

Algebra I

Vorlesung von **Prof. Dr. Klaus Bongartz** im Sommersemester 2001
Eine Mitschrift von Sven Blumberg

9. September 2001

Inhaltsverzeichnis

| | | |
|----------|---|-----------|
| 0 | Kurzer historischer Überblick über die Anfänge der Algebra | 1 |
| 1 | Gruppen | 3 |
| 1.1 | Grundlegende Begriffe und Definitionen | 3 |
| 1.2 | Die Sätze von Sylow | 9 |
| 1.3 | Die symmetrische und alternierende Gruppe | 11 |
| 1.4 | Auflösbare Gruppen | 13 |
| 2 | Ringe | 15 |
| 2.1 | Grundlegende Definitionen und Tatsachen | 15 |
| 2.2 | Teilbarkeitslehre | 17 |
| 3 | Polynomringe | 20 |
| 4 | Brüche | 22 |
| 4.1 | Endlich erzeugte Moduln über Hauptidealringen | 23 |
| 5 | Körpertheorie | 27 |
| 5.1 | Grundlegende Definitionen | 27 |
| 5.2 | Körpererweiterung | 27 |
| 5.3 | Konstruktionen mit Zirkel und Lineal | 29 |
| 5.4 | Der algebraische Abschluss | 31 |
| 5.5 | Separable Elemente und separable Körpererweiterungen | 33 |
| 5.6 | Zerfällkörper und normale Erweiterungen | 33 |
| 5.7 | Der Hauptsatz der Galoistheorie | 35 |
| 5.8 | Folgerungen aus dem Hauptsatz und Beispiele | 35 |
| A | Ergänzungen | 37 |

Kapitel 0

Kurzer historischer Überblick über die Anfänge der Algebra

1. **Problemkreis** Formeln für Nullstellen von Polynomen ("Cardanosche Formeln")

2. **Problemkreis** Konstruktionen mit Zirkel und Lineal

- Dreiteilung eines Winkels
- Würfelerdoppelung
- Quadratur des Kreises
- Konstruktionen von regelmäßigen n-Ecken (Satz von Gauss liefert hierbei die n, für die dies möglich ist).

Wir wollen uns nun einleitend mit dem ersten Problemkreis beschäftigen:

Gesucht sind Nullstellen von $f(x) = x^2 + px + q$, wobei $p, q \in k$ ($= \mathbb{Q}, \mathbb{R}, \mathbb{C}$), d.h. gesucht ist $x \in k$ mit $f(x) = 0$

1. **Problem** keine Existenz z.B. $x^2 - 2 = 0$ in $k = \mathbb{Q} \Rightarrow$ Konstruiere \mathbb{R}

2. **Problem** $f(x) = x^2 + 1$ mit $k = \mathbb{R} \Rightarrow$ es gibt keine Nullstelle von f in $k \Rightarrow$ Konstruiere \mathbb{C}

Der Fundamentalsatz der Algebra sagt nun, dass jedes Polynom f mit Koeffizienten in \mathbb{C} eine Nullstelle in \mathbb{C} besitzt!

Das Problem in der Renaissance war formalerer Natur:

Gib Rezept an, um die Nullstelle mit Hilfe von Wurzeln aus Ausdrücken in Koeffizienten des Polynoms zu erhalten. Dabei stellt für $a \in \mathbb{C}$ und in $n \in \mathbb{N}$ das Symbol $\sqrt[n]{a}$ für eine komplexe Zahl ζ mit $\zeta^n = a$. So ein ζ gibt es immer!

Ist $z = |z| \cdot e^{i\phi}$, so ist $z^n = |z|^n e^{i \cdot n \cdot \phi}$. Für $a = |a| \cdot e^{i\phi}$ ist also $\zeta = \sqrt[n]{|a|} \cdot e^{i \frac{\phi}{n}}$ eine gesuchte Zahl mit $\zeta^n = a$.

Alle Lösungen werden aus dieser erhalten durch Multiplikation mit einer sogenannten n-ten Einheitswurzel ρ , d.h. eine Lösung von $\rho^n = 1$.

Zurück zu quadratischen Gleichungen:

$$\begin{aligned}x^2 + px + q &= \left(x + \frac{p}{2}\right)^2 - \frac{p^2}{4} + q = 0 \\ \Rightarrow x \text{ Nullstelle} &\Leftrightarrow \left(x + \frac{p}{2}\right)^2 = \frac{p^2}{4} - q \\ &\Leftrightarrow x + \frac{p}{2} = \pm \sqrt{\frac{p^2}{4} - q} \\ &\Leftrightarrow x = -\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q}\end{aligned}$$

Von $x^3 + ay^2 + by + c$ sind die Nullstellen gesucht, nach Übungen von $y \rightarrow y'$ wie $y' := y + \alpha$ kann man $a = 0$ annehmen. Also vorgelegt

$$y^3 + ay + b \tag{1}$$

Führe zwei neue Unbekannte u, v ein und setze

$$y + uv \tag{2}$$

eingesetzt ergibt sich:

$$\begin{aligned} (u + v)^3 + a(u + v) + b &= u^3 + 3u^2v + 3uv^2 + v^3 + a(u + v) + b \\ &= u^3 + v^3 + (3uv + a)(u + v) + b \end{aligned} \tag{3}$$

Bestimme u, v durch

$$3uv = -1 \tag{4}$$

aus (3) ergibt sich dann

$$u^3 + v^3 = -b \tag{5}$$

nun ist

$$\begin{aligned} (u^3 - v^3)^2 &= (u^3 + v^3)^2 - 4u^3v^3 \\ &= b^2 + 4\frac{a^3}{27} \end{aligned} \tag{6}$$

zur Abkürzung

$$R := \frac{b^2}{4} + \frac{a^3}{27} \tag{7}$$

Es ergibt sich

$$\begin{aligned} u^3 - v^3 &= 2\sqrt{R} \\ u^3 + v^3 &= -b \\ \Rightarrow u^3 &= \sqrt{R} - \frac{b}{2} \\ u &= \sqrt[3]{\sqrt{R} - \frac{b}{2}} \text{ aus (4) ergibt sich } v \end{aligned}$$

Man erhält dann für $y = u+v$

$$y = \sqrt[3]{-\frac{b}{2} + \sqrt{R}} + \sqrt[3]{-\frac{b}{2} - \sqrt{R}} \text{ ist eine Nullstelle}$$

Dies nennt man die Formel von Cardano

Ähnliche Formeln gibts für Nullstellen von Polynomen vierten Grades.

Satz von Gauss und Abel Es existiert im allgemeinen keine Formel für Nullstellen eines Polynomes mit Hilfe von Wurzelausdrücken, sobald $\text{grad}(p) \geq 5$

Kapitel 1

Gruppen

1.1 Grundlegende Begriffe und Definitionen

Definition 1.1

Eine Gruppe G ist ein Tupel (G, \cdot, e) bestehend aus einer Menge G , einer Abbildung $\cdot : G \times G \rightarrow G$ und ein Element $e \in G$ mit folgender Eigenschaft (wir schreiben im Folgenden gh statt $g \cdot h$):

1. $(gh)k = g(hk) \forall g, h, k \in G$ (Assoziativität)
2. $eg = ge = g \forall g \in G$ (Neutrales Element)
3. $\forall g \in G \exists h \in G$ so dass $gh = hg = e$ (Existenz des Inversen)

Bemerkung 1.2

1. e und h sind eindeutig bestimmt. Man schreibt statt h auch g^{-1} und nennt g^{-1} das Inverse
2. Es gilt sogar eine allgemeine Assoziativität in dem Sinne, dass es bei einem Produkt $g_1 g_2 \cdots g_n$ nicht auf die Klammerung ankommt, d.h.

$$g_1(g_2(g_3 g_4)) = g_1((g_2 g_3)g_4) = \dots$$

3. Man kommt mit sparsameren Axiomen aus.

Definition 1.3

Eine Gruppe heisst kommutativ oder abelsch $:\Leftrightarrow$

$$gh = hg \quad \forall g, h \in G$$

Bemerkung 1.4

1. Ist $M \neq \emptyset$ eine Menge, so ist $S(M) = \{f \mid f : M \rightarrow M \text{ bijektiv}\}$ eine Gruppe unter der Abbildung $fg := f \circ g$ und

$$\begin{aligned} id_M : M &\longrightarrow M \\ m &\longmapsto m \end{aligned}$$

ist neutrales Element und das Inverse zu f bezüglich der Multiplikation ist gerade die inverse Abbildung f^{-1} zu f . $S(M)$ heißt die symmetrische Gruppe zu M oder Gruppe der Permutationen von M . Elemente aus $S(M)$ heißen Permutationen.

2. Sei k ein Körper, V ein k -Vektorraum und $n \in \mathbb{N}$. Dann ist

$$GL(V) := \{f \mid f : V \rightarrow V \text{ bijektiv und linear}\}$$

eine Gruppe mit der Komposition als Multiplikation (vgl. 1)

3. Sei k ein Körper und $n \in \mathbb{N}$. Dann ist

$$\begin{aligned} GL_n(k) &:= \{A \mid A \in k^{n \times n} \text{ A invertierbar}\} \\ &= \{A \mid A \in k^{n \times n} \text{ det}(A) \neq 0\} \end{aligned}$$

eine Gruppe mit der Matrixmultiplikation

4. Für $M = \{1, \dots, n\}$ schreibt man S_n statt $S(M)$. Man hat dann die Zykelschreibweise. Für $n \geq 3$ ist S_n nicht kommutativ

$$\begin{aligned} (12)(23) &= (123) \\ (23)(12) &= (132) \end{aligned}$$

Analog ist $GL(V)$ nicht kommutativ für $\dim(V) \geq 2$.

5. Ist G abelsch, so benutzt man für die Verknüpfung oft das Zeichen $+$, für 0 das Symbol 0 und für g^{-1} das Symbol $-g$. Mit anderen Worten: Abelsche Gruppen schreibt man oft additiv statt multiplikativ.

