H$ *ist eine Einbettung einer Untergruppe.*
4. $G \times | H \longrightarrow H$ *ist ein Homomorphismus.*

Semidirekte Produkte - 1

Lemma

1. $G \times | H := (G \times H, \circ_\rho, (1,1))$ *ist eine Gruppe.*
2. $G \longrightarrow G \times | H$ *ist eine Einbettung eines Normalteilers.*
3. $H \longrightarrow G \times | H$ *ist eine Einbettung einer Untergruppe.*
4. $G \times | H \longrightarrow H$ *ist ein Homomorphismus.*

Semidirekte Produkte - 1

Lemma

1. $G \times| H := (G \times H, \circ_\rho, (1,1))$ *ist eine Gruppe.*
2. $G \to G \times| H$ *ist eine Einbettung eines Normalteilers.*
3. $H \to G \times| H$ *ist eine Einbettung einer Untergruppe.*
4. $G \times| H \to H$ *ist ein Homomorphismus.*

Semidirekte Produkte - 1

Lemma

1. $G \times| H := (G \times H, \circ_\rho, (1,1))$ *ist eine Gruppe.*
2. $G \to G \times| H$ *ist eine Einbettung eines Normalteilers.*
3. $H \to G \times| H$ *ist eine Einbettung einer Untergruppe.*
4. $G \times| H \to H$ *ist ein Homomorphismus.*

Semidirekte Produkte - 2

Definition

$G \times | H$ heißt das semidirekte Produkt von G und H bezüglich ρ.

Semidirekte Produkte - 2

Definition

$G \times | H$ heißt das semidirekte Produkt von G und H bezüglich ρ.

Wenn ρ der triviale Homomorphismus ist, dann stimmt das semidirekte mit dem direkten Produkt überein.

Semidirekte Produkte - 2

Definition

$G \times | H$ heißt das semidirekte Produkt von G und H bezüglich ρ.

Wenn ρ der triviale Homomorphismus ist, dann stimmt das semidirekte mit dem direkten Produkt überein.

Lemma

Die Liste der Kompositionsfaktoren von $G \times | H$ ist die Vereinigung der Listen der Kompositionsfaktoren von G und H.

Zyklische Gruppen

Definition

Eine Gruppe G heißt zyklisch, wenn sie von einem Element erzeugt werden kann.

Zyklische Gruppen

Definition

Eine Gruppe G heißt zyklisch, wenn sie von einem Element erzeugt werden kann.

Lemma

Alle Untergruppen von $\mathbb{Z}$ sind zyklisch.

Zyklische Gruppen

Definition

Eine Gruppe G heißt zyklisch, wenn sie von einem Element erzeugt werden kann.

Lemma

Alle Untergruppen von $\mathbb{Z}$ sind zyklisch.

Lemma

Jede endliche zyklische Gruppe ist zu $\mathbb{Z}/n\mathbb{Z}$ für ein geeignetes eindeutig bestimmtes $n \in \mathbb{N}$ isomorph.

Untergruppen zyklischer Gruppen

Lemma

Sei G eine endliche Gruppe und $g, h \in G$ kommutierende Elemente mit teilerfremder Ordnung. Dann definiert $(g^r, h^s) \mapsto g^r h^s$ einen Isomorphismus $< g > \times < h > \cong < g, h >$. Insbesondere gilt $o(gh) = o(g)o(h)$.

Untergruppen zyklischer Gruppen

Lemma

Sei G eine endliche Gruppe und $g, h \in G$ kommutierende Elemente mit teilerfremder Ordnung. Dann definiert $(g^r, h^s) \mapsto g^r h^s$ einen Isomorphismus $< g > \times < h > \cong < g, h >$. Insbesondere gilt $o(gh) = o(g)o(h)$.

$G = < g >$ - eine endliche zyklische Gruppe

Untergruppen zyklischer Gruppen

Lemma

Sei G eine endliche Gruppe und $g, h \in G$ kommutierende Elemente mit teilerfremder Ordnung. Dann definiert $(g^r, h^s) \mapsto g^r h^s$ einen Isomorphismus $< g > \times < h > \cong < g, h >$. Insbesondere gilt $o(gh) = o(g)o(h)$.

$G =< g >$ - eine endliche zyklische Gruppe

Lemma

Die Untergruppen von G sind die Gruppen $< g^l >$ für alle Teiler l von $|G|$

Zerlegung in p-Gruppen

Definition

Eine endliche Gruppe ist eine p-Gruppe, wenn $|G| = p^e$ für ein geeignetes $e \in \mathbb{N}$ gilt.

Zerlegung in p-Gruppen

Definition

Eine endliche Gruppe ist eine p-Gruppe, wenn $|G| = p^e$ für ein geeignetes $e \in \mathbb{N}$ gilt.

Corollary

Jede zyklische Gruppe G ist isomorph zu einem Produkt von p-Gruppen

$$\mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{e_r}\mathbb{Z}, \quad |G| = p_1^{e_1} \dots p_r^{e_r} \ .$$

Komplemente

G - eine endliche abelsche Gruppe

Komplemente

G - eine endliche abelsche Gruppe

Lemma

Ist $U \subset G$ eine zyklische Untergruppe maximaler Ordnung, dann gilt $o(g)||U|$ für alle $g \in G$.

Komplemente

G - eine endliche abelsche Gruppe

Lemma

Ist $U \subset G$ eine zyklische Untergruppe maximaler Ordnung, dann gilt $o(g)||U|$ für alle $g \in G$.

Lemma

Ist $U \subset G$ eine maximale zyklische Untergruppe, so gibt es eine komplementäre Untergruppe $V \subset G$ so daß $G = U \times V$ ist.

Struktur endlicher abelscher Gruppen

Corollary

Jede endliche abelsche Gruppe ist isomorph zu einem Produkt zyklischer Gruppen.

Struktur endlicher abelscher Gruppen

Corollary

Jede endliche abelsche Gruppe ist isomorph zu einem Produkt zyklischer Gruppen.

Corollary

Jede endliche abelsche Gruppe ist isomorph zu einem Produkt zyklischer p-Gruppen.

Struktur endlicher abelscher Gruppen

Corollary

Jede endliche abelsche Gruppe ist isomorph zu einem Produkt zyklischer Gruppen.

Corollary

Jede endliche abelsche Gruppe ist isomorph zu einem Produkt zyklischer p-Gruppen.

$$G \cong \mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \mathbb{Z}/p_2^{e_2}\mathbb{Z} \cdots \times \mathbb{Z}/p_r^{e_r}\mathbb{Z}$$

Definition

Definition

Ein kommutativer Ring mit Eins ist ein Tupel $(R, +, \circ, 0, 1)$, aus einer nicht-leeren Menge R und Verknüpfungen $+$ und $\circ$ derart, daß

1. $(R, +, 0)$ eine abelsche Gruppe ist,
2. $(R, \circ, 1)$ ein abelsches Monoid ist,
3. und die Operationen $+$ und $\circ$ vermöge des Distributivgesetzes

$$a \circ (b + c) = a \circ b + a \circ c$$

verträglich sind.

Definition

Definition

Ein kommutativer Ring mit Eins ist ein Tupel $(R, +, \circ, 0, 1)$, aus einer nicht-leeren Menge R und Verknüpfungen $+$ und $\circ$ derart, daß

1. $(R, +, 0)$ eine abelsche Gruppe ist,
2. $(R, \circ, 1)$ ein abelsches Monoid ist,
3. und die Operationen $+$ und $\circ$ vermöge des Distributivgesetzes

$$a \circ (b + c) = a \circ b + a \circ c$$

verträglich sind.

Definition

Definition

Ein kommutativer Ring mit Eins ist ein Tupel $(R, +, \circ, 0, 1)$, aus einer nicht-leeren Menge R und Verknüpfungen $+$ und $\circ$ derart, daß

1. $(R, +, 0)$ eine abelsche Gruppe ist,
2. $(R, \circ, 1)$ ein abelsches Monoid ist,
3. und die Operationen $+$ und $\circ$ vermöge des Distributivgesetzes

$$a \circ (b + c) = a \circ b + a \circ c$$

verträglich sind.

Definition

Definition

Ein kommutativer Ring mit Eins ist ein Tupel $(R, +, \circ, 0, 1)$, aus einer nicht-leeren Menge R und Verknüpfungen $+$ und $\circ$ derart, daß

1. $(R, +, 0)$ eine abelsche Gruppe ist,
2. $(R, \circ, 1)$ ein abelsches Monoid ist,
3. und die Operationen $+$ und $\circ$ vermöge des Distributivgesetzes

$$a \circ (b + c) = a \circ b + a \circ c$$

verträglich sind.

Definition

Definition

Ein kommutativer Ring mit Eins ist ein Tupel $(R, +, \circ, 0, 1)$, aus einer nicht-leeren Menge R und Verknüpfungen $+$ und $\circ$ derart, daß

1. $(R, +, 0)$ eine abelsche Gruppe ist,
2. $(R, \circ, 1)$ ein abelsches Monoid ist,
3. und die Operationen $+$ und $\circ$ vermöge des Distributivgesetzes

$$a \circ (b + c) = a \circ b + a \circ c$$

verträglich sind.

Wir werden das Symbol $\circ$ für die Multiplikation gewöhnlich

Definition

Definition

Ein kommutativer Ring mit Eins ist ein Tupel $(R, +, \circ, 0, 1)$, aus einer nicht-leeren Menge R und Verknüpfungen $+$ und $\circ$ derart, daß

1. $(R, +, 0)$ eine abelsche Gruppe ist,
2. $(R, \circ, 1)$ ein abelsches Monoid ist,
3. und die Operationen $+$ und $\circ$ vermöge des Distributivgesetzes

$$a \circ (b + c) = a \circ b + a \circ c$$

verträglich sind.

Wir werden das Symbol $\circ$ für die Multiplikation gewöhnlich

Beispiele

1. Jeder Körper ist ein Ring.
2. Die ganzen Zahlen $\mathbb{Z}$ bilden einen Ring.
3. Ist R ein Ring, dann auch der Ring der der Polynome $R[x]$.
4. Für eine Menge X und einen Ring R bilden die Funktionen $R^X = \{f : X \to R\}$ einen Ring mit $(f+g)(x) = f(x) + g(x)$, $(fg)(x) = f(x)g(x)$
5. Für eine endliche abelsche Gruppe G ist $R(G) := R^G$ mit der Addition $(f+g)(x) := f(x) + g(x)$ und der Multiplikation $(fg)(x) = \sum_{y \in G} f(y)g(y^{-1}x)$ ein Ring.

Beispiele

1. Jeder Körper ist ein Ring.
2. Die ganzen Zahlen $\mathbb{Z}$ bilden einen Ring.
3. Ist R ein Ring, dann auch der Ring der der Polynome $R[x]$.
4. Für eine Menge X und einen Ring R bilden die Funktionen $R^X = \{f : X \to R\}$ einen Ring mit $(f+g)(x) = f(x) + g(x)$, $(fg)(x) = f(x)g(x)$
5. Für eine endliche abelsche Gruppe G ist $R(G) := R^G$ mit der Addition $(f+g)(x) := f(x) + g(x)$ und der Multiplikation $(fg)(x) = \sum_{y \in G} f(y)g(y^{-1}x)$ ein Ring.

Beispiele

1. Jeder Körper ist ein Ring.
2. Die ganzen Zahlen $\mathbb{Z}$ bilden einen Ring.
3. Ist R ein Ring, dann auch der Ring der der Polynome $R[x]$.
4. Für eine Menge X und einen Ring R bilden die Funktionen $R^X = \{f : X \to R\}$ einen Ring mit $(f+g)(x) = f(x) + g(x)$, $(fg)(x) = f(x)g(x)$
5. Für eine endliche abelsche Gruppe G ist $R(G) := R^G$ mit der Addition $(f+g)(x) := f(x) + g(x)$ und der Multiplikation $(fg)(x) = \sum_{y \in G} f(y)g(y^{-1}x)$ ein Ring.

Beispiele

1. Jeder Körper ist ein Ring.
2. Die ganzen Zahlen $\mathbb{Z}$ bilden einen Ring.
3. Ist R ein Ring, dann auch der Ring der der Polynome $R[x]$.
4. Für eine Menge X und einen Ring R bilden die Funktionen $R^X = \{f : X \to R\}$ einen Ring mit $(f+g)(x) = f(x) + g(x)$, $(fg)(x) = f(x)g(x)$
5. Für eine endliche abelsche Gruppe G ist $R(G) := R^G$ mit der Addition $(f+g)(x) := f(x) + g(x)$ und der Multiplikation $(fg)(x) = \sum_{y \in G} f(y)g(y^{-1}x)$ ein Ring.

Beispiele

1. Jeder Körper ist ein Ring.
2. Die ganzen Zahlen $\mathbb{Z}$ bilden einen Ring.
3. Ist R ein Ring, dann auch der Ring der der Polynome $R[x]$.
4. Für eine Menge X und einen Ring R bilden die Funktionen $R^X = \{f : X \to R\}$ einen Ring mit $(f+g)(x) = f(x) + g(x)$, $(fg)(x) = f(x)g(x)$
5. Für eine endliche abelsche Gruppe G ist $R(G) := R^G$ mit der Addition $(f+g)(x) := f(x) + g(x)$ und der Multiplikation $(fg)(x) = \sum_{y \in G} f(y)g(y^{-1}x)$ ein Ring.

Polynome

Definition

Die unterliegende additive Gruppe des Polynomringes $R[x]$ ist die Gruppe der Abbildungen $a : \mathbb{N} \to R$, welche nur an endlich vielen Stellen von Null verschiedene Werte annehmen. Das Produkt wird durch

$$(a \circ b)_n := \sum_{k,l \in \mathbb{N}, k+l=n} a_k b_l$$

definiert.

Polynome

Definition

Die unterliegende additive Gruppe des Polynomringes $R[x]$ ist die Gruppe der Abbildungen $a : \mathbb{N} \to R$, welche nur an endlich vielen Stellen von Null verschiedene Werte annehmen. Das Produkt wird durch

$$(a \circ b)_n := \sum_{k,l \in \mathbb{N}, k+l=n} a_k b_l$$

definiert.

Man kann $R[x]$ als den (Halb)Gruppenring von $\mathbb{N}$ auffassen.

Polynome

Definition

Die unterliegende additive Gruppe des Polynomringes $R[x]$ ist die Gruppe der Abbildungen $a : \mathbb{N} \to R$, welche nur an endlich vielen Stellen von Null verschiedene Werte annehmen. Das Produkt wird durch

$$(a \circ b)_n := \sum_{k,l \in \mathbb{N}, k+l=n} a_k b_l$$

definiert.

Man kann $R[x]$ als den (Halb)Gruppenring von $\mathbb{N}$ auffassen.

Lemma

Der Ring $R[x]$ ist wohldefiniert.

Polynome

Definition

Der Grad eines Polynoms $0 \neq a \in R[x]$ wird durch

$$\deg(a) := \max\{n \in \mathbb{N} | a_n \neq 0\}$$

definiert. Wir setzen $\deg(0) := \infty$.

