Inhaltsverzeichnis

1 Gruppen

0 Motivation:

0.1 Wiederholung:

Definition:

a) Eine Gruppe ist eine Menge G zusammen mit einer assoziativen Verknüpfung mit Einselement $e \in G$ und Inversen.

- Verknüpfung: $\cdot : G \times G \to G$ mit $(a, b) \mapsto a \cdot b =: ab$
- Eins (= neutrales Element) : $\forall a \in G : ae = ea = a$
- Inverse: $\forall a \in G \exists b \in G : ab = ba = e$ Notation: $b =: a^{-1}$
- assoziativ: $\forall a, b, c \in G : (ab)c = a(bc)$

b) G heißt abelsch oder kommutativ, falls $\forall a, b \in G : ab = ba$

c) Sind G, H Gruppen, so heißt $\varphi : G \to H$ Homomorphismus, falls gilt:

$$\forall a, b \in G : \quad \varphi(a \cdot_G b) = \varphi(a) \cdot_H \varphi(b)$$

hier gilt außerdem noch: $\varphi(e_G) = e_H$

0.2 Eindeutigkeit inverser Elemente:

Lemma: Sei M eine Menge mit einer assoziativen Verknüpfung $\cdot : M \times M \to M$, mit einem neutralem Element $e \in M$ und $\forall a \in M$ gilt: $\exists b \in M$ mit $ab = e$ (Rechtsinverse), dann existiert zu jedem $a \in M$ genau ein Inverses $b \in M$. Insbesondere ist $(M, \cdot, e)$ eine Gruppe und Inverse in Gruppen sind eindeutig.

Beweis:
zu $a \in M$ sei $b \in M$ das Rechtsinverse, also $ab = e$

a) b ist auch linkinvers, denn sei $c \in M$ rechtsinvers zu b, dann folgt:
$a = ae = a(bc) = (ab)c = c$ daraus folgt sofort: $ba = bc = e$
b) Eindeutigkeit der Inversen:
gelte $ab = ba = e = ab' = b'a$. Nun gilt: $b' = eb' = (ba)b' = b(ab') = be = b$
also sind die Inversen gleich.

□

0.3 Beispiele:

a) $(\mathbb{Z}, +, 0)$

b) $n \in \mathbb{N}\backslash\{0\}$, $\Rightarrow (\mathbb{Z}_{/n}, +, [0])$ hier ist $\mathbb{N} = \mathbb{N}_0$

c) Die additive Gruppe eines Körpers K: $(K, +, 0) =: K_a$

d) Die multiplikative Gruppe eines Körpers K: $(K\backslash\{0\}, \cdot, 1) =: K_m$

e) M Menge, so ist $B_{ij}(M) := \{\varphi : M \to M \mid \varphi \text{ ist bijektiv } \}$ mit der Verknüpfung: $(\varphi, \psi) \mapsto \varphi \circ \psi$ eine Gruppe. Hier ist $\circ$ die Komposition und φ^{-1} ist die Umkehrabbildung.
Speziell: ist $M = \{1, ..., n\}$ so heißt $S_n := B_{ij}(M)$ symetrische Gruppe auf n Elementen. Diese ist im Gegensatz zu a) - d) für $n > 2$ nicht abelsch.

f) Matrixgruppen: siehe lineare Algebra: $GL(n, K)$, $O(n)$, $SO(n)$, $U(n)$, $SU(n)$, $Sp(n)$,...

g) Sei V Vektorraum über K, dann bilden die affinen Transformationen:

$$Aff(V) := \{\varphi + v \mid \varphi \in GL(V), v \in V\}$$

eine Gruppe, die außer für $V = 0$ oder $K = \mathbb{F}_2$, $dim_K(V) = 1$ nicht abelsch ist.

h) $(V, <, >)$ euklidischer VR, so bilden die Bewegungen

$$Mor(V, <, >) := \{f = \varphi + v \mid \varphi \in O(V, <, >), v \in V\} \quad \text{(O Orthogonale Gruppe)}$$

eine Gruppe.

i) Produktgruppen: Sind $(G_1, e_1), (G_2, e_2)$ Gruppen, so auch

$$((G_1 \times G_2, (e_1, e_2)) \text{ mit } (a, b) \cdot (c, d) \mapsto (a \cdot_{G_1} b, c \cdot_{G_2} d)$$

Notationsmissbrauch: Die Gruppe $G_1 \times G_2$. Das gleiche gilt für $\prod_{i \in I} G_i$ mit Indexmenge I

0.4 Endliche Gruppen / Gruppentafeln:

Ist G eine Gruppe mit $\mid G \mid < \infty$, so ist die Verknüpfung durch die Gruppentafel gegeben, also $G = \{e, a_1, a_2, ..., a_r\}$ mit $\forall i \neq j : a_i \neq a_j \ , \ a_i \neq e$

	e	a_1	a_2	a_3	$\dots$
e	ee	ea_1	ea_2	ea_3	$\dots$
a_1	a_1e	a_1a_1	a_1a_2	a_1a_3	$\dots$
a_2	a_2e	a_2a_1	a_2a_2	a_2a_3	$\dots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

In jeder Zeile und in jeder Spalte kommt jedes Element genau einmal vor (*), denn für alle $b \in G$ haben die beiden Gleichungssysteme: $bc = a$ (Zeile b) und $db = a$ (Spalte a) genau eine Lösung $c = b^{-1}a$ und $d = ab^{-1}$ hierbei betrachten wir die $c-$te Spalte und die $d-$te Zeile.

Anwendung: Klassifizierung der Gruppen mit $\mid G \mid \leq 4$:

i.) $\mid G \mid = 1 \Rightarrow G = \{e\}$

ii.) $\mid G \mid = 2 \Rightarrow G = \{e, a\}$ betrachte also die Tafel:

	e	a
e	e	a
a	a	?

wegen (*) ist $? = e$.

d.h. $G \simeq \mathbb{Z}_{/2}$ mit $e \mapsto [0]$, $a \mapsto [1]$. Aufpassen, in G mult, in $\mathbb{Z}_{/n}$ add.

iii.) $\mid G \mid = 3 \Rightarrow G = \{e, a, b\}$

	e	a	b
e	e	a	b
a	a	?	e
b	b	e	a

$? = b$, denn wenn $? = a$ wäre $ab = b$, aber $a \neq e$

In der Tat gilt: $G \simeq \mathbb{Z}_{/3}$ mit $e \mapsto [0]$, $a \mapsto [1]$, $b \mapsto [2]$ Permutationen von a, b erlaubt.

iv.) $\mid G \mid = 4, \Rightarrow G = \{e, a, b, c\}$ Wir unterscheiden 2 Fälle:

1) $\forall x \in G : x^2 = e$

	e	a	b	c
e	e	a	b	c
a	a	e	?	b
b	b	c	e	a
c	c	b	a	e

$ab \neq b$ sonst $a = e$, und wegen (*) folgt $ab = c$

Es folgt: $G \simeq \mathbb{Z}_{/2} \times \mathbb{Z}_{/2}$ mit $e \mapsto (0,0)$, $a \mapsto (1,0)$, $b \mapsto (0,1)$, $c \mapsto (1,1)$ und Permutationen.

2) $\exists x \in G \backslash \{e\} : x^2 \neq e$, oBdA sei $x = a$ und $b := a^2$(**)

	e	a	b	c
e	e	a	b	c
a	a	b	?	e
b	b	c	!	a
c	c	e	a	b

? : $ab \neq a, b$ sonst $a, b = e$, und $ab = e$ führt zu Widerspruch, also $ab = c$
! : $b^2 = e$ denn $b \cdot b = a^2 b(**) = a(ab) = ac = e$
Es folgt: $G \simeq \mathbb{Z}_{/4}$ mit $e \mapsto [0]$, $a \mapsto [1]$, $b \mapsto [2]$, $c \mapsto [3]$. a, c können permutieren.

0.5 Symmetriegruppen:

Wichtiges Beispiel von Gruppen:
Symmetrien einer Figur in $\mathbb{R}^n$.

Definition:

a) Für $S \subset \mathbb{R}^n$ ist

$$Sym(S) := \{f \in Aff(\mathbb{R}^n) \mid f(S) = S\}$$

eine Gruppe, die Symmetriegruppe von S.

b) Analog: abstandserhaltende Transformationen:

$$OSym(S) := Sym(S) \cap Mor(\mathbb{R}^n, <, >_0) \qquad \text{mit } <, >_0 \text{ ist standard Skalarprodukt}$$

Beispiele:

a) S = reguläres l-Eck := $conv\{e^{2\pi \frac{k}{l}} \mid k = 0, ..., l-1\} \subset \mathbb{C} = \mathbb{R}^2$. Dabei sei $conv$ die konvexe Hülle
$D_l := Sym(S)$ nennt man Diedergruppe denn sie ist die eigentliche Symm. eines Dieders
$= OSym(S)$
Elemente von $D_l : l$ Drehungen um Vielfache von $\frac{2\pi}{l}$ und l Spiegelungen.

b) $S = \mathbb{Z}\left[e^{\frac{2\pi i}{6}}\right] \subset \mathbb{C} = \mathbb{R}^2 = \{a + b \cdot e^{\frac{2\pi i}{6}} \mid a, b \in \mathbb{Z}\}$
$e^{\frac{2\pi i}{6}} = \cos(\frac{2\pi}{6}) + i \cdot \sin(\frac{2\pi}{6}) = \frac{1+\sqrt{3}i}{2}$ und S bildet ein Gitter
$Sym(S) \subset Aff(\mathbb{R}^2)$ "erzeugt" von Transformationen um $x \in S$, Spiegelungen, Drehungen um Vielfache von $\frac{2\pi}{6}$

c) Polyedergruppe $= Sym(S)$ mit S : Polyeder.
Für die regulären Polyeder: S = regulärer Ikosaeder (20) (oder reg. Dodekaeder(12)), dann ist $Sym(S) \simeq A_5 = \{\sigma \in S_5 \mid sgn(\sigma) = 1\}$ (Zykel von (1,2,3,4,5) " Isokaedergruppe "
S = Tetraeder (4) dann ist $Sym(S) \simeq A_4$ (Drehung um Eckpunkt und Spiegelungen durch Kantenhalbierende) $\Rightarrow$ "Tetraedergruppe"
S = Einheitswürfel (Octaeder (8)), dann ist $Sym(S) \simeq S_4$, heißt deswegen auch die Würfelgruppe

Bemerkung: Symmetriegruppen liefern eine Auswertungsabbildung

$$Sym(S) \times \mathbb{R}^n \to \mathbb{R}^n \qquad \text{mit } (f, x) \mapsto f(x)$$

Diese ist äquivalent zu einer Abbildung

$$Sym(S) \to Aff(\mathbb{R}^n) \qquad \text{mit } f \mapsto (x \mapsto f(x))$$

Ist Beispiel einer Gruppenwirkung. (heißt Gruppe mischt auf einer Menge rum)
Man versteht Gruppen ganz wesentlich durch ihre Gruppenwirkungen.

1 Gruppenwirkungen

1.1 Definition:

1. - Eine Wirkung (von links) oder (Links-) Operation einer Gruppe G auf einer Menge M ist eine Abbildung
$$. : G \times M \to M, \qquad (a, x) \mapsto a.x$$
Mit den folgenden Eigenschaften:
   i) $a, b \in G$ und $x \in M$: $a.(b.x) = (ab).x$
   ii) $\forall x \in M : e.x = x$ mit $e = id$

   - Rechtsoperationen: $M \times G, , \qquad (x, a) \mapsto x.a$
   Mit den folgenden Eigenschaften:
   i) $a, b \in G$ und $x \in M$: $(x.a).b) = x.(ab)$
   ii) $\forall x \in M : x.e = x$ mit $e = id$

   Der große Unterschied ist: Links operiert zuerst mit b und dann mit a, Rechts zuerst mit a
   Hat man eine solche Wirkung, so nennt man M auch $G-$Raum
2. Seien M ein $G-$Raum, N ein $H-$Raum und $\varphi : G \to H$ ein Homom. Eine ($\varphi-$)äquivariante Abbildung ist eine Abbildung $f : M \to N$, die mit den Gruppenoperationen verträglich ist, d.h.:
   $\forall a \in G, \forall x \in M$ gilt: $f(a.x) = \varphi(a).f(x)$ wobei der erste Punkt auf M operiert und der 2. auf N. Häufigster Fall: $G = H, \varphi = id : f(a.x) = a.f(x) \Rightarrow$ Isomorphie von $G-$Räumen: f bijektiv und $\varphi = id$.

1.2 Beispiele

a) S_n operiert auf $M = \{1, ..., n\}$ (von links) : $\sigma.k := \sigma(k)$, wird also dadurch definiert

b) $GL(V)$ operiert auf V (v.l.) : $\varphi.x = \varphi(x)$

c) Jede Gruppe operiert auch auf sich selbst
   (a) von links: $G \times G(= M) \to G$ mit $(a, x) \mapsto a.x := a \cdot x$
   (b) von rechts: $G(= M) \times G \to G$ mit $(x, b) \mapsto x.b := x \cdot b$

d) triviale Wirkung: von G auf M: $\forall a \in G$, $\forall x \in M$ soll gelten: $a.x := x$
   (Jede Gruppe operiert auf jeder Menge und tut nichts)

1.3 Gruppenwirkungen als Homomorphismen:

Satz:

1. Eine Linksoperation von G auf M ist äquivalent zu einem Homomorphismus $\Phi : G \to B_{ij}(M)$
2. Eine Rechtsoperation von G auf M ist äquivalent zu einem Antihomomorphismus
$$\Phi : G \to B_{ij}(M) \quad \text{, d.h. } \forall a, b \in G \ : \ \Phi(ab) = \Phi(b) \circ \Phi(a))$$
   Beweis:
   1) Ist $G \times G \to M$ eine Linksoperation, so ist $\forall a \in G$
   $$\Phi(a) := (x \mapsto a.x)$$
   bijektiv mit Umkehrabbildung: $\Phi(a^{-1})$.
   $\forall x \in M : \Phi(a)(\Phi(a^{-1})(x)) = a.(a^{-1}.x) = (aa^{-1}).x = e.x = x$

Φ ist ein Gruppen hom.: $\forall x \in M$ gilt:

$$\Phi(ab)(x) = ab.x = a.(b.x) = \Phi(a)(\Phi(b)(x)) = (\Phi(a) \circ \Phi(b))(x)$$

$\Rightarrow \Phi(ab) = \Phi(a) \circ \Phi(b)$

Umgekehrt:

Sei $\Phi : G \to B_{ij}(M)$ ein Hom.. Definiere $a.x := \Phi(a)(x)$, ...
2) Analog $\Phi(a) := (x \mapsto x.a)$

$$\Phi(ab)(x) = x.(ab) = (x.a).b = \Phi(b)(\Phi(a)(x)) = (\Phi(b) \circ \Phi(a))(x)$$

□

1.4 Bemerkung: Links- und Rechtsoperationen:

Ist $. : G \times M \to M$, $(a, x) \mapsto a.x$ eine Linksoperation $_{(+)}$, so ist

$$. : M \times G \to M \text{ mit } (x, a) \mapsto a^{-1}.x$$

eine Rechtsoperation $_{(++)}$ und umgekehrt.
Begründung:
Ist Φ ein Homomorphismus von Gruppen, so ist $\Phi \circ Inv$ ein Antihomomorphismus mit:
$InvG \times G, a \mapsto a^{-1}$:

$$\Phi(Inv(ab)) = \Phi(b^{-1}a^{-1}) = \Phi(b^{-1}) \cdot \Phi(a^{-1}) = (\Phi \circ Inv)(b) \cdot (\Phi \circ Inv)(a)$$

$_{(+)}$ ist äquivalent zu $\Phi : G \to B_{ij}(M)$; $_{(++)}$ $\Phi \circ Inv : G \to B_{ij}(M)$
Dies ist ein Antihomomorphismus. Komponieren wir die beiden (der von der Rechtsoperation) erhalten wir einen Homomorphismus.
Im folgenden betrachten wir nur Linksoperationen, wenn nicht anders vermerkt.

Bemerkung:
- fast alles aus lineare Algebra war Dinge verstehen bis auf Gruppenwirkung

1.5 Bahnen:

Definition: Sei M ein $G-$Raum und $x \in M$, so heißt

$$G.x = \{a.x \mid a \in G\} \subset M$$

Bahn oder auch Orbit (der $G-$Wirkung) durch x.

Bemerkung: $G.x$ ist selbst wieder ein $G-$Raum durch: $b.(a.x) = (ba).x$

Beispiele:

a) $M = \mathbb{R}^2 = \mathbb{C}$, $G = SO(2) = U(1)$ mit der Standardwirkung (durch lin. Abbildungen)

$$G.x = S_{||x||}(0) = \{y \in \mathbb{R}^2 \mid ||y|| = ||x||\} = \begin{cases} \text{ein Punkt , für: } x = 0 \\ \text{ein Kreis , für: } x \neq 0 \end{cases}$$

b) $G = (\mathbb{R}_{>0}, \cdot)$ operiere auf $M = \mathbb{R}^2$ vermöge $t.(x, y) := (tx, ty)$

$$G.(x, y) := \begin{cases} (0,0), \text{ für: } (x, y) = (0, 0) \\ \text{Strahl ohne 0 , sonst} \end{cases}$$

c) $G = (\mathbb{R}_{>0}, \cdot)$ operiere auf $M = \mathbb{R}^2$ vermöge $t.(x, y) := (tx, t^{-1}y)$

d) $G = K^x$ die mult. Gruppe eines Körpers K, operiere auf $M = K^n \backslash \{0\}$ vermöge

$$t.x := tx \qquad \text{(Skalarmultipl.)}$$

Dann ist jede Bahn $\simeq K^x$

e) $G = \{e, (123), (132)\} \subset S_4$
Wobei $(123), (132)$ hier Zykel sind:

d.h. genauer: $(123) : 1 \mapsto 2, 2 \mapsto 3, 3 \mapsto 1, 4 \mapsto 4$ und
$(132) : 1 \mapsto 3, 2 \mapsto 1, 3 \mapsto 2, 4 \mapsto 4$

dann ist $G \simeq \mathbb{Z}/_3$ und somit: $G = \{e, \xi, \xi^2\}$
Setzte $M = \{1, ..., 4\} \times \{1, ..., 4\}$ Dann ist die $G-$Wirkung auf M:

$$a.(x, y) := (a.x, a.y) \qquad \text{(Diagonaloperation)}$$

Wir erhalten 4 Klassen:
$G.(1,1) = \{e.(1,1), (123).(1,1), (132).(1,1)\} = \{(1,1), (2,2), (3,3)\} = G.(2,2) = G.(3,3)$
$G.(1,2) = \{(1,2), (2,3), (3,1)\} = G.(2,3) = G.(3,1)$
$G.(3,4) = \{(3,4), (1,4), (2,4)\} = G.(1,4) = G.(2,4)$
$G.(4,4) = \{(4,4)\}$
$G.(1,3) = \{(1,3), (2,1), (3,2)\} = G.(2,1) = G.(3,2)$
$G.(4,1) = \{(4,1), (4,2), (4,3)\} = G.(4,2) = G.(4,3)$

f) $GL(n, \mathbb{C})$ operiere auf $M(n, \mathbb{C})$ durch Konjugation:

$$T.A := TAT^{-1}$$

Das heißt hier sind die Bahnen gerade die Matrizen mit gleicher Jordan-Normalform bis auf Permutation der Jordanblöcke.