6. \mathbb{Z} versehen mit gewöhnlicher Addition als Verknüpfung ist eine abelsche Gruppe

Definition 1.5

Sei G eine Gruppe

1. Eine Teilmenge $U \subset G$ heißt Untergruppe, falls

- (a) $e \in U$
- (b) $x, y \in U \Rightarrow xy \in U$
- (c) $x \in U \Rightarrow x^{-1} \in U$

Man schreibt dann hier $U \leq G$

2. Ist $M \leq G$ eine beliebige Teilmenge, so ist die von M erzeugte Untergruppe $\langle M \rangle$ definiert als

$$\langle M \rangle = \bigcap_{\substack{U \supset M \\ U \leq G}} U$$

Bemerkung 1.6

1. Ist U_i $i \in I$, eine Familie von Untergruppen, so ist $\bigcap_{i \in I} U_i$ auch Untergruppe. Also ist $\langle M \rangle$ überhaupt eine Untergruppe von G für $M \subset \langle M \rangle$ erfüllt. Ist U eine beliebige Untergruppe mit $U \supset M$, so $U \supset \langle M \rangle$. Also $\langle M \rangle$ kleinste Untergruppe von G , die M enthält, also eindeutig. Eine konkrete Beschreibung von $\langle M \rangle$ ist

$$\langle M \rangle = \{g_1 g_2 \cdots g_n \mid n \in \mathbb{N}, g_i \in M, g_i^{-1} \in M\}$$

2. $GL_n(k)$ hat $SL_n(k) = \{A \mid \det(A) = 1\}$ als Untergruppe

3. S_n hat $A_n = \{\pi \mid \pi \text{ gerade Permutation}\}$ als Untergruppe

4. $GL_n \geq O_n(\mathbb{R}) = \{A \mid A^T = A^{-1}\} \geq \{A \in O_n(\mathbb{R}) \mid \det(A) = 1\}$

5. $\mathbb{Z} \geq n\mathbb{Z} = \{nz \mid z \in \mathbb{Z}\} \forall n \in \mathbb{N}$

Definition 1.7

Eine Gruppe G operiert (von links) auf einer Menge M , falls man eine Abbildung $\nu: G \times M \rightarrow M$ hat mit $(\nu(g, m) =: gm)$

1. $em = m$

$\forall m \in M$

$$2. (gh)m = g(hm)$$

$$\forall g, h \in G, m \in M$$

Für $m \in M$ heißt

$$\text{Stab}(m) := \{g \mid g \in G, gm = m\}$$

der Stabilisator (Isotropiegruppe) und

$$G_m := \{gm \mid g \in G\}$$

die Bahn (der Orbit) von m unter G .

Bemerkung 1.8

$$1. \text{Stab}(m) \leq G$$

$$2. G = GL_n(\mathbb{C}), M = \mathbb{C}^{n \times n} \text{ mit}$$

$$\begin{aligned} \cdot : G \times M &\longrightarrow M \\ (g, A) &\longmapsto gAg^{-1} \end{aligned}$$

Operation durch Konjugation

$$(a) IAI^{-1} = A$$

$$(b) (gh)A = ghA(gh)^{-1} = ghAh^{-1}g^{-1}$$

Die Bahnen sind die Ähnlichkeitsklassen von Matrizen

$$3. M \text{ beliebig, } G = S(M). \text{ Dann operiert } G \text{ auf } M \text{ durch}$$

$$gm = g(m)$$

Es gibt nur eine Bahn.

$$4. G \text{ sei Gruppe, } H \leq G. \text{ Dann operiert } H \text{ von links auf } G \text{ via Translation, d.h.}$$

$$\begin{aligned} \cdot : H \times G &\longrightarrow G \\ (h, g) &\longmapsto hg \end{aligned}$$

Die Bahn von $g \in G$ ist dann

$$Hg = \{hg \mid h \in H\}$$

und heißt Rechtsnebenklasse von g bezüglich H . Die Abbildung

$$\begin{aligned} \cdot : H &\longrightarrow Hg \\ h &\longmapsto hg \end{aligned}$$

ist eine Bijektion. Mit $H \backslash G$ bezeichnet man die Menge aller Rechtsnebenklassen von G nach H

Lemma 1

G operiere auf M (M heißt dann G -Menge). Dann wird durch

$$m \sim m' \Leftrightarrow \exists g \in G : gm = m'$$

eine Äquivalenzrelation auf M definiert, deren Äquivalenzklassen gerade die Bahnen sind. Insbesondere ist M die disjunkte Vereinigung der Bahnen.

Beweis. klar! □

Satz 2 (Lagrange)

Für eine endliche Gruppe G mit Untergruppe H gilt

$$|G| = |H| \cdot |H \backslash G|$$

Insbesondere ist somit $|H|$ ein Teiler von $|G|$.

Beweis. Lasse H von links auf G via Translation operieren. Dann ist nach Lemma 1.9 G die disjunkte Vereinigung der Bahnen, d.h. der Rechtsnebenklassen Hg_1, \dots, Hg_n , d.h.

$$\begin{aligned} G &= \bigcup_{i=1}^n Hg_i \\ \Rightarrow |G| &= \sum_{i=1}^n |Hg_i| = t|H| \end{aligned}$$

da $\cdot : H \rightarrow Hg_i$ bijektiv ist, dabei ist $t = |H \backslash G|$ □

Wichtiger Spezialfall Sei G eine Gruppe, $H \leq G$ eine Untergruppe und eine Abbildung

$$\begin{aligned} H \times G &\longrightarrow G \\ (h, g) &\mapsto hg \end{aligned}$$

gegeben, die Linkstranslation, die Bahnen Hg sind die Rechtsnebenklassen. Analog kann man eine Rechtsoperation definieren

$$\begin{aligned} M \times G &\longrightarrow M \\ (m, g) &\mapsto mg \end{aligned}$$

mit

$$\begin{aligned} me &= m \quad \forall m \\ m(gh) &= (mg)h \quad \forall g, h \in G \quad m \in M \end{aligned}$$

sind die Bahnen in G definiert als $M \backslash G$

Bemerkung 1.9

$\lambda : G \times M \rightarrow M$ Linksoperation. Dann gehört dazu eine Rechtsoperation $\rho : M \times G \rightarrow M$ definiert durch

$$\rho(m, g) := \lambda(g^{-1}, m)$$

Umgekehrt gewinnt man durch $gm := mg^{-1}$ aus einer Rechtsoperation eine Linksoperation.

Speziell: $H \leq G$ operiert von rechts auf G durch Rechtstranslation

$$\begin{aligned} G \times H &\longrightarrow G \\ (g, h) &\mapsto gh \end{aligned}$$

Die Bahnen sind die Linksnebenklassen gH . Man hat eine Bijektion

$$\begin{aligned} H \backslash G &\cong G \backslash H \\ Hg &\mapsto (Hg)^{-1} = g^{-1}H \end{aligned}$$

Insbesondere gilt

$$|H \backslash G| = |G \backslash H| =: (G : H)$$

Definition 1.10

$(G : H)$ heißt Index von H in G

Definition 1.11

1. Eine Abbildung $f : G \rightarrow G'$ zwischen Gruppen heißt Homomorphismus $:\Leftrightarrow$

$$f(gh) = f(g)f(h) \quad \forall g, h \in G$$

2. Der Kern von f ist definiert als

$$\text{Kern}(f) = f^{-1}(e) = \{g \in G \mid f(g) = e\}$$

3. Das Bild von f ist definiert als

$$\text{Bild} = f(G) = \{f(g) \mid g \in G\}$$

4. Eine Untergruppe N von G heißt normal, falls

$$g^{-1}Ng = N \quad \forall g \in G$$

Man schreibt dann

$$N \trianglelefteq G$$

5. Für beliebige Teilmengen U, V von G sei

$$U \cdot V := \{uv \mid u \in U, v \in V\}$$

Ist dabei $U = \{u\}$ oder $V = \{v\}$ schreibt man auch uV oder Uv .

Lemma 3

Sei $f : G \rightarrow G'$ ein Gruppenhomomorphismus. Dann gilt:

1. $f(e) = e$, $f(g^{-1}) = (f(g))^{-1} \quad \forall g \in G$
2. Ist $N' \trianglelefteq G'$ oder $U' \leq G'$, so ist $f^{-1}(N') \trianglelefteq G$ und $f^{-1}(U') \leq G$, insbesondere ist $\text{Kern}(f) \trianglelefteq G$
3. Ist $U \leq G$, so ist $f(U) \leq G'$ (Achtung: für Normalität gilt etwas äquivalentes im allgemeinen nicht!)
4. f injektiv $\Leftrightarrow \text{Kern}(f) = \{e\}$

Definition 1.12

1. Ein Homomorphismus $f : G \rightarrow G'$ heißt Isomorphismus $:\Leftrightarrow f$ ist bijektiv.
2. Zwei Gruppen G, G' heißen isomorph $:\Leftrightarrow \exists$ Isomorphismus $f : G \rightarrow G'$, man schreibt in diesem Fall

$$G \cong G'$$

Lemma 4

Sei $N \trianglelefteq G$. Dann kann man auf G/N durch

$$(gN)(hN) := ghN$$

eine Gruppenstruktur einführen. Versehen mit dieser Multiplikation heißt G/N die Faktorgruppe von G nach N . Die sogenannte Projektion

$$\begin{aligned} \pi : G &\longrightarrow G/N \\ g &\longmapsto gN \end{aligned}$$

mit $\text{Kern}(\pi) = N$ ist ein surjektiver Homomorphismus. Ein Homomorphismus $f : G \rightarrow G'$ faktorisiert genau dann über π , d.h. es gibt genau einen Homomorphismus $f' : G/N \rightarrow G'$ mit

$$f' \circ \pi = f$$

falls $N \subset \text{Kern}(f)$. Man sagt, das folgende Dreieck kommutiert

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ \pi \searrow & & \nearrow f' \\ & G/N & \end{array}$$

Bemerkung 1.13

Sei M eine G -Menge. Dann assoziiert man dazu einen Homomorphismus

$$\begin{aligned} \phi : G &\longrightarrow S(M) \\ \phi(g)(m) &:= gm \quad \forall m \in M \end{aligned}$$

Es ist klar, dass dies ein Homomorphismus ist. Umgekehrt erhält man aus jedem Homomorphismus

$$\phi : G \longrightarrow S(M)$$

eine Links-Operation via

$$gm := \phi(g)(m)$$

Satz 5 (Homomorphiesatz)

Sei $f : G \rightarrow G'$ ein Homomorphismus mit $N = \text{Kern}(f)$. Sei $\pi : G \rightarrow G/N$ die kanonische Projektion, $i : \text{Bild}(f) \rightarrow G'$ die Inklusion, dann folgt: Es gibt genau einen Isomorphismus

$$\begin{aligned} f' : G/N &\longrightarrow \text{Bild}(f) \\ f &= i \circ f' \circ \pi \end{aligned}$$

Insbesondere gilt also

$$G/\text{Kern}(f) \cong \text{Bild}(f)$$

Satz 6 (Isomorphiesätze von E. Noether)

Sei G eine Gruppe

1. Sind $U \leq G$ und $N \leq G$, dann folgt $NU = UN \leq G$ und

$$U/U \cap N \cong UN/N$$

(Erster Isomorphiesatz)

2. Sind $N \leq G$, $M \leq G$ und $N \subset M$, dann folgt

$$(G/N)/(M/N) \cong G/M$$

(Zweiter Isomorphiesatz oder Kürzungssatz)

Definition 1.14

Eine Gruppe G heißt zyklisch, falls es ein $g \in G$ mit $G = \langle g \rangle$ gibt, d.h.

$$G = \langle g^i, i \in \mathbb{Z} \rangle$$

dabei heißt g Erzeuger von G .

Lemma 7

Bis auf Isomorphie gibt es genau die folgenden zyklischen Gruppen

$$(\mathbb{Z}, +) \text{ und } (\mathbb{Z}/n\mathbb{Z}, +) \quad \forall n \geq 1$$

Definition 1.15

In $\mathbb{Z}/n\mathbb{Z}$ schreibt man meist $\bar{x} = x + n\mathbb{Z}$, ferner bedeutet

$$a \equiv b(n) \quad \text{oder} \quad a \equiv b \pmod{n}$$

einfach $\bar{a} = \bar{b}$ in $\mathbb{Z}/n\mathbb{Z} \Leftrightarrow n|a - b$.