Polynome

Definition

Der Grad eines Polynoms $0 \neq a \in R[x]$ wird durch

$$\deg(a) := \max\{n \in \mathbb{N} | a_n \neq 0\}$$

definiert. Wir setzen $\deg(0) := \infty$.

Lemma

Es gilt:

1. $\deg(ab) \leq \deg(a) + \deg(b)$
2. $\deg(a+b) \leq \max\{\deg(a), \deg(b)\}$.

Polynome

Definition

Der Grad eines Polynoms $0 \neq a \in R[x]$ wird durch

$$\deg(a) := \max\{n \in \mathbb{N} | a_n \neq 0\}$$

definiert. Wir setzen $\deg(0) := \infty$.

Lemma

Es gilt:

1. $\deg(ab) \leq \deg(a) + \deg(b)$
2. $\deg(a+b) \leq \max\{\deg(a), \deg(b)\}$.

Polynome

Definition

Der Grad eines Polynoms $0 \neq a \in R[x]$ wird durch

$$\deg(a) := \max\{n \in \mathbb{N} | a_n \neq 0\}$$

definiert. Wir setzen $\deg(0) := \infty$.

Lemma

Es gilt:

1. $\deg(ab) \leq \deg(a) + \deg(b)$
2. $\deg(a+b) \leq \max\{\deg(a), \deg(b)\}$.

Quadratische Ringe

Sei $D \in \mathbb{Z}$ kein Quadrat (also etwa $D = -1$ oder $D = 2$).

Quadratische Ringe

Sei $D \in \mathbb{Z}$ kein Quadrat (also etwa $D = -1$ oder $D = 2$). Wir wählen eine Wurzel $\sqrt{D} \in \mathbb{C}$.

Quadratische Ringe

Sei $D \in \mathbb{Z}$ kein Quadrat (also etwa $D = -1$ oder $D = 2$). Wir wählen eine Wurzel $\sqrt{D} \in \mathbb{C}$.

Definition

Wir definieren $\mathbb{Z}[\sqrt{D}] := \{a + b\sqrt{D} | a, b \in \mathbb{Z}\} \subset \mathbb{C}$.

Quadratische Ringe

Sei $D \in \mathbb{Z}$ kein Quadrat (also etwa $D = -1$ oder $D = 2$). Wir wählen eine Wurzel $\sqrt{D} \in \mathbb{C}$.

Definition

Wir definieren $\mathbb{Z}[\sqrt{D}] := \{a + b\sqrt{D} | a, b \in \mathbb{Z}\} \subset \mathbb{C}$.

Lemma

Mit den von $\mathbb{C}$ induzierten Operationen ist $\mathbb{Z}[\sqrt{D}]$ ist ein Ring.

Quadratische Ringe

Sei $D \in \mathbb{Z}$ kein Quadrat (also etwa $D = -1$ oder $D = 2$). Wir wählen eine Wurzel $\sqrt{D} \in \mathbb{C}$.

Definition

Wir definieren $\mathbb{Q}(\sqrt{D}) := \{a + b\sqrt{D} | a, b \in \mathbb{Q}\} \subset \mathbb{C}$.

Quadratische Ringe

Sei $D \in \mathbb{Z}$ kein Quadrat (also etwa $D = -1$ oder $D = 2$). Wir wählen eine Wurzel $\sqrt{D} \in \mathbb{C}$.

Definition

Wir definieren $\mathbb{Q}(\sqrt{D}) := \{a + b\sqrt{D} | a, b \in \mathbb{Q}\} \subset \mathbb{C}$.

Lemma

Mit den von $\mathbb{C}$ induzierten Operationen ist $\mathbb{Q}(\sqrt{D})$ ist ein Körper.

Nullteiler

Sei R ein Ring.

Nullteiler

Sei R ein Ring.

Definition

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

Nullteiler

Sei R ein Ring.

Definition

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

Definition

Ein Integritätsbereich ist ein Ring, der keine nichttrivialen Nullteiler enthält.

Nullteiler

Definition

Ein Integritätsbereich ist ein Ring, der keine nichttrivialen Nullteiler enthält.

Die ganzen Zahlen bilden einen Integritätsbereich.

Nullteiler

Die ganzen Zahlen bilden einen Integritätsbereich.

Lemma

Ist R ein Integritätsbereich, so ist auch der Polynomring $R[x]$ ein Integritätsbereich.

Teilen und prime Elemente

Definition

1. Seien $a, b \in R$. Wenn es $c \in R$ mit $ac = b$ gibt, so sagen wir, daß a ein Teiler von b ist, also $a|b$ gilt.
2. Sei $M \subset R$ eine Teilmenge. Eine Element $a \in R$ heißt größter gemeinsamer Teiler von M ($a \in g.g.T(M)$), falls jedes $b \in R$, welches alle $m \in M$ teilt, auch a teilt.
3. $a \in R$ ist eine Einheit, wenn $a|1$.
4. $0 \neq b \in R$ ist irreduzibel, wenn b keine Einheit ist und aus $b = ac$ folgt, daß a oder c eine Einheit in R ist. ist.
5. $0 \neq p \in R$ ist prim, wenn p keine Einheit ist und aus $p|ab$ folgt, daß $p|a$ oder $p|b$.

Teilen und prime Elemente

Definition

1. Seien $a, b \in R$. Wenn es $c \in R$ mit $ac = b$ gibt, so sagen wir, daß a ein Teiler von b ist, also $a|b$ gilt.
2. Sei $M \subset R$ eine Teilmenge. Eine Element $a \in R$ heißt größter gemeinsamer Teiler von M ($a \in g.g.T(M)$), falls jedes $b \in R$, welches alle $m \in M$ teilt, auch a teilt.
3. $a \in R$ ist eine Einheit, wenn $a|1$.
4. $0 \neq b \in R$ ist irreduzibel, wenn b keine Einheit ist und aus $b = ac$ folgt, daß a oder c eine Einheit in R ist. ist.
5. $0 \neq p \in R$ ist prim, wenn p keine Einheit ist und aus $p|ab$ folgt, daß $p|a$ oder $p|b$.

Teilen und prime Elemente

Definition

1. Seien $a, b \in R$. Wenn es $c \in R$ mit $ac = b$ gibt, so sagen wir, daß a ein Teiler von b ist, also $a|b$ gilt.
2. Sei $M \subset R$ eine Teilmenge. Eine Element $a \in R$ heißt größter gemeinsamer Teiler von M ($a \in g.g.T(M)$), falls jedes $b \in R$, welches alle $m \in M$ teilt, auch a teilt.
3. $a \in R$ ist eine Einheit, wenn $a|1$.
4. $0 \neq b \in R$ ist irreduzibel, wenn b keine Einheit ist und aus $b = ac$ folgt, daß a oder c eine Einheit in R ist. ist.
5. $0 \neq p \in R$ ist prim, wenn p keine Einheit ist und aus $p|ab$ folgt, daß $p|a$ oder $p|b$.

Teilen und prime Elemente

Definition

1. Seien $a, b \in R$. Wenn es $c \in R$ mit $ac = b$ gibt, so sagen wir, daß a ein Teiler von b ist, also $a|b$ gilt.
2. Sei $M \subset R$ eine Teilmenge. Eine Element $a \in R$ heißt größter gemeinsamer Teiler von M ($a \in g.g.T(M)$), falls jedes $b \in R$, welches alle $m \in M$ teilt, auch a teilt.
3. $a \in R$ ist eine Einheit, wenn $a|1$.
4. $0 \neq b \in R$ ist irreduzibel, wenn b keine Einheit ist und aus $b = ac$ folgt, daß a oder c eine Einheit in R ist. ist.
5. $0 \neq p \in R$ ist prim, wenn p keine Einheit ist und aus $p|ab$ folgt, daß $p|a$ oder $p|b$.

Teilen und prime Elemente

Definition

1. Seien $a, b \in R$. Wenn es $c \in R$ mit $ac = b$ gibt, so sagen wir, daß a ein Teiler von b ist, also $a|b$ gilt.
2. Sei $M \subset R$ eine Teilmenge. Eine Element $a \in R$ heißt größter gemeinsamer Teiler von M ($a \in g.g.T(M)$), falls jedes $b \in R$, welches alle $m \in M$ teilt, auch a teilt.
3. $a \in R$ ist eine Einheit, wenn $a|1$.
4. $0 \neq b \in R$ ist irreduzibel, wenn b keine Einheit ist und aus $b = ac$ folgt, daß a oder c eine Einheit in R ist. ist.
5. $0 \neq p \in R$ ist prim, wenn p keine Einheit ist und aus $p|ab$ folgt, daß $p|a$ oder $p|b$.

Teilen und prime Elemente

Definition

1. Seien $a, b \in R$. Wenn es $c \in R$ mit $ac = b$ gibt, so sagen wir, daß a ein Teiler von b ist, also $a|b$ gilt.
2. Sei $M \subset R$ eine Teilmenge. Eine Element $a \in R$ heißt größter gemeinsamer Teiler von M ($a \in g.g.T(M)$), falls jedes $b \in R$, welches alle $m \in M$ teilt, auch a teilt.
3. $a \in R$ ist eine Einheit, wenn $a|1$.
4. $0 \neq b \in R$ ist irreduzibel, wenn b keine Einheit ist und aus $b = ac$ folgt, daß a oder c eine Einheit in R ist. ist.
5. $0 \neq p \in R$ ist prim, wenn p keine Einheit ist und aus $p|ab$ folgt, daß $p|a$ oder $p|b$.

Teilen und prime Elemente

Lemma

Die Einheiten von $\mathbb{Z}$ sind $\{1, -1\}$.

Teilen und prime Elemente

Lemma

Die Einheiten von $\mathbb{Z}$ sind $\{1, -1\}$.

Lemma

Die Einheiten von $K[x]$ sind $K^* = K \setminus \{0\}$.

Teilen und prime Elemente

Lemma

Die Einheiten von $\mathbb{Z}$ sind $\{1, -1\}$.

Lemma

Die Einheiten von $K[x]$ sind $K^* = K \setminus \{0\}$.

Lemma

Die Einheiten eines Ringes bilden eine abelsche Gruppe unter der Multipikation.

Einheiten

$D \in \mathbb{Z}$- quadratfrei,

Einheiten

$D \in \mathbb{Z}$- quadratfrei, Konjugation :

$$\overline{(\dots)} : \mathbb{Z}[\sqrt{D}] \to \mathbb{Z}[\sqrt{D}] \ ,$$

$$\overline{a + b\sqrt{D}} := a - b\sqrt{D} \ .$$

Einheiten

$D \in \mathbb{Z}$- quadratfrei, Konjugation :

$$\overline{(\dots)} : \mathbb{Z}[\sqrt{D}] \to \mathbb{Z}[\sqrt{D}] \ ,$$

$$\overline{a + b\sqrt{D}} := a - b\sqrt{D} \ .$$

Norm :

$$N : \mathbb{Z}[\sqrt{D}] \to \mathbb{Z} \ ,$$

$$N(x) := x\bar{x} \ .$$

Einheiten

Zunächst $D < 0$,

Einheiten

Zunächst $D < 0$, $\mathbb{Z}[\sqrt{D}] \subset \mathbb{C}$ ist ein Gitter mit Basis $1, \sqrt{D}$.

Einheiten

Zunächst $D < 0$, $\mathbb{Z}[\sqrt{D}] \subset \mathbb{C}$ ist ein Gitter mit Basis $1, \sqrt{D}$. N ist die Einschränkung der Norm von $\mathbb{C}$, $z \mapsto |z|^2$.

Einheiten

Zunächst $D < 0$, $\mathbb{Z}[\sqrt{D}] \subset \mathbb{C}$ ist ein Gitter mit Basis $1, \sqrt{D}$. N ist die Einschränkung der Norm von $\mathbb{C}$, $z \mapsto |z|^2$.

$$\{x \in \mathbb{Z}[\sqrt{D}] | N(x) < C\}$$

ist endlich für jedes $C \in \mathbb{R}$.

Einheiten

$$\{x \in \mathbb{Z}[\sqrt{D}] | N(x) < C\}$$

ist endlich für jedes $C \in \mathbb{R}$. Wenn $x \in \mathbb{Z}[\sqrt{D}]$ eine Einheit ist, dann muß $N(x) = 1$ gelten.

Einheiten

$$\{x \in \mathbb{Z}[\sqrt{D}] | N(x) < C\}$$

ist endlich für jedes $C \in \mathbb{R}$. Wenn $x \in \mathbb{Z}[\sqrt{D}]$ eine Einheit ist, dann muß $N(x) = 1$ gelten.

Lemma

Wenn $D < 0$, so ist die Gruppe der Einheiten von $\mathbb{Z}[\sqrt{D}]$ endlich.

Einheiten

$D > 0$

Einheiten

$D > 0$ Einbettung als Gitter

$$\mathbb{Z}[\sqrt{D}] \to \mathbb{R}^2$$

$$x \mapsto (x, \bar{x})$$

Einheiten

$D > 0$ Einbettung als Gitter

$$\mathbb{Z}[\sqrt{D}] \to \mathbb{R}^2$$

$$x \mapsto (x, \bar{x})$$

Die Norm ist dann die Einschränkung des hyperbolischen Produktes

$$(x, y) \mapsto xy \ .$$

Einheiten

Lemma

Wenn $D > 0$, dann ist die Gruppe der Einheiten in $\mathbb{Z}[\sqrt{D}]$ unendlich.

Homomorphismen

Seien R, S Ringe.

Homomorphismen

Seien R, S Ringe.

Definition

Eine Homomorphismus $\phi : R \to S$ ist eine Abbildung, welche Homomorphismen der additiven abelschen Gruppen und der multiplikativen Monoide induziert.

Homomorphismen

Lemma

Der Kern eines Homomorphismus $\phi : R \to S$ ist eine Untergruppe, welche abgeschlossen unter der Multiplikation mit Elementen aus R ist.

Homomorphismen

Lemma

Der Kern eines Homomorphismus $\phi : R \to S$ ist eine Untergruppe, welche abgeschlossen unter der Multiplikation mit Elementen aus R ist.

Definition

Ein Ideal $I \subset R$ ist eine Untergruppe, welche abgeschlossen unter der Multiplikation mit Elementen aus R ist.

Homomorphismen

Lemma

Ist $I \subset R$ ein Ideal, so läßt sich auf der Gruppe R/I eine Multiplikation vertreterweise definieren, so daß R/I die Struktur eines Ringes bekommt. Die Projektion $R \to R/I$ ist ein Homomorphismus von Ringen mit dem Kern I.

Homomorphismen

Lemma

Ist $I \subset R$ ein Ideal, so läßt sich auf der Gruppe R/I eine Multiplikation vertreterweise definieren, so daß R/I die Struktur eines Ringes bekommt. Die Projektion $R \to R/I$ ist ein Homomorphismus von Ringen mit dem Kern I.

Sei $n \in \mathbb{Z}$. Die Menge $(n) := n\mathbb{Z} \subset \mathbb{Z}$ ist ein Ideal.