Exkurs Zykelschreibweise für Elemente von $S_n = B_{ij}(\{1, ..., n\})$:
$\sigma \in S_n$ betrachte die durch die Potenzen von σ erzeugte Untergruppe :

$$< \sigma >= \{\sigma^n \in S_n \mid n \in \mathbb{Z}\} \subset S_n$$

Die Wirkung $< \sigma >$ auf $M = \{1, ..., n\}$ zerlegt M in paarweise disjunkte Bahnen (= Zykel). Z.B.:
$\sigma = (123) \in S_4$
In der Zykelschreibweise geben wir die durchlaufenen Bahnen von σ gemäß der von σ gegebenen Reihenfolge.
Zudem gilt hier das einelementige Bahnen weggelassen werden können und dass Permutationen als gleich angesehen werden:

$$(123) = (123)(4) = (231)(4) = (312)(4) = (4)(123)$$

je nach Startpunkt
Ein Beispiel sei $(173)(24) \in S_7$ Dies entspricht der Abbildung:

$$1 \mapsto 7, 2 \mapsto 4, 3 \mapsto 1, 4 \mapsto 2, 5 \mapsto 5, 6 \mapsto 6, 7 \mapsto 3$$

1.6 Standgruppen und die Struktur von Bahnen:

Definition: Ist M ein $G-$Raum, $x \in M$, so heißt

$$G_x := \{a \in G \mid a.x = x\}$$

Die Standgruppe (oder auch Isotropiegruppe , Stabilisator) von x.

Satz: Ist M ein $G-$Raum, die für $x \in M$ induzierte Abbildung $F : G \to M$ mit $a \mapsto a.x$ ist eine Bijektion des Quotientenraums $G/_{G_x}$ von G nach der Wirkung von G_x von rechts ($a \sim b :\Leftrightarrow \exists c \in G_x . b = ac$) mit der Bahn $G.x$.

Beweis:
Wir wissen, das $Bild(F) = G.x$ nach Def. von F und der Bahn. Nun müssen wir noch überprüfen, ob F auf den Äquivalenzklassen (der G_x-Wirkung) konstant ist:
$\forall a \in G$ und $\forall c \in G_x$: $F(ac) = (ac).x = a.(c.x) = a.x = F(a)$ (im vor letzten Schritt: $c \in G_x$)
Dies zeigt bereits: F induziert eine Surjektion

$$\bar{F} : G/_{G_x} \to G.x$$

Nun müssen wir noch zeigen, dass $\bar{F}$ auch injektiv ist:
Seinen $[a], [b] \in G/_{G_x}$ und $\bar{F}([a]) = \bar{F}([b])$.
$\overset{\text{Def}}{\Rightarrow} F(a) = F(b) \Rightarrow a.x = b.x \Rightarrow (b^{-1}a).x = b^{-1}.(a.x) = b^{-1}.(b.x) = (b^{-1}b).x = e.x = x$
$\Rightarrow c := b^{-1}a \in G_x \Rightarrow a = b.c \Rightarrow [a] = [b]$

□

Merke:

$$\text{(Äquivalenzklasse)} \qquad G/_{G_x} = G.x \qquad \text{(Teilmengen)}$$

hier ist wirklich Gleichheit gemeint, also dies ist eine kanonische Bijektion.

1.7 Beispiele

a) $G = S_4$ wirke auf $\mathbb{R}^4$ durch Permutation der Koordinaten:
$\sigma.(\lambda_1, ..., \lambda_4) = (\lambda_{\sigma(1)}, .., \lambda_{\sigma(4)})$.
Es gilt: $|G| = |S_4| = 24$

i) Standgruppe von $x = (\lambda, \lambda, \mu, \mu), \lambda \neq \mu$
$G_x = \{e, (12), (34), (12)(34)\}, \mid G_x \mid = 4$
Bahn:

$$G.x = \{(\lambda, \lambda, \mu, \mu), (\lambda, \mu, \lambda, \mu,), (\mu, \lambda, \lambda, \mu,), (\mu, \lambda, \mu, \lambda), (\mu, \mu, \lambda, \lambda), (\lambda, \mu, \mu, \lambda)\}$$

also $\mid G.x \mid = 6$ damit ist $\mid G \mid = \mid G.x \mid \cdot \mid G_x \mid = 6 \cdot 4 = 24$

ii) $x = (\lambda, \lambda, \lambda, \mu), \lambda \neq \mu$
$G_x = \{e, (123), (132), (12), (23), (13)\} \simeq S_3 \subset S_4$ also $\mid G_x \mid = 6$
Dann ist

$$G.x = \{(\lambda, \lambda, \lambda, \mu), (\lambda, \lambda, \mu, \lambda), (\lambda, \mu, \lambda, \lambda), (\mu, \lambda, \lambda, \lambda)\}$$

und $\mid G \mid = \mid G.x \mid \cdot \mid G_x \mid = 4 \cdot 6 = 24$

b) $G = GL(n, \mathbb{C})$, $G \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ =? Übung in LA.

Bemerkung: in Beispiel a)i) ist G_x die Kleinsche Vierergruppe.

1.8 Standgruppen längs einer Bahn

Satz: Sein M ein $G-$Raum, $x \in M$, $y = a.x \in G_x$. Dann gilt:

$$G_y = a \cdot G_x \cdot a^{-1}$$

also jedes Element von G_x konjugieren.

Beweis:
" $\subset$ " $b \in G_y \overset{\text{Def}}{\Rightarrow} b.y = y \Rightarrow b.(a.x) = a.x \Rightarrow (ba).x = a.x \Rightarrow (a^{-1}ba).x = e.x = x \Rightarrow a^{-1}ba \in G_x$

" $\supset$ " Da auch $x = a^{-1}.y$, d.h $x \in G.y$, zeigt die Hinrichtung " $\subset$ " schon:

$$G_x \subset (a^{-1}) \cdot G_y \cdot (a^{-1})^{-1} = a^{-1} \cdot G_y \cdot a$$
$$\Rightarrow \; a \cdot G_x \cdot a^{-1} \subset (a \cdot (a^{-1} \cdot G_y \cdot a) \cdot a^{-1} = G_y$$

□

Beispiel: Standwirkung von S_3 auf $M = \{1, 2, 3\}$.
Sei $x = 1$, $G_x = \{e, (23)\}$, $a = (123), G_{(123).x} = G_2 = \{e, (13)\}$ Aber ebenso: $G_{(12).x} = \{e, (13)\}$ denn:

$(123) \cdot G_x \cdot (123)^{-1} = \{e, (123) \cdot (23) \cdot (123)^{-1} (= 132)\} = \{e, (13)\} = G_2$ und:

$(12) \cdot G_x \cdot (12)^{-1} = \{e, (12) \cdot (23) \cdot (12)^{-1}\} = \{e, (13)\} = G_2$

Bei endlichen Gruppen haben alle Punkte einer Bahn die gleiche Kardinalität. Und längs einer Bahn kommt jede beliebige Gruppe vor.

1.9 Transitive Wirkungen

Hier gibt es nur eine Bahn.

Definition: G operiert auf M transitiv, falls ein $x \in M$ existiert mit

$$M = G.x \qquad (\Rightarrow \forall y \in M : G.y = M)$$

M heißt dann auch $(G-)$ homogener Raum.

Bemerkung: Aus (1.6) folgt dann: M ist isomorph als $G-$Raum zu $G/_{G_x}$. D.h. die Wirkung: $a.[b] := [ab]$ ist wohldef., da G_x auf G von rechts operiert.
Umgekehrt tritt jede Untergruppe $H \subset G$ als Isotrophiegruppe einer transitiven $G-$Wirkung auf, nämlich auf dem Raum $G/_H$, dem Raum der Links-Nebenklassen bzgl. H.

Wiederholung:

$G.x \subset M$ Bahn

$G_x \subset G$ Stabilisator

$G/_{G_x} \to G.x, [g] \mapsto g.x$ Bijektion

Transitive Wirkung: $G.x = M$

1.10 Nebenklassen

Definition: Sei G eine Gruppe

a) $H \subset G$ heißt Untergruppe, falls $e \in H$, $H \cdot H \subset H$ (Hier sogar Gleichheit gefordert!)

b) $G/_H$ist der Quotient von G nach der Äquivalenzrelation $a \sim b :\Leftrightarrow \exists h \in H : b = ah$
(H operiert auf G von rechts)

c) $H\backslash^G$ist der Quotient von G nach der Äquivalenzrelation $a \sim b :\Leftrightarrow \exists h \in H : b = ha$
(H operiert auf G von links).

d) Elemente von $G/_H : aH$ heißen Linksnebenklassen von H in G

Elemente von $H\backslash^G : Ha$ Rechtsnebenklassen von H in G

Beobachtung: $G = \bigsqcup_{[a] \in G/_H} [a] = \bigsqcup_{[a] \in G/_H} aH = \bigsqcup_{[a] \in H\backslash^G} [a] = \bigsqcup_{[a] \in H\backslash^G} Ha$
($\bigsqcup$ ist disjunkte Vereinigung)

1.11 $G-$Wirkung auf $G/_H$:

$$G \times G/_H \to G/_H \textbf{ mit: } (a, bH) \mapsto abH$$

wohldefiniert: angenommen wir hätten $b' = bh$, $h \in H$ einen anderen Repräsentant von bH, also $b'H = bH$

$$\Rightarrow ab'H = abhH = abH$$

denn $H \to H,\ h' \mapsto hh'$ ist bijektiv.
Diese Wirkung ist transitiv nach Definition.
Standgruppe von $[e] : G_{[e]} = \{a \in G \mid aH = H\} = H$

1.12 Zusammenfassung von 1.6 - 1.11:

Jede $G-$Bahn einer $G-$Wirkung auf einer Menge M ist isomorph als $G-$Raum zu $G/_H$ für eine Untergruppe $H \subset G$, und jede Untergruppe $H \subset G$ tritt auf diese Weise auf.

1.13 Anzahlformeln

Satz:

1. Sei Mein endlicher $G-$Raum und $G.x_1, ..., G.x_r$ die paarweise disjunkten Bahnen, dann gilt:

$$|M| = \sum_{i=1}^{r} |G.x_i|$$

2. Sei G eine endliche Gruppe und $H \subset G$ eine Untergruppe, dann gilt:

$$|G| = |G/_H| \cdot |H| = |H^{\backslash^G}| \cdot |H|$$

   Insbesondere $|H| \mid |G|$ (teilt)

Beweis:
a) $M = \bigsqcup_{i=1}^{r} G.x_i$
b) Wende a) an auf die Rechtswirkung von H auf G:

$$G \times H \to G,\ (a, h) \mapsto ah$$

Bahnen = Linksnebenklassen von H in $G \Rightarrow r = |G/_H|$

Ferner: $\forall a \in G : |aH| = |H| \Rightarrow |G| = |M| = \sum_{i=1}^{|G/_H|} |a_i H| = |G/_H| \cdot |H|$.

Analog für $H^{\backslash^G}$mit der Linkswirkung von H auf G.

□

1.14 Anwendung: Ordnung von Gruppenelementen

Definition: Sei G eine Gruppe. Die Ordnung $ord(g)$ eines Gruppenelementes $g \in G$ ist die Kardinalität der von g erzeugten Untergruppe

$$< g >:= \{g^n \mid n \in \mathbb{N}\backslash\{0\}\} \subset G \qquad (g^0 := e)$$

Bemerkung:

- alternativ: $ord(g) = \begin{cases} \infty & \text{, falls } \forall n \in \mathbb{N}\backslash\{0\} \text{ gilt } g^n \neq e \\ min\{n \in \mathbb{N}\backslash\{0\} \mid g^n = e\} & \text{, sonst} \end{cases}$

Korollar (aus Satz 1.13) $|G| < \infty \Rightarrow ord(g) \mid |G|$ (teilt).

Bemerkung: Später (zyklische Gruppen): $< g > \simeq \begin{cases} \mathbb{Z} & , ord(g) = \infty \\ \mathbb{Z}/_{ord(g)} & , \text{sonst} \end{cases}$

Beispiel: $|G| = p$, p prim, $\Rightarrow G \simeq \mathbb{Z}/_p$
Beweis:
Wähle $g \in G \backslash \{e\} \Rightarrow ord(g) \neq 1$, teilt aber p $\Rightarrow ord(g) = p$. $\Rightarrow G = \{e, g, g^2, ..., g^{p-1}\}$
dann ist der Isomorphismus gegeben mit:

$$iso : \mathbb{Z}/_p \to G,\ k \mapsto g^k$$

explizit: $G = \mathbb{Z}/_5$, $g = 2$: $\{e = 0, 2, 4, 6, 3\} \equiv \{0, 2, 4, 1, 3\}\ mod\ 5 = \mathbb{Z}/_5$

1.15 Index einer Untergruppe

Definition: Sei G eine Gruppe, $H \subset G$ eine Untergruppe mit einer endlichen Menge der Linksnebenklassen $(G/_H)$. Dann heißt

$$[G : H] := |G/_H|$$

Index von H in G.

Bemerkung: Wenn $|G| < \infty \overset{(1.13)}{\Rightarrow} [G : H] \mid |G|$

1.16 Der Bahnenraum M/G:

Ist M ein $G-$Raum und $x, y \in M$, so gilt entweder $G.x = G.y$ oder $G.x \cap G.y = \emptyset$:

$$\begin{aligned} z \in G.x \cap G.y &\Rightarrow \exists b, a \in G \text{ mit } z = a.x = b.y \\ &\Rightarrow x = (a^{-1}b).y \in G.y \\ &\Rightarrow G.x = G.(a^{-1}b.y) = (Ga^{-1}b).y = G.y \end{aligned}$$

2 Normale Untergruppen und Kerne

Für Mengen oder Vektorräume haben alle Teilmengen bzw. Unterräume (die strukturerhaltenden Teilmengen) die gleichen "Güte". Für Gruppen bilden die Kerne von Homomorphismen aber ausgezeichnete Unterobjekte, die normalen Untergruppen.

2.1 Normalteiler

Definition: Sei G eine Gruppe, eine Untergruppe $H \subset G$ heißt normal (oder Normalteiler), falls gilt:

$$\forall a \in G : aHa^{-1} = H \text{ (nur als Menge zu sehen)}$$

anders ausgedrückt: $(\forall h \in H : aha^{-1} \in H)$
Formelzeichen: $H \lhd G$ (für Untergruppen $H < G$).

Bemerkung: Es reicht $aHa^{-1} \subset H$ zu zeigen, dann gilt nämlich:

$$H = (aa^{-1})H(aa^{-1}) = a(a^{-1}Ha)a^{-1} \subset aHa^{-1}$$

Ebenso reicht: $\forall a \in G :\ aH = Ha$ (Linksnebenklassen = Rechtsnebenklassen)
Beweis:
"$\Rightarrow$" $H = (a^{-1}a)H = a^{-1}(aH) = a^{-1}Ha$
"$\Leftarrow$" $H = aHa^{-1} \Leftrightarrow aH = Ha$

□

Beispiele:

a) $G = S_3$, so ist $H = \{e, (12)\}$ nicht normal, denn etwa für $a = (13)$:

$$aHa^{-1} = \{e, (13) \circ (12) \circ (13)^{-1}\} = \{e, (23)\} \neq H$$

also keine normale Untergruppe.

b) $G = S_3$, so ist $H = \{e, (123), (132)\}$ ist normal, denn $\forall a \in S_3$ ist:

$$ord(aha^{-1}) = ord(h) \quad \text{und} \quad ord((123)) = ord((132)) = 3$$

c) $Aff(\mathbb{R}^n) = \{\varphi + v \mid \varphi \in GL(n, \mathbb{R}), v \in \mathbb{R}^n\}$. Die Translationen

$$T = \{id + v \mid v \in \mathbb{R}^n\} \subset Aff(\mathbb{R}^n) \quad , \quad T \simeq (\mathbb{R}^n, +)$$

bilden eine normale Untergruppe (oder einen Normalteiler.

NR: $a = \varphi + v \Rightarrow a^{-1} = \varphi^{-1} - \varphi^{-1}(v)$:
denn:
$a \circ a^{-1} = a \circ (\varphi^{-1} - \varphi^{-1}(v)) = \varphi(\varphi^{-1} - \varphi^{-1}(v)) + v = id - v + v = id$

$a^{-1} \circ a = a^{-1} \circ (\varphi + v) = \varphi^{-1}(\varphi + v) - \varphi^{-1}(v) = id$

Sei $\tau = id + u \in T$, $a = \varphi + v \in Aff(\mathbb{R}^n)$

$a \circ \tau \circ a^{-1} = \varphi(\tau \circ a^{-1}) + v = \varphi(a^{-1} + u) + v = \varphi(\varphi^{-1} - \varphi^{-1}(v) + u) + v = id + \varphi(u)$

$\Rightarrow Gl(n, \mathbb{R}) \subset Aff(\mathbb{R}^n)$ ist keine normale Untergruppe.

d) In einer abelschen Gruppe ist jede Untergruppe normal.

2.2 Die Restklassengruppe

Satz: $H \subset G$ ist ein Normalteiler gdw. die Gruppenstruktur auf G eine solche auf $G/_H$ induziert.
Beweis:
Erinnerung: $[a] := aH$
" $\Rightarrow$ ": Es ist wohldefiniert:

$$(aH)(bH) \overset{H \text{ normal}}{=} a(bHb^{-1})bH \overset{H \cdot H = H}{=} (ab)HH = (ab)H$$

Dies zeigt: $[a] \cdot [b] := [a \cdot b]$ ist wohldefiniert.
Assoziativität wird "geerbt"von G : $([a] \cdot [b]) \cdot [c] = [a \cdot b \cdot c] = [a] \cdot ([b] \cdot [c])$
Neutrales Element:$[e] = H$
" $\Leftarrow$ " :

$$\forall a \in G : aHa^{-1} \overset{\text{Def}}{\subset} (aH)(a^{-1}H) = [a] \cdot [a^{-1}] = [aa^{-1}] = [e] = H$$

□

(Lieblings-) Beispiel: $Aff(\mathbb{R}^n)/_{\mathbb{R}^n} \overset{\simeq}{\to} GL(n, \mathbb{R}),\ [\varphi + v] \mapsto \varphi$ ist wohldefiniert.