1.2 Die Sätze von Sylow

Definition 1.16

1. Zwei G -Mengen M und N heißen isomorph $:\Leftrightarrow \exists$ eine Bijektion

$$\begin{aligned} f : M &\longrightarrow N \text{ mit} \\ f(gm) &= gf(m) \quad \forall g \in G, m \in M \end{aligned}$$

2. Eine G -Menge heißt transitiv, falls G nur eine Bahn besitzt. Man sagt G operiert transitiv.

Lemma 1 (Bahnenlemma)

G operiere auf M . Sei $m \in M$ und $Gm = \{gm \mid g \in G\}$ die zugehörige Bahn, $H = \text{Stab}_G(m) = \{g \in G \mid gm = m\}$ der Stabilisator, dann gilt

1. $\text{Stab}(gm) = g\text{Stab}(m)g^{-1} \quad \forall g \in G$.
(Punkte in derselben Bahn haben konjugierte Stabilisatoren)
2. Die Abbildung $gG \mapsto gm$ liefert einen Isomorphismus von G -Mengen $G/H \cong Gm$, wobei G auf G/H durch Linkstranslation operiert.
Insbesondere ist für $|G| < \infty$ die Bahnenlänge $|Gm| = (G : H)$ ein Teiler der Gruppenordnung $|G|$

Bemerkung 1.17

Man hat eine Bijektion zwischen

$$\{\text{Isoklassen transitiver } G\text{-Mengen}\} \cong \{\text{Konjugationsklassen von Untergruppen}\}$$

Definition 1.18

Sei G eine Gruppe, p eine Primzahl

1. Das Zentrum von G ist definiert durch

$$Z(G) = \{g \in G \mid gh = hg \quad \forall h \in G\}$$

$g \in Z(G)$ heißt dann zentral.

2. Für $U \leq G$ ist der Normalteiler

$$N_G(U) = \{g \in G \mid gUg^{-1} = U\}$$

die größte Untergruppe von G , in der U normale Untergruppe ist.

3. Eine Gruppe U heißt p -Gruppe, falls $|U| = p^n$, $n \in \mathbb{N}$
4. Sei $|G| < \infty$ und $|G| = p^n q$ mit teilerfremden p, q . Eine p -Sylowgruppe von G ist eine Untergruppe P von G mit $|P| = p^n$.

Satz 2 (Sätze von Sylow)

Sei $|G| = p^n q$ mit p Primzahl wie in Definition 2., dann gilt

1. Es gibt eine p -Sylowgruppe P in G
2. Ist $U \leq G$ eine p -Gruppe, so gibt es ein $g \in G$ mit $U \subset gPg^{-1}$
Insbesondere sind alle p -Sylowgruppen konjugiert.
3. Für die Anzahl der p -Sylowgruppen gilt:
 - (a) $N_p \equiv 1(p)$ d.h. $N_p = lp + 1$ für ein l
 - (b) $N_p = (G : N_G(P))$ ist Teiler von q

Lemma 3

Es sei G eine p -Gruppe, p eine Primzahl, dann gilt

1. $Z(G) \neq \{e\}$
2. Ist $|G| = p^n$, so gibt es $\forall i$ mit $1 \leq i \leq n$ ein $U_i \leq G$ mit $|U_i| = p^i$. Insbesondere gibt es zu jedem Teiler von $|G|$ eine Untergruppe dieser Ordnung.

Bemerkung 1.19

Ist $N \trianglelefteq G$ und $G \xrightarrow{\pi} G/N$ eine Projektion, so hat man eine Bijektion

$$\begin{aligned} \{\text{Untergruppe } U \text{ von } G/N\} &\cong \{\text{Untergruppe von } G, \text{ die } N \text{ enthalten}\} \\ U &\mapsto \pi^{-1}(U) \end{aligned}$$

Dabei werden Inklusionen erhalten und normale Untergruppen respektiert (d.h. Normalität bleibt erhalten).

Bemerkung 1.20

- 1.

Satz 4 (Satz von Cauchy)

Ist $|G| = p^n q$ mit p prim, $n \geq 1$, so $\exists x \in G$ der Ordnung p .

2. In S_5 gibt es keine Untergruppe der Ordnung 40. Es gibt also nicht zu jedem Teiler von $|G|$ eine Untergruppe dieser Ordnung.
3. I.a. sind Untergruppen gleicher Ordnung nicht zueinander konjugiert (z.B. die Diedergruppe)

Definition 1.21

Seien G, H Gruppen

1. Auf $G \times H$ definiert man eine Multiplikation durch

$$((g, h)(g', h')) = (gg', hh')$$

Dadurch wird $G \times H$ zu einer Gruppe und nennt sie das direkte Produkt von G und H .

2. Sei

$$\alpha : H \longrightarrow \text{Aut}(G)$$

eine Abbildung in die Automorphismen von G . Auf $G \times H$ definiert man eine Verknüpfung durch

$$(g, h)(g', h') := (g\alpha(h)g', hh')$$

dadurch wird auf $G \times H$ eine Gruppenstruktur definiert. Man schreibt dafür

$$G \rtimes_{\alpha} H$$

und nennt dies das semidirekte Produkt von G und H via α .

Bemerkung 1.22

Es ist

$$\begin{aligned}\phi : G &\hookrightarrow G \rtimes^{\alpha} H \\ g &\mapsto (g, e)\end{aligned}$$

dann folgt $G \cong \text{Bild}(\phi) \leq G \rtimes^{\alpha} H$, also

$$G \rtimes^{\alpha} H / \text{Bild}(\phi) \cong H$$

Lemma 5

Sei F eine Gruppe, $G \leq F$, $H \leq F$ mit

$$GH = F \quad G \cap H = \{e\}$$

dann gilt

1. Man hat einen Homomorphismus

$$\begin{aligned}\alpha : H &\longrightarrow \text{Aut}(G) \\ h &\mapsto \alpha(h)\end{aligned}$$

2. Die Abbildung

$$\begin{aligned}\phi : G \rtimes^{\alpha} H &\longrightarrow F \\ (g, h) &\mapsto gh\end{aligned}$$

ist ein Isomorphismus.

3. Ist $H \leq F$, dann folgt: α ist der triviale Homomorphismus und $G \times H \cong F$

1.3 Die symmetrische und alternierende Gruppe

Definition 1.23

1. Sei $\{a_1, \dots, a_l\}$ eine l -elementige Teilmenge von $\{1, \dots, n\}$. Unter einem Zyklus $z = (a_1, a_2, \dots, a_l)$ versteht man eine Permutation aus S_n mit

$$z(a_i) = a_{i+1} \quad 1 \leq i \leq l-1 \quad z(a_l) = a_1$$

und $z(x) = x$ für alle sonstigen x . Dabei heißt l die Zykluslänge und man schreibt $|z| = l$.

2. Eine Transposition ist ein Zyklus der Länge 2.
3. Zwei Zyklen heißen disjunkt, wenn die zugrunde liegenden Mengen der Zyklen disjunkt sind.

Bemerkung 1.24

1. Ab $n=11$ schreibt man Kommata.
2. Zyklische Vertauschung der Einträge liefert die gleiche Permutation. Das Inverse erhält man durch Umkehrung der Einträge
3. für $\pi \in S_n$ gilt

$$\pi(a_1, \dots, a_l)\pi^{-1} = (\pi a_1, \dots, \pi a_l)$$

Lemma 1

Jede Permutation ist Produkt von disjunkten Zykeln, wobei die Zerlegung bis auf Reihenfolge der Faktoren eindeutig ist.

Bemerkung 1.25

1-Zykeln lässt man weg

Definition 1.26

1. Sei n eine natürliche Zahl, dann ist eine Partition von n eine endliche Folge (n_1, \dots, n_r) von natürlichen Zahlen so dass $n_1 \geq n_2 \geq \dots \geq n_r \geq 1$ und

$$\sum_{i=1}^r n_i = n$$

2. Schreibt man $\pi \in S_n$ als Produkt disjunkter Zyklen

$$z = z_1 \dots z_r$$

mit $|z_1| \geq \dots \geq |z_r|$, wobei auch Zykeln der Länge 1 berücksichtigt werden, so heißt

$$|\pi| = (|z_1|, \dots, |z_r|)$$

die Zykelstruktur von π

Bemerkung 1.27

1. $|\pi|$ ist eine Partition von n .
2. Sei $P(n)$ die Menge aller Partitionen von n . Dann gibt es für die Anzahl der Elemente von $P(n)$ nur rekursive oder asymptotische Formeln, keine exakten!

Lemma 2

Sei n eine natürliche Zahl. Dann induziert die Abbildung $\pi \mapsto |\pi|$ eine Bijektion zwischen den Konjugationsklassen in S_n und $P(n)$

Definition 1.28

Wir definieren durch

$$\begin{aligned} \text{sgn} : S_n &\longrightarrow \{\pm 1\} \\ \pi &\longmapsto \prod_{i < j} \frac{\pi(i) - \pi(j)}{i - j} \end{aligned}$$

einen Homomorphismus. Der Kern von sgn heißt die alternierende Gruppe A_n . Die Elemente von A_n heißen gerade Permutationen

Bemerkung 1.29

1. Nach dem Homomorphiesatz gilt $S_n/A_n \cong \mathbb{Z}/2\mathbb{Z}$
2. Ist $\pi = z_1 \dots z_r$, so ist

$$\begin{aligned} \text{sgn}(\pi) &= \text{sgn}(z_1) \dots \text{sgn}(z_r) \\ \text{sgn}(\pi) &= (-1)^{|z_1|+1} \dots (-1)^{|z_r|+1} \end{aligned}$$

Definition 1.30

Eine Gruppe G heißt einfach, falls $\{e\}$ und G die einzigen normalen Untergruppen von G sind.

Lemma 3

1. S_n wird von Transpositionen erzeugt.
2. Für $n \geq 3$ wird A_n von 3-Zykeln erzeugt.
3. Ist $n \geq 5$ so sind alle 3-Zykeln in A_n zueinander konjugiert

Satz 4 (Abel)

Für $n \geq 5$ ist A_n einfach.

Bemerkung 1.31

1. Dies ist der tiefliegende Grund dafür, dass man für gewisse Polynome 5. Grades keinen Ausdruck für die Nullstellen finden kann, in dem nur die Koeffizienten des Polynoms und Wurzelausdrücke auftreten.
2. Für jede Primzahl p ist $\mathbb{Z}/p\mathbb{Z}$ einfach.

1.4 Auflösbare Gruppen

Bemerkung 1.32

Hat eine Gruppe G eine normale Untergruppe $\{e\} \neq N \neq G$, so setzt sich G in gewisser Weise aus N und G/N zusammen.

Gibt es z.B. eine Untergruppe U mit $U \rightarrow G/N$ unter $\pi : G \rightarrow G/N$, so ist $G \cong N \rtimes U$

Also sind die einfachen Gruppen die Bausteine, aus denen sich eine beliebige Gruppe wie oben zusammensetzt.