Homomorphismen

Lemma

Ist $I \subset R$ ein Ideal, so läßt sich auf der Gruppe R/I eine Multiplikation vertreterweise definieren, so daß R/I die Struktur eines Ringes bekommt. Die Projektion $R \to R/I$ ist ein Homomorphismus von Ringen mit dem Kern I.

Sei $n \in \mathbb{Z}$. Die Menge $(n) := n\mathbb{Z} \subset \mathbb{Z}$ ist ein Ideal.

Lemma

Der Quotient $\mathbb{Z}/n\mathbb{Z}$ ist genau dann ein Integritätbereich, wenn n eine Primzahl ist.

Hauptideale

Sei R ein Ring.

Hauptideale

Sei R ein Ring.

Definition

Ein Ideal $I \subset R$ heißt Hauptideal, wenn es ein $a \in R$ mit $I = aR$ gibt. Wir schreiben dann auch $(a) := I$.

Hauptideale

Sei R ein Ring.

Definition

Ein Ideal $I \subset R$ heißt Hauptideal, wenn es ein $a \in R$ mit $I = aR$ gibt. Wir schreiben dann auch $(a) := I$.

Definition

Ein Ring heißt Hauptidealring, wenn alle seine Ideale Hauptideale sind.

Hauptideale

Wir werden sehen, daß $\mathbb{Z}$ und $K[x]$ für einen Körper Hauptidealringe sind.

Hauptideale

Wir werden sehen, daß $\mathbb{Z}$ und $K[x]$ für einen Körper Hauptidealringe sind.

Lemma

Ein Ring ist genau dann ein Hauptidealring, wenn für jede Teilmenge ein größter gemeinsamer Teiler der Form $a = a_1 m_1 + \cdots + a_r m_r$ mit $a_i \in R$ und $m_i \in M$ existiert.

Höhen

Sei R ein Ring.

Höhen

Sei R ein Ring.

Definition

Eine Höhe auf R ist eine Abbildung $H : R \setminus \{0\} \to \mathbb{N} \cup 0$ mit: Für alle $a, b \in R$ existieren $q, r \in R$ mit $a = bq + r$ und $H(r) < H(b)$ oder $r = 0$.

Höhen

Lemma

Durch $\mathbb{Z} \ni n \mapsto |n|$ wird eine Höhe auf $\mathbb{Z}$ definiert.

Höhen

Lemma

Durch $\mathbb{Z} \ni n \mapsto |n|$ wird eine Höhe auf $\mathbb{Z}$ definiert.

Lemma

Durch $K[x] \ni p \mapsto \deg(p)$ wird eine Höhe auf $K[x]$ definiert.

Höhen

Lemma

Durch $K[x] \ni p \mapsto \deg(p)$ wird eine Höhe auf $K[x]$ definiert.

Lemma

Der Ring $\mathbb{Z}[i]$ ist ein euklidischer Ring.

Konsequenzen

Lemma

Ein Euklidischer Ring (R, H) ist ein Hauptidealring.

Konsequenzen

Lemma

Ein Euklidischer Ring (R, H) ist ein Hauptidealring.

Corollary

In einem Euklidischen Ring hat jede Teilmenge einen g.g.T.

Konsequenzen

Lemma

Ein Euklidischer Ring (R, H) ist ein Hauptidealring.

Corollary

In einem Euklidischen Ring hat jede Teilmenge einen g.g.T.

Corollary

Für einen Körper K ist $K[x]$ ein Hauptidealring.

Euklidischer Algorithmus I

R - ein Euklidischer Ring mit Höhe H

Euklidischer Algorithmus I

R - ein Euklidischer Ring mit Höhe H

Lemma

Für $\{a, b\} \in R$ wird der g.g.T durch folgenden Algorithmus bestimmt.

1. $f := a$ und $g := b$
2. $f = qg + r$ mit $N(g) > N(r)$
3. Wenn $r = 0$ so ist $g = g.g.T\{a, b\}$. Sonst $f := g$ und $g := r$ und gehe zu 2.

Euklidischer Algorithmus I

R - ein Euklidischer Ring mit Höhe H

Lemma

Für $\{a, b\} \in R$ wird der g.g.T durch folgenden Algorithmus bestimmt.

1. $f := a$ *und* $g := b$
2. $f = qg + r$ *mit* $N(g) > N(r)$
3. *Wenn* $r = 0$ *so ist* $g = g.g.T\{a, b\}$. *Sonst* $f := g$ *und* $g := r$ *und gehe zu 2.*

Euklidischer Algorithmus I

R - ein Euklidischer Ring mit Höhe H

Lemma

Für $\{a, b\} \in R$ wird der g.g.T durch folgenden Algorithmus bestimmt.

1. $f := a$ *und* $g := b$
2. $f = qg + r$ *mit* $N(g) > N(r)$
3. *Wenn* $r = 0$ *so ist* $g = g.g.T\{a, b\}$. *Sonst* $f := g$ *und* $g := r$ *und gehe zu 2.*

Euklidischer Algorithmus I

R - ein Euklidischer Ring mit Höhe H

Lemma

Für $\{a, b\} \in R$ wird der g.g.T durch folgenden Algorithmus bestimmt.

1. $f := a$ *und* $g := b$
2. $f = qg + r$ *mit* $N(g) > N(r)$
3. *Wenn* $r = 0$ *so ist* $g = g.g.T\{a, b\}$. *Sonst* $f := g$ *und* $g := r$ *und gehe zu 2.*

Euklidischer Algorithmus II

$a := 196, b := 72$

1. $196 = 2x72 + 52$
2. $72 = 1x52 + 20$
3. $52 = 2x20 + 12$
4. $20 = 1x12 + 8$
5. $12 = 1x8 + 4$
6. $8 = 2x4$

Euklidischer Algorithmus II

$a := 196, b := 72$

1. $196 = 2x72 + 52$
2. $72 = 1x52 + 20$
3. $52 = 2x20 + 12$
4. $20 = 1x12 + 8$
5. $12 = 1x8 + 4$
6. $8 = 2x4$

Euklidischer Algorithmus II

$a := 196, b := 72$

1. $196 = 2x72 + 52$
2. $72 = 1x52 + 20$
3. $52 = 2x20 + 12$
4. $20 = 1x12 + 8$
5. $12 = 1x8 + 4$
6. $8 = 2x4$

Euklidischer Algorithmus II

$a := 196, b := 72$

1. $196 = 2x72 + 52$
2. $72 = 1x52 + 20$
3. $52 = 2x20 + 12$
4. $20 = 1x12 + 8$
5. $12 = 1x8 + 4$
6. $8 = 2x4$

Euklidischer Algorithmus II

$a := 196, b := 72$

1. $196 = 2x72 + 52$
2. $72 = 1x52 + 20$
3. $52 = 2x20 + 12$
4. $20 = 1x12 + 8$
5. $12 = 1x8 + 4$
6. $8 = 2x4$

Euklidischer Algorithmus II

$a := 196, b := 72$

1. $196 = 2x72 + 52$
2. $72 = 1x52 + 20$
3. $52 = 2x20 + 12$
4. $20 = 1x12 + 8$
5. $12 = 1x8 + 4$
6. $8 = 2x4$

Euklidischer Algorithmus II

$a := 196, b := 72$

1. $196 = 2x72 + 52$
2. $72 = 1x52 + 20$
3. $52 = 2x20 + 12$
4. $20 = 1x12 + 8$
5. $12 = 1x8 + 4$
6. $8 = 2x4$

Polynome und Nullstellen

R - ein Ring.

Polynome und Nullstellen

R - ein Ring. $R[x]$ ist nicht notwendig Euklidisch

Polynome und Nullstellen

R - ein Ring. $R[x]$ ist nicht notwendig Euklidisch

Lemma

Seien $f, g \in R[x]$, $g = g_m x^m + \cdots + g_0$ und g_m eine Einheit. Dann existieren $q, r \in R[x]$ mit $\deg(g) > \deg(r)$ und

$$f = qg + r \ .$$

Polynome und Nullstellen

Lemma

Seien $f, g \in R[x]$, $g = g_m x^m + \cdots + g_0$ und g_m eine Einheit. Dann existieren $q, r \in R[x]$ mit $\deg(g) > \deg(r)$ und

$$f = qg + r \ .$$

Lemma

Sei $f \in R[x]$ und $w \in R$ mit $f(w) = 0$. Dann gilt $f(x) = (x - w)g$ für ein $g \in R[x]$.

Polynome und Nullstellen

Lemma

Sei $f \in R[x]$ und $w \in R$ mit $f(w) = 0$. Dann gilt $f(x) = (x - w)g$ für ein $g \in R[x]$.

Lemma

Sei R ein Integritätsbereich und $f \in R[x]$. Dann hat f höchstens $\deg(n)$ *paarweise verschiedene Nullstellen.*

Polynome und Nullstellen

Lemma

Sei $f \in R[x]$ und $w \in R$ mit $f(w) = 0$. Dann gilt $f(x) = (x - w)g$ für ein $g \in R[x]$.

Lemma

Sei R ein Integritätsbereich und $f \in R[x]$. Dann hat f höchstens $\deg(n)$ *paarweise verschiedene Nullstellen.*

Corollary

Ist R ein unendlicher Integritätsbereich, so ist die Abbildung $R[x] \to R^R$ injektiv.

prim versus irreduzibel

R - ein Integritätsbereich,

prim versus irreduzibel

R - ein Integritätsbereich,

Definition

$a, b \in R$ heißen genau dann assoziiert, wenn $a = eb$ für eine Einheit $e \in R$ gilt. Wir schreiben diese Äquivalenzrelation als $a \sim b$.

prim versus irreduzibel

R - ein Integritätsbereich,
Sei $p \in R$ prim

prim versus irreduzibel

R - ein Integritätsbereich,
Sei $p \in R$ prim

Lemma

1. *p is irreduzibel.*
2. *Ist $q \in R$ prim und $p|q$ so ist $q \sim p$.*
3. *Ist $q \in R$ prim und $p|q$ so ist $q \sim p$.*
4. *Wenn $p|a_1 \dots a_k$, so existiert ein $i \in \{1, \dots, k\}$ mit $p|a_i$.*

prim versus irreduzibel

R - ein Integritätsbereich,
Sei $p \in R$ prim

Lemma

1. *p is irreduzibel.*
2. *Ist $q \in R$ prim und $p|q$ so ist $q \sim p$.*
3. *Ist $q \in R$ prim und $p|q$ so ist $q \sim p$.*
4. *Wenn $p|a_1 \dots a_k$, so existiert ein $i \in \{1, \dots, k\}$ mit $p|a_i$.*

prim versus irreduzibel

R - ein Integritätsbereich,
Sei $p \in R$ prim

Lemma

1. *p is irreduzibel.*
2. *Ist $q \in R$ prim und $p|q$ so ist $q \sim p$.*
3. *Ist $q \in R$ prim und $p|q$ so ist $q \sim p$.*
4. *Wenn $p|a_1 \dots a_k$, so existiert ein $i \in \{1, \dots, k\}$ mit $p|a_i$.*

prim versus irreduzibel

R - ein Integritätsbereich,
Sei $p \in R$ prim

Lemma

1. *p is irreduzibel.*
2. *Ist $q \in R$ prim und $p|q$ so ist $q \sim p$.*
3. *Ist $q \in R$ prim und $p|q$ so ist $q \sim p$.*
4. *Wenn $p|a_1 \dots a_k$, so existiert ein $i \in \{1, \dots, k\}$ mit $p|a_i$.*

prim versus irreduzibel

R - ein Integritätsbereich,
Sei $p \in R$ prim

Lemma

1. *p is irreduzibel.*
2. *Ist $q \in R$ prim und $p|q$ so ist $q \sim p$.*
3. *Ist $q \in R$ prim und $p|q$ so ist $q \sim p$.*
4. *Wenn $p|a_1 \dots a_k$, so existiert ein $i \in \{1, \dots, k\}$ mit $p|a_i$.*

prim versus irreduzibel

R - ein Integritätsbereich,

Lemma

1. *p is irreduzibel.*
2. *Ist $q \in R$ prim und $p|q$ so ist $q \sim p$.*
3. *Ist $q \in R$ prim und $p|q$ so ist $q \sim p$.*
4. *Wenn $p|a_1 \dots a_k$, so existiert ein $i \in \{1, \dots, k\}$ mit $p|a_i$.*

Im allgemeinen sind irreduzible Elemente nicht prim.

Primzahlen in $\mathbb{Z}[i]$

Lemma (Satz von Wilson)

Für jede Primzahl gilt

$$(p-1)! \equiv -1 (\mod p) .$$

Primzahlen in $\mathbb{Z}[i]$

Theorem

Die Primelemente von $\mathbb{Z}[i]$ sind assoziiert zu

1. $\pi = 1 + i$
2. $\pi = a + bi$, $a^2 + b^2 = p$, $p \equiv 1 (\mod 4)$, $a > |b| > 0$
3. $\pi = p$, $p \equiv 3 (\mod 4)$

(p ist prim in $\mathbb{Z}$).

Primzahlen in $\mathbb{Z}[i]$

Theorem

Die Primelemente von $\mathbb{Z}[i]$ sind assoziiert zu

1. $\pi = 1 + i$
2. $\pi = a + bi,\ a^2 + b^2 = p,\ p \equiv 1(\mod 4)\ ,\ a > |b| > 0$
3. $\pi = p,\ p \equiv 3(\mod 4)$

(p ist prim in $\mathbb{Z}$).

Primzahlen in $\mathbb{Z}[i]$

Theorem

Die Primelemente von $\mathbb{Z}[i]$ sind assoziiert zu

1. $\pi = 1 + i$
2. $\pi = a + bi,\ a^2 + b^2 = p,\ p \equiv 1(\mod 4)\ ,\ a > |b| > 0$
3. $\pi = p,\ p \equiv 3(\mod 4)$

(p ist prim in $\mathbb{Z}$).

Primzahlen in $\mathbb{Z}[i]$

Theorem

Die Primelemente von $\mathbb{Z}[i]$ sind assoziiert zu

1. $\pi = 1 + i$
2. $\pi = a + bi$, $a^2 + b^2 = p$, $p \equiv 1 (\mod 4)$, $a > |b| > 0$
3. $\pi = p$, $p \equiv 3 (\mod 4)$

(p ist prim in $\mathbb{Z}$).

Zerfall von Primzahlen

$$R = \mathbb{Z}[\sqrt{D}] \text{ oder } R = \mathbb{Z}[\omega_D],\ \omega_D = \frac{1+\sqrt{D}}{2} \text{ mir } 4|(D-1)$$

Zerfall von Primzahlen

$R = \mathbb{Z}[\sqrt{D}]$ oder $R = \mathbb{Z}[\omega_D]$, $\omega_D = \frac{1+\sqrt{D}}{2}$ mir $4|(D-1)$ $p \in \mathbb{Z}$ - eine Primzahl

Zerfall von Primzahlen

$R = \mathbb{Z}[\sqrt{D}]$ oder $R = \mathbb{Z}[\omega_D]$, $\omega_D = \frac{1+\sqrt{D}}{2}$ mir $4|(D-1)$ $p \in \mathbb{Z}$ - eine Primzahl

Definition

1. p ist verzweigt, wenn $p = \pi\bar{\pi}$ für ein Primelement $\pi \in R$ mit $\pi \sim \bar{\pi}$ gilt.
2. p ist zerlegt, wenn $p = \pi\bar{\pi}$ für zwei nicht assoziierte Primelemente $\pi, \bar{\pi}$ in R.
3. p ist träge, wenn p in R prim bleibt.