2.3 Normalteiler und Kerne

Satz: Ist $\varphi : G \to G'$ ein Gruppenhom., so ist $ker(\varphi) \subset G$ normal und jeder Normalteiler tritt in dieser Weise (für irgendein φ) auf.
Beweis:
" $\Rightarrow$ "~~z~~ : $a \in \ker(f), b \in G \Rightarrow bab^{-1} \in ker(\varphi)$.
In der Tat gilt:

$$\varphi(bab^{-1}) \overset{\text{Hom.}}{=} \varphi(b) \underbrace{\varphi(a)}_{=e} \varphi(b^{-1}) = \varphi(b)\varphi(b^{-1}) \overset{\text{Hom.}}{=} \varphi(bb^{-1}) = \varphi(e) = e$$

" $\Leftarrow$ " : $H \lhd G \Rightarrow \varphi : G \to G/_H, a \mapsto [a] = aH$ hat $ker(\varphi) = H$, denn

$$\varphi(a) = [e] \Leftrightarrow aH = H \Leftrightarrow a \in H$$

□

2.4 Induzierte Abbildungen

Satz: Sei $\varphi : G \to G'$ ein Gruppenhom. und $H \lhd G$ mit $H \subset ker(\varphi)$. Dann gibt es genau einen Gruppenhom. $\bar{\varphi} : G/_H \to G'$ mit (*) $\varphi = \bar{\varphi} \circ q$ mit $q : G \to G/_H$ die Quotientenabbildung
Beweis:
Es muss gelten (Eindeutigkeit): $\bar{\varphi}([a]) = \bar{\varphi}(q(a)) = (\bar{\varphi} \circ q)(a) \overset{(*)}{=} \varphi(a)$
Umgekehrt ist (Existenz): $\bar{\varphi}([a]) := \varphi(a)$ ist wohldefiniert:

$$\varphi(aH) = \varphi(a) \cdot \varphi(H) \overset{H \subset ker(\varphi)}{=} \varphi(a) \cdot \{e\} = \{\varphi(a)\}$$

□

2.5 Die Struktur von Gruppenhomomorphismen

Erinnerung aus LA: $\varphi : V \to W$ lineare Abbildung zwischen K-VRen faktorisiert wie folgt:
$V \overset{q}{\twoheadrightarrow} V/_{ker(\varphi)} \underset{\simeq}{\overset{\bar{\varphi}}{\to}} Im(\varphi) \hookrightarrow W$ ($\hookrightarrow$ ist Inklusion eines Unterraums, injektiv), ($\twoheadrightarrow$ Surjektion).
Für Gruppen:

Satz: Ein Gruppenhom. $\varphi : G \to G'$ induziert einen Isomorphismus $\bar{\varphi} : G/_{ker(\varphi)} \to Im(\varphi)$. Insbesondere erhält man eine Faktorisierung:

$$G \overset{q}{\twoheadrightarrow} G/_{ker(\varphi)} \underset{\simeq}{\overset{\bar{\varphi}}{\to}} Im(\varphi) \hookrightarrow G'$$

Beweis:
$\bar{\varphi}$ ist surjektiv nach Def.
$\bar{\varphi}$ ist injektiv:

$$\bar{\varphi}([a]) = e \Rightarrow \varphi(a) = e \Rightarrow a \in ker(\varphi) \Rightarrow [a] = [e] \in G/_{ker(\varphi)}$$

d.h. zu zeigen ist: $ker(\bar{\varphi}) = \{[e]\}$
Wir wissen: $ker(\psi : G_1 \to G_2) = \{e\} \Rightarrow \psi$ injektiv, denn:

$$\psi(a) = \psi(b) \Rightarrow \psi(ab^{-1}) = e \Rightarrow ab^{-1} = e \Rightarrow a = b$$

□

2.6 Bilder & Urbilder von Normalteilern

Satz: Sei $\phi : G \to G'$ ein Gruppenhom.

a) $N' \lhd G' \Rightarrow \phi^{-1}(N') \lhd G$. ("Urbilder von Normalteilern sind normal")

b) $N \lhd G$ und ϕ surjektiv $\Rightarrow \phi(N) \lhd G'$.

Beweis:
a) $a \in \phi^{-1}(N'), b \in G$. ↯ : $bab^{-1} \in \phi^{-1}(N')$:

$$\phi(bab^{-1}) = \phi(b)\phi(a)\phi(b^{-1}) \in N' \text{ , da } \phi(a) \in N',\ N' \lhd G'$$

b) $a \in N, b' \in G'$. ↯ $b'\phi(a)(b)^{-1} \in \phi(N)$, da aber ϕ surjektiv $\Rightarrow \exists b \in G : b' = \phi(b)$. Damit:

$$b'\phi(a)(b')^{-1} = \phi(b)\phi(a)\phi(b)^{-1} = \phi(bab^{-1}) \in \phi(N), \text{ da schon } bab^{-1} \in N \text{ , denn: } N \lhd G$$

□

2.7 (Erster) Isomorphiesatz (Kürzungsregel für normale Untergruppen)

Satz: Sei G eine Gruppe und sein $K \lhd G$, $H \lhd G$ zwei Normalteiler mit $K \subset H$. ($\Rightarrow K \lhd H$)
Dann ist

$$H/_K \subset G/_K$$

normal und die Komposition kanonischer Abbildungen

$$\phi : G \overset{q_1}{\twoheadrightarrow} G/_K \overset{q_2}{\twoheadrightarrow} (G/_K)/(H/_K), \quad a \mapsto [a] \mapsto [[a]]$$

induziert einen kanonischen Isomorphismus $G/_H \simeq (G/_K)/_{(H/_K)}$.
Beweis:

1) $\underline{H/_K \lhd G/_K}$: $a \in H, b \in G$, dann gilt: $b(\underbrace{aK}_{\in G/_K})b^{-1} \in bHb^{-1} \overset{H \text{normal}}{=} H$

2) $\underline{ker(\phi) = H}$:
" $\supset$ " : $a \mapsto [a] \mapsto [[a]]$.$\surd$
" $\subset$ " : $a \in ker(\phi) \Rightarrow [a] = aK = q_1(a) \in ker(q_2) = H/_K = \{hK \mid h \in H\} \subset G/_K \Rightarrow \exists h \in H$: $aK = hK \subset H \Rightarrow aH \subset H \Rightarrow a \in H$.
Nun fertig nach Satz (2.5).

Der zweite Isomorphiesatz wird in den Übungen behandelt.

□

3 Zyklische Gruppen

3.1 Definition

Eine Gruppe G heißt zyklisch, falls ein $a \in G$ existiert mit $G =< a >= \{a^n \mid n \in \mathbb{Z}\}$
Bemerkung:
G ist dann abelsch: $a^\mu \cdot a^\nu = a^{\mu+\nu} = a^{\nu+\mu} = a^\nu \cdot a^\mu$.

3.2 Beispiele:

a) $(\mathbb{Z}, 0, +)$ ist zyklisch: $\mathbb{Z} =< 1 >$, d.h. 1 ist additiver Erzeuger.

b) $\mathbb{Z}/_n$ ist zyklisch, $\mathbb{Z}/_n =< [1] >$.

c) $G = \mathbb{Z}/_2 \times \mathbb{Z}/_2$ ist nicht zyklisch, denn $\forall a \in G : a^2 = e \Rightarrow | < a > | \leq 2$ aber $|G| = 4$
(Achtung: $\mathbb{Z}/_2 \times \mathbb{Z}/_2$ ist nicht isomorph zu $\mathbb{Z}/_4$!)

d) $|G| = p$ prim. $\Rightarrow G$ zyklisch. In der Tat: $G \simeq \mathbb{Z}/_p$, siehe Bsp. 1.14.

3.3 Untergruppen von $\mathbb{Z}$

Satz: Jede Untergruppe $H \subset \mathbb{Z}$ ist zyklisch, d.h.$\exists n \in \mathbb{N} : H =< n >= n \cdot \mathbb{Z}$
Beweis:
Fall 1: Ist $H = \{0\}$, so ist $H = n \cdot \mathbb{Z}$ mit $n = 0$.
Fall 2: $H \neq \{0\}$, dann gibt es ein kleinstes $n \in \mathbb{N}\backslash\{0\}$ mit $n \in H \not\subset_{\mathbb{Z}} H =< n >$:
" $\subset$ " mit jedem Element liegen auch die Vielfachen drin.
" $\supset$ " $m \in H$ Teilen mit Rest: $m = an + b,\ b \in \{0, ..., n-1\}, a \in \mathbb{Z}$ (**)
$\Rightarrow b = m - an \in H$ und $b < n$
$\Rightarrow b = 0$ nach Wahl von n
$\Rightarrow m = an \in < n >$

□

Bemerke: in (**) betrachten wir eigentlich: $an = n^a = n + n + n + ... + n$ a mal

3.4 Struktur zyklischer Gruppen

Satz: Sei $G =< a >$ eine zyklische Gruppe. Betrachte $\varphi : \mathbb{Z} \to G,\ \nu \mapsto a^\nu$. Es gilt das folgende:

1. entweder: $ord(a) = \infty$ und φ ist ein Isomorphismus
2. oder: $ord(a) < \infty$ und φ induziert einen Isomorphismus $\bar{\varphi}\mathbb{Z}/_n \to G$ für ein $n \in \mathbb{N}\backslash\{0\}$

Beweis:

1. φ ist Hom.: $\varphi(\mu + \nu) = a^{\mu+\nu} = a^\mu a^\nu = \varphi(\mu)\varphi(\nu)$
2. φ ist surjektiv, da $G =< a >$
   $\overset{2.5}{\Rightarrow}$ φ induziert einen Isomorphismus $\bar{\varphi} : \mathbb{Z}/ker(\varphi) \to G$
   $\overset{3.3}{\Rightarrow}$ $ker(\varphi) = n\mathbb{Z}$ für ein $n \in \mathbb{N}$
   - $n = 0$: liefert (1.)
   - $n > 0$: liefert (2.)

□

3.5 Korollar:

Im Fall (2) gilt:

$$ord(a) = \min\{\nu \in \mathbb{N}\backslash\{0\} \mid a^\nu = e\} \text{ und } G = \{e, a, a_2, , , , a^{n-1}\} = \{a^0, ..., a^{n-1}\}$$

□

3.6 Untergruppen

Satz: Jede Untergruppe einer endlichen zyklischen Gruppe $G =< a >$ ist selbst eine zyklische Gruppe. Ferner hat man für $|G| < \infty$ eine Bijektion für :

$$\Lambda : \{Teiler\ d \in \mathbb{N} \text{ von } |G|\} \to \{H \subset G \text{ Ugrp.}\},\ d \mapsto < a^d >$$

Beweis:

1. $|G| = \infty \Rightarrow G \simeq \mathbb{Z}$, fertig mit Satz 3.3
2. Also o.E. (Satz 3.4): $G = \mathbb{Z}/n$, $n \in \mathbb{N}\backslash\{0\}$.

   Betrachte: $q : \mathbb{Z} \to \mathbb{Z}/_n$ die kanonische Abbildung.
   Sei nun $H \subset \mathbb{Z}/_n$ Ugrp. $\Rightarrow q^{-1}(H) \subset \mathbb{Z}$ Ugrp.

   $$\overset{3.3}{\Rightarrow} \exists d \in \mathbb{N} : q^{-1}(H) = d\mathbb{Z}\ , (d \neq 0\ ,\ \text{da } n \in \mathbb{N}\backslash\{0\}$$

   Ferner:

   $$d\mathbb{Z} = q^{-1}(H) \supset ker(q) = n\mathbb{Z}, \Rightarrow d \mid n$$

   Dies zeigt: $H = q(q^{-1}(H)) =< d >\subset \mathbb{Z}/_n \ \Rightarrow \Lambda$ ist surjektiv.

   Λ ist injektiv:

   $$\begin{aligned} < d > = < d' > \subset \mathbb{Z}/_n,\ d \mid |G| \ &\Rightarrow d\mathbb{Z} = q^{-1}(< d >) = q^{-1}(< d' >) = d'\mathbb{Z} \\ &\Rightarrow d \mid d' \text{und } d' \mid d \\ &\Rightarrow d = d' \end{aligned}$$

□

3.7 Zerlegung Zyklischer Gruppen (Chinesischer Restsatz)

Satz: Ist $m = q_1, ..., q_r$ mit paarweise teilerfremden $q_i \in \mathbb{N}\backslash\{0\}$, so ist:

a) die kanonische Abbildung

$$\varphi : \mathbb{Z}/_m \to \mathbb{Z}/_{q_1} \times ... \times \mathbb{Z}/_{q_r},\ a + m\mathbb{Z} \mapsto (a + q_1\mathbb{Z}, ..., a + q_r\mathbb{Z})$$

ein Isomorphismus. Insbesondere ist

$$\mathbb{Z}/_{q_1} \times ... \times \mathbb{Z}/_{q_r}$$

zyklisch.

b) (Chinesischer Restsatz - klassische Form)
Für alle $a_1, ..., a_r \in \mathbb{Z}$ sind die simultanen Kongruenzen

$$\begin{aligned} a &\equiv a_1 \quad mod\ q_1 \\ a &\equiv a_2 \quad mod\ q_2 \\ &\vdots \quad \vdots \qquad \vdots \\ a &\equiv a_r \quad mod\ q_r \end{aligned}$$

eindeutig lösbar modulo m (gesucht ist a)
Beweis:
$a) \Rightarrow b)$: $a = \varphi^{-1}(a_1, ..., a_r)$. Das heißt :

$$\text{Existenz von } a \Leftrightarrow \varphi \text{ surjektiv}$$
$$\text{Eindeutigkeit von } a \Leftrightarrow \varphi \text{ injektiv}$$

$a)$ Induktion nach r:

- $r = 1$: ist trivial: $id : \mathbb{Z}/_1 \to \mathbb{Z}/_1, a + 1\mathbb{Z} \mapsto 1 + 1\mathbb{Z}$
- $r = 2$: Übung Blatt 1 Aufgabe 2. ($\exists \alpha_1, \alpha_2 \in \mathbb{Z} :\ \alpha_1 q_1 + \alpha_2 q_2 = 1$
  (α_1, α_2 erhält man via Euklidischem Algorithmus.)
- $(r-1) \to r, (r > 2)$: Setze $q' := q_1,\ q'' := q_2 \cdot ... \cdot q_r$.

Diese sind teilterfremd. Nach Induktion sind die kanonischen Abbildungen:

$$\mathbb{Z}/_{q''} \overset{\varphi_1}{\Rightarrow} \mathbb{Z}/_{q_2} \times ... \times \mathbb{Z}/_{q_r}$$

$$\mathbb{Z}/_m \overset{\varphi_2}{\Rightarrow} \mathbb{Z}/_{q'} \times \mathbb{Z}/_{q''}$$

Isomorphismen.
$\Rightarrow$ Die Komposition

$$\varphi : \mathbb{Z}/_m \overset{\varphi_2}{\Rightarrow} \mathbb{Z}/_{q'} \times \mathbb{Z}/_{q''} \overset{id \times \varphi_1}{\Rightarrow} \mathbb{Z}/_{q_1} \times ... \times \mathbb{Z}/_{q_r}$$

ist auch ein Isomorphismus:

$$a + m\mathbb{Z} \mapsto (a + q'\mathbb{Z}, a + q''\mathbb{Z}) \mapsto (a + q_1\mathbb{Z}, ..., a + q_r\mathbb{Z})$$

□

4 Endlich erzeugte abelsche Gruppen

Konvention: in diesem Kapitel haben wir die Konvention, dass abelsche Gruppen additiv geschrieben werden, also

- $ab \rightsquigarrow a + b$
- $a^d \rightsquigarrow d \cdot a,\ d \in \mathbb{Z}, a \in G$

- $< a_1, ..., a_r > \rightsquigarrow \mathbb{Z}/_{a_1} + ... + \mathbb{Z}/_{a_r}$

Sei G abelsch und endlich erzeugt, d.h. $\exists a_1, ..., a_r \in G : G =< a_1, ..., a_r >$.
Wir suchen Klassifikationen.

Beispiel: $|G| = 4 \Rightarrow G \simeq \mathbb{Z}/_4$ oder $G \simeq \mathbb{Z}/_2 \times \mathbb{Z}/_2 =< (1,0), (0,1) >$. Wir werden sehen, dass stets $G \simeq \mathbb{Z}/_{n_1} \times ... \times \mathbb{Z}/_{n_r},\ n_i \in \mathbb{N}$ gilt.
$(\forall i : n_i > 0 \Rightarrow |G| = n_1 + ... + n_r)$ (soll hier + stehen ????)
Die n_i kann man eindeutig auf zwei Arten erhalten:

4.1 Hauptsatz über endlich erzeugte abelsche Gruppen

Sei G eine endlich erzeugte abelsche Gruppe.

(a) Es gibt genau eine endliche Folge natürlicher Zahlen $d_1, ..., d_t \in \mathbb{N}\backslash\{1\} = \{0, 2, 3, ...\}$ mit $d_i \mid d_{i+1}$.
Konvention: $\forall n \in \mathbb{N} : n \mid 0$ und $0 \mid n \Rightarrow n = 0$ gdw. $a \mid b \Leftrightarrow \exists c : b = ca$
Derart, dass

$$G \simeq \mathbb{Z}/_{d_1} \times ... \times \mathbb{Z}/_{d_t}$$

(b) Es gibt bis auf Reihenfolge eindeutige Primzahlpotenzen $q_1 = p_1^{n_1}, ..., q_s = p_s^{n_s}$, ($p_1$ prim) und ein eindeutiges $r \in \mathbb{N}$ mit

$$G \simeq \mathbb{Z}/_{q_1} \times ... \times \mathbb{Z}/_{q_s} \times \mathbb{Z}^r$$

Die p_i brauchen nicht paarweise verschieden zu sein. Wir betrachten sie hier nicht als Gruppenelemente, deshalb verletzen wir unsere Konvention für dieses Kapitel auch nicht.
Beweis:
Wird das gesamte Kapitel beanspruchen.

Beispiele

a) $G = \mathbb{Z}/_6$, dann ist $\mathbb{Z}/_6$ die Darstellung nach (a), $\mathbb{Z}/_2 \times \mathbb{Z}/_3$ die Darstellung nach (b).
Es würde hier auch schon reichen $|G| = 6$ anzugeben, dann würde das gleiche Folgen.

b) $G \overset{darst.(b)}{=} \mathbb{Z}/_2 \times \mathbb{Z}/_{2^2} \times \mathbb{Z}/_{2^3} \times \mathbb{Z}/_3 \times \mathbb{Z}/_{3^3} \times \mathbb{Z}/_5 \overset{darst.(a)}{\simeq} \mathbb{Z}/_2 \times \mathbb{Z}/_{2^2 \cdot 3} \times \mathbb{Z}/_{2^2 3^3 5}$ mit

$$d_1 = 2,\ d_2 = 2^2 \cdot 3,\ d_3 = 2^3 3^3 \cdot 5$$

c) $\mathbb{Z}/_4$: nach Darstellung (a): $\mathbb{Z}/_4$ sonst andere Gruppe, nach (b) : $\mathbb{Z}/_{2^2}$
$\mathbb{Z}/_2 \times \mathbb{Z}/_2$: nach (a): $\mathbb{Z}/_2 \times \mathbb{Z}/_2$ nach (b) : $\mathbb{Z}/_{2^1} \times \mathbb{Z}/_{2^1}$

4.2 Bemerkung:

Ist $G \simeq \mathbb{Z}/_{n_1} \times ... \times \mathbb{Z}/_{n_r}$, so sind die Faktoren $\mathbb{Z}/_{n_i}$ Untergruppen von G. Vermöge:

$$\varphi_i : \mathbb{Z}/_{n_i} \to G,\ [a] \mapsto \varphi^{-1}((0, ..., [a], ..., 0))$$

Diese Untergruppen (und die Zerlegung von G in ein Produkt der $\mathbb{Z}/_{n_i}$) sind aber nicht eindeutig, denn ist etwa

$$\psi : \mathbb{Z}/_{n_i} \to \mathbb{Z}/_{n_1} \times ... \times \mathbb{Z}/_{n_{i-1}} \times \mathbb{Z}/_{n_{i+1}} \times ... \times \mathbb{Z}/_{n_r} \hookrightarrow G$$

nicht trivial ($\neq 0$), so liefert $\varphi_i + \psi$ eine andere Identifikation von $\mathbb{Z}/_{n_i}$ mit einer Ugrp. von G.
Insbesondere gilt die Bemerkung: für $\mathbb{Z}/_{d_i} \subset G$ und für $\mathbb{Z}/_{p_i^{n_i}} \subset G$ im Satz.
Beispiel:
$G = \mathbb{Z}/_2 \times \mathbb{Z}/_2$ hat $\binom{3}{2} = 3$ Zerlegungen als Produkt:
$\forall a, b \in G\backslash\{0\}, a \neq b$ ist $\mathbb{Z}/_2 \times \mathbb{Z}/_2 \to G,\ (m, n) \mapsto ma + nb$ ein Isomorphismus.