Definition 1.33

Sei G eine Gruppe

1. Eine Normalreihe der Länge m von G ist eine Kette

$$G = N_0 \supset \dots \supset N_m = \{e\}$$

von Untergruppen N_i mit $N_{i+1} \trianglelefteq N_i$.

2. Eine Kompositionsreihe K ist eine Normalreihe, bei der die Faktorgruppe N_i/N_{i+1} einfach ist für jedes i . Ist E eine einfache Gruppe, so bezeichnet die Vielfachheit von E in K

$$v(K, E) = \#\{i \mid N_i/N_{i+1} \cong E\}$$

Die E mit positiver Vielfachheit heißen Kompositionsfaktoren von K

Satz 1 (Jordan-Hölder)

Die Vielfachheit einer einfachen Gruppe ist nicht von der Kompositionsreihe abhängig, deren Länge eindeutig ist.

Definition 1.34

Wir definieren die Länge von G als die Länge einer Kompositionsreihe, falls G eine besitzt, sonst $lg(G) := \infty$. Die Vielfachheit von E ist $v(G, E) := v(K, E)$ für eine beliebige Kompositionsreihe K .

Bemerkung 1.35

1. Jede endliche Gruppe hat Kompositionsreihen
2. Zerlegung von Gruppen in Kompositionsreihen ist eindeutig!

Definition 1.36

Sei G eine Gruppe

1. Für $U, V \subset G$ setzt man

$$\begin{aligned} [U, V] &:= \langle [u, v] \rangle \\ [u, v] &:= uvu^{-1}v^{-1} \end{aligned}$$

die von Kommutatoren erzeugte Untergruppe

2. Setze $D^0G = G$ und $D^{i+1}G := [D^iG, D^iG]$. Man nennt D^iG die i -te derivierte Gruppe von G .

3. G heißt auflösbar, falls es ein m gibt mit $D^m G = \{e\}$

Bemerkung 1.37

1. u, v kommutieren genau dann, wenn ihr Kommutator das neutrale Element ist. G ist also genau dann abelsch, wenn $D^1 G = \{e\}$ gilt.
2. Derivation und Anwenden des Kommutators erhalten Normalheit.
3. $G/[G, G] =: G_{ab}$ ist abelsch

Satz 2

Sei G eine Gruppe, dann gilt

1. G ist auflösbar $\Leftrightarrow G$ besitzt eine Normalreihe mit abelschen Quotienten
2. Ist G auflösbar, dann auch jede Untergruppe von G
3. Ist $N \trianglelefteq G$, dann ist G auflösbar $\Leftrightarrow N$ und G/N sind auflösbar
4. Ist G endlich, dann ist G auflösbar \Leftrightarrow alle k -Faktoren von G sind von der Form $\mathbb{Z}/p\mathbb{Z}$ mit p Primzahl.

Bemerkung 1.38

1. Später assoziieren wir zu jedem Polynom f eine Gruppe $G(f) =$ Galois-Gruppe von f . Dann wird sich ergeben, dass die Nullstellen von f genau dann in Radikale auflösbar sind, wenn $G(f)$ auflösbar ist.
2. $[S_n, S_n] = A_n$, denn:
 $\forall \pi, \sigma$ ist $\text{sign}(\pi\sigma\pi^{-1}\sigma^{-1})=1$ also ist $[S_n, S_n] \leq A_n$. Nun genügt es zu zeigen, dass jeder Dreierzykel in S_n liegt, da die Dreierzykel A_n erzeugen. Es ist aber $(ab)(ac)(ab)(ac) = (bc)(ac) = (abc)$
3. Gesucht ist eine Kompositionsreihe von S_4 . Beginnen wir zunächst mit der normalen Untergruppe A_4 , nennen wir nun G_2 die Untergruppe, die aus den Permutationen besteht, die Produkt von zwei Transpositionen sind, so liegt auch dies normal in A_4 , sei nun noch G_3 die Gruppe, die von einem Dreierzyklus erzeugt wird, dann ist

$$\{e\} \trianglelefteq G_3 \trianglelefteq G_2 \trianglelefteq A_4 \trianglelefteq S_4$$

und es ist klar, dass die Quotienten abelsch sind, also ist S_4 auflösbar.

4. S_n ist für $n \geq 5$ nicht mehr auflösbar, da die erste derivierte Gruppe A_n einfach ist!
5. Es gibt Isomorphieklassen von Gruppen der Ordnung 8:

$$\mathbb{Z}/8\mathbb{Z}, \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, (\mathbb{Z}/2\mathbb{Z})^3, (\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z})/N, D_4$$

6. Es gibt nur endlich viele Gruppen der Ordnung n

Kapitel 2

Ringe

2.1 Grundlegende Definitionen und Tatsachen

Definition 2.1

Ein Ring ist ein 5-Tupel $(R, +, 0, \cdot, 1)$ mit

1. Einer nicht leeren Menge R
2. $+: R \times R \rightarrow R$ so dass
 - (a) $(R, +, 0)$ ist abelsche Gruppe
3. $\cdot: R \times R \rightarrow R$ mit
 - (a) \cdot ist assoziativ
 - (b) $1r = r1 = r$ für alle $r \in R$
4. Es gelten die Links- und Rechtsdistributivgesetze
5. Ist \cdot kommutativ, so heißt R kommutativ

Bemerkung 2.2

Ist $0 = 1$, so kann der Ring nur aus der 0 bestehen

Definition 2.3

Es sei R ein Ring, ein Element $x \in R$ heißt

1. Einheit, falls es ein y gibt, so dass $xy = yx = 1$. R^* bezeichne die Menge aller Einheiten in R .
2. nilpotent, falls $x^n = 0$ für eine natürliche Zahl n
3. Nullteiler, falls $x \neq 0$ und es ein $y \neq 0$ gibt, so dass $xy = 0$
4. Ein Ring heißt Körper $:\Leftrightarrow$
 - (a) R ist kommutativ
 - (b) $R^* = R \setminus \{0\}$

Definition 2.4

1. Ein Ringhomomorphismus ist eine Abbildung

$$\phi: R \rightarrow S$$

zwischen Ringen, die folgendes $\forall r, s \in R$ erfüllt

$$\begin{aligned}\phi(r + s) &= \phi(r) + \phi(s) \\ \phi(rs) &= \phi(r)\phi(s)\end{aligned}$$

Es bezeichne den Kern von ϕ

$$\text{Kern}(\phi) = \{x \in R \mid \phi(x) = 0\}$$

2. Ein Linksideal I ist eine Teilmenge eines Ringes mit

- (a) $0 \in I$
- (b) $x, y \in I \Rightarrow x + y, -x \in I$
- (c) $x \in I, r \in R \Rightarrow rx \in I$

Ein zweiseitiges Ideal ist ein Linksideal, für das gilt

- (a) $x \in I, r \in R \Rightarrow xr \in I$

In diesem Fall schreibt man $I \trianglelefteq R$

Bemerkung 2.5

1. In einem kommutativem Ring ist jedes Ideal zweiseitiges Ideal, sonst auch Rechtsideal
2. $\text{Kern}(\phi)$ ist zweiseitiges Ideal
3. Ist $I \trianglelefteq R$, so kann man auf $R/I = \{r + I\}$ nicht nur eine Addition (da I insbesondere normale Untergruppe ist), sondern auch eine Multiplikation einführen, durch:

$$\begin{aligned}(r + I) + (s + I) &= (r + s) + I \\ (r + I)(s + I) &= (rs)I\end{aligned}$$

4. Dabei ist die sogenannte kanonische Projektion

$$\begin{aligned}\pi : R &\longrightarrow R/I \\ r &\longmapsto r + I\end{aligned}$$

ein surjektiver Ringhomomorphismus mit $\text{Kern}(\pi) = I$.

5. Wie bei Gruppen gilt ein Homomorphiesatz

$$f : R \longrightarrow S$$

sei Ringhomomorphismus, ist dann $N = \text{Kern}(f)$ dann folgt es gibt genau einen Isomorphismus

$$\begin{aligned}f' : G/N &\longrightarrow \text{Bild}(f) \\ f &= i \circ f' \circ \pi\end{aligned}$$

Insbesondere gilt also

$$G/\text{Kern}(f) \cong \text{Bild}(f)$$

Definition 2.6

1. Ist R ein Ring mit einer Familie von Idealen I_j $j \in J$, so definieren wir

$$\sum_{j \in J} I_j := \{x \mid \exists n \exists j_1, \dots, j_n : x = x_{j_1} + \dots + x_{j_n}\}$$

Dies ist das kleinste Ideal, das alle I_j enthält. Sind alle Ideale zweiseitig, so auch ihre Summe.

2. Sind R_1, \dots, R_s Ringe, so trägt die Produktmenge $\prod_{i=1}^s R_i$ eine kanonische Ringstruktur:

$$\begin{aligned}(r_1, \dots, r_s) + (r'_1, \dots, r'_s) &= (r_1 + r'_1, \dots, r_s + r'_s) \\ (r_1, \dots, r_s)(r'_1, \dots, r'_s) &= (r_1 r'_1, \dots, r_s r'_s)\end{aligned}$$

Satz 1 (Chinesischer Restsatz)

Sei R ein Ring mit zweiseitigen Idealen I_1, \dots, I_s , ist dann $I_i + I_j = R$ für $i \neq j$. Dann ist die Abbildung

$$\begin{aligned}\phi : R &\longrightarrow \prod_{j=1}^s (R/I_j) \\ r &\longmapsto (r + I_1, r + I_2, \dots, r + I_s)\end{aligned}$$

surjektiv mit

$$\text{Kern}(\phi) = \bigcap_{i=1}^s I_i$$

Nach dem Homomorphiesatz gilt also insbesondere

$$R / \left(\bigcap_{i=1}^s I_i \right) \cong \prod_{j=1}^s (R/I_j)$$

2.2 Teilbarkeitslehre

Definition 2.7

Sei R ein kommutativer Ring mit Elementen $x, y \in R$

1. x teilt y , $x|y \Leftrightarrow \exists z \in R: xz = y$
2. R heißt Integritätsbereich oder nullteilerfrei, falls

$$xy = 0 \Rightarrow x = 0 \text{ oder } y = 0$$

3. Sei R Integritätsbereich, $x \notin R^* \setminus \{0\}$ heißt irreduzibel, falls

$$x = ab \Rightarrow a \in R^* \text{ oder } b \in R^*$$

4. Sei R Integritätsbereich, $x \notin R^* \setminus \{0\}$ heißt prim, falls

$$x|ab \Rightarrow x|a \text{ oder } x|b$$

5. x und y heißen assoziiert, falls $\exists z \in R^*$ mit $zx = y$. Man schreibt dann $x \sim y$

Bemerkung 2.8

1. Assoziiertheit ist eine Äquivalenzrelation und erhält Irreduzibilität und prim.
2. $\mathbb{Z}/n\mathbb{Z}$ Integritätsbereich $\Leftrightarrow n$ ist prim.
3. \mathbb{Z} ist Integritätsbereich aber kein Körper
4. Ist x prim $\Rightarrow x$ ist irreduzibel.