Zerfall von Primzahlen

$R = \mathbb{Z}[\sqrt{D}]$ oder $R = \mathbb{Z}[\omega_D]$, $\omega_D = \frac{1+\sqrt{D}}{2}$ mir $4|(D-1)$ $p \in \mathbb{Z}$ - eine Primzahl

Definition

1. p ist verzweigt, wenn $p = \pi\bar{\pi}$ für ein Primelement $\pi \in R$ mit $\pi \sim \bar{\pi}$ gilt.
2. p ist zerlegt, wenn $p = \pi\bar{\pi}$ für zwei nicht assoziierte Primelemente $\pi, \bar{\pi}$ in R.
3. p ist träge, wenn p in R prim bleibt.

Zerfall von Primzahlen

$R = \mathbb{Z}[\sqrt{D}]$ oder $R = \mathbb{Z}[\omega_D]$, $\omega_D = \frac{1+\sqrt{D}}{2}$ mir $4|(D-1)$ $p \in \mathbb{Z}$ - eine Primzahl

Definition

1. p ist verzweigt, wenn $p = \pi\bar{\pi}$ für ein Primelement $\pi \in R$ mit $\pi \sim \bar{\pi}$ gilt.
2. p ist zerlegt, wenn $p = \pi\bar{\pi}$ für zwei nicht assoziierte Primelemente $\pi, \bar{\pi}$ in R.
3. p ist träge, wenn p in R prim bleibt.

Zerfall von Primzahlen

$R = \mathbb{Z}[\sqrt{D}]$ oder $R = \mathbb{Z}[\omega_D]$, $\omega_D = \frac{1+\sqrt{D}}{2}$ mir $4|(D-1)$ $p \in \mathbb{Z}$ - eine Primzahl

Definition

1. p ist verzweigt, wenn $p = \pi\bar{\pi}$ für ein Primelement $\pi \in R$ mit $\pi \sim \bar{\pi}$ gilt.
2. p ist zerlegt, wenn $p = \pi\bar{\pi}$ für zwei nicht assoziierte Primelemente $\pi, \bar{\pi}$ in R.
3. p ist träge, wenn p in R prim bleibt.

Zerfall von Primzahlen

$$R = \mathbb{Z}[\omega_{-3}]$$

Zerfall von Primzahlen

$R = \mathbb{Z}[\omega_{-3}]$

Theorem

Sei $p \in \mathbb{Z}$ prim.

1. *p ist genau dann verzweigt, wenn $p = 3$.*
2. *p ist genau dann zerlegt, wenn $p = a^2 + ab + b^2$ (oder äquivalent $4p = c^2 + 3b^2$).*
3. *In allen weiteren Fällen ist p träge.*

Zerfall von Primzahlen

$R = \mathbb{Z}[\omega_{-3}]$

Theorem

Sei $p \in \mathbb{Z}$ prim.

1. *p ist genau dann verzweigt, wenn $p = 3$.*
2. *p ist genau dann zerlegt, wenn $p = a^2 + ab + b^2$ (oder äquivalent $4p = c^2 + 3b^2$).*
3. *In allen weiteren Fällen ist p träge.*

Zerfall von Primzahlen

$R = \mathbb{Z}[\omega_{-3}]$

Theorem

Sei $p \in \mathbb{Z}$ prim.

1. *p ist genau dann verzweigt, wenn $p = 3$.*
2. *p ist genau dann zerlegt, wenn $p = a^2 + ab + b^2$ (oder äquivalent $4p = c^2 + 3b^2$).*
3. *In allen weiteren Fällen ist p träge.*

Zerfall von Primzahlen

$R = \mathbb{Z}[\omega_{-3}]$

Theorem

Sei $p \in \mathbb{Z}$ prim.

1. *p ist genau dann verzweigt, wenn $p = 3$.*
2. *p ist genau dann zerlegt, wenn $p = a^2 + ab + b^2$ (oder äquivalent $4p = c^2 + 3b^2$).*
3. *In allen weiteren Fällen ist p träge.*

Zerlegungen

R ein Integritätsbereich,

Zerlegungen

R ein Integritätsbereich, $a \in R$

Zerlegungen

R ein Integritätsbereich, $a \in R$

Definition

Das Element a hat eine im wesentlichen eindeutige Zerlegung in irreduzible Elemente, wenn $a = p_1 \dots p_r$ für irreduzible Elemente p_i gilt, und wenn für jede andere solche Darstellung $a = q_1 \dots q_s$ gilt:

1. $r = s$
2. Es existiert eine Permutation $\sigma \in S_r$ mit $p_{\sigma(i)} \sim q_i$ für alle $i = 1, \dots r$.

Zerlegungen

Definition

Ein Integritätsbereich heißt faktoriell, wenn jedes von Null verschiedene Element eine im wesentlichen eindeutige Zerlegung in irreduzible Elemente besitzt.

Teilerketten

R - ein Integritätbereich,

Teilerketten

R - ein Integritätbereich, $a \in R$

Teilerketten

R - ein Integritätbereich, $a \in R$

Definition

1. Eine Teilerkette von a ist eine Folge $(a_i)_{i\in\mathbb{N}}$ mit $a_{i+1}|a_i$ für alle $i \in \mathbb{N}$.
2. Wir sagen, daß in R der Teilerkettensatz gilt, wenn für jedes $a \in R$ und jede Teilerkette $(a_i)_{i\in R}$ von a ein $n \in \mathbb{N}$ existiert, so daß für $i \geq n$ auch $a_i|a_{i+1}$ gilt.

Teilerketten

R - ein Integritätbereich, $a \in R$

Definition

1. Eine Teilerkette von a ist eine Folge $(a_i)_{i\in\mathbb{N}}$ mit $a_{i+1}|a_i$ für alle $i \in \mathbb{N}$.
2. Wir sagen, daß in R der Teilerkettensatz gilt, wenn für jedes $a \in R$ und jede Teilerkette $(a_i)_{i\in R}$ von a ein $n \in \mathbb{N}$ existiert, so daß für $i \geq n$ auch $a_i|a_{i+1}$ gilt.

Teilerketten

R - ein Integritätbereich, $a \in R$

Definition

1. Eine Teilerkette von a ist eine Folge $(a_i)_{i\in\mathbb{N}}$ mit $a_{i+1}|a_i$ für alle $i \in \mathbb{N}$.
2. Wir sagen, daß in R der Teilerkettensatz gilt, wenn für jedes $a \in R$ und jede Teilerkette $(a_i)_{i\in R}$ von a ein $n \in \mathbb{N}$ existiert, so daß für $i \geq n$ auch $a_i|a_{i+1}$ gilt.

Teilerkettensatz

Lemma

Wenn in R der Teilerkettensatz gilt, dann besitzt jedes von Null verschiedene Element eine Zerlegung in irreduzible Elemente.

Teilerkettensatz

Lemma

Wenn in R der Teilerkettensatz gilt, dann besitzt jedes von Null verschiedene Element eine Zerlegung in irreduzible Elemente.

Theorem

In den folgenden Ringen gilt der Teilerkettensatz.

1. $\mathbb{Z}$,
2. $K[X]$ *für einen Körper* K,
3. $\mathbb{Z}[\sqrt{D}]$
4. R *Hauptidealring*
5. R *Euklidischer Ring*
6. $R[X]$, *wenn Teilerkettensatz für* R *gilt*

Teilerkettensatz

Lemma

Wenn in R der Teilerkettensatz gilt, dann besitzt jedes von Null verschiedene Element eine Zerlegung in irreduzible Elemente.

Theorem

In den folgenden Ringen gilt der Teilerkettensatz.

1. $\mathbb{Z}$,
2. $K[X]$ *für einen Körper* K,
3. $\mathbb{Z}[\sqrt{D}]$
4. R *Hauptidealring*
5. R *Euklidischer Ring*
6. $R[X]$ *wenn Teilerkettensatz für* R *gilt*

Teilerkettensatz

Lemma

Wenn in R der Teilerkettensatz gilt, dann besitzt jedes von Null verschiedene Element eine Zerlegung in irreduzible Elemente.

Theorem

In den folgenden Ringen gilt der Teilerkettensatz.

1. $\mathbb{Z}$,
2. $K[X]$ *für einen Körper* K,
3. $\mathbb{Z}[\sqrt{D}]$
4. R *Hauptidealring*
5. R *Euklidischer Ring*
6. $R[X]$ *wenn Teilerkettensatz für* R *gilt*

Teilerkettensatz

Lemma

Wenn in R der Teilerkettensatz gilt, dann besitzt jedes von Null verschiedene Element eine Zerlegung in irreduzible Elemente.

Theorem

In den folgenden Ringen gilt der Teilerkettensatz.

1. $\mathbb{Z}$,
2. $K[X]$ *für einen Körper* K,
3. $\mathbb{Z}[\sqrt{D}]$
4. R *Hauptidealring*
5. R *Euklidischer Ring*
6. $R[X]$, *wenn Teilerkettensatz für* R *gilt*

Teilerkettensatz

Theorem

In den folgenden Ringen gilt der Teilerkettensatz.

1. $\mathbb{Z}$,
2. $K[X]$ *für einen Körper* K,
3. $\mathbb{Z}[\sqrt{D}]$
4. R *Hauptidealring*
5. R *Euklidischer Ring*
6. $R[X]$, *wenn Teilerkettensatz für* R *gilt.*

Teilerkettensatz

Theorem

In den folgenden Ringen gilt der Teilerkettensatz.

1. $\mathbb{Z}$,
2. $K[X]$ *für einen Körper* K,
3. $\mathbb{Z}[\sqrt{D}]$
4. R *Hauptidealring*
5. R *Euklidischer Ring*
6. $R[X]$, *wenn Teilerkettensatz für* R *gilt.*

Teilerkettensatz

Theorem

In den folgenden Ringen gilt der Teilerkettensatz.

1. $\mathbb{Z}$,
2. $K[X]$ *für einen Körper* K,
3. $\mathbb{Z}[\sqrt{D}]$
4. R *Hauptidealring*
5. R *Euklidischer Ring*
6. $R[X]$, *wenn Teilerkettensatz für* R *gilt.*

irreduzibel versus prim

R - ein Integritätsbereich,

irreduzibel versus prim

R - ein Integritätsbereich, $a \in R$

irreduzibel versus prim

R - ein Integritätsbereich, $a \in R$

Lemma

Seien $a = p_1 \dots p_r$ und $a = q_1 \dots q_s$ Zerlegungen in prime Elemente, dann gilt $r = s$ und $p_i \sim q_i$ (nach geeigneter Umnummerierung).

irreduzibel versus prim

R - ein Integritätsbereich, $a \in R$

Lemma

Seien $a = p_1 \dots p_r$ und $a = q_1 \dots q_s$ Zerlegungen in prime Elemente, dann gilt $r = s$ und $p_i \sim q_i$ (nach geeigneter Umnummerierung).

Lemma

In einem Hauptidealring R sind alle irreduziblen Elemente prim.

irreduzibel versus prim

Theorem

Sei R ein Integritätsbereich. Dann ist R genau dann faktoriell, wenn in R der Teilerkettensatz gilt und alle irreduziblen Elemente prim sind.

irreduzibel versus prim

Theorem

Sei R ein Integritätsbereich. Dann ist R genau dann faktoriell, wenn in R der Teilerkettensatz gilt und alle irreduziblen Elemente prim sind.

Theorem

Hauptidealringe sind faktoriell.

irreduzibel versus prim

Theorem

Sei R ein Integritätsbereich. Dann ist R genau dann faktoriell, wenn in R der Teilerkettensatz gilt und alle irreduziblen Elemente prim sind.

Theorem

Hauptidealringe sind faktoriell.

Corollary

1. *$\mathbb{Z}$ ist faktoriell.*
2. *Euklidische Ringe sind faktoriell.*
3. *$K[x]$ für einen Körper K ist faktoriell.*

irreduzibel versus prim

Theorem

Hauptidealringe sind faktoriell.

Corollary

1. $\mathbb{Z}$ *ist faktoriell.*
2. *Euklidische Ringe sind faktoriell.*
3. $K[x]$ *für einen Körper* K *ist faktoriell.*

irreduzibel versus prim

Corollary

1. $\mathbb{Z}$ *ist faktoriell.*
2. *Euklidische Ringe sind faktoriell.*
3. $K[x]$ *für einen Körper* K *ist faktoriell.*

irreduzibel versus prim

Corollary

1. $\mathbb{Z}$ *ist faktoriell.*
2. *Euklidische Ringe sind faktoriell.*
3. $K[x]$ *für einen Körper* K *ist faktoriell.*

Kongruenzen

$m \in \mathbb{Z}$,

.

Kongruenzen

$m \in \mathbb{Z}$,
$(m) \subset \mathbb{Z}$ das von m erzeugte Hauptideal,
.

Kongruenzen

$m \in \mathbb{Z}$,
$(m) \subset \mathbb{Z}$ das von m erzeugte Hauptideal,
$\mathbb{Z}/(m)$ Restklassenring.

Kongruenzen

$m \in \mathbb{Z}$,
$(m) \subset \mathbb{Z}$ das von m erzeugte Hauptideal,
$\mathbb{Z}/(m)$ Restklassenring.
Wir schreiben Elemente dieses Ringes in der Form $[a]$, $a \in \mathbb{Z}$. Die Gleichung $[a] = [b]$ is gleichbedeutend mit $a \equiv b(\mod m)$.

Kongruenzen

.

Lemma

1. *Die Gleichung $[a]x = 1$ ist in $\mathbb{Z}/(m)$ genau dann lösbar, wenn $g.g.T.(a, m) = 1$.*
2. *Die Gleichung $[a]x = [b]$ ist in $\mathbb{Z}/(m)$ genau dann lösbar, wenn für $d := g.g.T(a, m)$ gilt $d|b$.*
3. *Wenn $d|b$, so gibt es d verschiedene Lösungen.*

Kongruenzen

.

Lemma

1. *Die Gleichung* $[a]x = 1$ *ist in* $\mathbb{Z}/(m)$ *genau dann lösbar, wenn* $g.g.T.(a, m) = 1$.
2. *Die Gleichung* $[a]x = [b]$ *ist in* $\mathbb{Z}/(m)$ *genau dann lösbar, wenn für* $d := g.g.T(a, m)$ *gilt* $d|b$.
3. *Wenn* $d|b$, *so gibt es* d *verschiedene Lösungen.*

Kongruenzen

.