Wdh.: G abelsch, endlich erzeugt, dann gilt:

a) $G \simeq \mathbb{Z}_{d_1} \times ... \times \mathbb{Z}_{d_t}$, $d_i | d_{i+1}$

b) $G \simeq \mathbb{Z}/_{q_1^{n_1}} \times ... \times \mathbb{Z}/_{q_s^{n_s}}$, $d_i | d_{i+1}$ p_j prim. mit $q_\alpha = p_\alpha^{s_\alpha}$

4.3 (b) ⇒ (a)

Wir konstruierten die unindizierte Folge $d'_i := d_{t-i}$. Gefordert ist dann $d'_{i+1} | d'_i$. Nach Konvention der Teilbarkeit von 0 müssen wir setzen

$$d'_1 = ... = d'_r = 0 \qquad \text{"verarztet" } \mathbb{Z}^r$$

Durch Übergang zu $G/_{\mathbb{Z}^r} \xrightarrow{\simeq} \mathbb{Z}_{q_1} \times ... \times \mathbb{Z}_{q_s}$ mit $(a_1, ..., a_s, b) \mapsto (a_1, ..., a_s)$ können wir jetzt o.E. $r = 0$ annehmen.
Dann gilt $|G| = q_1 \cdot ... \cdot q_s < \infty$.
Sortiere die q_i nach Primzahlpotenzen, d.h. schreibe q_{ij} statt q_μ mit $q_{ij} := p_i^{n_{ij}}$ mit $p_i \neq p_{i'}$ für $i \neq i'$ und $\forall i, j: \; n_{i,j} \leq n_{i,j+1}$.
Dann ist:

$$(*) \qquad \begin{aligned} d'_1 &:= p_1^{n_{1,s_1}} ... p_e^{n_{e,s_e}} \\ d'_2 &:= p_1^{n_{1,s_1-1}} ... p_e^{n_{e,s_e-1}} \\ &\vdots \qquad\qquad \vdots \\ d'_m &:= p_1^{n_{1,s_1-m+1}} ... p_e^{n_{e,s_e-m+1}} \end{aligned}$$

mit $m := max\ s_1$ und $n_{ij} := 0$ für $j \leq 0$ ist die <u>eindeutige</u> Folge von d'_i mit $d'_{i+1} | d'_i$, die Produkt von q_{ij} ist so, dass $\prod d'_i = |G|$
(hier besser Ausdrücken!!!!)

Mit anderen Worten:
d'_1 := Produkt mit den höchsten Primzahlpotenzen
d'_2 := Produkt mit den zweithöchsten Primzahlpotenzen
$\vdots$
d'_m := Produkt mit den niedrigsten Primzahlpotenzen

Nach dem chinesischem Restsatz (3.7) gilt:

$$\forall i: \; \mathbb{Z}/_{d'_{i+1}} \simeq \mathbb{Z}/_{p_1^{n_{1,s_1-i}}} \times ... \times \mathbb{Z}/_{p_e^{n_{e,s_e-i}}}$$

Und damit folgt aus (b): $G \simeq \mathbb{Z}/_{d'_1} \times ... \times \mathbb{Z}/_{d'_m}$

□

vergleiche Beispiel 4.1.b):
$G \simeq \mathbb{Z}/_2 \times \mathbb{Z}/_{2^2} \times \mathbb{Z}/_{2^3} \times \mathbb{Z}/_3 \times \mathbb{Z}/_{3^3} \times \mathbb{Z}/_{5^2}$
mit $p_1 := 2, p_2 := 3, p_3 = 5$ folgt dann.

$$\begin{array}{lll} n_{11} = 1, n_{12} = 2, n_{13} = 3 & \to s_1 = 3 & \\ n_{21} = 1, n_{22} = 3 & \to s_2 = 2 & \Rightarrow m = 3 \\ n_{31} = 2 & \to s_1 = 1 & \end{array}$$

weiter folgt:

$$\begin{aligned} d'_1 &= 2^{n_{13}} \cdot 3^{n_{22}} \cdot 5^{n_{31}} &&= 2^3 \cdot 3^3 \cdot 5^2 \\ d'_2 &= 2^{n_{12}} \cdot 3^{n_{21}} \cdot 5^{n_{30}} &&= 2^3 \cdot 3 \cdot 1 \\ d'_3 &= 2^{n_{11}} \cdot 3^{n_{20}} \cdot 5^{n_{3,-1}} &&= 2^1 \cdot 1 \cdot 1 \end{aligned}$$

4.4 Zum Beweis von 4.1,b

Zum Beweis von 4.1,b werden wir zunächst den "freien Anteil" $\mathbb{Z}^r$ abspalten.

Definition:

a) Ein Element endlicher Ordnung in einer Gruppe heißt Torisionselement.

b) Eine Gruppe ohne Torisionselemente $\neq e$ heißt torisionsfrei

c) Eine abelsche Gruppe heißt frei, wenn $G \simeq \bigotimes_{i\in I} \mathbb{Z} := \{(n_i)_{i\in I} \in \prod_{i\in I} \mathbb{Z} |\ n_i \neq 0 \text{ für endlich viele } i\}$ für eine Menge I. (Ist G endlich erzeugt, dann ist $G \simeq \mathbb{Z}^r$ für ein r)

4.5 Satz: Charakterisierung von freien Gruppen

Eine torsionsfreie, endlich erzeugte abelsche Gruppe ist frei.

Bemerkung: vorsicht, dies ist nicht nichtig ohne "endlich erzeugt" z.B. ist $\mathbb{Q}$ torsionsfrei, aber nicht frei. (Bew. Übung)

Beweis Satz:
Seien $a_1, ..., a_r \in G$ Erzeuger. $\Rightarrow \varphi : \mathbb{Z}^r \to G,\ (n_1, ..., n_r) \mapsto n_1a_1 + ... + n_ra_r$ ist surjektiv.
φ ist injektiv $\Leftrightarrow a_1, ..., a_r$ sind "linear unabhängig", im folgenden Sinne:

$$n_1a_1 + ... + n_ra_r = 0 \Rightarrow n_1 = ... = n_r = 0$$

Annahme: jede Menge von Erzeugern ist "linear unabhängig".
Wähle unter den Mengen von Erzeugern mit ninimalem r eine aus mit

$$\sum_{i=1}^{r} n_ia_i = 0 \text{ und } \sum_{i=1}^{r} |n_i|$$

auch minimal.
Wenn G torsionsfrei ist und $\forall i : a_i \neq 0$ (Minimalität von r), dann ist $|\{i \mid n_i \neq 0\}| \geq 2$. Sei also o.E. $n_1, n_2 \neq 0$, genauer $0 < n_1 \leq n_2$ (evtl. $1 \leftrightarrow 2$, und $a_i \leftrightarrow -a_i$)
Betrachte das neue Erzeugendensystem:

$$a_1' := a_1 + a_2, a_i' := a_i,\ i \geq 1$$

Relation: $0 = n_1a_1' + (n_2 - n_1)a_2' + n_3a_3' + ... + n_ra_r'$, aber $|n_2 - n_1| \leq |n_2|$ dies ist ein Widerspruch zur Minimalität von $\sum |n_i|$
$\Rightarrow \exists$ "linear unabhängige" $a_1, ..., a_r$
und für diese gilt:

$$\varphi : \mathbb{Z}^r \to G$$

ist ein Isomorphismus.

□

4.6 Eindeutigkeit von r, Def Rang

Definition: G, H Gruppen, dann ist $Hom(G, H) := \{\varphi : G \to H |\ \varphi \text{ ist Homomorphismus}\}$ die Menge der Homomorphismen.
Dann folgt:

$$(e_1, ..., e_r) \in G \simeq \mathbb{Z}^r \Rightarrow Hom(G, \mathbb{Q}, +) \simeq \mathbb{Q}^r$$

denn

$$Hom(G, \mathbb{Q}) \to \mathbb{Q}^r\ ,\ \varphi \mapsto (\varphi(e_1), ..., \varphi(e_r)$$

ist ein Isomorphismus, mit der Umkehrabbildung:

$$\left(G \to \mathbb{Q}, \sum_{i=1}^{r} n_ie_i \mapsto \sum_{i=1}^{r} n_ia_i\right) \leftarrow\!\shortmid (a_1, ..., a_r)$$

Insbesondere ist $r = dim_{\mathbb{Q}} Hom(G, \mathbb{Q})$ eindeutig festgelegt.

Definition: Für eine endlich erzeugte abelsche Gruppe heißt

$$rk(G) := dim_{\mathbb{Q}} Hom(G, \mathbb{Q})$$

Rang von G. (rk von engl. rank)

Bemerkung: Ist $a \in G$ ein Torsionselement ($a^k = 0, k > 0$), so gilt für alle $\varphi : G \to \mathbb{Q} :\ \varphi(a) = 0$, denn $k \cdot \varphi(a) = \varphi(ka) = \varphi(0) = 0 \in \mathbb{Q}$.
Mit anderen Worten: diese Definition sieht nicht den Torsionsanteil von G.

Bsp.: $\mathbb{Z}/_2 \times \mathbb{Z} = G,\ \{g \in G \mid ord(g) = \infty\} = \{\mathbb{Z}/_2 \times \mathbb{Z} \backslash \{0\}\} = A$ ist keine Untergruppe $G \backslash A = \{(0,0), (1,0)\}$

4.7 Die Torsionsgruppe

Definition: Ist G abelsch, so heißt

$$G_{tor} := \{a \in G \mid ord(a) < \infty\}$$

Torsionsgruppe von G.

Bemerkung: $G_{tor} \subset G$ ist tatsächlich eine Untergruppe, denn: $a, b \in G_{tor} \Rightarrow \exists n, m \neq 0$ mit $ma = 0, nb = 0\ \Rightarrow (mn) \cdot (a + b) = 0 \Rightarrow a + b \in G_{tor}$

□

4.8 Abspalten von G_{tor}

Lemma: Sei G abelsch und endlich erzeugt, und $T := G_{tor}$, dann gilt:

a) $G/_T \simeq \mathbb{Z}^r,\ r = rk(G)$

b) $G \simeq T \times G/_T$

Beweis:
a) Nach Satz 4.5 ist ~~$\mathbb{Z}$~~:

(i) $G/_T$ ist endlich erzeugt

(ii) $G/_T$ ist torsionsfrei

(iii) $rk(G/_T) = rk(G)$

Diese gelten, denn:

(i) Erzeuger von G liefern Erzeuger von $G/_T$. Vermöge $q : G \to G/_T$ (Projektion)

(ii) Sei $\bar{a} \in G/_T$ mit $m\bar{a} = 0$. Wähle $a \in G$ mit $\bar{a} = q(a)$. Dann ist $q(ma) = mq(a) = m\bar{a} = 0$
$\Rightarrow ma \in T \Rightarrow odr(a) < \infty \Rightarrow a \in T \Rightarrow \bar{a} = q(a) = 0$

(iii) $Hom(G, \mathbb{Q}) \simeq Hom(G/\_T, \mathbb{Q})$ denn $\varphi : G \to \mathbb{Q}$ faktorisiert eindeutig über $q : G \to G/_T$
$(\forall a \in T. \varphi(a) \overset{!}{=} 0)$

b) Betrachte die Surjektion:

$$q : G \overset{kan}{\to} G/_T \overset{\simeq}{\to} \mathbb{Z}^r$$

Wähle $a_1, ..., a_r \in G$ mit $q(a_i) = e_i,\ i = 1, ..., r$ (d.h. Standarderzeuger hochheben), dann ist:

$$s : \mathbb{Z}^r \to G,\ (m_1, ..., m_r) \mapsto \sum m_i a_i$$

ein Rechtsinverses zu q (=Spaltung), d.h. $q \circ s = Id_{\mathbb{Z}^r}$, denn $e_i \overset{s}{\to} a_i \overset{q}{\to} e_i$.
Eine Spaltung eines Hom. von abelschen Gruppen liefert eine Produktzerlegung:

$$\psi : T \times \mathbb{Z}^r \to G,\ (a, b) \mapsto a + s(b) \qquad \text{(ist ein Hom. !)}$$

Der Umkehrhomomorphismus dazu ist gegeben durch:

$$\Phi : G \to T \times \mathbb{Z}^r,\ a \mapsto (a - (s \circ q)(a), q(a)$$

dann ist für $a - (s \circ q)(a) \in T$:

$$q(a - (s \circ q)(a)) = q(a) - (q \circ s)(q(a)) = 0 \quad \text{denn}(q \circ s) = Id_{\mathbb{Z}^r}$$

Weiter gilt:

$$\begin{aligned}\Phi \circ \Psi(a,b) = \Phi(a + s(b)) &= (a + s(b) - (s \circ q)(a + s(b)), q(a + s(b)) \\ &= (a + s(b) - \underbrace{s(q(a))}_{=0} - s(\underbrace{(q \circ s)(b)}_{=b}), \underbrace{q(a)}_{=0} + \underbrace{(q \circ s)(b)}_{=b}) \\ &= (a + s(b) - s(b), b) = (a, b)\end{aligned}$$

und

$$\Psi \circ \Phi(a) = \psi(a - (s \circ q)(a), q(a)) = a - (s \circ q)(a) + (s \circ q)(a) = a$$

□

Bemerkung: Spaltung für nicht abelsche Gruppen führt zu einem semidirekten Produkt. (Übung 4.4)

4.9 Bemerkung ?????

Nach 4.8 reicht es jetzt den Hauptsatz 4.1,b für $T = G_{tor}$ zu zeigen. Dazu brauchen wir allerdings noch, dass T endlich erzeugt ist. Das folgt aus dem folgenden Lemma.

Lemma: G endlich erzeugt, abelsch, $H \subset G$ Untergruppe, dann ist auch H endlich erzeugt.
Der Beweis hierzu später.

Bemerkung: Ist T eine endlich erzeugte Tausionsuntergruppe, dann folgt $|T| < \infty$, also:

$$T =< a_1, ..., a_r > \ \Rightarrow \quad T = \left\{ \sum m_i a_i \mid o \leq m_i \leq ord(a_i) \right\}$$

4.10 Zerlegung in $p-$Gruppen

Definition: Sei p prim. Eine $p-$Gruppe ist eine endliche Gruppe, in der die Ordnungen der Elemente $p-$Potenzen sind:

$$\forall a \in G\ \exists e :\ ord(a) = p^e$$

Lemma: Sei T abelsch

a) Für p prim ist
$$T(p) := \{a \in T \mid \exists e :\ ord(a) = p^e\} \subset \mathbb{Z}$$
eine Untergruppe (und eine $p-$Gruppe)

b) Ist $|T| < \infty$, und sind p_n die Primfaktoren von $|T|$, so definiert die Verknüpfung einen Isomorphismus
$$\Phi : T(p_1) \times ... \times T(p_n) \to T$$

Beweis:

a) Beobachtung:
Seien $a, b \in T$, $\alpha := ord(a),\ \beta := ord(b)$, dann ist

$$\alpha\beta(a+b) = \beta(\alpha a) + \alpha(\beta b) = 0 + 0 = 0$$

Woraus folgt, dass $\alpha\beta \in \mathbb{Z} \cdot ord(a+b)$ und daraus:

$$ord(a+b) | ord(a) \cdot ord(b)$$

Inverse: $p^e \cdot a = 0 \Leftrightarrow p^e \cdot (-a) = 0$ Demnach sehen wir wenn: $a, b \in T \Rightarrow a + b \in T(p)$

b) Φ ist surjektiv:

Für $a \in T$ betrachte $< a > \subset T$. Dann ist $< a >$ zyklisch. Dann gilt:

$$\exists m : < a > \simeq \mathbb{Z}/_m \Rightarrow m || T| \qquad \text{also: } m = \prod_{i=1}^{n} p_i^{d_i}$$

Nach dem Chin. Restsatz ist dann:

$$< a > \simeq \mathbb{Z}/_m \xrightarrow{\simeq} \mathbb{Z}/_{p_1^{d_1}} \times ... \times \mathbb{Z}/_{p_n^{d_n}}$$

das Bild von $T(p_i) \cap < a >$ also $\mathbb{Z}_{p_i^{d_i}}$, erzeugt von $a^{\prod_{j \neq i} p_j^{d_j}}$. Dies zeigt: $a \in Im(\Phi)$.
Φ ist injektiv:

Seien $t_i \in T(p_i)$, mit $t_1 + ... + t_n = 0$. Für jedes j zeigen wir: $t_j = 0$.

Setze $t' := t_j,\ \ t'' := \sum_{i \neq j} t_i,\ \ q := |T(p_j)|,\ \ q'' := \prod_{i \neq j} |T(p_i)| = \frac{|T|}{q'}$, also q', q'' sind Teilerfremd.

$\Rightarrow \exists n, m \in \mathbb{Z} :\ mq' + nq'' = 1$

$\Rightarrow t' = (mq' + nq'')t' = m \underbrace{q't'}_{=0} + nq''t' = -nq''t'' = 0$

□

Beispiel:
$Z = \mathbb{Z}/_{2^2} \times \mathbb{Z}/_{2^3} \times \mathbb{Z}/_3 \times \mathbb{Z}/_{3^3} \times \mathbb{Z}/_5$, dann ist:

$$|T| =: p_1 \cdot p_2 \cdot p_3 \qquad \text{mit: } p_1 := 2^5,\ p_2 := 3^4,\ p_3 := 5$$

Damit sind dann:

- $T(2) = \mathbb{Z}/_{2^2} \times \mathbb{Z}/_{2^3} \times \{(0,0,0)\}$
- $T(3) = \{(0,0)\} \times \mathbb{Z}/_3 \times \mathbb{Z}/_{3^3} \times \{0\}$
- $T(3) = \{(0,0)\} \times \mathbb{Z}/_3 \times \mathbb{Z}/_{3^3} \times \{0\}$

4.11 Zerlegung von $p-$Gruppen

Zum Beweis der Existenz im Hauptsatz 4.1,a bleibt noch:

Satz: Zerlegung von $p-$Gruppen:
Jede endliche, abelsche $p-$Gruppe zerfällt in ein Produkt zyklischer $p-$Gruppen.
Beweis durch Induktion nach $|T|$:
IA: $|T| = 1$: trivial.
IS: Wähle $a \in T$ maximaler Ordnung $ord(a) = p^e$:

$$\forall b \in T :\ ord(b) \leq ord(a) \qquad (\Rightarrow q \neq 0)$$

Betrachte die von a erzeugte zyklische Untergruppe $< a > \simeq \mathbb{Z}/_{p^e}$ (da $p-$Gruppe).
Weiter sei $H \subset T$ maximal unter den Untergruppen mit $H \cap < a > = \{0\}$ (existieren: $H = 0$ist eine!)
$T \neq T$, da a nicht in H. Daraus folgt:

$$|H| < |T| \overset{Ind.Vor.}{\Rightarrow} H \simeq \mathbb{Z}/_{p^{e_1}} \times ... \times \mathbb{Z}/_{p^{e_n}}$$

Es bleibt zu zeigen:

$$\underbrace{< a > \times H}_{\mathbb{Z}/_{p^{e_1}} \times ... \times \mathbb{Z}/_{p^{e_n}}} \to T,\ (ma, b) \mapsto ma + b$$

ist ein Isomorphismus:

injektiv: $ma + b = 0 \Rightarrow b = -ma \in H \cap < a > = \{(0)\} \Rightarrow b = 0, ma = 0$
surjektiv: Es reicht zu zeigen, dass die folgende Komposition

$$< a > \to < a > \times H \ \to T \overset{\underset{q}{kan}}{\to} T/_H \ =: \bar{T},\ a^m \mapsto \bar{a}^m$$

surjektiv ist. (also "surjektivität mod H").
angenommen nicht, dann existiert ein $\bar{b} \in \bar{T} \setminus < \bar{a} >$. Sei d so dass $p^d \bar{d} = 0$. Sei d minimal mit dieser Eigenschaft. Ersetze $\bar{b}$ durch $p^{d-1}\bar{b} \notin < \bar{a} >$. Dann ist $p \cdot \bar{b} = 0$, d.h. o.E. $d = 1$.
Sei $b \in T$ eine Hochhebung von $\bar{b} : \bar{b} = q(b)$. Nach Wahl von a gilt:

$$ord(b) \leq ord(b) \Rightarrow ord(p\bar{b}) = \frac{ord(\bar{b})}{p} < ord(a) = ord(\bar{a})$$

da $< a > \cap H = \{0\}$. Hier nächstes mal weiter. weiter zum Beweis des letzten Satzes: Sei $T p-$Gruppe, abelsch und endlich erzeugt. Weiter $< a > \subset T$ zyklische Gruppe, dann folgt:

1. $< a > = \mathbb{Z}/_{p^e}$
2. Jede echte Untergruppe von $< a >$ ist sogar in $< p \cdot a >$ enthalten, denn Teiler von $| < a > | = p^e \overset{1:1}{\underset{3.6}{\longleftrightarrow}}$ Ugrp. von $< a >$ mit $d \mapsto < da >$

Weiter folgt aus der Annahme:

- $ord(a)$ ist max.