Definition 2.9

Sei R ein Integritätsbereich

1. Ein Element $x \in R$ besitzt eine Primfaktorzerlegung, falls x endliches Produkt von primen Elementen ist.
2. R heißt faktoriell $:\Leftrightarrow$ jedes von 0 verschiedene Element eine Primfaktorzerlegung besitzt.

Lemma 1

Sei R Integritätsbereich

1. Ist

$$\begin{aligned} x &= p_1 \cdots p_s \\ x &= q_1 \cdots q_r \end{aligned}$$

so folgt $s = r$ und nach Ummummern $p_i \sim q_i$

2. Ist R faktoriell, so fallen prim und Irreduzibilität zusammen.

Definition 2.10

Sei R ein kommutativer Ring

1. Ein Ideal m heißt maximal, falls aus $m \subset I \subseteq R$ stets $m = I$ oder $I = R$ folgt.
2. Ein Ideal I heißt von $r_1, \dots, r_n \in R$ erzeugt, falls I die Menge aller endlichen Linearkombinationen der r_i ist. Man schreibt dann $I = \langle r_1, \dots, r_n \rangle = (r_1, \dots, r_n)$
Für $n = 1$ heißt I das von r_1 erzeugte Hauptideal.
3. R heißt Hauptidealring, falls jedes Ideal Hauptideal ist.
4. Ein Ring heißt noethersch, falls jedes Ideal endlich erzeugt ist

Bemerkung 2.11

1. Ein Ideal M ist maximal $\Leftrightarrow R/M$ Körper ist.
2. $R = \mathbb{Z}$ ist Hauptidealring
3. $\mathbb{R}[x, y]$ ist kein Hauptidealring, aber noethersch.
4. Ist k Körper $\Rightarrow k[x]$ ist Hauptidealring

Lemma 2

Sei R kommutativer Ring, dann sind äquivalent

1. Jede aufsteigende Folge von Idealen wird stationär
2. Jede nicht-leere Menge von Idealen besitzt ein maximales Element
3. R ist noethersch

Satz 3

Jeder nullteilerfreie Hauptidealring ist noethersch

Definition 2.12

Sei R Integritätsbereich, $a, b \in R$

1. Ein Element $d \in R$ heißt ggT von a und b (a, b), falls
 - (a) $d|a$ und $d|b$
 - (b) $d'|a$ und $d'|b \Rightarrow d'|d$
2. Entsprechend kgV $[a, b]$ von a, b

Bemerkung 2.13

1. Weder kgV noch ggT müssen existieren. Jedoch wenn es sie gibt, dann sind sie eindeutig bis auf Einheiten.
2. In R gilt $x \sim y \Leftrightarrow (x) = (y)$

Lemma 4

Sei R nullteilerfreier Hauptidealring

1. $(a) + (b) = (a, b) = ((a, b))$ und $(a) \cap (b) = ([a, b])$
2. Sind a, b teilerfremd, so ist

$$R/(a \cdot b) \cong R/(a) \times R/(b)$$

3. b liefert eine Einheit in $R/(a)$ $\bar{b} = b + (a) \Leftrightarrow (a, b) = 1 \Leftrightarrow (a) + (b) = R$
4. $R/(a)$ ist Körper $\Leftrightarrow a$ prim oder ($a = 0$ und R Körper)

Definition 2.14

Die eulersche φ -Funktion

$$\varphi : \mathbb{N} \longrightarrow \mathbb{N}$$

ist definiert als

$$\varphi(n) = \#\{m \mid 1 \leq m \leq n, (m, n) = 1\}$$

Bemerkung 2.15

$\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|$ und da $(\mathbb{Z}/n\mathbb{Z})^* \cong \prod_{i=1}^n (\mathbb{Z}/p_i^{r_i}\mathbb{Z})^*$ wenn $n = p_1^{r_1} \dots p_n^{r_n}$ die Primfaktorzerlegung von n ist.

Also gilt

$$\varphi(n) = \prod_{i=1}^n \varphi(p_i^{r_i})$$

wobei für eine Primzahlpotenz p^n gilt

$$\varphi(p^n) = (p - 1)p^{n-1}$$

Kapitel 3

Polynomringe

Definition 3.1

Es sei R ein kommutativer Ring, definiere auf $R^{(\mathbb{N})} = \{f \mid f : \mathbb{N} \rightarrow R, f_i \neq 0 \text{ für fast alle } i\}$ eine Addition und Multiplikation durch:

$$\begin{aligned}(f + g)(i) &= f(i) + g(i) \\ (fg)(i) &= \sum_{j=0}^i f(j)g(i-j)\end{aligned}$$

offensichtlich sind beide wieder in $R^{(\mathbb{N})}$. Man verifiziert, dass hiermit $R^{(\mathbb{N})}$ ein kommutativer Ring wird.

Bemerkung 3.2

Definiert man nun für $X \in R^{(\mathbb{N})}$ durch

$$X(i) = \begin{cases} 1 & i = 1 \\ 0 & \text{sonst} \end{cases}$$

Dann gilt

$$X^i(j) = \begin{cases} 1 & i = j \\ 0 & \text{sonst} \end{cases}$$

setzt man nun $X^0 := (1, 0, \dots)$, so lässt sich jedes $f \in R^{(\mathbb{N})}$ schreiben als

$$f = \sum_{i=0}^n f_i X^i$$

Man schreibt dann auch $R[X]$, den Polynomring in einer Unbekannten über dem Ring R .

Definition 3.3

Ist $f \in R[X]$ mit $f = \sum_{i=0}^n f_i X^i$ mit $f_n \neq 0$, so ist der Grad von f

$$\text{grad}(f) := n$$

f_n heißt Leitkoeffizient. $\text{grad}(0) := -\infty$ und Polynome vom Grade kleiner gleich Null nennt man konstante Polynome.

Bemerkung 3.4

$\text{grad}(p + g) \leq \max\{\text{grad}(p), \text{grad}(g)\}$ und $\text{grad}(pq) = \text{grad}(p) + \text{grad}(q)$, falls R nullteilerfrei

Satz 5 (Division mit Rest)

Sei R Integritätsbereich. $q = q_0 + \dots + q_m X^m \in R[X]$, dann folgt $\forall p \in R[X] \exists! s, t$ so dass

$$p = sq + t$$

mit $\text{grad}(q) \leq \text{grad}(p)$

Bemerkung 3.5

Ist R ein Körper, so ist die Division mit Rest für jedes von Null verschiedene Element definiert.

Definition 3.6

Ein Integritätsbereich R heißt euklidisch, wenn es eine Abbildung

$$d : R \longrightarrow \mathbb{N}$$

gibt mit:

zu $p, q \in R$ mit $q \neq 0$, existierten $s, t \in R$ mit $p = sq + t$ mit $t = 0$ oder $d(t) < d(q)$.

Satz 6

Jeder euklidische Ring ist Hauptidealring und somit faktoriell.

Kapitel 4

Brüche

Definition 4.1

Sei R ein Integritätsbereich. Dann ist der Quotientenkörper $Q(R)$ wie folgt definiert

Auf $R \times R \setminus \{0\}$ definiert man die Äquivalenzrelation $(a, b) \sim (c, d) :\Leftrightarrow ad = cb$. Für die Äquivalenzklasse von (a, b) schreibt man dann $\frac{a}{b}$ und bezeichnet mit $Q(R)$ die Menge aller Äquivalenzklassen und definiert Addition und Multiplikation via

$$\begin{aligned}\frac{a}{b} + \frac{c}{d} &= \frac{ad + cb}{bd} \\ \frac{a}{b} \frac{c}{d} &= \frac{ac}{bd}\end{aligned}$$

Man rechnet die Wohldefiniertheit nach und erhält, dass $Q(R)$ zu einem Körper wird, in dem man R als Unterring durch $a \mapsto \frac{a}{1}$ einbetten kann.

Definition 4.2

Sei R ein kommutativer Ring. Eine R -Algebra ist ein Ringhomomorphismus $\phi : R \rightarrow A$ mit $\text{Bild}(\phi) \subset \text{Zentrum}(A)$. Man nennt dann auch A eine R -Algebra.

Bemerkung 4.3

Meistens ist ϕ injektiv, also nach dem Homomorphiesatz, $R \cong \phi(R)$. Man fasst dann R als Unterring von A auf.

Lemma 7

Sei R ein kommutativer Ring, $\varphi : R \rightarrow A$, $a \in A$. Dann gibt es genau einen Homomorphismus $\phi_a : R[X] \rightarrow A$ mit $\phi_a(r) = \varphi(r)$ für $R \subset R[X]$ und $\phi_a(X) = a$.

Definition 4.4

Sei R ein Integritätsbereich mit Quotientenkörper k , $p \in R[X]$. Ein Element $a \in k$ heißt Nullstelle von p , wenn $p(a) := \phi_a(p) = 0$.

Lemma 8

Sei $R = k$ ein Körper, $p \in k[X]$, a Nullstelle von p in K , dann folgt $p = (X - a)\tilde{p}$. Insbesondere hat ein Polynom vom Grad $n \geq 1$ höchstens n Nullstellen

Bemerkung 4.5

k sei Körper, P_k die k -Algebra der polynomialen Funktionen, dann hat man einen surjektiven Ringhomomorphismus $\psi : k[X] \rightarrow P_k$, $F \mapsto \psi(F)(a) = F(a)$.

Es ist $\text{Kern}(\psi) = \{0\}$ wenn $|k| = \infty$, in $\mathbb{Z}/(2)$ ist aber $X^3 - X \in \text{Kern}(\psi)$.

Definition 4.6

Sei R faktoriell, $f \in R[X]$ heißt primitiv, wenn der ggT der Koeffizienten 1 ist.

Lemma 9

Sei R faktoriell mit Quotientenkörper k , dann gilt:

1. Jedes f aus $k[X]$ hat eine Darstellung $f = \frac{a}{b} \tilde{f}$ mit $(a, b) = 1$ und \tilde{f} primitiv.
2. Das Produkt von primitiven Polynomen ist primitiv.

Satz 10

Sei R faktoriell mit Quotientenkörper k , dann ist auch $R[X]$ faktoriell, wobei die folgenden Elemente prim sind

1. $p \in R$ prim als konstantes Polynom aufgefaßt.
2. $f \in R[X]$ primitiv und irreduzibel in $k[X]$

Bemerkung 4.7

$k[X]$ ist euklidisch, als Hauptidealring, als faktoriell, also fallen prime und irreduzible Elemente zusammen.

Bemerkung 4.8

$f \in \mathbb{Z}[X]$ primitiv, dann gilt: f irreduzibel in $\mathbb{Z}[X] \Leftrightarrow f$ irreduzibel in $\mathbb{Q}[X]$.

4.1 Endlich erzeugte Moduln über Hauptidealringen

Definition 4.9

Sei R ein Hauptidealring. Man betrachte $\text{Mat}(m \times n, R)$, dann gibt es in der linearen Algebra bekannt 4 verschiedene (auch wenn die beiden ersten die alle erzeugen) elementare Zeilen- bzw. Spaltentransformationen

1. Multiplikation einer Zeile mit einer Einheit
2. Addition einer Zeile zu einer anderen Zeile
3. Addition des Vielfachen einer Zeile zu einer anderen Zeile
4. Vertauschen von Zeilen

analog erhält man die Spaltentransformationen durch Ersetzen von Zeile durch Spalte.