Lemma

1. *Die Gleichung* $[a]x = 1$ *ist in* $\mathbb{Z}/(m)$ *genau dann lösbar, wenn* $g.g.T.(a, m) = 1$.
2. *Die Gleichung* $[a]x = [b]$ *ist in* $\mathbb{Z}/(m)$ *genau dann lösbar, wenn für* $d := g.g.T(a, m)$ *gilt* $d|b$.
3. *Wenn* $d|b$, *so gibt es* d *verschiedene Lösungen.*

Kongruenzen

.

Lemma

1. *Die Gleichung* $[a]x = 1$ *ist in* $\mathbb{Z}/(m)$ *genau dann lösbar, wenn* $g.g.T.(a, m) = 1$.
2. *Die Gleichung* $[a]x = [b]$ *ist in* $\mathbb{Z}/(m)$ *genau dann lösbar, wenn für* $d := g.g.T(a, m)$ *gilt* $d|b$.
3. *Wenn* $d|b$, *so gibt es* d *verschiedene Lösungen.*

Chinesischer Restsatz

$m_1, \ldots, m_r \in \mathbb{Z}$ paarweise teilerfremd,

Chinesischer Restsatz

$m_1, \ldots, m_r \in \mathbb{Z}$ paarweise teilerfremd,
$a_1, \ldots a_r \in \mathbb{Z}$

Chinesischer Restsatz

$m_1, \ldots, m_r \in \mathbb{Z}$ paarweise teilerfremd,
$a_1, \ldots a_r \in \mathbb{Z}$

Theorem

Es existiert ein $x \in \mathbb{Z}$ mit

$$x \equiv a_i (\mod m_i) \quad i = 1, \ldots r \ .$$

Die Klasse $[x] \in \mathbb{Z}/(m)$ ist eindeutig bestimmt mit $m = m_1 \ldots m_r$.

Chinesischer Restsatz

$m_1, \ldots, m_r \in \mathbb{Z}$ paarweise teilerfremd,
$a_1, \ldots a_r \in \mathbb{Z}$

Theorem

Es existiert ein $x \in \mathbb{Z}$ mit

$$x \equiv a_i (\mod m_i) \quad i = 1, \ldots r \ .$$

Die Klasse $[x] \in \mathbb{Z}/(m)$ ist eindeutig bestimmt mit $m = m_1 \ldots m_r$.

Dieser Satz gilt für jeden Hauptidealring an der Stelle von $\mathbb{Z}$ mit dem gleichen Beweis.

Chinesischer Restsatz

Dieser Satz gilt für jeden Hauptidealring an der Stelle von $\mathbb{Z}$ mit dem gleichen Beweis.

Theorem

Die Abbildung

$$x \mapsto ([x]_{m_1}, \ldots, [x]_{m_r})$$

induziert einen Isomorphismus

$$\mathbb{Z}/(m) \xrightarrow{\sim} \mathbb{Z}/(m_1) \times \cdots \times \mathbb{Z}/(m_r) \ .$$

Eulersche φ-Funktion

Sei $m \in \mathbb{Z}$.

Eulersche φ-Funktion

Sei $m \in \mathbb{Z}$.
Die Einheiten von $\mathbb{Z}/(m)$ sind genau die Klassen $[a]$ mit $g.g.T(a, m) = 1$.

Eulersche φ-Funktion

Sei $m \in \mathbb{Z}$.
Die Einheiten von $\mathbb{Z}/(m)$ sind genau die Klassen $[a]$ mit $g.g.T(a, m) = 1$.

Definition

Wir definieren $\varphi(m) \in \mathbb{N}$ als die Anzahl der Einheiten in $\mathbb{Z}/(m)$.

Eulersche φ-Funktion

Sei $m \in \mathbb{Z}$.
Die Einheiten von $\mathbb{Z}/(m)$ sind genau die Klassen $[a]$ mit $g.g.T(a, m) = 1$.

Definition

Wir definieren $\varphi(m) \in \mathbb{N}$ als die Anzahl der Einheiten in $\mathbb{Z}/(m)$.

1. $\varphi(1) = 1$.
2. $\varphi(p) = p - 1$ für eine Primzahl $m := p \in \mathbb{Z}$.
3. $\varphi(p^n) = p^{n-1}(p-1)$ für eine Primzahl $p \in \mathbb{Z}$.

Eulersche φ-Funktion

Sei $m \in \mathbb{Z}$.
Die Einheiten von $\mathbb{Z}/(m)$ sind genau die Klassen $[a]$ mit $g.g.T(a, m) = 1$.

Definition

Wir definieren $\varphi(m) \in \mathbb{N}$ als die Anzahl der Einheiten in $\mathbb{Z}/(m)$.

1. $\varphi(1) = 1$.
2. $\varphi(p) = p - 1$ für eine Primzahl $m := p \in \mathbb{Z}$.
3. $\varphi(p^n) = p^{n-1}(p-1)$ für eine Primzahl $p \in \mathbb{Z}$.

Eulersche φ-Funktion

Sei $m \in \mathbb{Z}$.
Die Einheiten von $\mathbb{Z}/(m)$ sind genau die Klassen $[a]$ mit $g.g.T(a, m) = 1$.

Definition

Wir definieren $\varphi(m) \in \mathbb{N}$ als die Anzahl der Einheiten in $\mathbb{Z}/(m)$.

1. $\varphi(1) = 1$.
2. $\varphi(p) = p - 1$ für eine Primzahl $m := p \in \mathbb{Z}$.
3. $\varphi(p^n) = p^{n-1}(p-1)$ für eine Primzahl $p \in \mathbb{Z}$.

Eulersche φ-Funktion

$$m = \prod_{i=1}^{r} p_i^{l_i}$$

Eulersche φ-Funktion

$m = \prod_{i=1}^{r} p_i^{l_i}$

Lemma

Es gilt $\varphi(m) = m \prod_{p|m}(1 - \frac{1}{p})$.

Eulersche φ-Funktion

$m = \prod_{i=1}^{r} p_i^{l_i}$

Lemma

Es gilt $\varphi(m) = m \prod_{p|m}(1 - \frac{1}{p})$.

Lemma

Wenn $g.g.T(m, n) = 1$, *so gilt* $\varphi(mn) = \varphi(m)\varphi(n)$.

Eulersche φ-Funktion

Lemma

Wenn g.g.T $(m, n) = 1$, *so gilt* $\varphi(mn) = \varphi(m)\varphi(n)$.

Lemma (Euler-Fermat)

Sei $m \in \mathbb{Z}$ *und* $a \in \mathbb{Z}$ *prim zu* m. *Dann gilt* $a^{\varphi(m)} \equiv 1 (\mod m)$.

Eulersche φ-Funktion

Lemma (Euler-Fermat)

Sei $m \in \mathbb{Z}$ und $a \in \mathbb{Z}$ prim zu m. Dann gilt $a^{\varphi(m)} \equiv 1 (\mod m)$.

Lemma (Fermat)

Für eine Primzahl $p \in \mathbb{Z}$ und jedes $a \in \mathbb{Z}$ mit $p \not| a$ gilt $a^p \equiv a (\mod m)$.

Struktur der Einheitengruppe

$q \in \mathbb{Z}$ - prim

Struktur der Einheitengruppe

$q \in \mathbb{Z}$ - prim
$F_q := \mathbb{Z}/(q)$

Struktur der Einheitengruppe

$q \in \mathbb{Z}$ - prim
$F_q := \mathbb{Z}/(q)$

Lemma

Die Gruppe der Einheiten $\mathbb{F}_q^*$ ist zyklisch.

Struktur der Einheitengruppe

$q \in \mathbb{Z}$ - prim
$F_q := \mathbb{Z}/(q)$

Lemma

Die Gruppe der Einheiten $\mathbb{F}_q^*$ ist zyklisch.

Lemma

Die Gruppe der Einheiten in $\mathbb{Z}/(m)$ ist genau dann zyklisch, wenn $m = 2$, $m = 4$, $m = p^n$, oder $m = 2p^n$, wobei p eine ungerade Primzahl ist.

Anwendung des Euklidischen Algorithmus

Wir zeigen nun, wie man Inverse in $\mathbb{Z}/(m)^*$ mit dem Euklidischen Algorithmus bestimmen kann.

Anwendung des Euklidischen Algorithmus

Wir zeigen nun, wie man Inverse in $\mathbb{Z}/(m)^*$ mit dem Euklidischen Algorithmus bestimmen kann.
Sei a zu m Teilerfremd.

Anwendung des Euklidischen Algorithmus

Wir zeigen nun, wie man Inverse in $\mathbb{Z}/(m)^*$ mit dem Euklidischen Algorithmus bestimmen kann.
Sei a zu m Teilerfremd.
Dann ist $[a] \in \mathbb{Z}/(m)^*$.

Anwendung des Euklidischen Algorithmus

Wir zeigen nun, wie man Inverse in $\mathbb{Z}/(m)^*$ mit dem Euklidischen Algorithmus bestimmen kann.
Sei a zu m Teilerfremd.
Dann ist $[a] \in \mathbb{Z}/(m)^*$.
Wir suchen $[b] \in Z/(m)^*$ mit $[a][b] = 1$, also $1 = ab + rm$.

Anwendung des Euklidischen Algorithmus

Sei a zu m Teilerfremd.
Dann ist $[a] \in \mathbb{Z}/(m)^*$.
Wir suchen $[b] \in Z/(m)^*$ mit $[a][b] = 1$, also $1 = ab + rm$.
Seien $u, v \in \mathbb{Z}$ vorgegeben.

Anwendung des Euklidischen Algorithmus

Sei a zu m Teilerfremd.
Dann ist $[a] \in \mathbb{Z}/(m)^*$.
Wir suchen $[b] \in Z/(m)^*$ mit $[a][b] = 1$, also $1 = ab + rm$.
Seien $u, v \in \mathbb{Z}$ vorgegeben.
Dann liefert der Algorithmus eine Folge $F(u, v) := (w_n)$ durch folgende Vorschrift

Anwendung des Euklidischen Algorithmus

Seien $u, v \in \mathbb{Z}$ vorgegeben.
Dann liefert der Algorithmus eine Folge $F(u, v) := (w_n)$ durch folgende Vorschrift

1. $w_1 := u$
2. $w_2 := v$
3. Bestimme w_{n+2} durch $w_n = x_{n+1} w_{n+1} + w_{n+2}$ mit $0 \leq w_{n+3} < |w_{n+1}|$.

Anwendung des Euklidischen Algorithmus

Seien $u, v \in \mathbb{Z}$ vorgegeben.
Dann liefert der Algorithmus eine Folge $F(u, v) := (w_n)$ durch folgende Vorschrift

1. $w_1 := u$
2. $w_2 := v$
3. Bestimme w_{n+2} durch $w_n = x_{n+1} w_{n+1} + w_{n+2}$ mit $0 \leq w_{n+3} < |w_{n+1}|$.

Anwendung des Euklidischen Algorithmus

Seien $u, v \in \mathbb{Z}$ vorgegeben.
Dann liefert der Algorithmus eine Folge $F(u, v) := (w_n)$ durch folgende Vorschrift

1. $w_1 := u$
2. $w_2 := v$
3. Bestimme w_{n+2} durch $w_n = x_{n+1} w_{n+1} + w_{n+2}$ mit $0 \leq w_{n+3} < |w_{n+1}|$.

Anwendung des Euklidischen Algorithmus

$$w_n = w_{n-2} - x_{n-1} w_{n-1}$$

.

Anwendung des Euklidischen Algorithmus

$$\begin{aligned} w_n &= w_{n-2} - x_{n-1} w_{n-1} \\ &= w_{n-2} - x_{n-1}\left(w_{n-3} - x_{n-2} w_{n-2}\right) \end{aligned}$$

.

Anwendung des Euklidischen Algorithmus

$$\begin{aligned} w_n &= w_{n-2} - x_{n-1} w_{n-1} \\ &= w_{n-2} - x_{n-1}\left(w_{n-3} - x_{n-2} w_{n-2}\right) \\ &= \left(1 + x_{n-2}\right) w_{n-2} - x_{n-1} w_{n-3} \end{aligned}$$

.

Anwendung des Euklidischen Algorithmus

$$\begin{aligned} w_n &= w_{n-2} - x_{n-1} w_{n-1} \\ &= w_{n-2} - x_{n-1}\left(w_{n-3} - x_{n-2} w_{n-2}\right) \\ &= \left(1 + x_{n-2}\right) w_{n-2} - x_{n-1} w_{n-3} \\ &= \left(1 + x_{n-2}\right)\left(w_{n-4} - x_{n-3} w_{n-3}\right) - x_{n-1} w_{n-3} \end{aligned}$$

.

Anwendung des Euklidischen Algorithmus

$$\begin{aligned} w_n &= w_{n-2} - x_{n-1}w_{n-1} \\ &= w_{n-2} - x_{n-1}(w_{n-3} - x_{n-2}w_{n-2}) \\ &= (1 + x_{n-2})w_{n-2} - x_{n-1}w_{n-3} \\ &= (1 + x_{n-2})(w_{n-4} - x_{n-3}w_{n-3}) - x_{n-1}w_{n-3} \\ &= (1 + x_{n-2})w_{n-4} - ((1 + x_{n-2})x_{n-3} + x_{n-1})w_{n-3} \end{aligned}$$

.

Anwendung des Euklidischen Algorithmus

$$
\begin{aligned}
w_n &= w_{n-2} - x_{n-1}w_{n-1} \\
&= w_{n-2} - x_{n-1}\big(w_{n-3} - x_{n-2}w_{n-2}\big) \\
&= \big(1 + x_{n-2}\big)w_{n-2} - x_{n-1}w_{n-3} \\
&= \big(1 + x_{n-2}\big)\big(w_{n-4} - x_{n-3}w_{n-3}\big) - x_{n-1}w_{n-3} \\
&= \big(1 + x_{n-2}\big)w_{n-4} - \big(\big(1 + x_{n-2}\big)x_{n-3} + x_{n-1}\big)w_{n-3} \\
&\vdots
\end{aligned}
$$

.

Anwendung des Euklidischen Algorithmus

$$
\begin{aligned}
w_n &= w_{n-2} - x_{n-1} w_{n-1} \\
&= w_{n-2} - x_{n-1}\big(w_{n-3} - x_{n-2} w_{n-2}\big) \\
&= \big(1 + x_{n-2}\big) w_{n-2} - x_{n-1} w_{n-3} \\
&= \big(1 + x_{n-2}\big)\big(w_{n-4} - x_{n-3} w_{n-3}\big) - x_{n-1} w_{n-3} \\
&= \big(1 + x_{n-2}\big) w_{n-4} - \big(\big(1 + x_{n-2}\big) x_{n-3} + x_{n-1}\big) w_{n-3} \\
&\vdots \\
&= c_1 w_1 + c_2 w_2 \ .
\end{aligned}
$$

Anwendung des Euklidischen Algorithmus

Wir betrachten nun die Folge $(w_n) = F(m, a)$.