- $H \subset T$ Ugrp. mit $H \cap < a > = \{0\}$ maximal

Beweis:
zz.: $+ :< a > \times H \overset{+}{\to} T$ ist Isomorphismus.

1) $+$ ist injektiv. okay

2) $< a > \overset{-}{\to} \bar{T} := T/_H$ ist surjektiv. Angenommen das wäre nicht so, dann gilt:
$\exists \bar{b} \in \bar{T} \setminus \{< \bar{a} >\}$ mit $p\bar{b} \in < \bar{a} >$ udn $p\bar{b} \neq \bar{a}$

$\overset{2)}{\Rightarrow} p\bar{b} \in < p\bar{a} >$
$\Rightarrow \exists \bar{c} :\ p(\bar{b} - \bar{c}) = o$ aber $\bar{b} \neq \bar{c}$, da $\bar{b} \notin < \bar{a} >$
$\Rightarrow < \bar{b} - \bar{c} > \cap < \bar{a} > = \{0\}$, da einzige echte Untergruppe von $\mathbb{Z}/_p$
$\Rightarrow$ setze $\tilde{H} := H + < \bar{b} - \bar{c} >$ ist eine $T-$Gruppe mit $\tilde{H} \cap < a > = 0$, aber $H < \tilde{H}$.

Widerspruch zur Annahme H maximal.

□

4.12 Eindeutigkeit der Zerlegung der Torsionsgruppe T

$T \simeq T(p_1) \times .... \times T(p_r)$ ist eindeutig nach Konstruktion. Mit 4.11 folgt dann:

$$T(p_1) \cong \mathbb{Z}/_{p^{d_1}} \times ... \times \mathbb{Z}/_{p^{d_s}}$$

Es stellt sich die Frage: Ist die Partition (d_i) von $n : |T(p)| = p^n$ eindeutig?
Ja, Beweis über absteigende Induktion nach $|T(p)|$:

Betrachte $ker(T(p) \xrightarrow{p\cdot} T(p) : \ t \mapsto pt) := T_p$.

$\Rightarrow T_p \simeq < (p^{d_1-1}, 0, ..., 0), ..., (0, ..., 0, p^{d_s-1} >$

$\Rightarrow T_p \cong (\mathbb{Z}/_p)^s \Rightarrow$ bestimmt s durch $|T_p| = p^s$

$\Rightarrow T(p)/_{T_p} \cong \mathbb{Z}/_{p^{d_1-1}} \times ... \times \mathbb{Z}/_{p^{d_s-1}}$

□

4.13 Nachtrag:

G endlich erzeugte, abelsche Gruppe, $H \subset G$ Untergruppe. Dann ist auch H endlich erzeugt.
Beweis über Induktion nach Anzahl der Erzeuger:

- $H = \{0\}$ okay
- $G =< a_1, ..., a_r >$, $\bar{G} := G/_{<ar>}$, $\quad g \mapsto \bar{g}$.

  Nach Induktionsvoraussetzung gilt: $\bar{H} =< \bar{b_1}, ..., \bar{b_s} > \subset \bar{G}$ endlich erzeugt.
  Wähle Repräsentanten $b_i \in G$ von $\bar{b_i} \in G/_{<a_r>}$

  $\Rightarrow H \subset < b_1, ..., b_s; a_r >$

  $\Rightarrow H \cap < a_r> \text{ ist Untergruppe } \overset{3.6}{\Rightarrow} H \cap < a_r > =< da_r >$

  $\Rightarrow H =< b_1, ..., b_s; da_r > \ \text{ mit } da_r = b_{s+1} \ \Rightarrow$ okay

□

5 Konjugation

5.1 Beobachtung:

Eine Gruppe G ist nicht abelsch genau dann wenn sich die Wirkung von G durch Konjugation

$$i : G \times G \to G : \ (ax) \mapsto axa^{-1}$$

nicht trivial ist.

5.2 Bemerkung

Im Gegensatz zur Multiplikation wirkt die Konjugation durch Automorphismen von G, d.h.:

$$i_a(xy) := axya^{-1} = axaa^{-1}aya^{-1} = i_a(x) \cdot i_a(y)$$

(das heißt $i : G \to Aut(G)$). Solche durch i gegebenen Automorphismen heißen innere Automorphismen.

Bemerkung: bei Multiplikation gilt: $g(xy) \neq gx \cdot gy$

5.3 Definition:

1. Bahnen der Konjugation heißen Konjugationsklassen und zwei Räpresentanten der selben Konjugationsklasse heißen konjugiert.(d.h. a ist konjugiert zu $b \Leftrightarrow \exists c \in G : \ a = cbc^{-1}$)

2. Die Standgruppe von $a \in G$ unter der Konjugation heißt Zentralisator $Z_G(a)$ von a:
   $Z_G(a) = \{b \in G \mid bab^{-1} = a\}$
3. Die Fixpunktmenge der Konj. heißt Zentrum $Z(G)$ von G

$$Z(G) = \{a \in G \mid \underbrace{bab^{-1} = a}_{\Rightarrow abelsch} \ \forall b \in G\}$$

Beobachtung: $A \subset G$ Ugrp. ist normal $\Leftrightarrow$ A ist Vereinigung von Konjugationsklassen. Also wenn A invariant gegen Konjugation ist.
$\Rightarrow$ insbesondere ist $Z(G) \lhd G$ normal.

5.4 Beispiel:

Für die Menge der Permutationsgruppe S_n ist
die Menge der Konjugationsklassen $\overset{\sim}{\leftrightarrow}$ Summenpartition von $n = \sum_{i=1}^{?} d_i$, $d_i > 0$
mit $[\pi] \mapsto$ Zykeltyp von π.
Beweis: Übung 2 Aufgabe 2

5.5 Klassengleichung

Sei G endlich und $a_1, ..., a_r$ Repräsentanten der Konjugationsklassen (mit a_i nicht konjugiert zu a_j falls $i \neq j$), dann folgt:

$$|G| = \sum_{i=1}^{r} |G|/_{|Z_G(a_i)|}$$

Beweis:
Zerlege G in Bahnen:

$$G = \coprod G.a_i; \text{ Bahn } G.a_i = G/_{G_{a_i}} = G/_{Z_G(a_i)}$$

Dann folgt daraus:

$$|G| = \sum |G.a_i| = \sum_{i=1}^{r} |G|/_{|Z_G(a_i)|}$$

□

5.6 Anwendung: Zentrum von $p-$Gruppen

Satz: Jede $p-$Gruppe hat ein nicht-triviales Zentrum
(z.B. im Gegensatz zu S_n : $Z(S_n) = \{e\}$ oder $GL(n, K) : Z(Gl(n, K)) = K \cdot 1$ (Einheitsmatrix))

$$p^e = |G| = |Z(G)| + \sum_{i=1}^{s} |G|/_{|Z_G(a_i)|}$$

mit a_i Repräsentanten der nicht-trivialen Konjugationsklassen.
Dann folgt dass $|Z(G)|$ durch p teilbar ist, da p^e und die Summe durch p teilbar sind.

□

Ergänzung: Nicht-triviale Konjugationsklassen sind solche, die aus mehr als einem Punkt bestehen, also gerade das Komplement der Fixpunktmenge $Z(G)$.

Wiederholung zur Konjugation: (hier bin ich mir nicht sicher dass das alles stimmig ist)

$$y(a, x) \mapsto axa^{-1} =: \kappa_a(x)$$

Konjugation $G \curvearrowright G$, $[G \curvearrowright X]$
Zentralisator von $a \in G$:

$$(G_a =) \quad Z_G(a) := \{b \in G \mid bab^{-1} = a\} \quad (ba = ab)$$

und G_a Stabilisator von a unter der Konjugationswirkung.
Wir erhalten die Bahnenformel für Konjugationswirkung $\Rightarrow$ Klassenzahlformel.
Konjugationsklassen repräsentiert durch $a_1, ..., a_r \in G$ mit

$$|G| = \sum \frac{|G|}{|Z_G(a_i)|}$$

Weiter hatten wir das Zentrum von $p-$Gruppen.
Das Zentrum ist:

$$Z(G) = \{a \in G \mid \forall b \in G : ba = ab\}$$

Hier stammt der Begriff der $p-$Gruppe daraus dass:
$|G| = p^r$ für p prim $\Rightarrow Z(G) \neq \{e\}$.
Ein Zentrum ist immer normal, also ist

$$Z(G) = \{x \mid |\kappa_a(x)| = 1\}$$

Punkt: $(x) : |G| = \sum_{a \in Z(G)} \frac{|G|}{|G|} + \sum_{a_i \neq Z(G)} \frac{|G|}{Z_G(a_i)} = |Z(G)| + p.(...) \Rightarrow p \mid |Z(G)|$

5.7 Satz

Aus $|G| = p^2$ folgt G abelsch ($\Rightarrow G \simeq \mathbb{Z}/_{p^2}$ oder $\mathbb{Z}/_p \times \mathbb{Z}/_p$).
Beweis:

$$\begin{aligned} |G| = p^2 &\overset{S.5.6}{\Rightarrow} Z(G) \neq \{e\} \\ &\Rightarrow |G/_{Z(G)}| \in \{1, p\} \\ &\Rightarrow G/_{Z(G)} \text{ ist zyklisch.} \end{aligned}$$

Sei $a \in G$ Erzeuger: $G/_{Z(G)} = < \bar{a} >$.

$$\Rightarrow \forall b \in G : b = a^i \cdot c \text{ für ein } i \in \mathbb{Z},\ c \in Z(G).$$

G ist abelsch:
Seien $x = a^i \cdot c,\ y = a^{i'} \cdot c'$, gegeben dann ist :

$$xy = (a^i c)(a^{i'} c') \overset{(*)}{=} a^i a^{i'} cc' = a^{i+i'} cc' = a^{i'} a^i c'c = a^{i'} c' a^i c = yx$$

$(*) c \in Z(G)$

□

5.8 Konjugierte Untergruppe, Normalisator

Diese Konjugation induziert auch eine Operation auf der Menge der Untergruppen von G.

Definition:

a) $H, H' \in G$ heißen konjugiert, falls

$$H' = aHa^{-1}$$

für ein $a \in G$. (Also gerade die Bahnen)

b) Der Normalisator einer Untergruppe $H \subset G$ ist der Stabilisator der Wirkung von G auf der Menge der Untergruppen:

$$N_G(H) := \{a \in G \mid aHa^{-1} = H\}$$

Bemerkung: $H \subset N_G(H)$ und H ist Normalteiler von $N_G(H)$ nach Definition. (es wurden gerade die Elemente ausgesucht die das erfüllen)
Ferner ist $N_G(H)$ ist die größte Untergruppe von G mit dieser Eigenschaft:

$$H' \subset G,\ H \lhd H' \ \Rightarrow\ H' \subset N_G(H)$$

5.9 Beispiel:

Sei $G := < \underbrace{(1234)(56)}_{=:a}, \underbrace{(123456)}_{=:b} > \subset S_6$ (nicht abelsch)

Weiter sei $H = < \underbrace{(13)(24)}_{=a^2} > \simeq \mathbb{Z}/_2$

mit GAP folgt: $|G| = 72$
Dann sind die Normalen Untergruppen von G:

$|N_1| = 36, \quad N_1 = < (1234)(56), (35)(46), (264)(135) >$
$|N_2| = 36, \quad N_2 = < (123654), (35)(46), (264), (135) >$
$|N_3| = 36, \quad N_3 = < (46), (35)(46), (264), (135) >$
$|N_4| = 18 = \frac{72}{4}, \quad N_4 = < (35)(46), (264), (135) >$
$|N_5| = 9, \quad N_5 = < (264), (135) > \simeq \mathbb{Z}/_3 \times \mathbb{Z}/_3$
$\{e\}$

Nebenrechnung:

$$(135) \cdot (35)(46) \cdot (264) = (13)(24)$$

Also ist die kleinste Untergruppe, die H enthält gerade N_4. N_4 heißt dann normaler Abschluss.
Der Normalisator $N_G(H) = < (24), (12)(34)(56) >$ ist nicht normal in G, $|N_G(H)| = 8$, und $N_G(H)/_H \simeq \mathbb{Z}/_2 \times \mathbb{Z}/_2$

PC- Programm GAP: "Groups, Algorithms, Programming"kostenlos zum runterladen.

5.10 Beispiel aus linearen Algebra:

Sei $G = GL(2, K),\ H = \left\{ \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \mid \lambda \in K \right\}$

$$N_G(H) = \left\{ A \in GL(2,K) \mid \forall \lambda\ \exists \mu : \ A \cdot \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix} \cdot A \right\} \Leftrightarrow A \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} A^{-1} = \begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix}$$

Wir suchen also eine Lösung für das Gleichungssystem:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & a\lambda + b \\ c & c\lambda + d \end{pmatrix}$$

$$\begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a + c\mu & b + d\mu \\ c & d \end{pmatrix}$$

Wir such also a, b, c, d so dass: $\forall \lambda \exists \mu$....
Dies ist lösbar in μ g.d.w. $c = 0 : (\Rightarrow d \neq 0)$, $a\lambda + b = b + d\mu$ g.d.w. $\mu := \frac{a\lambda}{d}$

Dies zeigt: $N_G(H) = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid ad \neq 0 \right\}$ also obere Dreiecksmatrizen.

6 Die Sylowsätze

Die Sylowsätze behandeln $p-$Untergruppen von endlichen Gruppen. Sehr mächtiges Hilfsmittel zum Studium von Gruppen! Korektur: G heißt $p-$Gruppe, falls $|G| = p^r$ für ein r. (4.10: $\forall a \in G : ord(a) = p^r$ für ein $r \rightsquigarrow T(p)$ für endlich erzeugte abelshes G.
Beweis:
a) $|G| = p^r,\ a \in G \Rightarrow < a > \subset G : | < a > | \ | |G| = p^r \Rightarrow ord(a) = p^e$ für ein $e \leq r$.
b) Hauptsatz für endlich erzeugte abelsche Gruppen: aus

- $G \simeq \mathbb{Z}/_{p_1^{e_1}} \times ... \times \mathbb{Z}/_{p_r^{e_r}}$ und
- $p_1 = ... = p_s = p,\ p_i \neq p > s$

muss folgen: $T(p) = \mathbb{Z}/_{p_1^{e_1}} \times ... \times \mathbb{Z}/_{p_s^{e_s}}$ und somit: $|T(p)| = p^{e_1+...+e_s}$.

□

6.1 Satz Sylow I

Sei G eine endliche Gruppe und sei p prim mit $p^r \mid |G|, r \geq 0$. Dann existiert eine Untergruppe $H \subset G$ mit $|H| = p^r$.

Beweis nach Induktion nach r:
$r = 0$ trivial.
$r \geq 0$:
Schritt 1:
Sei $K \subset G$ minimal unter den Untergruppe $H \subset G$ mit der Eigenschaft: $p \nmid [G : H]$.
Dann wissen wir:

$$|G| = |K| \cdot [G : K] \ \Rightarrow p^r \mid |K|$$

Ferner gilt: $\forall H \subsetneq K$ Untergruppe: $p \mid [K : H]$, denn $p \mid [G : H]$ (Minimalität von K) und $[G : H] = [G : K] \cdot [K : H]$, denn aus den Isomorphiesätzen folgt:

$$H \subset K \subset G \Rightarrow G/_K \simeq (G/_H)/_{(K/_H)} \Rightarrow [G : K] = [G : H]/[K : H]$$

Ersetze G durch K. Dann haben wir gewonnen:

$$(*)\forall H \subsetneq G(= K) : \ p \mid [G : H]$$

Also wenn wir den Satz für K zeigen ist er bewiesen. Also können wir ohne Einschränkung können wir $(*)$ für G annehmen. (siehe auch nächstes Lemma)

Schritt 2:
Wie in Beweis von Satz 5.6 zeigt die Klassenzahlformel jetzt: $p \mid |Z(G)|$ (benutzt $(*)$)
Sei $Z(G)$ abelsch $\overset{4}{\Rightarrow} \exists a \in Z(G) : ord(a) = p$. Weiter ist für $a \in Z(G)$:

$$< a > \ \lhd G \ \Rightarrow \ \bar{G} = G/_{<a>}$$

Gruppe mit $p^{r-1} \mid |G|$

Schritt 3:
Nach Induktionsannahme existiert $\bar{H} \subset \bar{G}$ mit $|\bar{H}| = p^{r-1}$.
Betrachte die Quotientenabbildung $q : G \to \bar{G}$ und setze $H := q^{-1}(\bar{H})$

$$\begin{array}{ccc} H & \twoheadrightarrow & \bar{H} \\ \bigcap & & \bigcap \\ G & \xrightarrow{q} & \bar{G} \end{array}$$

$\bar{H} \simeq H/_{(ker(q) \cap H)} = H/_{(q|_H)} = H/_{<a>} \Rightarrow |H| = |\bar{H}| \cdot ord(a) = p^{r-1} \cdot p = p^r$

□

Lemma:
Sei G eine endliche Gruppe und sei p prim mir $p^r \mid |G|, r \geq 0$, $\forall H \subsetneq G : p \mid [G : H] \Rightarrow \exists H \subset G : |H| = p^r$
genau dieses Lemma wird in Schritt 1 des Beweises des letzten Satzes bewiesen.