Bemerkung 4.10

1. Jede elementare Operation lässt sich rückgängig machen!
2. Jede elementare Operation lässt sich durch Multiplikation mit einer Elementarmatrix von links (Zeilenoperation) bzw. von rechts (Spaltenoperation) rückgängig machen.

Satz 1 (Elementarteilersatz)

Sei R ein nullteilerfreier Hauptidealring, dann folgt jede Matrix $M \in \text{Mat}(m \times n, R)$ lässt sich durch elementare Zeilenoperationen auf folgende Gestalt bringen

$$\begin{pmatrix} \epsilon_1 & & & 0 \\ & \ddots & & \\ & & \epsilon_r & \\ 0 & & & 0 \end{pmatrix} \quad 0 \neq \epsilon_i \in R, \quad \epsilon_i | \epsilon_{i+1} \quad \forall i$$

Dabei sind die ϵ_i bis auf Einheiten eindeutig bestimmt. Insbesondere folgt, dass $Gl_m(R)$ von Elementarmatrizen erzeugt wird.

Bemerkung 4.11

Falls $R=K$ Körper ist dies der Gauss-Algorithmus und es ist $\text{Rang}(M) = r$

Definition 4.12

1. Sei R ein Ring. Ein R -Links-Modul ist ein Tripel $(M, +, \cdot)$ bestehend aus einer nichtleeren Menge M und zwei Abbildungen

$$\begin{aligned} + : M \times M &\longrightarrow M \\ \cdot : R \times M &\longrightarrow M, \end{aligned}$$

so dass gilt

- (a) $(M, +)$ ist eine abelsche Gruppe
 - (b) Rechts- und Linksdistributivgesetze und das Assoziativgesetz gelten, sowie $1m = m \forall m$.
2. Sind M, N R -Moduln so heißt

$$f : M \longrightarrow N$$

ein R -Modul-Homomorphismus, falls

$$\begin{aligned} f(m + m') &= f(m) + f(m') \\ f(rm) &= rf(m) \end{aligned}$$

wir bezeichnen mit

$$\text{Hom}_R(M, N) := \{f : M \longrightarrow N \mid f \text{ } R\text{-Homomorphismus}\}$$

Bemerkung 4.13

1. Ist R ein Körper, so ist ein R -Modul ein R -Vektorraum.
2. Ist $R = \text{Mat}(2 \times 2, \mathbb{R})$, dann ist $M = \mathbb{R}^2$ ein R -Modul.
3. $\text{Hom}_R(M, N)$ ist eine abelsche Gruppe, ist R kommutativ, so ist $\text{Hom}_R(M, N)$ ein R -Modul

Definition 4.14

Sei M ein R -Modul

1. Eine Teilmenge $U \subset M$ heißt Untermodul, wenn $U \neq \emptyset$ und gegenüber Addition und Skalarmultiplikation abgeschlossen ist.
2. Eine Teilmenge $N \subset M$ heißt Erzeugendensystem, falls alle $m \in M$ als Linearkombination von Elementen von N darstellbar sind.
3. M heißt endlich erzeugt, wenn es ein endliches Erzeugendensystem besitzt.

Bemerkung 4.15

1. Ist R Körper, so sind die Untermoduln die Unterräume.
Achtung! Untermoduln müssen kein Modul-Komplement besitzen (es gilt nicht die Hauptraumzerlegung).
2. Abelsche Gruppen sind \mathbb{Z} -Moduln
3. Ist M ein R -Modul und U ein Untermodul, dann existiert in kanonischer Weise M/U der Faktormodul.
4. Ist $f : M \longrightarrow N$ ein Modulhomomorphismus, so sind $\text{Kern}(f)$ und $\text{Bild}(f)$ Untermoduln.
5. Es gelten die Homomorphiesätze
6. Ein Modul E heißt einfach, wenn 0 und E die einzigen Untermoduln von E sind. Es gilt auch für Moduln der Satz von Jordan-Hölder

Definition 4.16

1. Seien M_1, \dots, M_n R -Moduln. Die direkte Summe $\bigoplus_{j=1}^n M_j$ ist der R -Modul mit der zugrundeliegenden Menge $\{(m_1, \dots, m_n) \mid m_i \in M_i\}$ mit kanonischer Addition und Multiplikation, wir definieren

$$\bigoplus_{i=1}^n M =: M^n$$

2. Ein R -Modul M heißt frei mit Basis $\{m_1, \dots, m_n\}$, falls sich jedes $m \in M$ als eindeutige Linearkombination der m_i schreiben lässt.
3. Eine Folge von Homomorphismen

$$\dots \longrightarrow M_i \xrightarrow{f_i} M_{i+1} \xrightarrow{f_{i+1}} \dots$$

heißt exakt an der Stelle $i+1$, falls $\text{Kern}(f_{i+1}) = \text{Bild}(f_i)$ ist. Die Folge heißt exakt, wenn sie es an jeder Stelle ist.

Bemerkung 4.17

1. Ist

$$0 \longrightarrow U \xrightarrow{f} M \xrightarrow{g} V \longrightarrow 0$$

exakt, so ist f injektiv und g surjektiv.

2. Ist M frei mit Basis $\{m_1, \dots, m_n\}$, so gilt $R^n \cong M$
Ist N ein weiterer R -Modul und $n_1, \dots, n_n \in N$, dann gibt es genau einen Homomorphismus

$$\begin{aligned} \phi: M &\longrightarrow N \\ \phi(m_i) &= n_i \end{aligned}$$

3. Ist R ein Körper, so ist jeder R -Modul frei.

Lemma 2

Sei M ein R -Modul, U ein Untermodul

1. Sind U und M/U endlich erzeugt, so auch M .
2. Ist R links-noethersch und M endlich erzeugt, so auch U .

Satz 3 (Struktursatz)

Sei R nullteilerfreier Hauptidealring, es sei M ein endlich erzeugter R -Modul

1. $\exists s, t \in \mathbb{N}, \epsilon_1, \dots, \epsilon_s \in R$ mit $\epsilon_i \mid \epsilon_{i+1} \forall i$, so dass

$$M \cong R^t \oplus \left(\bigoplus_{i=1}^s R/(\epsilon_i) \right)$$

wobei s, t eindeutig und die ϵ_i bis auf Einheiten eindeutig bestimmt sind.

2. Ist $0 \neq \epsilon = p_1^{n_1} \cdots p_s^{n_s}$ mit p_i prim und $p_i \not\sim p_j$ wenn $i \neq j$, so gilt

$$R/(\epsilon) \cong \bigoplus_{i=1}^s R/(p_i^{n_i})$$

3. Jeder endlich erzeugte Modul M ist endliche Summe von Moduln der Form R oder R/p^n , wobei p prim ist.

Bemerkung 4.18

Jede endliche abelsche Gruppe ist direktes Produkt von zyklischen Gruppen der Form $\mathbb{Z}/p^n\mathbb{Z}$ mit eindeutigen Faktoren, dies ermöglicht eine einfache Berechnung der Isomorphieklassen von abelschen Gruppen.

Definition 4.19

Sei R Hauptidealring, M ein R -Modul. Dann ist der Torsionsteil

$$T(M) := \{m \in M \mid \exists r \neq 0 \ rm = 0\}$$

ein Untermodul. M heißt torsionsfrei, wenn $T(M) = 0$ ist.

Definition 4.20

Sei p ein Primelement in R , dann ist der p -Torsionsmodul eines R -Moduls M

$$T_p M = \{x \in M \mid \exists n : p^n x = 0\}$$

Kapitel 5

Körpertheorie

5.1 Grundlegende Definitionen

Bemerkung 5.1

Sei k ein Körper. Dann gibt es genau einen Ringhomomorphismus $\varphi : \mathbb{Z} \rightarrow k$ mit $\varphi(1) = 1$. Nach dem Homomorphiesatz ist dann $\mathbb{Z}/\text{Kern}(\varphi) \cong \text{Bild}(\varphi) = \text{Integritätsbereich}$ als Unterring von k . Also $\text{Kern}(\varphi)$ Primideal. Das liefert nun folgende Möglichkeiten:

1. $\text{Kern}(\varphi) = (0)$
2. $\text{Kern}(\varphi) = (p)$ $p = \text{prim}$

Definition 5.2

Ist k ein Körper, so definiert man seine Charakteristik

$$\text{char}(k) = \begin{cases} 0 & \text{falls } \varphi \text{ injektiv ist} \\ p & \text{falls } \text{Kern}(\varphi) = (p) \text{ ist} \end{cases}$$

Definition 5.3

Ist k ein Körper, so heißt der kleinste in k enthaltene Körper der Primkörper \mathbb{P} von k .

Bemerkung 5.4

1. Ist k ein Körper mit $\text{char}(k) = p$, so ist

$$\mathbb{P} \cong \begin{cases} \mathbb{Z}/(p) & p \neq 0 \\ \mathbb{Q} & \text{sonst} \end{cases}$$

2. Ist $\text{char}(k) = p$, so ist $F : k \rightarrow k$ mit $x \mapsto x^p$ ein Körperhomomorphismus, der zwar injektiv, aber im allgemeinen nicht surjektiv ist

5.2 Körpererweiterung

Definition 5.5

Eine Körpererweiterung ist ein Paar $K \supset k$ von Körpern. Man schreibt dafür K/k oder $\begin{pmatrix} K \\ | \\ k \end{pmatrix}$. K heißt Oberkörper oder Erweiterungskörper von k , k heißt Unterkörper oder Teilkörper von K .

Bemerkung 5.6

1. $\mathbb{F}_p[X]$ ist ein Integritätsbereich und man schreibt stattdessen $\mathbb{F}_p(X)$ den Körper der rationalen Funktionen und es ergibt sich $\text{char}(\mathbb{F}_p(X)) = p$. Allgemeiner bezeichnet man mit $k(X)$ den Quotientenkörper von $k[X]$

2. Es sei $k \subset K$, dann ist K in kanonischer Weise ein k -Vektorraum.

Definition 5.7

Der Körpergrad $[K : k]$ ist definiert durch

$$[K : k] := \dim_k(K)$$

Satz 1

Seien $K \supset L \supset k$ Körper dann folgt: K/k ist endlich genau dann, wenn K/L und L/k endlich sind. In diesem Fall gilt dann

$$[K : k] = [K : L] \cdot [L : k]$$

Definition 5.8

Sei $K \supset k$

1. Für $M \subset k$ ist $k[M]$ der kleinste Unterring, der k und M enthält
2. Für $M \subset k$ ist $k(M)$ der kleinste Unterkörper, der k und M enthält. Für $M = \{a_1, \dots, a_n\}$ schreibt man auch

$$k[a_1, \dots, a_n] \quad \text{bzw.} \quad k(a_1, \dots, a_n)$$

3. $a \in K$ heißt algebraisch über k , falls es ein Polynom $f \in k[X] \setminus \{0\}$ gibt mit $f(a) = 0$. In diesem Fall gibt es genau ein normiertes Polynom kleinsten Grades m_a mit dieser Eigenschaft. m_a heißt Minimalpolynom.
4. $a \in k$ heißt transzendent, wenn a nicht algebraisch ist.
5. $K \supset k$ heißt einfach (oder primitiv), falls $\exists a \in K$ mit $K = k(a)$.