Anwendung des Euklidischen Algorithmus

Wir betrachten nun die Folge $(w_n) = F(m, a)$.
Wegen $g.g.T.(m, a) = 1$ gilt $w_n = 1$ für ein geeignetes n.

Anwendung des Euklidischen Algorithmus

Wir betrachten nun die Folge $(w_n) = F(m, a)$.
Wegen $g.g.T.(m, a) = 1$ gilt $w_n = 1$ für ein geeignetes n.
Mit dem obigen Verfahren erhalten wir

$$1 = c_1 m + c_2 a \ .$$

Anwendung des Euklidischen Algorithmus

Wir betrachten nun die Folge $(w_n) = F(m, a)$.
Wegen $g.g.T.(m, a) = 1$ gilt $w_n = 1$ für ein geeignetes n.
Mit dem obigen Verfahren erhalten wir

$$1 = c_1 m + c_2 a \ .$$

Also gilt für $[c_2][a] = 1$ in $\mathbb{Z}/(m)$.

Anwendung des Euklidischen Algorithmus

Beispiel: $m = 37$ und $a = 12$.

1. $w_1 := 37$
2. $w_2 := 11$
3. $37 = 3.11 + 4,\ x_2 = 3,\ w_3 = 4$
4. $11 = 2.4 + 3,\ x_3 = 2,\ w_4 = 3$
5. $4 = 1.3 + 1,\ x_4 = 1,\ w_5 = 1$

Anwendung des Euklidischen Algorithmus

Beispiel: $m = 37$ und $a = 12$.

1. $w_1 := 37$
2. $w_2 := 11$
3. $37 = 3.11 + 4,\ x_2 = 3,\ w_3 = 4$
4. $11 = 2.4 + 3,\ x_3 = 2,\ w_4 = 3$
5. $4 = 1.3 + 1,\ x_4 = 1,\ w_5 = 1$

Anwendung des Euklidischen Algorithmus

Beispiel: $m = 37$ und $a = 12$.

1. $w_1 := 37$
2. $w_2 := 11$
3. $37 = 3.11 + 4,\ x_2 = 3,\ w_3 = 4$
4. $11 = 2.4 + 3,\ x_3 = 2,\ w_4 = 3$
5. $4 = 1.3 + 1,\ x_4 = 1,\ w_5 = 1$

Anwendung des Euklidischen Algorithmus

Beispiel: $m = 37$ und $a = 12$.

1. $w_1 := 37$
2. $w_2 := 11$
3. $37 = 3.11 + 4,\ x_2 = 3,\ w_3 = 4$
4. $11 = 2.4 + 3,\ x_3 = 2,\ w_4 = 3$
5. $4 = 1.3 + 1,\ x_4 = 1,\ w_5 = 1$

Anwendung des Euklidischen Algorithmus

Beispiel: $m = 37$ und $a = 12$.

1. $w_1 := 37$
2. $w_2 := 11$
3. $37 = 3.11 + 4,\ x_2 = 3,\ w_3 = 4$
4. $11 = 2.4 + 3,\ x_3 = 2,\ w_4 = 3$
5. $4 = 1.3 + 1,\ x_4 = 1,\ w_5 = 1$

Anwendung des Euklidischen Algorithmus

Beispiel: $m = 37$ und $a = 12$.

1. $w_1 := 37$
2. $w_2 := 11$
3. $37 = 3.11 + 4,\ x_2 = 3,\ w_3 = 4$
4. $11 = 2.4 + 3,\ x_3 = 2,\ w_4 = 3$
5. $4 = 1.3 + 1,\ x_4 = 1,\ w_5 = 1$

Anwendung des Euklidischen Algorithmus

Beispiel: $m = 37$ und $a = 12$.

1. $w_1 := 37$
2. $w_2 := 11$
3. $37 = 3.11 + 4,\ x_2 = 3,\ w_3 = 4$
4. $11 = 2.4 + 3,\ x_3 = 2,\ w_4 = 3$
5. $4 = 1.3 + 1,\ x_4 = 1,\ w_5 = 1$

Wir haben also $n = 5$

$$1 = (1 + 2)37 - ((1 + 2)3 + 1)11 = 3.37 - 10.11$$

Anwendung des Euklidischen Algorithmus

Beispiel: $m = 37$ und $a = 12$.

1. $w_1 := 37$
2. $w_2 := 11$
3. $37 = 3.11 + 4,\ x_2 = 3,\ w_3 = 4$
4. $11 = 2.4 + 3,\ x_3 = 2,\ w_4 = 3$
5. $4 = 1.3 + 1,\ x_4 = 1,\ w_5 = 1$

Wir haben also $n = 5$

$$1 = (1 + 2)37 - ((1 + 2)3 + 1)11 = 3.37 - 10.11$$

Also gilt $[10]_{37}[11]_{37} = [1]_{37}$.

RSA

Bob will Nachrichten empfangen. Jeder Sender soll in die Lage versetzt werden, zu verschlüsseln, jedoch soll nur Bob entschlüsseln können.

RSA

Bob will Nachrichten empfangen. Jeder Sender soll in die Lage versetzt werden, zu verschlüsseln, jedoch soll nur Bob entschlüsseln können.
Bob geht wie folgt vor.

RSA

Bob geht wie folgt vor.
Er bestimmt zwei sehr große Primzahlen p, q und setzt $m = pq$. Er berechnet $\varphi(m) = (p-1)(q-1)$. Die Nachrichten werden Elemente $[x]_m \in \mathbb{Z}/(m)$sein für welche x klein gegen p, q ist.
Solche x sind dann prim zu p, q.

RSA

Er bestimmt zwei sehr große Primzahlen p, q und setzt $m = pq$. Er berechnet $\varphi(m) = (p-1)(q-1)$. Die Nachrichten werden Elemente $[x]_m \in \mathbb{Z}/(m)$sein für welche x klein gegen p, q ist.
Solche x sind dann prim zu p, q.
Bob bestimmt weiter eine Zahl e mit $g.g.T(e, \varphi(m))$. Er kann mit dem euklidischen Algorithmus ein d finden so daß

$$[e]_{\varphi(m)}[d]_{\varphi(m)} = [1]_{\varphi(m)} \ .$$

Bob veröffentlicht nun das Paar (m, e).

RSA

Bob bestimmt weiter eine Zahl e mit $g.g.T(e, \varphi(m))$. Er kann mit dem euklidischen Algorithmus ein d finden so daß

$$[e]_{\varphi(m)}[d]_{\varphi(m)} = [1]_{\varphi(m)} \ .$$

Bob veröffentlicht nun das Paar (m, e).
Alice möchte Bob eine Nachricht $x \in \mathbb{Z}/(m)$ übermitteln. Sie kennt (wie alle Mithörer) das Paar (m, e). Sie wird $y := x^e$ senden.

RSA

Alice möchte Bob eine Nachricht $x \in \mathbb{Z}/(m)$ übermitteln. Sie kennt (wie alle Mithörer) das Paar (m, e). Sie wird $y := x^e$ senden.
Um zu entschlüsseln, bildet Bob $z := y^d$. Da x zu $m = pq$ prim ist, gilt in $\mathbb{Z}/(m)$

$$z = x^{ed} = x^{1+\varphi(m)r} = x \quad .$$

Reduktion

$f(x_1, \ldots, x_n)$ - Polynom mit ganzen Koeffizienten

Reduktion

$f(x_1, \ldots, x_n)$ - Polynom mit ganzen Koeffizienten
Hat $f = 0$ ganzzahlige Lösungen $(a_1, \ldots, a_n) \in \mathbb{Z}^n$?

Reduktion

$f(x_1, \ldots, x_n)$ - Polynom mit ganzen Koeffizienten
Hat $f = 0$ ganzzahlige Lösungen $(a_1, \ldots, a_n) \in \mathbb{Z}^n$?
$m \in \mathbb{Z}$

Reduktion

$f(x_1, \ldots, x_n)$ - Polynom mit ganzen Koeffizienten
Hat $f = 0$ ganzzahlige Lösungen $(a_1, \ldots, a_n) \in \mathbb{Z}^n$?
$m \in \mathbb{Z}$
$[f]_m$ Reduktion von f modulo m

Reduktion

$[f]_m$ Reduktion von f modulo m

Definition

$$N_f(m) := \sharp\{[f]_m([a_1]_m, \ldots, [a_n]_m) = 0\} \ .$$

Reduktion

Definition

$$N_f(m) := \sharp\{[f]_m([a_1]_m, \ldots, [a_n]_m) = 0\} \ .$$

Lemma

Eine notwendige Bedingung für die Lösbarkeit von $f = 0$ *ist* $N_f(m) \neq 0$ *für alle* $m \in \mathbb{N}$.

$N_f(m)$

$$m = m_1 m_2 \ , \ g.g.T.(m_1, m_2) = 1.$$

$N_f(m)$

$m = m_1 m_2$, $g.g.T.(m_1, m_2) = 1$.

Lemma

Es gilt $N_f(m) = N_f(m_1) N_f(m_2)$.

$N_f(m)$

$m = m_1 m_2$, $g.g.T.(m_1, m_2) = 1$.

Lemma

Es gilt $N_f(m) = N_f(m_1)N_f(m_2)$.

$m = \prod_p p^{e_p}$ - die Primfaktorenzerlegung

$N_f(m)$

$m = \prod_p p^{e_p}$ - die Primfaktorenzerlegung

Lemma

Es gilt

$$N_f(m) = \prod_p N_f(p^{e_p}) \ .$$

Liften

Lemma

Liften

Lemma

Sei $p \in \mathbb{Z}$ prim, $n, k \in \mathbb{N}$, $0 \leq 2k < n$, und $f \in \mathbb{Z}[x]$. Sei weiterhin $x \in \mathbb{Z}$ mit

Liften

Lemma

Sei $p \in \mathbb{Z}$ prim, $n, k \in \mathbb{N}$, $0 \leq 2k < n$, und $f \in \mathbb{Z}[x]$. Sei weiterhin $x \in \mathbb{Z}$ mit

$$\begin{aligned} f(x) &\equiv 0 \mod p^n \\ f'(x) &\equiv 0 \mod p^k \\ f'(x) &\not\equiv 0 \mod p^{k+1} . \end{aligned}$$

Liften

Lemma

Dann gibt es ein modulo p^{n-k+1} eindeutig bestimmtes $y \in \mathbb{Z}$ derart, daß

Liften

Lemma

$$\begin{aligned} f(x) &\equiv 0 \mod p^n \\ f'(x) &\equiv 0 \mod p^k \\ f'(x) &\not\equiv 0 \mod p^{k+1} . \end{aligned}$$

$$\begin{aligned} f(y) &\equiv 0 \mod p^{n+1} \\ f'(y) &\equiv 0 \mod p^k \\ f'(x) &\not\equiv 0 \mod p^{k+1} \\ y &\equiv x \mod p^{n-k} . \end{aligned}$$

Das Problem

$$x^2 - a \equiv 0 \mod m$$

$$g.g.T.(m, a) = 1$$

Das Problem

$$x^2 - a \equiv 0 \mod m$$

$g.g.T.(m, a) = 1$

Definition

Wenn diese Gleichung eine Lösung hat, so heißt a quadratischer Rest (QR) modulo m. Andernfalls ist a ein quadratischer Nichtrest (QNR) modulo m

Das Problem

$$x^2 - a \equiv 0 \mod m$$

$g.g.T.(m, a) = 1$

Definition

Wenn diese Gleichung eine Lösung hat, so heißt a quadratischer Rest (QR) modulo m. Andernfalls ist a ein quadratischer Nichtrest (QNR) modulo m

$m = \prod_p p^{e_p}$ - die Primzerlegung

Das Problem

$m = \prod_p p^{e_p}$ - die Primzerlegung

Lemma

1. *a ist QR modulo m genau dann, wenn a ein QR modulo p^{e_p} für alle Primfaktoren p von m ist.*
2. *Ist $p > 2$, dann ist a ein QR modulo p^e genau dann, wenn a ein QR modulo p ist.*
3. *Ist $p = 2$, dann ist a ein QR modulo 2^e genau dann, wenn a ein QR modulo $2^{\min(e,3)}$ ist.*

Das Problem

$m = \prod_p p^{e_p}$ - die Primzerlegung

Lemma

1. *a ist QR modulo m genau dann, wenn a ein QR modulo p^{e_p} für alle Primfaktoren p von m ist.*
2. *Ist $p > 2$, dann ist a ein QR modulo p^e genau dann, wenn a ein QR modulo p ist.*
3. *Ist $p = 2$, dann ist a ein QR modulo 2^e genau dann, wenn a ein QR modulo $2^{\min(e,3)}$ ist.*

Das Problem

$m = \prod_p p^{e_p}$ - die Primzerlegung

Lemma

1. *a ist QR modulo m genau dann, wenn a ein QR modulo p^{e_p} für alle Primfaktoren p von m ist.*
2. *Ist $p > 2$, dann ist a ein QR modulo p^e genau dann, wenn a ein QR modulo p ist.*
3. *Ist $p = 2$, dann ist a ein QR modulo 2^e genau dann, wenn a ein QR modulo $2^{\min(e,3)}$ ist.*

Das Problem

1. Gegeben sei eine Primzahl $p > 2$. Bestimme die QR modulo p.
2. Gegeben sei a. Bestimme alle p, für welche a ein QR modulo p ist.

Das Problem

1. Gegeben sei eine Primzahl $p > 2$. Bestimme die QR modulo p.
2. Gegeben sei a. Bestimme alle p, für welche a ein QR modulo p ist.

Symbole

$a, p \in \mathbb{Z}$, $p \neq 2$ eine Primzahl, und $p \nmid a$.

Symbole

$a, p \in \mathbb{Z}$, $p \neq 2$ eine Primzahl, und $p \nmid a$.

Definition

Das Legendresymbol wird durch

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & a \text{ ist QR modulo } p \\ -1 & a \text{ ist QNR modulo } p \end{cases}$$

definiert.

Symbole

$a, p \in \mathbb{Z}$, $p \neq 2$ eine Primzahl, und $p \nmid a$.

Definition

Das Legendresymbol wird durch

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & a \text{ ist QR modulo } p \\ -1 & a \text{ ist QNR modulo } p \end{cases}$$

definiert.

Offensichtlich hängt $\left(\frac{a}{p}\right)$ nur von $[a]_p$ ab.

Symbole

$a, p \in \mathbb{Z}$, $p \neq 2$ eine Primzahl, und $p \nmid a$.

Lemma

1. **[Eulerkriterium]** *Es gilt*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p \ .$$

2. *Wenn a, b prim zu p sind, dann gilt*

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right) \ .$$

Symbole

$a, p \in \mathbb{Z}$, $p \neq 2$ eine Primzahl, und $p \nmid a$.