6.2 Korollar (Cauchy):

$p||G| \Rightarrow \exists g \in G$ mit $ord(g) = p$, nämlich z.B. alle $g \in H \backslash \{e\}$ mit H wie in 6.1 $(ord(g)|ord(H))$

6.3 Definition $p-$Szlow-Untergruppen:

Sei G eine endliche Gruppe mit $|G| = p^r \cdot m$ mit p, m teilerfremd, dann heißen die Untergruppen der Ordnung p^r $p-$Szlow-Untergruppen, oder $p-$Szlows. Die existeny folgt aus 6.1

6.4 Beispiele:

- $K = \mathbb{Z}/_p,\ G = GL(n, K)$

  $|G| = \underbrace{(p^n - 1)}_{(*)} \cdot \underbrace{(p^n - p)}_{(**)} \cdot (p^n - p^2) \cdot ... \cdot (p^n - p^{n-1})$

  $(*)$#der Möglichkeiten der 1.Spalte $= |(\mathbb{Z}/_p)^n - \{0\}|$

  $(**)$#der Möglichkeiten der 2.Spalte, unabhängig zur 1. $= |(\mathbb{Z}/_p)^n - \mathbb{Z}/_p \cdot$ 1.Spalte$|$

  Daraus folgt:
  $|G| = (p^n - 1)p \cdot (p^{n-1} - 1)p^2 \cdot ... \cdot (p^{n-n+1} - 1)p^{n-1} = pp^2p^3 \cdot ... \cdot p^{n-1} \cdot m\ ,\ p \nmid m!$

  Sei H definiert als:

$$H := \left\{ \begin{pmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \right\}$$

  also $H \subset GL(n, K)$, dann folgt:
  $|H| = p^{n-1}p^{n-2}...p \Rightarrow H$ ist $p-$Sylow

- G abelsch $|G| = p^r m$, $p \neq 2$ prim, dann folgt:

  es existiert genau eine $p-$Sylow, nähmlich:

$$T(p) = \left\{ g \in G \mid ord(g) \in p^{\mathbb{N}} \right\}$$

6.5 Anwendung:

Es sei $|G| = 2p$, $p \neq 2$ prim., dann folgt:

$$\text{entweder: } G \cong \mathbb{Z}/_{2p}$$
$$\text{oder: } G \cong D_p \cong \mathbb{Z}/_2 \times \mathbb{Z}/_p$$

Beweis:
Aus 6.2 folgt:
$\exists r, s \in G$ mit $ord(r) = p$ und $ord(s) = 2$. Weiter folgt:

$H := < r > \cong \mathbb{Z}/_p$ hat Index 2 in

$$G := \{e, r^1, r^2, ..., r^{p-1}, s, sr, sr^1, ..., sr^{p-1}\}$$

$\overset{\text{Ü } 31}{\Rightarrow} H$ ist Normalteiler, also $s \cdot r \cdot s^{-1} = r^l$ für ein $l \in \{1, ..., p\}$
Wegen $s^2 = 1$ gilt:

$$r = s^2 \cdot r \cdot s^{-2} = s \cdot r^l \cdot s^{-1} = r^{2l}$$

woraus folgt:

$$l \equiv \pm\ 1\ mod\ p$$

und daraus wiederum:

$$\begin{cases} l = 1: & srs^{-1} = r \Rightarrow G \text{ abelsch} \Rightarrow G \cong \mathbb{Z}/_{2p} \\ l = -1: & srs^{-1} = r^{-1} \overset{\text{Übung}}{\Rightarrow} G \cong \mathbb{Z}/_2 \times \mathbb{Z}/_p \end{cases}$$

□

6.6 Satz (Sylowsätze):

Es sei G endliche Gruppe mit $|G| = p^r m$, p, m teilerfremd, dann gilt:

a) je zwei $p-$Sylows sind konjugiert.

b) $H \subset G$ untergruppe mit $|H| = p^s$, $s \leq r$, dann ist H in einer $p-$Sylow enthalten.

c) Sei s_p die Anzahl der $p-$Sylows in G dann gilt:

i) $s_p \equiv 1 \; mod \; p$

ii) s_p teilt $\frac{|G|}{p^r} = m$

Beweis:
Betrachte die Wirkung von G durch *Konjugation* auf der Menge $S := \{P \mid P \subset G \; p-\text{Sylow}\}$ der $p-$Sylow Untergruppen von G.

1) Behauptung: Bahnenlänge $|G.P|$ ist teilerfremd zu $p \; \forall P \in S$

Beweis:
$P \subset G_P := \{g \in G \mid gPg^{-1} = P\}$
$\Rightarrow |G_P|$ enthält alle $p-$Potenzen von $|G|$, da $|P|$ schon alle enthält (per Def.)
$\Rightarrow |G.P| = \frac{|G|}{|G_P|}$ ist teilerfremd zu p.

□

2) Sei $P \in S$ fest gewählt. Betrachte $H \subset G$ mit $|H| = p^s$ (wie in b) byw a) für $H = P_i \in S$)
Die Einschränkung der $G-$Wirkung auf S zu einer $H-$Wirkung auf einer Bahn $G.P$ definiert eine Zerlegung von $G.P$ in H Bahnen.

$$G.P = H.P_1 \bigsqcup ... \bigsqcup H.P_l, \quad P_1, ..., P_l \in S$$

Behauptung:
$H-$Wirkung hat einen Fixpunkt P_i ($\Leftrightarrow h \cdot P_i \cdot h^{-1} = P_i, \; \forall h \in H$).
Beweis:
$|H.P_j| = \frac{|H|}{|H.P_j|}$ teilt $|H|$, also $|H.P_j| = p^{r_j}$ ist $p-$Potenz
aber nach 1(teilt p <u>nicht</u> $|G.P| = \sum_{j=1}^{l} |H.P_j| = \sum_{j=1}^{l} p^{r_j}$
$\Rightarrow \exists i : r_i = 0 \Rightarrow P_i$ ist Fixpunkt , $|H.P_i| = 1$

□

3) Behauptung:

$$H \subset P_i = H.P \text{ (H Fixpunkt)}$$

Daraus folgt dann a) und b):

a) denn für alle $H, P \in S \overset{2),3)}{\Rightarrow} H, P \in G.P$
Beweis: $P_i = H.P \Leftrightarrow hP_ih^{-1} = P_i \; \forall h \in H$

$\Rightarrow H \subset N_G(P_i) = \{g \in G \mid g.P_i.g^{-1} = P_i\}$ (Normalisator von P_i)

$\rightsquigarrow$ Brauchen 2 <u>Isomorphiesätze</u>:

Ist $H \subset N$ Ugrp. , $P \lhd N$ normal dann gilt:

1) $PH = \{ph \mid p \in P, \; h \in H\}$ ist eine Untergruppe von N

2) $P/_{P \cap H} \simeq PH/_H$

Beweis des Isosatz.:
$\forall p, p' \in P, \; h, h' \in H$ gilt:

- $ph(p'h')^{-1} = ph \cdot h'^{-1}p'^{-1} \cdot \overbrace{h' \cdot h^{-1} \cdot h \cdot h'^{-1}}^{e} \in PH$

und $ph \cdot h'^{-1}p'^{-1} \cdot h' \cdot h^{-1} \in P, da P \lhd N$
$\Rightarrow PH$ Untergruppe.

- $P \to PH/_H, \; p \mapsto pH$ ist surjektiv mit kern $P \cap H$

□

<u>zu 3):</u>

$|P_iH| = |P_iH/_H| \cdot |H| \overset{2.Iso}{=} \underbrace{\frac{\overbrace{|P_i|}^{p^r}}{|P_i \cap H|}}_{p^x} \cdot \underbrace{|H|}_{p^s}$ ist $p-$Potenz, also ist $P_i = H.P_i$ auch P_iH eine $p-$Sylow $|HP_i| = p^v$

$\Rightarrow P_i = HP_i = P_iH \Rightarrow H \subset P_i$

□

4) Sei nun $H = P_i$ also $G.P = P_1P_i \coprod ... \coprod P_lP_i$

aus 2,3) folgt $P_jP_i = \begin{cases} 1, & \text{falls } i = j \\ p - \text{Potenz} \neq 1, & \text{sonst} \end{cases} \Rightarrow$ Anzahl der $p-$Sylow $Sp \overset{a)}{=} |G.P| \equiv 1 \ mod \ p$

Außerdem $P \subset G_P \Rightarrow |P|$ teilt $|G_P| \Rightarrow$

$$Sp = |G.P| = \frac{|G|}{|G_P|} \text{ teilt } \frac{|G|}{|P|} = \frac{|G|}{p^r}$$

□

□

6.7 Korollar

es sei $H \subset G$ $p-$Sylow, dann gilt:

$$H \lhd G \Leftrightarrow s_p = 1$$

Beweis:
" $\Rightarrow$ " $s = \{H\}$
" $\Leftarrow$ " $s = 1 \Rightarrow s = \{H\} \Rightarrow H \lhd G$

□

Nun zur Anwendung zur Klassifikation von endlichen Gruppen:

6.8 Anwendung 1:

Gruppen der Ordnung 15:
Beweis:
Dann ist $|G| = 15 = 3 \cdot 5$. Wir betrachten also die $3-$Sylows und $5-$Sylows:
nach Satz 6.6 iii) gilt:

$$s_5|3, \ s_5 \equiv 1 \ mod \ 5 \Rightarrow s_5 = 1$$
$$s_3|3, \ s_3 \equiv 1 \ mod \ 3 \Rightarrow s_3 = 1$$

$\Rightarrow$ Anzahl der Elemente der Ordnung:

$$\begin{aligned} 1: &\quad 1(e) \\ 3: &\quad 2 = 3 - 1(\text{Elemente von } P\backslash\{e\}, P3 - \text{Sylpw }) \\ 5: &\quad 4 = 5 - 1(\text{Elemente von } P\backslash\{e\}, P5 - \text{Sylpw }) \end{aligned}$$

Also insgesamt 7
$\Rightarrow G$ hat 15-7= 8 Elemente der Ordnung 15. Insbesondere ist G zyklisch:

$$G \simeq \mathbb{Z}/_{15} \simeq \mathbb{Z}/_3 \times \mathbb{Z}/_5$$

□

Der zweite Teil des Beweises folgt aus :

6.9 Lemma:

Es sei G eine endliche Gruppe, $|G| = \prod_{i=1}^{n} p_i^{r_i}$ mit p_i prim, paarweise verschieden. Für jedes i existiere genau eine p_i-Sylow, dann folgt:

$$G = \prod_{i=1}^{n} P_i = P_1 \times ... \times P_n$$

Beweis:
$\forall i : P_i \lhd G$ nach Korollar 6.7. Wir behaupten, dass

$$P_1 \times ... \times P_n \to G,\ (a_1, ..., a_n) \mapsto a_1 \cdot ... \cdot a_n$$

ein Isomorphismus von Gruppen ist.
Beweis über Induktion nach n:
$\underline{n = 1}$ okay
$\underline{n > 1}$: $Q := P_2 \cdot ... \cdot P_n = \{a_1 \cdot ... \cdot a_n \mid a_i \in P_i\}$
Aus $P \lhd G$ folgt: Q ist die von $P_2, ..., P_n$ erzeugte Untergruppe von G:

$\forall a_i, b_i \in P_i\ \exists c_i \in P_i$ mit $(a_2, ..., a_n) \cdot (b_2, ..., b_n) = (c_2, ..., c_n)$, in der Tat $a_i b_j = b'_j a_i$

$\underline{\text{Ferner:}}$ $Q \lhd G$ und $P_1 \cap Q = \{e\}$, denn

$$a \in P_1 \cap Q \Rightarrow ord(a) | p_1^{r_1} \text{ und } ord(a) || Q| = p_1^{r_1} \cdot ... \cdot p_n^{r_n} \Rightarrow ord(a) = 1$$

Nächster Schritt:
$\forall a \in Q, \forall b \in P_1 : ab = ba$ (induktiv φ ist ein Hom.)

$$\begin{aligned} aba^{-1}b^{-1} &= a(ba^{-1}b^{-1}) \in Q \qquad (\text{ wobei } a \in Q \text{ und } ba^{-1}b^{-1} \in Q) \\ &= (aba^{-1})b^{-1} \in P_1 \qquad\qquad (\text{ wobei } aba^{-1}, b^{-1} \in P_1) \end{aligned}$$

Insbesondere $P_1 \times Q \to G,\ (b, a) \mapsto ba$ ist ein Hom., nach Induktionsvoraussetzung gilt dann:

$$\varphi : P_1 \times P_2 \times ... \times P_n \to P_1 \times Q \to G$$

ist auch ein Hom.
Zu zeigen ist nun noch: $P_1 \times Q \to G$ ist bijektiv:

$\underline{\text{injektiv:}}$ $b \in P_1, q \in Q : ba = e \Rightarrow b = a^{-1} \in P_1 \cap Q = \{e\} \Rightarrow a = b = e$

$\underline{\text{surjektiv:}}$ $|G| = |P_1| \cdot |Q|$

□

6.10 Anwendung 2:

Sei $|G| = 99$ dann folgt: G ist abelsch $\quad (\Rightarrow$ **i)** $G \simeq \mathbb{Z}/_3^2 \times \mathbb{Z}/_{11}$ **ii)** $G \simeq \mathbb{Z}/_9 \times \mathbb{Z}/_{11})$
Beweis:

$$\begin{aligned} s_{11} &\equiv 1\ mod\ 11, \quad s_{11} | 9 \Rightarrow s_{11} = 1 \\ s_3 &\equiv 1\ mod\ 3, \quad\ s_3 | 11 \Rightarrow s_3 = 1 \end{aligned}$$

$|P_3| = 9 = 3^2 \overset{Satz 5.7}{\Rightarrow} P_3$ abelsch , und aus Lemma 6.9 (sagt welcher Fall) folgt:
$G \simeq P_{11} \times P_3$ abelsch

□

6.11 Anwendung 3: (allgemein)

$|G| = p \cdot q,\ p, q$ verschiedene Primzahlen, oBdA sei $p < q$. Seien weiter $P \subset G$ $p-$Sylow, $Q \subset G$ $q-$Sylow, dann ist:

$$s_q \equiv 1\ mod\ q \text{ und } \quad s_q | p \overset{q>p}{\Rightarrow} s_{q=1}$$

d.h. Q ist eindeutig , $Q \lhd G$.
Man kann dann zeigen:

$$G \simeq Q \rtimes^{\sigma} P, \sigma : P \to Aut(Q) \simeq \mathbb{Z}/_{q-1}$$

7 Kompositionsreihen

Ziel ist die Klassifikation endlicher Gruppen.

Definition:
Sei

$$G = G_r \rhd G_{r-1} \rhd G_{r-2} \rhd ... \rhd G_0 = \{e\}$$

wobei G_{r-1} maximale Untergruppe $\neq G_r$.
dann heißt $G_r \rhd G_{r-1} \rhd G_{r-2} \rhd ... \rhd G_0 = \{e\}$ Kompositionsreihe.
Maximalität $\Leftrightarrow G_i/_{G_{i-1}}$ ist einfach, d.h. $G_i/_{G_{i-1}}$ hat keine nichttriv. Normalteiler.

Der Satz von Jordan Hölder sagt nun: für jede endliche Gruppe G sind die Quotienten

$$\{G_r/G_{r-1}, ..., G_1/_{G_0}\}$$

sind bis auf Reihenfolge eindeutig.

Die Klassifikation reduziert sich zu:

- Klassifikation einfacher Gruppen
- Klassifikation von Erweiterungen durch einfache Gruppen:

gegeben G und einfache Gruppe N. Die Erweiterung von G durch N sei:

$$ker(\varphi) = N \lhd \tilde{G} \xrightarrow{\varphi} G$$

Definition: G heißt auflößbar $:\Leftrightarrow$ es existiert eine Kompositionsreihe mit $G_i/_{G_{i-1}}$ zyklisch.

8 Einfache Gruppen

Klassifikation (1980 er): G endlich, einfach, dann folgt:
$G \simeq$

(1) $\mathbb{Z}/_p, p$ prim (zyklisch)

(2) $A_n \subset S_n$, $n \geq 5$ (alternierend)

(3) $PSL(n, \mathbb{F}_q) = SL(n, \mathbb{F}_q)/_{(\mathbb{F}_q \setminus \{0\})}, PSU(n, \mathbb{F}_q), \mathbb{P}Sp, P\Omega^{\varepsilon}$ (klassisch linear)

(4) Exzeptionelle algebraische Gruppen über $\mathbb{F}_q$ (exzeptioneller Lie- Typ)

(5) (Sporadisch) 26 Gruppen:

- 5 Mathieu-Gruppen $M_{11}, M_{12}, M_{22}, M_{23}, M_{24}$
- 3 Fischer-Gruppen (1966- '81)
- weitere, die größte hei sst Monstergruppe $M, |M| = 8 \cdot 10^{54}$ (1981)
  kleinste: $|M_{11}| = 7920$ Elemente (1961)

2 Ringe

(später: Konstruktion von Körpern)

9 Grundlegendes

9.1 Erinnerung

Definition: Ein Ring ist eine Menge R mit zwei assoziativen Verknüpfungen, der Addition $+$ und der Multiplikation $\cdot$, so dass:

i.) $(R, +)$ ist eine kommutative Gruppe (neutrales Element $0 := 0_R$), (d.h. stets unitär)

ii.) $(R, \cdot)$ hat ein neutrales Element $1 = 1_R$ (ist eindeutig, $(R, \cdot, 1_R)$ heißt Monoid

iii.) Es gelten die Distributivgesetze

iv.) Ist $(R, \cdot)$, kommutativ, so heißt der Ring kommutativ.