Satz 2

Sei $K \supset k$, $a \in K$, dann gilt

1. a algebraisch $\Rightarrow k[X]/(m_a) \cong k[a] \cong k(a)$. Weiterhin ist $[k[a] : k] = \text{grad}(m_a)$. Ferner teilt m_a jedes Polynom f mit $f(a) = 0$.
2. Ist a transzendent so ist $k[X] \cong k[a]$ und $k(X) \cong k(a)$ und somit $[k(a) : k] = \infty$

Bemerkung 5.9

1. Ist a algebraisch über k , so ist m_a irreduzibel, wie der Satz zeigt, darum nennt man auch m_a das irreduzible Polynom über k .
2. π ist transzendent über \mathbb{Q} also ist die Quadratur des Kreises nicht möglich.
3. Ist $K = k(a) \supset k$ einfach, so gilt $K \cong k[X]/(p)$ oder $K \cong k(X)$

Definition 5.10

Eine Körpererweiterung K/k heißt algebraisch, falls jedes $a \in K$ algebraisch über k ist

Satz 3

Sei K/k gegeben, dann gilt

1. Folgende Aussagen sind äquivalent
 - (a) K/k ist endlich
 - (b) $\exists a_1, \dots, a_n$ mit a_i algebraisch und $K = k(a_1, \dots, a_n)$
 - (c) K/k ist endlich erzeugt und algebraisch

2. Ist $K \supset L \supset k$ gegeben, dann ist K/k endlich $\Leftrightarrow K/L$ und L/k sind endlich

Definition 5.11

K/k heißt endlich erzeugt $:\Leftrightarrow \exists$ eine endliche Menge M , so dass $K = k(M)$

Bemerkung 5.12

1. $K \supset k$ und $L = \{a \in k \mid a \text{ algebraisch über } k\}$ ist ein Teilkörper
2. $\mathbb{R} \supset L \supset \mathbb{Q}$, L wie oben, dann ist L/\mathbb{Q} nicht endlich erzeugt, da sonst \mathbb{R}/\mathbb{Q} endlich erzeugt wäre.

5.3 Konstruktionen mit Zirkel und Lineal

Es bezeichne im folgenden E die euklidische Ebene.

Definition 5.13

1. Für eine endliche Teilmenge $\subset E$ sei $K(X)$ die Menge aller Punkte, die man aus X in einem Schritt mit Zirkel und Lineal konstruieren kann. Dabei entsteht P aus X durch einen Schritt genau dann, wenn

(a) $P \in X$

(b) P ist Schnittpunkt von zwei Geraden, zwei Kreisen oder einer Geraden mit einem Kreis durch Punkte aus X

$\Rightarrow K(X) \supset X$ ist endlich.

2. Setze $K_0 := \{(0, 0), (1, 0)\}$ und $K_i := K(K_{i-1})$.
3. $P \in E$ heißt konstruierbar, falls es ein $n_0 \in \mathbb{N}$ gibt, mit $P \in K_{n_0}$
4. $x \in \mathbb{R}$ heißt konstruierbar, falls ein $P = (x, r)$ oder $P = (r, x)$ konstruierbar ist
5. $L_n := \{z \in \mathbb{R} \mid z \text{ ist Koordinate eines Punktes in } K_n\}$
6. Das regelmäßige n -Eck ist konstruierbar $\Leftrightarrow P = e^{\frac{2\pi i}{n}} = \left(\cos\left(\frac{2\pi i}{n}\right), \sin\left(\frac{2\pi i}{n}\right) \right)$ ist konstruierbar

Satz 1 (Gauss, 1796)

Ein regelmäßiges n -Eck ist konstruierbar $\Leftrightarrow n = 2^m p_1 \cdot p_r$ ist, wobei m eine beliebige natürliche Zahl ist und die p_i paarweise verschiedene Fermatsche Primzahlen.

Definition 5.14

Eine Fermatsche Primzahl ist eine Primzahl der Form

$$F_m = 2^{2^m} + 1$$

Bemerkung 5.15

1. $F_0 = 3, F_1 = 5, \dots$
2. Winkeldreiteilung ist i.a. nicht möglich, da z.B. das Neuneck nicht konstruierbar ist.

Lemma 2

Es sei $X = \{(x_i, y_i) \mid i = 1, \dots, n\}$ $P = (x, y) \in K(X)$, ist $L = \mathbb{Q}(x_1, y_1, \dots, x_n, y_n)$. Dann gilt $[L(X), L] \leq 2$

Bemerkung 5.16

1. $P = (x, y)$ ist konstruierbar $\Leftrightarrow x, y$ sind konstruierbar
2. $a, b > 0$ konstruierbar $\Rightarrow a \pm b, ab, \frac{a}{b}, \sqrt{b}$ sind konstruierbar

Satz 3

1. Sei $z \in \mathbb{R}$ dann folgt $[\mathbb{Q}(z), \mathbb{Q}] = 2^l$, wobei l eine natürliche Zahl ist.
2. In einer Kette $L_0 \supset \dots \supset L_t = \mathbb{Q}$ mit $[L_i : L_{i+1}] = 2$ sind alle Elemente aus L_0 konstruierbar.

Corollar 5.17

1. Quadratur des Kreises ist unmöglich, denn zu Kreis mit Radius 1 ist das Quadrat der Kantenlänge mit gleichem Flächeninhalt zu konstruieren. Also wären die Nullstellen von $x^2 = \pi$ in \mathbb{Q} enthalten, Widerspruch zu Satz von Lindemann.
2. Würfelverdoppelung geht nicht, denn zu konstruieren ist $\sqrt[3]{2}$, d.h. gesucht ist die Nullstelle von $X^3 - 2$, das nach Eisenstein irreduzibel ist. D.h. $[\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}] = 3$, nach Satz 3a) ist das ein Widerspruch.

Definition 5.18

Sei n ein natürliche Zahl.

1. $\sqrt[n]{1} = \{z \in \mathbb{C} \mid z^n = 1\}$ heißt Gruppe der n -ten Einheitswurzeln.
2. $\zeta \in \sqrt[n]{1}$ heißt primitiv, falls $\sqrt[n]{1} = \langle \zeta \rangle$
3. $\phi_n(X) = \prod_{\zeta \text{ primitiv}} (X - \zeta)$ heißt Kreisteilungspolynom
4. Ist ζ eine primitive n -te Einheitswurzel, so heißt $\mathbb{Q}(\zeta) = \mathbb{Q}(M)$ mit $M = \{z \mid z \in \sqrt[n]{1}\}$ der n -te Kreisteilungskörper.

Bemerkung 5.19

1. $\zeta = \exp(\frac{2\pi i}{n})$ ist eine primitive n -te Einheitswurzel
2. ζ^j ist eine primitive n -te Einheitswurzel genau dann, wenn $(n, j) = 1$, ihre Anzahl ist $\varphi(n)$.

Lemma 4

1. Sei $f \in \mathbb{Z}[X]$ und $g, h \in \mathbb{Q}[X]$ normiert, ist dann $f = gh$, so ist schon $g, h \in \mathbb{Z}[X]$
2. $X^n - 1 = \prod_{d|n} \phi_d(X)$
3. $\phi_n(X) \in \mathbb{Z}[X]$ normiert.

Definition 5.20

Sei R ein kommutativer Ring, $f \in R[X]$ ein Polynom mit

$$f(X) = a_0 + a_1X + \dots + a_nX^n$$

dann definieren wir seine Ableitung als

$$f'(X) = \sum_{i=1}^n ia_iX^{i-1}$$

Bemerkung 5.21

1. Mit dieser Definition gelten die üblichen Rechenregeln für die Differentiation, wie z.B. die Summen-, Faktor- und Produktregel.
2. Es kann $f' = 0$ sein, ohne dass f konstant ist.

Satz 5

Das Polynom ϕ_n ist irreduzibel, also das Minimalpolynom von $\zeta = \exp(\frac{2\pi i}{n})$ über \mathbb{Q} . Folglich ist

$$\text{grad}(\phi_n) = \varphi(n)$$

Corollar 5.22

Ist das regelmäßige n -Eck konstruierbar, dann ist $n = 2^m p_1 \cdots p_r$, wobei die p_i Fermatsche Primzahlen sind.

5.4 Der algebraische Abschluss

Definition 5.23

1. Ein Körper K heißt algebraisch abgeschlossen $:\Leftrightarrow$ jedes nicht-konstante Polynom eine Nullstelle in K hat.
2. Ein Körper $K \supset k$ heißt algebraischer Abschluss von k , falls
 - (a) K ist algebraisch abgeschlossen
 - (b) K/k ist algebraisch

Man schreibt dann $K = \bar{k}$.

Ziel Für jeden Körper k gibt es einen bis auf Isomorphie eindeutig bestimmten algebraischen Abschluss.

Lemma 1 (Kroneckers Konstruktion)

Sei k ein Körper und f ein nichtkonstantes Polynom. Dann gibt es eine endliche Körpererweiterung K von k , in der f eine Nullstelle hat.

Bemerkung 5.24

Per Induktion erhält man leicht einen Erweiterungskörper K , so dass jedes nichtkonstante Polynom f_1, \dots, f_n eine Nullstelle in K hat.

Problem Wie konstruiert man ein K , so dass alle nicht-konstanten Polynome in K eine Nullstelle haben.

Antwort Via Zorns Lemma

Definition 5.25 (Zorns Lemma)

Sei M eine nicht-leere partiell geordnete Menge. Falls jede Kette aus M eine obere Schranke besitzt, so gibt es ein maximales Element.

Definition 5.26

1. Eine partiell geordnete Menge ist eine Menge mit einer Ordnungsrelation (die nicht unbedingt eine Totalordnung sein muss)
2. $K \subset M$ heißt Kette, falls die induzierte Ordnungsrelation auf K eine Totalordnung ist.
3. $x \in M$ heißt maximal, falls aus $x \leq y$ schon $x = y$ folgt.
4. $x \in K$ mit K Kette heißt obere Schranke, falls $y \leq x$ für alle $y \in K$ gilt.

Lemma 2

Sei R ein Ring und $I \neq R$ ein Ideal, dann gibt es ein maximales Ideal $m \supset I$

Satz 3

Jeder Körper k liegt in einem algebraisch abgeschlossenen Körper K .

Bemerkung 5.27

1. \mathbb{C} ist nach dem Fundamentalsatz der Algebra algebraisch abgeschlossen.
2. Ist k endlich, so folgt \bar{k} ist nicht endlich.
3. Folgende Aussagen sind äquivalent
 - (a) K ist algebraisch abgeschlossen
 - (b) Jedes Polynom $f \in K[X]$ zerfällt über K in Linearfaktoren
 - (c) K hat keine endliche Körpererweiterung
 - (d) K hat keine algebraische Körpererweiterung

4. Ist k abzählbar, so auch \bar{k} .

Definition 5.28

Sei $\sigma : K \rightarrow L$ Körperhomomorphismus, $f = \sum_{i=0}^m a_i X^i \in K[X]$. Dann definiert man $f^\sigma \in L[X]$ durch

$$f^\sigma(X) := \sum_{i=0}^m \sigma(a_i) X^i$$

f^σ heißt dann Fortsetzung von f .