Lemma

1. **[Eulerkriterium]** *Es gilt*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p \ .$$

2. *Wenn a, b prim zu p sind, dann gilt*

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right) \ .$$

Das quadratische Reziprozitätsgesetz

$2 \neq p \in \mathbb{Z}$ prim

Das quadratische Reziprozitätsgesetz

$2 \neq p \in \mathbb{Z}$ prim
$a = (-1)^\nu \prod_q q^{e_q}$

Das quadratische Reziprozitätsgesetz

$2 \neq p \in \mathbb{Z}$ prim
$a = (-1)^\nu \prod_q q^{e_q}$

$$\left(\frac{a}{p}\right) = \left(\frac{(-1)^\nu}{p}\right)\left(\frac{2}{p}\right)\prod_{p\neq 2}\left(\frac{q}{p}\right) \ .$$

Das quadratische Reziprozitätsgesetz

Lemma (1. Ergänzungssatz)

Es gilt $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

Das quadratische Reziprozitätsgesetz

Lemma (1. Ergänzungssatz)

Es gilt $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

Lemma (2. Ergänzungssatz)

Es gilt $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Das quadratische Reziprozitätsgesetz

Lemma (2. Ergänzungssatz)

Es gilt $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Theorem (Quadratisches Reziprozitätsgesetz)

Seien p, q verschiedene ungerade Primzahlen. Dann gilt

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right) .$$

Beispiele

Ist 37 ein QR bezüglich 103 ?

Beispiele

Ist 37 ein QR bezüglich 103 ?

$$\begin{aligned}\left(\frac{37}{103}\right) &= \left(\frac{103}{37}\right)\\ &= \left(\frac{29}{37}\right)\\ &= \left(\frac{37}{29}\right)\\ &= \left(\frac{8}{29}\right)\\ &= \left(\frac{2}{29}\right)\\ &= -1\ .\end{aligned}$$

Beispiele

Ist 24 ein QR bezüglich 31 ?

Beispiele

Ist 24 ein QR bezüglich 31 ?

$$\begin{aligned}
\left(\frac{24}{31}\right) &= \left(\frac{2^3}{31}\right)\left(\frac{3}{31}\right) \\
&= \left(\frac{2}{31}\right)\left(\frac{3}{31}\right) \\
&= -\left(\frac{31}{3}\right) \\
&= -\left(\frac{1}{3}\right) \\
&= -1
\end{aligned}$$

Beispiele

$$\begin{aligned}\left(\frac{24}{31}\right) &= \left(\frac{2^3}{31}\right)\left(\frac{3}{31}\right)\\ &= \left(\frac{2}{31}\right)\left(\frac{3}{31}\right)\\ &= -\left(\frac{31}{3}\right)\\ &= -\left(\frac{1}{3}\right)\\ &= -1\end{aligned}$$

Hier sind die Quadrate mod 31

$$\{1, 4, 9, 16, 25, 5, 18, 2, 10, 7, 28, 20, 14, 10, 8\}.$$

Beispiele

$$\begin{aligned}\left(\frac{10}{31}\right) &= \left(\frac{2}{31}\right)\left(\frac{5}{31}\right)\\ &= \left(\frac{5}{31}\right)\\ &= -\left(\frac{31}{5}\right)\\ &= \left(\frac{1}{5}\right)\\ &= 1\end{aligned}$$

Verzweigung von Primzahlen

$D \in \mathbb{Z}$ - quadratfrei und

$$R := \begin{cases} \mathbb{Z}[\sqrt{D}] & D \not\equiv 1 \mod 4 \\ \mathbb{Z}[\frac{1+\sqrt{D}}{2}] & D \equiv 1 \mod 4 \end{cases}.$$

Verzweigung von Primzahlen

$D \in \mathbb{Z}$ - quadratfrei und

$$R := \begin{cases} \mathbb{Z}[\sqrt{D}] & D \not\equiv 1 \mod 4 \\ \mathbb{Z}[\frac{1+\sqrt{D}}{2}] & D \equiv 1 \mod 4 \end{cases} .$$

Wir nehmen an, daß R faktoriell ist.

Verzweigung von Primzahlen

$D \in \mathbb{Z}$ - quadratfrei und

$$R := \begin{cases} \mathbb{Z}[\sqrt{D}] & D \not\equiv 1 \mod 4 \\ \mathbb{Z}[\frac{1+\sqrt{D}}{2}] & D \equiv 1 \mod 4 \end{cases} .$$

Wir nehmen an, daß R faktoriell ist.
Wenn $D < 0$, dann gilt

$$D \in \{-1, -2, -3, -5, -7, -11, -19, -43, -67, -163\} .$$

Verzweigung von Primzahlen

$D \in \mathbb{Z}$ - quadratfrei und

$$R := \begin{cases} \mathbb{Z}[\sqrt{D}] & D \not\equiv 1 \mod 4 \\ \mathbb{Z}[\frac{1+\sqrt{D}}{2}] & D \equiv 1 \mod 4 \end{cases} .$$

Wir nehmen an, daß R faktoriell ist.
Wenn $D < 0$, dann gilt

$$D \in \{-1, -2, -3, -5, -7, -11, -19, -43, -67, -163\} .$$

Es wird vermutet, daß R für undendlich viele $D > 0$ faktoriell ist.

Verzweigung von Primzahlen

Wir setzen

$$d := \begin{cases} & 4D \not\equiv 1 \mod 4 \\ \mathbb{Z}[\frac{1+\sqrt{D}}{2}] & D \equiv 1 \mod 4 \end{cases}.$$

Verzweigung von Primzahlen

Wir setzen

$$d := \begin{cases} & 4D \not\equiv 1 \mod 4 \\ \mathbb{Z}[\frac{1+\sqrt{D}}{2}] & D \equiv 1 \mod 4 \end{cases}.$$

Lemma

Eine Primzahl $p \in \mathbb{Z}$ ist genau dann träge in R, wenn $p \nmid d$ und d ein QR modulo p ist.

Körpererweiterungen und Teilkörper

K - ein Körper.

Körpererweiterungen und Teilkörper

K - ein Körper.

Definition

Unter einer Körpererweiterung von K verstehen wir einen Körper L mit einer Einbettung $K \hookrightarrow L$. In der Regel identifizieren wir K mit dem Bild dieser Einbettung.

Körpererweiterungen und Teilkörper

$K \subset L$ - eine Körpererweiterung. Dann ist L ein K-Vektorraum.

Körpererweiterungen und Teilkörper

$K \subset L$ - eine Körpererweiterung. Dann ist L ein K-Vektorraum.

Definition

Wir definieren den Grad dieser Erweiterung als

$$[L : K] = \deg_K(L) := \dim_K(L) \ .$$

Körpererweiterungen und Teilkörper

Definition

Wir definieren den Grad dieser Erweiterung als

$$[L : K] = \deg_K(L) := \dim_K(L) \ .$$

Lemma

Ist $L \subset M$ eine Erweiterung, dann ist auch die Komposition $K \subset M$ eine Körpererweiterung und es gilt

$$[M : K] = [M : L][L : K] \ .$$

Eine Konstruktion

$k \subset K$- ein Teilkörper.

Eine Konstruktion

$k \subset K$- ein Teilkörper.
$\alpha_1, \ldots, \alpha_r \in K$.

Eine Konstruktion

$k \subset K$- ein Teilkörper.
$\alpha_1, \ldots, \alpha_r \in K$.

Definition

Wir definieren den Körper $k(\alpha_1, \ldots, \alpha_r), \subset K$ als den kleinsten Unterkörper von K, welcher sowohl α_i, $i = 1, \ldots, r$ als auch k enthält.

Eine Konstruktion

$k \subset K$- ein Teilkörper.
$\alpha_1, \ldots, \alpha_r \in K$.

Definition

Wir definieren den Körper $k(\alpha_1, \ldots, \alpha_r), \subset K$ als den kleinsten Unterkörper von K, welcher sowohl α_i, $i = 1, \ldots, r$ als auch k enthält.

Sei $\alpha \in L$.

Eine Konstruktion

Definition

Wir definieren den Körper $k(\alpha_1, \ldots, \alpha_r), \subset K$ als den kleinsten Unterkörper von K, welcher sowohl α_i, $i = 1, \ldots, r$ als auch k enthält.

Sei $\alpha \in L$.

Lemma

Es gilt $k(\alpha) = \{\frac{g(\alpha)}{f(\alpha)} | f, g \in k[x], f(\alpha) \neq 0\}$.

Zerfällungskörper

$f \in K[x]$ - ein nichtkonstantes Polynom,

Zerfällungskörper

$f \in K[x]$ - ein nichtkonstantes Polynom,
$K \subset L$

Zerfällungskörper

$f \in K[x]$ - ein nichtkonstantes Polynom,
$K \subset L$
$K[x] \subset L[x]$

Zerfällungskörper

$f \in K[x]$ - ein nichtkonstantes Polynom,
$K \subset L$
$K[x] \subset L[x]$

Definition

f zerfällt über L, falls in $L[x]$ gilt

$$f = \prod_{i=1}^{\deg(f)} (x - a_i) \ .$$

Zerfällungskörper

Jedes Polynom in $\mathbb{Q}[x]$ zerfällt über $\mathbb{C}$.

Zerfällungskörper

Jedes Polynom in $\mathbb{Q}[x]$ zerfällt über $\mathbb{C}$.

Definition

Die Erweiterung $K \subset L$ heißt Zerfällungskörper von f, falls es keinen Zwischenkörper $K \subset M \subset L$ gibt, so daß f über M zerfällt.

Zerfällungskörper

$$\mathbb{Q} \subset K \subset \mathbb{C}$$

Zerfällungskörper

$\mathbb{Q} \subset K \subset \mathbb{C}$
$f \in K[x]$

Zerfällungskörper

$\mathbb{Q} \subset K \subset \mathbb{C}$
$f \in K[x]$
$\alpha_1, \ldots, \alpha_r$ - die komplexen Nullstellen von f.

Zerfällungskörper

$\mathbb{Q} \subset K \subset \mathbb{C}$
$f \in K[x]$
$\alpha_1, \ldots, \alpha_r$ - die komplexen Nullstellen von f.

Lemma

f zerfällt über der Erweiterung $K \subset K(\alpha_1, \ldots, \alpha_r) \subset \mathbb{C}$.
Insbesondere besitzt f einen Zerfällungskörper
$K \subset L \subset K(\alpha_1, \ldots, \alpha_r)$ derart, daß $[L : K] \leq \deg(f)$.

Adjunktion

K - ein Körper

Adjunktion

K - ein Körper
$K[x]$ ist euklidisch und damit Hauptidealring

Adjunktion

K - ein Körper
$K[x]$ ist euklidisch und damit Hauptidealring
$I \subset K[x]$ - ein echtes Ideal

Adjunktion

K - ein Körper
$K[x]$ ist euklidisch und damit Hauptidealring
$I \subset K[x]$ - ein echtes Ideal
$I = (f)$ für ein geeignetes $f \in K[x]$

Adjunktion

K - ein Körper
$K[x]$ ist euklidisch und damit Hauptidealring
$I \subset K[x]$ - ein echtes Ideal
$I = (f)$ für ein geeignetes $f \in K[x]$
Sei

$$0 \to I \to K[x] \to K[x]/I \to 0 \ .$$

Adjunktion

Sei

$$0 \longrightarrow I \longrightarrow K[x] \longrightarrow K[x]/I \longrightarrow 0 \ .$$

Lemma

Der Ring $K[x]/I$ ist genau dann ein Körper, wenn f irreduzibel ist.

Adjunktion

Lemma

Der Ring $K[x]/I$ ist genau dann ein Körper, wenn f irreduzibel ist.

Lemma

Die Klassen der Polynome $[1], [x], \ldots, [x^{\deg(f)-1}]$ bilden eine Basis von K_f über K. Insbesondere gilt $[K_f : K] = \deg(f)$.

Adjunktion

Lemma

Die Klassen der Polynome $[1], [x], \ldots, [x^{\deg(f)-1}]$ *bilden eine Basis von* K_f *über* K. *Insbesondere gilt* $[K_f : K] = \deg(f)$.

$K \subset K_f$, $f \in K[x]$ irreduzibel

Adjunktion

$K \subset K_f$, $f \in K[x]$ irreduzibel
$\alpha = [x] \in K_f$

Adjunktion

$\alpha = [x] \in K_f$

Lemma

Es gilt in K_f daß $f(\alpha) = 0$.

Adjunktion

Lemma

Es gilt in K_f daß $f(\alpha) = 0$.

Lemma

Sei K ein Körper und $f \in K[x]$. Dann existiert eine Erweiterung $K \subset L$ so daß f über L zerfällt und $[L : K] \leq \deg(f)$ ist. Insbesondere besitzt f einen Zerfällungskörper vom Grade $\leq \deg(f)$ über K.

Fortsetzung I

K -ein Körper

Fortsetzung I

K -ein Körper
$f \in K[x]$ - irreduzibel

Fortsetzung I

K -ein Körper
$f \in K[x]$ - irreduzibel
$K \subset L$ - eine Erweiterung

Fortsetzung I

K -ein Körper
$f \in K[x]$ - irreduzibel
$K \subset L$ - eine Erweiterung
$\alpha \in L$ eine Nullstelle von f

Fortsetzung I

K -ein Körper
$f \in K[x]$ - irreduzibel
$K \subset L$ - eine Erweiterung
$\alpha \in L$ eine Nullstelle von f
Homomorphismus $\phi_\alpha : K_f \to K(\alpha)$

$$\phi_\alpha([g]) := g(\alpha) \ .$$

Fortsetzung I

K -ein Körper
$f \in K[x]$ - irreduzibel
$K \subset L$ - eine Erweiterung
$\alpha \in L$ eine Nullstelle von f
Homomorphismus $\phi_\alpha : K_f \to K(\alpha)$

$$\phi_\alpha([g]) := g(\alpha) \ .$$

Lemma

$\phi_\alpha : K_f \to K(\alpha)$ ist ein Isomorphismus.

Fortsetzung II

$\phi : K \to K'$- ein Isomorphismus

Fortsetzung II

$\phi : K \to K'$- ein Isomorphismus
f' - das Bild von f unter

$$\Phi : K[x] \to K'[x]$$

Fortsetzung II

$\phi : K \to K'$- ein Isomorphismus
f' - das Bild von f unter

$$\Phi : K[x] \to K'[x]$$

$K' \subset L'$ - eine Erweiterung

Fortsetzung II

$\phi : K \to K'$- ein Isomorphismus
f' - das Bild von f unter

$$\Phi : K[x] \to K'[x]$$

$K' \subset L'$ - eine Erweiterung
$\alpha' \in L'$ - eine Nullstelle von f'

Fortsetzung II

$\phi : K \to K'$- ein Isomorphismus
f' - das Bild von f unter

$$\Phi : K[x] \to K'[x]$$

$K' \subset L'$ - eine Erweiterung
$\alpha' \in L'$ - eine Nullstelle von f'

Lemma

Es gibt genau eine Ausdehnung $\hat{\phi} : K(\alpha) \to K'(\alpha')$ *von* ϕ *mit* $\phi(\alpha) = \alpha'$.