Bemerkung:

a) Gewöhnlich spricht man nur von " dem Ring " $(= (R, +\cdot, 1_R))$

b) Konvention: " Punkt vor Strich "

c) $\forall a \in R$ gilt: $0 \cdot a = 0$

d) $\forall a \in R$ gilt: $(-1) \cdot a = -a$

9.2 Beispiele:

a) $\mathbb{Z}, \mathbb{Z}/_n$ ($\rightsquigarrow$ Zahlentheorie)

b) Körper K

c) Der Nullring, also $R = \{0\}$ ($0_R = 1_R$!)

d) Sei V ein $k - VR$, dann ist:
$End_k(V)(\varphi \cdot \psi := \varphi \circ \psi)$ nicht kommutativer Ring wenn $dim(V) > 1$.

e) Polynomringe $K[X] = \left\{ \sum_{i=0}^{n} a_i X^i \mid n \in \mathbb{N}, a_i \in K \right\}$ (die Summe hier ist formaler Ausdruck)
Mengentheoretisch: $\sum_{i=0}^{n} a_i X^i \leftrightarrow (a_0, ..., a_n, 0, ...)$ und

$$\left(\sum_{i=0}^{n} a_i X^i \right) + \left(\sum_{j=0}^{n} b_j X^j \right) := \sum_{i=0}^{max(n,m)} (a_i + b_i) X^i, \text{ mit } a_i = 0 \text{ für } i > n, b_j = 0 \text{ für } j > m$$

und der Multiplikation:

$$\left(\sum_{i=0}^{n} a_i X^i \right) \cdot \left(\sum_{j=0}^{n} b_j X^j \right) := \sum_{k} \left(\sum_{i+j=k} a_i b_i \right) X^k$$

f) induktiv R Ring, $R[X_1, ..., X_n] = (R[X_1, ..., X_{n-1}])[X_n] = \left\{ \sum a_{i_1} ... a_{i_n} X_1^{i_1} ... X_n^{i_n}, a_i \in R \right\}$
$\rightsquigarrow$ benutze Multiindizes $I = (i_1, ..., i_n) \in \mathbb{N}^n$, $a_I = a_{i_1 i_2 ... i_n}$, $X^I := X_1^{i_1} ... X_n^{i_n}$

- Add. $(\sum a_I X^i) + (\sum b_j X^j) = \sum_{i \in \mathbb{N}^n} (a_i + b_j) X^I$
- Mult.: $\left(\sum a_I X^I \right) \cdot \left(\sum b_J X^J \right) := \sum_{k \in \mathbb{N}^n} \left(\sum_{I+J=K} a_I b_J \right) X^K$

g) ist allgemein $(M, \cdot)$ ein Monoid (d.h. eine Menge mit einer assoziativen Verknüpfung udn 1), so definiere:
Monoidring über R:

$$R(M) := \left\{ \sum_{m \in M} a_m X^m \mid a_m \in R, |\{m \mid a_m \neg 0\}| < \infty \right\}$$

- Add.: $(\sum a_m X^m) + (\sum b_n X^n) = \sum_{m \in M} (a_m + b_m) X^m$
- Mult.: $\left(\sum_{m \in M} a_m X^m \right) \cdot \left(\sum_{n \in M} b_n X^n \right) := \sum_{k \in M} \left(\sum_{n \circ m = K} a_n b_m \right) X^K$

Bemerkung

- zu Beispiel e): in dieser Notation identifizieren wir

$$(\sum_{i=0}^{m} a_i X^i) \text{ mit } (\sum_{i=0}^{n} a'_i X^i) \qquad , m \leq n$$

  falls $a_i = a'_i$ und für $i \leq m$ gilt a'_i für $i > m$

- Ab jetzt behandeln wir nur noch kommutative Monoide. Hierbei gilt:
  $R(M)$ kommutativ $\Leftrightarrow (M, \cdot)$ kommutativ, (schreibe $(M, +)$)
  insbesondere ist $R[X_1, ..., X_n] = R[\mathbb{N}^n]$

9.3 Homomorphismen von Ringen

R, S Ringe, dann nennen wir eine Abbildung $R \to Sp$ einen (Ring-) Homomorphismus, falls:

i) $\varphi(1_R) = 1_S$

ii) $\varphi(a + b) = \varphi(a) + \varphi(b)$

iii) $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$

$ker(\varphi) := \varphi^{-1}(0)$ ist kein Ring, da $1 \notin ker(\varphi)$

9.4 Beispiele:

a) $\varphi : \mathbb{Z} \to \mathbb{Z}/_n,\ m \mapsto m + n\mathbb{Z} \Rightarrow ker(\varphi) = n\mathbb{Z}$

b) Auswertungsmorphismus in Polynomringen: R Ring, $\lambda \in R$:

$$ev_\lambda : R[X] \to R, \quad \sum a_i X^i \mapsto \sum a_i \lambda^i \in R$$

(genauso für andere Monoide)

9.5 Unterobjekte I: Unterringe

Sei R ein Ring, $A \subset R$ heißt Unterring, falls:

$$1 \in A, \quad A \cdot A \subset A, \quad (A, +) \text{ ist abelsche Untergruppe}$$

Sei $\varphi : R \to S$ Homom. von Ringen, dann ist $Im(\varphi)$ ein Unterring.

9.6 Unterobjekte II: Ideale

Sei R ein Ring, $I \subset R$ heißt Ideal, falls gilt:

i.) $(I, +) \subset (R, +)$ ist (additive) Untergruppe

ii.) $R \cdot I \subset I$, $I \cdot R \subset I$

9.7 Satz:

a) Ideale in R sind genau die Kerne von Ringhomomorphismen $\varphi : R \to S$

b) Sei $I \subset R$ Ideal, dann folgt dass die Multiplikation in R eine Multiplikation auf $R/_I$ induziert, s.d. $R/_I$ wieder ein Ring ist.
(in b) gilt sogar Äquivalenz, wir zeigen aber nur eine Richtung)

Beweis:
a) " $\Leftarrow$ " sei $I := ker(\varphi : R \to S), \varphi$ Ringhomomorphismus, dann gilt:

i.) Da $\varphi : (R, +) \to (S, +)$ Gruppenhom, ist $ker(\varphi)$ Untergruppe

ii.) $a \in R,\ b \in I \Rightarrow \varphi(ab) = \varphi(a)\varphi(b) = 0$, da $\varphi(b) = 0$
$\Rightarrow ab \in I$

" $\Rightarrow$ " Sei $I \subset R$ Ideal $\Rightarrow I = ker(R \to R/_I)$, und $R/_I$ ist Ring nach b)

b) Definiere $(a + I) \cdot (b + I) := ab + I$. zeige dazu:

- wohldefiniert: $\underbrace{a' - a}_{f} \in I$ und $\underbrace{b' - b}_{g} \in I$, dann ist:
$a'b' - ab = (f + a)(g + b) - ab = fg + fb + ag \in I$, da alle Summanden in I
Die Wohldefiniertheit der Addition wurde schon bei Gruppen gezeigt.

- Ringaxiome: für $R/_I$: geerbt von R

□

Bemerkung wir definieren $R/_I$ als $R/_I := \{r+ \mid r \in R\}$

9.8 Wie für Gruppen folgt:

Satz:

a) jeder Ringhom. $\varphi : R \to S$ faktorisiert als:

$$R \to R/_{ker(\varphi)} \to in(\varphi) \hookrightarrow S$$

b) Ist weiter $I \subset R$ Ideal, so faktorisiert φ über $R/_I$ genau dann wenn $I \subset ker(\varphi)$

9.9 Beispiele:

a) $\{0\} \in \mathbb{R}$ Ideal

b) $R \subset R$ ist Ideal

c) $I \subset \mathbb{Z} \Rightarrow I$ (additive) Untergruppe $(\mathbb{Z}, +) \overset{Satz 3.3}{\Rightarrow} I = m \cdot \mathbb{Z}$ für ein $m \in \mathbb{Z}$

d) $a_1, ..., a_s \in R$, dann ist $(a_1, ..., a_s) := Ra_1 + ... + Ra_s$ das von $a_1, ..., a_s$ erzeute Ideal.
Solche Ideale heißen endlich erzeugt.

Beispiel:
Ideale von $\mathbb{Z}$ sind endlich erzeugt nach c):

$$I \subset \mathbb{Z} \text{ Ideal } \Leftrightarrow I = (m) \text{ für ein } m \in \mathbb{Z}$$

Bemerkung

1. Beispiele a),b) sind die "trivialen Beispiele"
2. Jedes Ideal von $\mathbb{Z}[X_1, ..., X_n]$ ist damit endlich erzeugt. Ringe mit dieser Eigenschaft heißen Noethersch

9.10 Eigenschaften von Idealen

Satz: Sei R ein Ring, I, J Ideale, dann gilt:

a) $I \cap J$, $I + J$ sind wieder Ideale

b) $\{i \cdot j \mid i \in I, j \in J\}$ ist im allgemeinen kein Ideal, definiere stattdessen (Achtung neue Notation!!):

$$I \cdot J := \{\sum_{i,j} a_i b_j \mid a_i \in I, b_j \in J\}$$

Weiter gilt:

$$I \cdot J \subset I \cap J \subset I + J$$

Beweis hierzu in den Übungen

9.11 Beispiele

Sei $R = \mathbb{Z}$, $I = (m) = m\mathbb{Z}$, $J = (n) = n\mathbb{Z}$, dann folgt:

- $(m)(n) = (nm)$
- $(m) \cap (n) =: (kgV(n, m))$ kleinste gemeinsame Vielfache
- $(m) + (n) =: (ggT(m, n))$ größte gemeinsame Teiler

9.12 Bemerkung:

$I = (f_1, ..., f_n)$, $J = (g_1, ..., g_m)$ endlich erzeugt, dann ist:

$$I \cdot J := (f_i g_j \mid i = 1, ..., n;\ j = 1, ..., m)$$
$$I + J := (f_1, ..., f_n, g_1, ..., g_m)$$

Erzeuger für $I \cap J$ im Allgemeinen schwieriger

10 Integritätsbereiche und Körper

In diesem Kapitel betrachten wir kommutative Ringe.

10.1 Definition:

Sei R ein Ring

a) Für $a, b \in R$ ist a ein Teiler von b (" a teilt b ", " b ist Vielfaches von a "), falls eine der folgenden Bedingungen gilt:

   i) $\exists c \in R :\ b = a \cdot c$

   ii) $b \in (a) = Ra$

   iii) $(b) \subset (a)$

   und schreiben $a|b$

b) $a \in R$ heißt Nullteiler, falls es ein $c \in R \backslash \{0\}$ gibt mit $a \cdot c = 0$

c) Ein Integritätsbereich ist ein Ring $\neq \{0\}$, der keine Nullteiler $\neq 0$ besitzt

10.2 Beispiele für Integritätsbereiche

- $\mathbb{Z}$, Körper, $K[X]$ für K Körper, $R[X]$ für R Integritätsbereich

10.3 Kürzen in Ringen

Lemma:
In einem Ring R gelte $ax = ay$, für $a, x, y \in R$ und sei a kein Nullteiler, dann ist $x = y$
Beweis:

$$ax = ay \Leftrightarrow a(x - y) = 0 \Rightarrow x - y = 0$$

□

10.4 endliche Integritätsbereich

Satz:
Jeder endliche Integritätsbereich ist ein Körper.
Beweis:
Zu zeigen ist die Existenz von multiplikativen Inversen:
Für $a \in R\backslash\{0\}$ betrachte

$$\mu_a : R \to R, \quad b \mapsto ab$$

(dies ist in Allgemeinen kein Hom.)
injektiv:

$$\mu_a(b) = \mu_a(b') \Rightarrow ab = ab' \overset{10.3}{\Rightarrow} b = b'$$

Ist R endlich folgt auch dass μ_a surjektiv ist und daraus schließlich :

$$\exists b \in R : \mu_a(b) = ab = 1$$

Somit besitzt R multiplikative Inverse.

□

10.5 Restklassenringe und Integritätsbereiche

Satz Für $n \leq 2$ ist $\mathbb{Z}/_n$ Integritätsbereich genau dann wenn n eine Primzahl ist.
Beweis:
" $\Rightarrow$ ": z.z. n ist prim.:
$\exists a, b \in \mathbb{N}$ mit:

$$\begin{aligned} n = ab \Rightarrow \bar{a}\bar{b} = 0 \text{ in} \mathbb{Z}/_n \\ \Rightarrow \bar{a} = 0 \text{ oder } \bar{b} = 0 \text{ (da Int.bereich)} \\ \Rightarrow a = n \text{ oder } b = n \end{aligned}$$

" $\Leftarrow$ ": Sei n prim.:

$$\begin{aligned} \bar{a}\bar{b} = 0 \text{ in} \mathbb{Z}/_n \Rightarrow ab \in n\mathbb{Z} \\ \Rightarrow n|ab \\ (n \text{ prim}) \Rightarrow n|a \text{ oder } n|b \\ \Rightarrow \bar{a} = 0 \text{ oder } \bar{b} = 0 \end{aligned}$$

□

10.6 Die Charakteristik eines Integritätsbereiches

Sei R ein Integritätsbereich, betrachte den Homomorphismus

$$\varphi : \mathbb{Z} \to \mathbb{R}, \quad m \mapsto n \cdot 1_R = sgn(n) \cdot \underbrace{(1 + 1 + ... + 1)}_{n \text{ mal}}$$

Dann ist $ker(\varphi) = (a)$ mit $a \in \mathbb{N}\backslash\{1\}$ (hier $1_R \neq 0_R$)

Lemma a ist Primzahl.
Beweis:
Sei $a = bc, \quad bc \in \mathbb{N}$:

$$\begin{aligned} &\Rightarrow 0 = \varphi(a) = \varphi(bc) = \varphi(b)\varphi(c) \\ (R \text{ Int.bereich}) &\Rightarrow \varphi(b) = 0 \text{ oder } \varphi(c) = 0 \\ &\Rightarrow b \in (a) \text{ oder } c \in (a) \\ (a = bc) &\Rightarrow b = a \text{ oder } c = a \end{aligned}$$

□

Definition: Die Zahl a (0 oder prim) heißt Charakteristik von R. Wir schreiben $char(R)$

10.7 Bemerkung

enthält R einen Körper K als Unterring, so gilt nach Definition

$$char(R) = char(K)$$

Definition: Der Durchschnitt aller solcher Körper $K \subset R$ heißt Primkörper vom R

Bemerkung: Für Integritätsbereiche der Charakteristik 0 müssen keine Primkörper existieren (z.B. $\mathbb{Z}[X]$). Für endliche Charakteristik hat man dagegen den folgenden Satz.

Satz: Ein Integritätsbereich R der Charakteristik $p > 0$ hat einen Primkörper K. Ferner gilt:

$$K \simeq \mathbb{F}_p := (\mathbb{Z}/_p, +, \cdot)$$

Beweis:
Die Abbildung $\varphi : \mathbb{Z} \to R$ aus 10.6 induziert eine Injektion $\mathbb{Z}/_p \hookrightarrow R$. Das Bild ist K.

10.8

Umgekehrt kann man sich für beliebige Ringe R die Frage stellen, welche Faktorringe $R/_I$ mit $I \subset R$ Ideal, Integritätsbereiche oder Körper sind.

Definition:

a) Ein Ideal $I \subset R$ heißt Primideal, falls gilt:

$$I \neq R \text{ und } [ab \in I \Rightarrow a \in I \text{ oder } b \in I]$$

b) Ein Ideal $J \subset R$ heißt maximal, falls:

$$J \neq R \text{ und } [I \subsetneq R \text{ Ideal }, J \subset I \Rightarrow J = I]$$

Beispiel: $R = \mathbb{Z}, I = (n)$ dann ist:

$$ab \in I \Leftrightarrow n|ab \overset{n \text{ prim}}{\Rightarrow} n|a \text{ oder } bn|b \Leftrightarrow n \text{ prim}$$

Satz: Sei R Ring und $J, I \subset R$ Ideale, dann gilt:

a) $R/_I$ ist Integritätsbereich $\Leftrightarrow$ I Primideal

b) $R/_J$ ist Körper $\Leftrightarrow$ J ist maximales Ideal

Beweis:

a) (direkt aus der Definition):
$a, b \in R \rightsquigarrow \bar{a}, \bar{b} \in R/_I$

$$\begin{array}{rcccc} I \text{ Primideal} & \Leftrightarrow [ab \in I \Rightarrow & a \in I \text{ oder} & b \in I] \\ & \Updownarrow & \Updownarrow & \Updownarrow \\ R/_I \text{ Integritätsbereich} & \Leftrightarrow [\bar{a}\bar{b} = 0 \Rightarrow & \bar{a} = 0 \text{ oder} & \bar{b} = 0] \end{array}$$

b) " $\Rightarrow$ ": $q : R \to R/_J =: K$ Körper
Sei $I \subset R$ mit $J \subset I$ z.z. $I = J$ oder $I = R$.
Dann folgt: $q(I) \subset K$ Ideal (q surjektiv impliziert dann $q(I) = (0)$ oder $q(I) = K$) und $I = I + J = q^{-1}(q(I))$.

Es gilt <u>entweder</u>: $q(I) = (0) \Rightarrow I = J$

<u>oder</u>: $q(I) = K \Rightarrow I = q^{-1}(K) = R$

" $\Leftarrow$ " Sei J maximales Ideal und $a \in R \backslash \{J\}$

$$\begin{aligned} (J \text{ maximal}) &\Rightarrow J + (a) = R \\ &\Rightarrow \exists b \in J, c \in R : b + ac = 1_R \Rightarrow \bar{a}\bar{c} = 1_{R/_J} \end{aligned}$$

□

Bemerkung: Hinter dem Beweis steckt:

$$\begin{array}{ccc} R & & R/_I \\ \cup & \overset{q}{\to} & \cup \\ I' & & I' \\ \cup & \overset{q^{-1}}{\leftarrow} & \cup \\ I & & (\bar{0}) \end{array} \qquad \left\{ \begin{array}{c} I' \subset R \text{ Ideal} \\ I' \supset I \end{array} \right\} \overset{1:1}{\longleftrightarrow} \left\{ \begin{array}{c} \text{Ideale} \\ \text{in } R/_I \end{array} \right\}$$

10.9 Beispiele

a) $(a) \subset \mathbb{Z}$ Primideal $\overset{10.5}{\Leftrightarrow}$ n Primzahl oder $n = 0$
$(n) \subset \mathbb{Z}$ maximal $\Leftrightarrow$ n Primzahl

b) Ein Ring R ist ein Integritätsbereich $\Leftrightarrow$ $(0) \subset R$ ein Primideal ist

c) In $\mathbb{Z}[X]$ sind z.B. prim.

- $I = (p) = \left\{ \sum a_i x^i \mid \forall i : p | a_i \right\}$
$$R/_I \simeq \mathbb{F}_p[x]$$
- $I = (x^2 + 1)$. Sei $i \in \mathbb{C}$ mit $i^2 = 1$:
$$R/_I \simeq \mathbb{Z}[i] = \{a + b_i \mid a, b \in \mathbb{Z}\}$$
hierbei ist $\simeq$ induziert von $R \to \mathbb{Z}[i], \quad x \mapsto i$ und $\sum a_\mu x^\mu \mapsto \sum a_\mu i^\mu$
- $I = (p, x^2 + 1)$, $R/_I \simeq \mathbb{F}_p[i] = \{a + b_i \mid a, b \in \mathbb{F}_p\}$
- $I = (3, x - 5), R/_I \simeq \mathbb{Z}/_3$: $R \to \mathbb{Z}/_3, \quad x \mapsto \bar{5}$

Die beiden ersten I sind Primideale, $R/_I$ Integritätsbereiche
Die letzten beiden I sind maximal, $R/_I$ ist Körper

10.10 Bruchrechnung - der Quotientenkörper

Wie $\mathbb{Z}$ in $\mathbb{Q}$, so ist jeder Integritätsbereich R Unterring eines kleinsten Körpers, des Quotientenkörpers von R.

Definition: sei R ein Integritätsbereich. Ein Quotientenkörper von R ist ein Körper K zusammen mit einem injektiven Homomorphismus $\iota : R \to K$ mit der folgenden universellen Eigenschaft:
Ist $\varphi : R \to L$ ein injektiver Hom. in einen Körper L, so faktorisiert φ in eindeutiger Weise über ι, d.h.

$$\exists!\ \psi : K \to L \quad \text{mit } \varphi = \psi \circ \iota$$

Bemerkung: Wie stets in solchen Situationen folgt die Eindeutigkeit von K und $R \hookrightarrow K$ bis auf eindeutige Isomorphie. R Integritätsbereich, $Quot(R)$ Quotientenkörper mit:

Beispiel: $R = \mathbb{Z}$, $Quot(\mathbb{Z}) = \mathbb{Q}$. φ injektiv ist notwendig für die Existenz von ψ:

10.11 Existenz von $Quot(R)$

Satz: Jeder Integrit"atsbereich$R$ hat einen Quotientenkörper.
Beweis:
Konstruktion: (vergleiche Konstruktion von $\mathbb{Q}$ aus $\mathbb{Z}$)

Auf $R \times (R\backslash\{0\})$ betrachte die Äquivalenzrelation

$$(a, b) \sim (a', b') :\Leftrightarrow ab' = a'b$$

Definiere: $K := (R \times (R\backslash\{0\}))/_\sim$.
Schreibweise: a/b oder auch $\frac{a}{b}$ für die Äquivalenzklasse $[(a, b)]$. Insbesondere gilt: $\forall c \in R\backslash\{0\} : a/b = ca/cb$.