Lemma 4 (Schlüssellemma zur Fortsetzung von Körperhomomorphismen)

Sei $\sigma : K \rightarrow L$ Körperhomomorphismus und es sei $K' = K(\alpha) = K[\alpha]$ eine einfache endliche Erweiterung von K . Sei $f \in K[X]$ das Minimalpolynom von α über K . Dann gilt:

1. Ist σ' eine Fortsetzung von σ , d.h. ist

$$\begin{array}{ccc} K & \xrightarrow{\sigma} & L \\ & \searrow & \nearrow \sigma' \\ & K(\alpha) & \end{array}$$

kommutativ, dann ist $\sigma'(\alpha)$ Nullstelle von f^σ .

2. Ist umgekehrt β eine Nullstelle von f^σ , so gibt es eine Fortsetzung σ' von σ mit $\sigma'(\alpha) = \beta$.

3. Man erhält somit eine Bijektion

$$\begin{aligned} \{\sigma' : K' \rightarrow L \mid \sigma' \text{ ist Fortsetzung von } \sigma\} &\cong \{\text{Nullstellen von } f^\sigma \text{ in } L\} \\ \sigma' &\mapsto \sigma'(\alpha) \end{aligned}$$

Insbesondere entspricht die Anzahl der Fortsetzungen der Anzahl der Nullstellen.

Corollar 5.29

Ist K/k eine algebraische Körpererweiterung und ist L algebraisch abgeschlossen, dann besitzt jeder Körperhomomorphismus $\sigma : k \rightarrow L$ eine Fortsetzung $\sigma' : K \rightarrow L$.

Bemerkung 5.30

Seien \bar{k} , L algebraische Abschlüsse von k , dann gibt es einen Körperisomorphismus $\tau : \bar{k} \rightarrow L$.

5.5 Separable Elemente und separable Körpererweiterungen

Definition 5.31

Sei k ein Körper, $K \supset k$ eine endliche Körpererweiterung

1. Ein Polynom $f \in k[x] \setminus k$ heißt separabel, falls f in $\bar{k}[x]$ keine doppelten Nullstellen besitzt.
2. Ein Element $a \in K$ heißt separabel, falls das zugehörige Minimalpolynom über k separabel ist.
3. K/k heißt separabel, wenn alle $a \in K$ separabel über k sind.
4. k heißt vollkommen, falls alle endlichen Körpererweiterungen separabel sind.

Satz 1

Sei k ein Körper, $f \in k[x] \setminus k$, dann gilt

1. f ist separabel genau dann, wenn f und f' in $k[X]$ teilerfremd sind.
2. Ist f irreduzibel, so ist f genau dann separabel, wenn $f' \neq 0$

Bemerkung 5.32

1. Jeder Körper der Charakteristik 0 ist vollkommen
2. Jeder endliche Körper ist vollkommen
3. $\mathbb{F}_2(t)[X]/(X^2 - t)$ ist nicht vollkommen.

Satz 2

Sei K/k eine endliche Körpererweiterung mit $[K : k] = n$, dann gilt

1. Es gibt höchstens n Einbettungen $\sigma : K \rightarrow \bar{k}$ mit $\sigma|_k = id$
2. Folgende Aussagen sind äquivalent
 - (a) Die Erweiterung ist separabel
 - (b) $K = [a_1, \dots, a_n]$, wobei die a_i separabel über $k[a_1, \dots, a_{i-1}]$ sind und a_1 über k
 - (c) Es gibt genau n Einbettungen
3. Ist $K \supset L \supset k$ eine Körperkette, so ist K/k separabel genau dann, wenn K/L und L/k separabel sind.

5.6 Zerfällkörper und normale Erweiterungen

Definition 5.33

Sei k ein Körper, $f \in k[X] \setminus k$. Eine Körpererweiterung K/k heißt Zerfällkörper von f , falls

1. f zerfällt in $K[X]$ in Linearfaktoren
2. $K = k(a_1, \dots, a_n) = k[a_1, \dots, a_n]$

Satz 1

Sei k ein Körper, $f \in k[X] \setminus k$. Dann gibt es einen Zerfällkörper K von f , der bis auf Isomorphie eindeutig ist.

Bemerkung 5.34

Einen Zerfällkörper findet man immer durch Adjunktion von Nullstellen in einem algebraisch abgeschlossenen Körper.

Satz 2

Sei K/k endlich, mit $K \subset \bar{k}$, dann sind folgende Aussagen äquivalent

1. K ist Zerfällkörper von f aus $k[X] \setminus k$
2. Jeder Körperhomomorphismus $\sigma : K \longrightarrow \bar{k}$ mit $\sigma|_k = id_k$ erfüllt $\sigma(K) = K$
3. Hat ein irreduzibles Polynom $g \in k[X] \setminus k$ eine Nullstelle in K , so liegen alle Nullstellen von g in K

Definition 5.35

Sei K/k eine endliche Körpererweiterung

1. K/k heißt normal, falls die drei Bedingungen des Satzes erfüllt sind.
2. K/k heißt galoissch oder Galois-Erweiterung, falls K/k normal und separabel ist
3. Die Galois-Gruppe von K/k ist definiert als

$$\text{Gal}(K/k) := \{\sigma \in \text{Aut}(K) : \sigma|_k = id_k\}$$

Bemerkung 5.36

1. $\text{Gal}(K/k)$ ist immer definiert, auch wenn K/k nicht galoissch ist.
2. Vorsicht bei normalen Erweiterungen! Für $K \supset L \supset k$ gilt i.a. nur K/k normal $\Rightarrow K/L$ normal, aber weder folgt die Normalität von L/K noch folgt aus der Normalität von K/L und L/k , dass K/k normal ist!!! Ähnliches gilt für Galois-Erweiterungen.

Satz 3

Sei K/k eine endliche Körpererweiterung. Folgende Aussagen sind äquivalent

1. K/k ist galoissch
2. K ist Zerfällkörper eines separierbaren Polynoms $f \in k[X]$
3. $|\text{Gal}(K/k)| = [K : k]$

Bemerkung 5.37

Es gilt immer $|\text{Gal}(K/k)| \leq [K : k]$

Definition 5.38

Für $f \in k[X]$ definiert man die Galoisgruppe $\text{Gal}(f)$ als Galoisgruppe $\text{Gal}(K/k)$, wobei K der Zerfällkörper von f ist.

Bemerkung 5.39

1. $\text{Gal}(f)$ ist eindeutig bis auf Isomorphie.
2. Sei $f = a \prod_{i=1}^n (X - a_i)$, $a_i \in K$, wobei K der Zerfällkörper von f ist, dann gibt es einen Homomorphismus $\varphi : \text{Gal}(f) \hookrightarrow S_n$

Zusatz

Ist f irreduzibel, so operiert $\text{Gal}(f)$ transitiv auf den Nullstellen von f , d.h. für beliebige $a_i \neq a_j$ gibt es ein $\sigma \in \text{Gal}(f)$ mit $\sigma(a_i) = a_j$

5.7 Der Hauptsatz der Galoistheorie

Definition 5.40

Sei K ein Körper, G eine Gruppe von Automorphismen von K . Dann heißt

$$K^G := \{x \in K \mid \sigma(x) = x \forall \sigma \in G\}$$

der Fixkörper von G .

Bemerkung 5.41

K^G ist ein Teilkörper.

Satz 1 (Artin)

Sei K ein Körper, G eine endliche Automorphismengruppe. Dann gilt

$$[K : K^G] = |G|$$

Also ist K/K^G eine Galoiserweiterung mit Galoisgruppe G .

Satz 2 (Hauptsatz)

Sei K/k eine Galoiserweiterung mit Galoisgruppe G . Es sei

$$\mathcal{U} := \{U \mid U \leq G\}$$

die Menge der Untergruppen von G und

$$\mathcal{Z} := \{L \mid K \supset L \supset k\}$$

die Menge der Zwischenkörper. Dann gilt

1. Die Abbildung $U \mapsto K^U$ ist Bijektion von \mathcal{U} und \mathcal{Z} . Die Umkehrabbildung ist $L \mapsto \text{Gal}(K/L)$. Beide Abbildungen sind antiton, d.h. sie drehen die Inklusion um.
2. Für $\sigma \in G$, $U \leq G$ gilt

$$\sigma(K^U) = K^{\sigma U \sigma^{-1}}$$

Insbesondere ist K^U/k normal genau dann, wenn U normal in G ist. In diesem Fall gilt:

$$\text{Gal}(K^U/k) \cong G/U$$

3. Stets ist K/K^U eine Galoiserweiterung mit Galoisgruppe $\text{Gal}(K/K^U) = U$ und

$$[K : K^U] = |U|$$

5.8 Folgerungen aus dem Hauptsatz und Beispiele

Corollar 5.42

Ist $n = 2^m p_1 \cdots p_r$, wobei die p_i Fermatsche Primzahlen sind, so ist das regelmäßige n -Eck konstruierbar.

Satz 1

Sei G eine endliche Untergruppe mit n Elementen von der multiplikativen Gruppe K^* eines Körpers, dann ist G zyklisch.

Bemerkung 5.43

Insbesondere gilt für einen endlichen Körper k stets $k^* = \langle \nu \rangle$. Allerdings existiert keine Formel für die Berechnung von ν .

Satz 2 (Satz vom primitiven Element)

Sei $K = k[x_1, \dots, x_n] \supset k$ eine endliche Erweiterung. Dabei seien die x_2, \dots, x_n separabel über k , dann folgt: Es gibt ein primitives Element $\alpha \in K$ mit $K = k[\alpha]$, insbesondere lässt sich jede endliche separable und damit jede Galoiserweiterung K/k von einem Element erzeugen.

Corollar 5.44

\mathbb{C} ist algebraisch abgeschlossen.

Anhang A

Ergänzungen

Definition A.1

Es sei k ein Körper. Eine Fahne F in k^n ist eine Folge (F_1, \dots, F_n) , von Unterräumen des k^n , mit $F_i \subset F_{i+1}$ und $\dim(F_i) = i$.

Definition A.2

Diedergruppe

Definition A.3

Es sei R ein kommutativer Ring und $M \subset R$ eine Teilmenge, dann ist das von M erzeugte Ideal definiert als

$$(M) := \left\{ \sum_{i=1}^n r_i m_i \mid n \in \mathbb{N}, r_i \in R, m_i \in M \right\}$$

Definition A.4

Sei R ein kommutativer Ring und $p \subset R$ ein Ideal. p heißt Primideal, wenn aus $x \cdot y \in p$ schon $x \in p$ und $y \in p$ folgt.

Satz 3 (Eisenstein)

Sei R ein faktorieller Ring. Sei p prim und $f = \sum_{i=0}^n a_i X^i$, wobei die a_i für $i < n$ von p geteilt werden, aber p^2 kein Teiler von a_0 ist. Dann ist f irreduzibel.