Fortsetzung II

Lemma

Sei $f \in K[x]$ irreduzibel, $\phi : K \to K'$ ein Isomorphismus, und $\Phi : K[x] \to K'[x]$ seine Ausdehnung. Seien $K \subset L$ und $K' \subset L'$ Zerfällungskörper von f und $\Phi(f)$. Dann existiert ein Isomorphismus $\psi : L \to L'$ mit $\psi_{|K} = \phi$ derart, daß $\phi(\{\alpha \in L | f(\alpha) = 0\}) = \{\alpha' \in L' | \Phi(f)(\alpha') = 0\}$.

Inhalt eines Polynoms

$R \subset K$- ein faktorieller Unterring mit $K = \{\frac{a}{b} | a, b \in R, b \neq 0\}$

Inhalt eines Polynoms

$R \subset K$- ein faktorieller Unterring mit $K = \{\frac{a}{b} | a, b \in R, b \neq 0\}$
$f = a_n x^n + \cdots + a_0$

Inhalt eines Polynoms

$R \subset K$- ein faktorieller Unterring mit $K = \{\frac{a}{b} | a, b \in R, b \neq 0\}$
$f = a_n x^n + \cdots + a_0$

Definition

Der Inhalt von f sei $I(f) := g.g.T.(a_0, \ldots, a_n)$. Wenn $I(f) = 1$, so nennen wir f primitiv.

Inhalt eines Polynoms

$R \subset K$- ein faktorieller Unterring mit $K = \{\frac{a}{b} | a, b \in R, b \neq 0\}$
$f = a_n x^n + \cdots + a_0$

Definition

Der Inhalt von f sei $I(f) := g.g.T.(a_0, \ldots, a_n)$. Wenn $I(f) = 1$, so nennen wir f primitiv.

Lemma

Es gilt $I(fg) = I(f)I(g)$.

Teilen durch primitive Polynome

Lemma

Wenn $h \in K[x]$, $g \in R[x]$ primitiv und $f = gh \in R[x]$ ist, dann gilt $h \in R[x]$.

Teilen durch primitive Polynome

Lemma

Wenn $h \in K[x]$, $g \in R[x]$ primitiv und $f = gh \in R[x]$ ist, dann gilt $h \in R[x]$.

Lemma

Ist $f \in R[x]$ irreduzibel, so auch in $K[x]$.

Der Satz von Gauss

R - ein faktorieller Ring

Der Satz von Gauss

R - ein faktorieller Ring

Lemma

$R[x]$ is faktoriell.

Eisenstein

R - faktoriell mit dem Quotientenkörper K

Eisenstein

R - faktoriell mit dem Quotientenkörper K
$p \in R$ prim

Eisenstein

R - faktoriell mit dem Quotientenkörper K
$p \in R$ prim
$f = a_n x^n + \cdots + a_0 \in R[x]$, $n > 0$.

Eisenstein

R - faktoriell mit dem Quotientenkörper K
$p \in R$ prim
$f = a_n x^n + \cdots + a_0 \in R[x]$, $n > 0$.
$p | a_0, \ldots, p | a_{n-1}$ und $p^2 \nmid a_0$ und $p \nmid a_n$.

Eisenstein

R - faktoriell mit dem Quotientenkörper K
$p \in R$ prim
$f = a_n x^n + \cdots + a_0 \in R[x]$, $n > 0$.
$p|a_0, \ldots, p|a_{n-1}$ und $p^2 \nmid a_0$ und $p \nmid a_n$.

Lemma

f ist in $K[x]$ irreduzibel.

Irreduzibilität in Quotienten

$I \subset R$ - ein Ideal so daß R/I ein Integritätsbereich ist

Irreduzibilität in Quotienten

$I \subset R$ - ein Ideal so daß R/I ein Integritätsbereich ist
$f = a_n x^n + \cdots + a_0 \in R[x]$ primitiv mit $a_n \notin I$.

Irreduzibilität in Quotienten

$I \subset R$ - ein Ideal so daß R/I ein Integritätsbereich ist
$f = a_n x^n + \cdots + a_0 \in R[x]$ primitiv mit $a_n \notin I$.
$\bar{R} := R/I$

Irreduzibilität in Quotienten

$I \subset R$ - ein Ideal so daß R/I ein Integritätsbereich ist
$f = a_n x^n + \cdots + a_0 \in R[x]$ primitiv mit $a_n \notin I$.
$\bar{R} := R/I$
$\bar{f} \in \bar{R}[x]$

Irreduzibilität in Quotienten

$I \subset R$ - ein Ideal so daß R/I ein Integritätsbereich ist
$f = a_n x^n + \cdots + a_0 \in R[x]$ primitiv mit $a_n \notin I$.
$\bar{R} := R/I$
$\bar{f} \in \bar{R}[x]$

Lemma

Ist $\bar{f}$ irreduzibel in $\bar{R}[x]$, so ist $f \in K[x]$ irreduzibel.

K_n

K ein Körper

K_n

K ein Körper

Definition

Der n-te Einheitswurzelkörper über K ist der Zerfällungskörper K_n von $X^n - 1$. Die Nullstellen von $X^n - 1$ in K_n heißen n-te Einheitswurzeln. Die Erzeugenden der Gruppe μ_n der n-ten Einheitswurzeln heißen primitive Einheitswurzeln.

K_n

K ein Körper

Definition

Der n-te Einheitswurzelkörper über K ist der Zerfällungskörper K_n von $X^n - 1$. Die Nullstellen von $X^n - 1$ in K_n heißen n-te Einheitswurzeln. Die Erzeugenden der Gruppe μ_n der n-ten Einheitswurzeln heißen primitive Einheitswurzeln.

Corollary

Sei K ein Körper und $n \in \mathbb{N}$. Dann gibt es eine Erweiterung $K \subset L$ derart, daß L eine primitive n-te Einheitswurzel enthält.

μ_n

Ist $\zeta \in \mu_n$ primitiv, so gilt $K_n = K(\zeta)$.

μ_n

Ist $\zeta \in \mu_n$ primitiv, so gilt $K_n = K(\zeta)$.
Ist $\mathtt{char}(K) = p$ und $n = p^e m$ mit $e \geq 1$, so ist

$$x^n - 1 = 0 \Leftrightarrow x^{p^e m} - 1 = 0 \Leftrightarrow (x^m - 1)^p = 0 \Leftrightarrow X^m - 1 = 0 \ .$$

μ_n

Ist $\zeta \in \mu_n$ primitiv, so gilt $K_n = K(\zeta)$.
Ist $\mathtt{char}(K) = p$ und $n = p^e m$ mit $e \geq 1$, so ist

$$x^n - 1 = 0 \Leftrightarrow x^{p^e m} - 1 = 0 \Leftrightarrow (x^m - 1)^p = 0 \Leftrightarrow X^m - 1 = 0 \ .$$

Folglich gilt $|\mu_n(K)| \leq m < n$.

μ_n

Ist $\zeta \in \mu_n$ primitiv, so gilt $K_n = K(\zeta)$.
Ist $\mathtt{char}(K) = p$ und $n = p^e m$ mit $e \geq 1$, so ist

$$x^n - 1 = 0 \Leftrightarrow x^{p^e m} - 1 = 0 \Leftrightarrow (x^m - 1)^p = 0 \Leftrightarrow X^m - 1 = 0 \ .$$

Folglich gilt $|\mu_n(K)| \leq m < n$.
Wir betrachten jetzt nur den Fall, daß $\mathtt{char}(K) \not| n$.

μ_n

Ist $\zeta \in \mu_n$ primitiv, so gilt $K_n = K(\zeta)$.
Ist $\mathtt{char}(K) = p$ und $n = p^e m$ mit $e \geq 1$, so ist

$$x^n - 1 = 0 \Leftrightarrow x^{p^e m} - 1 = 0 \Leftrightarrow (x^m - 1)^p = 0 \Leftrightarrow X^m - 1 = 0 \ .$$

Folglich gilt $|\mu_n(K)| \leq m < n$.
Wir betrachten jetzt nur den Fall, daß $\mathtt{char}(K) \not| n$.
Dann gilt $f'(\xi) = n\zeta \neq 0$ für $\zeta \in \mu_n$. Die Nullstellen von f sind also einfach und $|\mu_n| = n$.

μ_n

Ist $\zeta \in \mu_n$ primitiv, so gilt $K_n = K(\zeta)$.
Ist $\mathtt{char}(K) = p$ und $n = p^e m$ mit $e \geq 1$, so ist

$$x^n - 1 = 0 \Leftrightarrow x^{p^e m} - 1 = 0 \Leftrightarrow (x^m - 1)^p = 0 \Leftrightarrow X^m - 1 = 0 \ .$$

Folglich gilt $|\mu_n(K)| \leq m < n$.
Wir betrachten jetzt nur den Fall, daß $\mathtt{char}(K) \not| n$.
Dann gilt $f'(\xi) = n\zeta \neq 0$ für $\zeta \in \mu_n$. Die Nullstellen von f sind also einfach und $|\mu_n| = n$.
μ_n ist eine Untergruppe von K_n^* und deshalb zyklisch. Es gibt $\varphi(n)$ primitive Einheitswurzeln.

Φ_n

Definition

Das n-te Kreisteilungspolynom ist durch

$$\Phi_n := \prod_{i=1}^{\varphi(n)} (x - \zeta_i)$$

definiert.

Φ_n

Definition

Das n-te Kreisteilungspolynom ist durch

$$\Phi_n := \prod_{i=1}^{\varphi(n)} (x - \zeta_i)$$

definiert.

Lemma

1. *Es gilt* $\Phi_n \in \mathbb{Z}[x]$ *falls* $\mathrm{char}(K) = 0$ *und* $\Phi_n \in \mathbb{F}_p[x]$ *falls* $\mathrm{char}(K) = p$.
2. *Weiterhin*

$$x^n - 1 = \prod \Phi_d \ .$$

Φ_n

Definition

Das n-te Kreisteilungspolynom ist durch

$$\Phi_n := \prod_{i=1}^{\varphi(n)} (x - \zeta_i)$$

definiert.

Lemma

1. *Es gilt* $\Phi_n \in \mathbb{Z}[x]$ *falls* $\mathtt{char}(K) = 0$ *und* $\Phi_n \in \mathbb{F}_p[x]$ *falls* $\mathtt{char}(K) = p$.
2. *Weiterhin*

$$x^n - 1 = \prod \Phi_d \ .$$

Φ_n

Lemma

1. *Es gilt* $\Phi_n \in \mathbb{Z}[x]$ *falls* $\mathtt{char}(K) = 0$ *und* $\Phi_n \in \mathbb{F}_p[x]$ *falls* $\mathtt{char}(K) = p$.
2. *Weiterhin*

$$x^n - 1 = \prod_{d|n} \Phi_d \ .$$

Φ_n

Lemma

1. *Es gilt* $\Phi_n \in \mathbb{Z}[x]$ *falls* $\mathtt{char}(K) = 0$ *und* $\Phi_n \in \mathbb{F}_p[x]$ *falls* $\mathtt{char}(K) = p$.
2. *Weiterhin*

$$x^n - 1 = \prod_{d|n} \Phi_d \ .$$

Lemma (Gauß,Dedekind)

Φ_n *in* $\mathbb{Q}[x]$ *ist irreduzibel.*

Algebraische und Transzendente Erweiterungen

$K \subset L$ - eine Erweiterung

Algebraische und Transzendente Erweiterungen

$K \subset L$ - eine Erweiterung
$\alpha \in L \setminus K$

Algebraische und Transzendente Erweiterungen

$K \subset L$ - eine Erweiterung
$\alpha \in L \setminus K$
$\phi_\alpha : K[x] \to L$ durch $\phi_\alpha(f) := f(\alpha)$. Sei $I_\alpha := \texttt{ker}(\phi_\alpha)$

Algebraische und Transzendente Erweiterungen

$K \subset L$ - eine Erweiterung
$\alpha \in L \setminus K$
$\phi_\alpha : K[x] \to L$ durch $\phi_\alpha(f) := f(\alpha)$. Sei $I_\alpha := \texttt{ker}(\phi_\alpha)$
$I_\alpha = (f_\alpha)$

Algebraische und Transzendente Erweiterungen

$I_\alpha = (f_\alpha)$

Definition

Das Element α heißt transzendent über K, falls $I_\alpha = 0$. Andernfalls heißt α algebraisch. Der normierte Erzeuger f_α ist in diesem Fall das Minimalpolynom von α.

Algebraische und Transzendente Erweiterungen

Definition

Das Element α heißt transzendent über K, falls $I_\alpha = 0$. Andernfalls heißt α algebraisch. Der normierte Erzeuger f_α ist in diesem Fall das Minimalpolynom von α.

Corollary

Ist α transzendent, so gilt $K(\alpha) \cong K[x]$. Andernfalls ist f_α ist irreduzibel und $K(\alpha) \cong K_{f_\alpha}$. Es gilt $[K(\alpha) : K] = \deg(f_\alpha)$.

Algebraische und Transzendente Erweiterungen

Theorem

1. *e ist transzendent.(Hermite, 1873)*
2. *π ist transzendent. (Lindemann, 1882)*

Galoisgruppen

$\mathtt{char}(K) \nmid n$ und $K_n = K(\zeta)$

Galoisgruppen

$\mathtt{char}(K) \not| n$ und $K_n = K(\zeta)$
f - ein Minimalpolynom von ζ

Galoisgruppen

$\mathtt{char}(K) \nmid n$ und $K_n = K(\zeta)$
f - ein Minimalpolynom von ζ
$K_f = K(\zeta)$

Galoisgruppen

$\mathtt{char}(K) \nmid n$ und $K_n = K(\zeta)$
f - ein Minimalpolynom von ζ
$K_f = K(\zeta)$
$\zeta_1 := \zeta, \zeta_2, \ldots, \zeta_m$ -die Wurzeln von f, $\deg(f) = m$.

Galoisgruppen

$\mathtt{char}(K) \nmid n$ und $K_n = K(\zeta)$
f - ein Minimalpolynom von ζ
$K_f = K(\zeta)$
$\zeta_1 := \zeta, \zeta_2, \ldots, \zeta_m$ -die Wurzeln von f, $\deg(f) = m$.
Durch $\zeta \mapsto \zeta_i$ wird also ein Automorphismus σ_i von $K(\zeta)/K$ induziert und umgekehrt.

Galoisgruppen

$\mathrm{char}(K) \nmid n$ und $K_n = K(\zeta)$
f - ein Minimalpolynom von ζ
$K_f = K(\zeta)$
$\zeta_1 := \zeta, \zeta_2, \ldots, \zeta_m$ -die Wurzeln von f, $\deg(f) = m$.
Durch $\zeta \mapsto \zeta_i$ wird also ein Automorphismus σ_i von $K(\zeta)/K$ induziert und umgekehrt.

Definition

Sei $Gal(K(\zeta)/K)$ die Gruppe dieser Automorphismen.

Galoisgruppen

Lemma

Es gilt $|Gal(K(\zeta)/K)| = m$. *Insbesondere, wenn* $K = \mathbb{Q}$ *ist, so gilt* $|Gal(\mathbb{Q}(\zeta)/\mathbb{Q})| = \varphi(n)$.