Addition: $a/b + c/d := (ad + bc)/bd$

Multiplikation: $(a/b) \cdot (c/d) := ac/bd$. diese sind wohldefiniert, Körperaxiome gelten.

zu zeigen ist noch die Universelle Eigenschaft von $\iota : R \to K, \quad a \mapsto a/1$:

Sei $\varphi : R \to L$ ein injektiver Ringhomomorphismus in einen Körper.
Mit $\varphi = \psi \circ \iota$ muss dann gelten: $\psi(a/1) = \varphi(a)$. Dann gilt aber auch:

$$\varphi(a) = \psi(a/1) = \varphi(a/b \cdot b/1) = \psi(a/b) \cdot \psi(b/1) = \psi(a/b) \cdot \varphi(b)$$

$\Rightarrow \psi(a/b) = \varphi(a) \cdot \varphi(b)^{-1}$

Dies zeigt die Eindeutigkeit von ψ.
Existenz: Umgekehrt definiert $\psi : K \to L, \quad a/b \mapsto \varphi(a) \cdot \varphi(b)^{-1}$ einen wohldefinierten (!) Hom. $\psi : K \to L$ mit $\varphi = \psi \circ \iota$

□

Bemerkung

- Injektivität gefordert, sonst bekommt man Probleme beim teilen.
- Ist $R \subset K'$ mit K' Körper, dann ist $Quot(R) = \left\{ab^{-1} \in K' \mid a \in R, b \in R\backslash\{0\}\right\}$ der von R erzeugte Unterkörper, $\iota : R \to Quot(R)$ kanonische Inklusion.

10.12 Beispiele:

a) K Körper, so definieren wir:

$$K(X) := Quot(K[X]) = \left\{ \frac{a_0 + a_1 x + ... + a_n x^n}{b_0 + b_1 x + ... + b_n x^n} \mid a_i, b_i \in K, b_m \neq 0 \forall m \right\}$$

rationale Funktionen mit Koeffizienten in K.

b) R Integrit"atsbereich$\Rightarrow Quot(R[X]) = K[X]$ mit $K = Quot(R)$.
$R[X]$ ist Integrit"atsbereich(auch Gauß -Lemma):

$$(a_0 + a_1 x + ... + a_n x^n) \cdot (b_0 + b_1 x + ... + b_m x^m) = (a_0 b_0 + ... + a_n b_m x^{n+m})$$

Sind die ersten beiden Polynome ungleich 0, so auch das Produkt.

10.13 Ausblick:

Allgemeiner kann man die Nenner auf eine beliebige multiplikativ abgeschlossene Teilmenge $S \subset R\backslash\{0\}$ einschränken. $(1 \in S, S \cdot S \subset S)$:

$S^{-1}R := \{a/b \in Quot(R) \mid b \in S\}$ ist Unterring von $Quot(R)$.
Man nennt dies die Lokalisierung von R in S. Der Begriff stammt aus der Algebraischen Geometrie, insbesondere im Fall $S = R/_I$ mit $I \subset R$ Primideal ($\Leftrightarrow R/_I$ mult. abgeschlossen).
Etwa der Fall $R = K[X]$. $I = (x - \lambda), \lambda \in K$, definiert dann: $f/g \in S^{-1}R$ d.h. $(g \notin (X - \lambda))$ eine (algebraische) Funktion:

$$K \supset \{a \in K \mid g(x) \neq 0\} \to K, \quad x \mapsto f(x) \cdot g(x)^{-1} \text{ (ist wohldefiniert!)}$$

Mit anderen Worten schränkt die Lokalisierung die Betrachtung auf solche rationalen Funktionen ein, die in $x = \lambda$ definiert sind, denn $\lambda \in \{a \in K \mid g(x) \neq 0\}$, da $g(\lambda) \neq 0$, denn $g \notin (X - \lambda)$.
In Algebraischer Geometrie:

$$\begin{aligned} \text{Ringe } R &\leftrightarrow \text{Räume } (Spec(R)) \\ f \in R &\leftrightarrow \text{Funktionen} spec(R) \to K \\ f/g &\leftrightarrow \text{Funktionen} spec(R\backslash\{g = 0\}) \to K \end{aligned}$$

10.14 Zusammenfassendes Beispiel:

Für $R = \mathbb{R}[X]$ und das maximale Ideal $I = (X^2 + 1)$ haben wir vier Körper betrachtet:

- den Primkörper $\mathbb{Q} \subset \mathbb{R}[X]$ also den Körper der konstanten Polynome
- den Körper der Koeffizienten $\mathbb{R}$
- den Restklassenkörper $R/_I = \mathbb{R}[X]/(X^2 + 1) \simeq \mathbb{C}, \quad X \to i$
- den Quotientenkörper $Quot(R) = \mathbb{R}(X)$

Vorsicht:
Falls $I \neq R$, (0) (= Nulllideal), so gibt es keine Hom: $R/_I \to Quot(R)$ oder Hom:$Quot(R) \to R/_I$.

11 Teilbarkeitstheorie

11.1 Unzerlegbare Elemente

Definition: Sei R Integrit"atsbereich,

a) Für $a, b \in R \quad a|b$, schreibe a/b oder $\frac{a}{b}$ für das eindeutige Element $c \in R$ mit $a = bc$

b) $a \in R$ heißt Einheit, falls $\exists b \in R : \ ab = 1$ und die Menge der Einheiten: R^x (bilden multiplikative Gruppe)

c) $b \in R\backslash R^x$ heißt echter Teiler von a, falls $a = bc$ und $c \notin R^x$.

d) $a \in R$ heißt irreduzibel oder unzerlegbar, falls $a \notin R^x$, $a \neq 0$ und falls a keine echte Teiler besitzt. Ansonsten heißt a zerlegbar oder reduzibel.

11.2 Beispiele:

a) $R = \mathbb{Z}$, dann ist $R^x = \{1, -1\}$ und $a \in \mathbb{Z}\backslash\{0, \pm 1\}$ ist unzerlegbar $\Leftrightarrow a = \pm p, \quad p$ prim.

b) Die unzerlegbaren Elemente in $K[X]$, K Körper, so sind die Polynome f mit $deg(f) \geq 1$ $(K[X]^x = K^x)$, mit Koeffizienten in K, die irreduzibel als Polynome in K sind, etwa:
$f = X^2 + 1 \overset{!}{\to} g \cdot h$ o.E. sei g, h normiert(höchster Koeff = 1), $deg(g) = deg(h) = 1$. Schreibe: $g = X - \lambda$, $h = X - \mu$ mit $\lambda, \mu \in K$, dann ist $gh = X^2 - (\lambda + \mu)X + \lambda\mu$.
Demnach:
$f = gh \Leftrightarrow \lambda + \mu = 0, \lambda\mu = 1 \Leftrightarrow \mu = -\lambda, \lambda^2 = 1$
Dies zeigt: $f \in K[X]$ irreduziebel $\Leftrightarrow -1$ ist kein Quadrat in K. Z.B. ist f irreduzibel über $\mathbb{R}, \mathbb{F}_3$, aber f ist reduzibel über $\mathbb{C}, \mathbb{F}_5$, da $2 \cdot 2 = 4 = -1$

c) Schreibe $\mathbb{Z}[i] \subset \mathbb{C}$ für den von $\mathbb{Z}$ und i erzeugten Unterring.

$$[i^2 = -1 \Rightarrow \mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}]$$

Dann ist $2 = (1+i)(1-i)$ eine Zerlegung von 2 in irreduziblen Elemente.
Beweis:
Die Norm in $\mathbb{C}$ liefert einen Hom. von Monoiden:

$$\nu : (\mathbb{Z}[i], \cdot) \to (\mathbb{N}, \cdot), \quad a + bi \mapsto |a + bi|^2 = a^2 + b^2$$

denn $|(a+bi)(c+di)|^2 = |a+bi|^2 \cdot |c+di|^2$. Daraus folgt:
$\nu(\mathbb{Z}[i]^x) = 1$ und $a + bi$ zerlegbar $\Rightarrow \nu(a + bi)$ hat mehrere Primteiler:
$\nu(1+i) = \nu(1-i) = 2 \Rightarrow 1+i$ und $1-i$ unzerlegbar und keine Einheiten. Keine Einheiten, da $\nu(1 \pm i) \neq 1$. Angenommen $1 + i = \alpha\beta$ mit $\alpha, \beta \notin \mathbb{Z}[i]^x \Rightarrow 2 = \nu(1+i) = \nu(\alpha) \cdot \nu(\beta)$ aber beide ungleich 1, also Widerspruch

11.3 Konvention:

Ist $R \subset S$ Unterring und $\zeta_1, ..., \zeta_n$, so schreiben wir $R[\zeta_1, ..., \zeta_n] \subset S$ für den kleinsten Unterring von S der R und $\zeta_1, ..., \zeta_n$ enthält, explizit:

$$R[\zeta_1, ..., \zeta_n] = Im\left(R[X_1, ..., X_n] \to S, \quad \sum a_{i_1,....,i_n} X_1^{i_1} ....X_n^{i_n} \mapsto \sum a_{i_1,....,i_1} \zeta_1^{i_1}, ..., \zeta_n^{i_n}\right)$$

Einsetzungshom. $X_i \mapsto \zeta_i$

11.4 Existenz von Zerlegungen in irreduzible Elemente

Satz: Sei R Integrit"atsbereich, in dem jede Folge

$$(a_1) \subset (a_2) \subset ... \subset R \qquad \Leftrightarrow \forall \nu : a_{\nu+1} \mid a_\nu$$

von (Haupt-) Idealen stabilisiert, d.h. $\exists N$ mit $(a_\mu) = (a_\nu) \forall \nu, \mu \geq N$. Dann ist jede Nichteinheit $a \in R \backslash \{0\}$ ein Produkt von irreduziblen Elementen.
Beweis:

Schritt 1:
$a \in R \backslash \{R^x \cap \{0\}\}$ hat einen irreduziblen Teiler.
Induktiv: wähle a_ν mit $a_1 = a$, $a_{\nu+1}$ echter Teiler von a_ν. Dies bricht ab, falls a_ν irreduzibel.
Sonst: $(a_1) \subset (a_2) \subset ...$
Nach Voraussetzung folgt: $\exists \nu \geq N : \ (a_\nu) = (a_{\nu+1})$.
Insbesondere gilt:

$$a_{\nu+1} \in (a_\nu) \text{ und } a_\nu \in (a_{\nu+1}) \Rightarrow \exists b, c \in R : a_{\nu+1} = ba_\nu = bca_{\nu+1}$$

Da R Integrit"atsbereich folgt $bc = 1$ dies ist ein Widerspruch denn $a_{\nu+1}$ ist kein echter Teiler von a_ν.

Schritt 2:
Sei induktiv $b_{\nu+1}$ein irreduzibler Teiler von $a/(b_1 \cdot ... \cdot b_\nu)$. Die Induktion bricht ab, falls $e := a/(b_1 \cdot ... \cdot b_\nu)$ eine Einheit ist. $(\Rightarrow a = ((eb_1) \cdot ... \cdot b_\nu)$.
Falls nicht:
$(a) \subset (a/b_1) \subset (a/(b_1 b_2)) \subset ...$
Wie in Schritt 1 existiert ν mit: $a/(b_1 \cdot ... \cdot b_\nu)$ und $a/(b_1 \cdot ... \cdot b_{\nu+1})$ unterscheiden sich nur um eine Einheit, d.h. kein echter Teiler von $a/(b_1 \cdot ... \cdot b_\nu)$.

□

11.5 Bemerkung

a) Ringe, in denen aufsteigende Ketten von Idealen stabilisieren, heißen Noethersch. Alle "natürlich" vorkommenden Ringe sind Noethersch, z.B. $\mathbb{Z}, K[X_1, ..., X_n]$, Quotienten und Lokalisierung von Noetherschen Ringen.

Nicht Noethersch ist z.B. $K[\mathbb{R}_{>0}] = \left\{ \sum_{\text{endlich}} a_{\lambda_i} t^{\lambda_i} \mid a_{\lambda_i} \in K, \ \lambda_i \in \mathbb{R} \right\}$ $(t) \subset (t^{\frac{1}{2}}) \subset (t^{\frac{1}{4}}) \subset ...$

b) Für $R = \mathbb{Z}$ oder $R = K[X]$ haben wir Abbildungen

$$\gamma : R\backslash\{0\} \to \mathbb{N}$$

nämlich $a \mapsto |a|$ für $\mathbb{Z}$ und $f \mapsto deg(f)$ für $K[X]$, mit den folgenden Eigenschaften $\forall a, b \in R\backslash\{0\}$: (vergl. Gradfunktion in 11.9)

- $\nu(ab) \geq max\{\nu(a), \nu(b)\}$
- Die Gleichheit gilt genau dann wenn: $a \in R^x$ oder $b \in R^x$

Die Voraussetzungen des Satzes 11.4 gilt für solche, sehr speziellen Ringe:

$$(a_1) \subset (a_2) \subset ... \Rightarrow \nu(a_1) \geq \nu(a_2) \geq ...$$

Alternativ beweist man den Satz für diese Ringe sofort nach Induktion nach $\nu(a)$

11.6 Zur Eindeutigkeit der Zerlegung in irreduzible Elemente

In $\mathbb{Z}[i\sqrt{5}] \subset [\mathbb{C}]$ hat 21 keine eindeutige Zerlegung:

1. $21 = 3 \cdot 7$
2. $21 = (1 + 2i\sqrt{5})(1 - 2i\sqrt{5})$

$3, 7, 1 \pm i\sqrt{5}$ sind irreduzibel:

$$|a + bi\sqrt{5}|^2 = a^2 + 5b^2 \ , \quad |3|^2 = 3^2 \ , \quad |7|^2 = 7^2 \ , \quad |1 \pm 2i\sqrt{5}|^2 = 21$$

keine dieser ganzen Zahlen lässt sich nichttrivial als $(a^2 + 5b^2) \cdot (c^2 + 5d^2)$ schreiben.
Es gibt jedoch eine eindeutige Zerlegung auf den Niveau von Idealen:

$$\pi_1 := (7, 1 + 2i\sqrt{5}) \quad \pi_2 := (7, 1 - 2i\sqrt{5})$$
$$\varrho_1 := (3, 1 + 2i\sqrt{5}) \quad \varrho_2 := (3, 1 - 2i\sqrt{5})$$

sind Primideale und

$\pi_1 \cdot \pi_2 = (7)$

$\varrho_1 \cdot \varrho_2 = (3)$

$\pi_1 \cdot \varrho_1 = (1 + 2i\sqrt{5})$

$\pi_2 \cdot \varrho_2 = (1 - 2i\sqrt{5})$

und somit:

$$\begin{aligned}(21) = (3) \cdot (7) &= (1 + 2i\sqrt{5}) \cdot (1 - 2i\sqrt{5}) \text{ nicht eindeutig} \\ &= (\pi_1 \cdot \pi_2) \cdot (\varrho_1 \cdot \varrho_2) \\ &= (\pi_1 \cdot \varrho_1) \cdot (\pi_2 \cdot \varrho_2) \\ &= \pi_1 \cdot \pi_2 \cdot \varrho_1 \cdot \varrho_2\end{aligned}$$

eindeutig bis auf Reihenfolge.

Bemerkung Kummer und Dedekind führten den Begriff "ideale Zahlen" in der Zahlentheorie ein. Diese erlauben eine eindeutige Zerlegung (bis auf Reihenfolge) in irreduzible ideale Zahlen. In moderner Sprache zeigt man, dass in jedem Dedekind-Ring jedes Ideal I eine bis auf Reihenfolge eindeutige Darstellung als Produkt von Primidealen hat:

$$I = \pi_1^{m_1} .... \pi_k^{m_k}$$

Dedekind-Ringe sind die "eindimensionalen, regulären" Ringe, wobei:

$$(dim(R) = 1) :\Leftrightarrow (\pi \subset R \text{ Primideal } \Rightarrow \pi = (0) \vee \pi \text{ maximal}$$

mit R Integrit"atsbereich.
Solche Ringe sind also recht speziell.
Im allgemeinen (R Noethersch) erhält man nur eine sogenannte Primärzerlegung:

$$I = \varrho_1 \cap ... \cap \varrho_k$$

mit ϱ_i "Primärideale" (z.B. Potenzen von Primidealen)

Beispiel: In $K[x,y,z]: (xy, yz, zx) = (x,y) \cap (y,z) \cap (z,x) \quad (\supsetneq (x,y)\cdot(y,z)\cdot(z,x))$

11.7 Eindeutigkeit der Zerlegung in irreduzible Elemente

Da die Eindeutigkeit der Zerlegung in irreduzible Elemente demnach eine Eigenschaft des Rings ist definieren wir:

Definition: Sei R ein Integrit"atsbereich

a) $u \in R$ heißt prim, falls $(u) \subset R$ Primideal ist.

b) R heißt faktoriell, falls jede Nichteinheit $\neq 0$ bis auf Reihenfolge und Einheiten eindeutiges Produkt von Primelementen ist.

Bemerkung:

a)

$$\begin{array}{rccccc} \text{"u prim "} \Leftrightarrow & u \mid ab & \Rightarrow & u \mid a & \vee & u \mid b \\ & \Updownarrow & & \Updownarrow & & \Updownarrow \\ & ab \in (u) & \Rightarrow & a \in (u) & \vee & b \in (u) \end{array}$$

b) Ist R Noethersch, dann ist: R faktoriell $\Leftrightarrow$ jedes irreduzible Element ist prim. (siehe auch Beispiel "21")

11.8 Beweis der Eindeutigkeit der Zerlegung in irreduzible Elemente

Wir werden die Eindeutigkeit der Zerlegung in irreduzible Elemente in $\mathbb{Z}, \mathbb{Z}[i], K[X]$ wie folgt abstrakt in 3 Schritten beweisen:

i) $\mathbb{Z}, \mathbb{Z}[i], K[X]$ sind Euklidische Ringe (11.9, 11.10) ($\exists\nu$...)

ii) Euklidische Ringe sind Hauptidealringe (11.11, 11.12)

iii) Hauptidealringe sind faktoriell (11.13, 11.14)

11.9 Definition: Euklidisch

Ein Integrit"atsbereich$R$ heißt Euklidisch, falls es ein Abbildung

$$\nu : R\backslash\{0\} \to \mathbb{N} \quad \text{(Gradfunktion)}$$

gibt mit der folgenden Eigenschaft:
$a, b \in R, b \neq 0 \Rightarrow \exists q, r \in R : a = qb + r$ (Teilen mit Rest) und $r \neq 0 \Rightarrow \nu(r) < \nu(b)$

Bemerkung: $b \neq 0$, dann ist $\nu(b) = 0 \Rightarrow b \in R^x$:
Teile 1 mit Rest durch b: $1 = qb + r$ und $r = 0$, denn $\nu(b) = 0$ dann ist b eine Einheit, denn $q = b^{-1}$.

11.10 Beispiele:

a) $\mathbb{Z}$ ist Euklidisch, mit $\nu(a) := |a|$ (bekannt: teilen mit Rest)

b) $K[X]$ ist Euklidisch mit $\nu(f) := deg(f)$ (bekannt: teilen mit Rest)

c) $\mathbb{Z}[i]$ mit $\nu(a + bi) := a^2 + b^2$ ist Euklidisch (Übung!)

11.11 Hauptideal,

Definition: Sei R Ring,

a) Ein Ideal $I \subset R$ heißt Hauptideal, falls $I = (a)$ für ein $a \in R$ (wird von nur einem Element erzeugt)

b) R heißt Hauptidealring, wenn jedes Ideal ein Hauptideal ist.

Zwischenbemerkung: Bei Aufgabe 4 Blatt 8: $p = \sum_{n\geq 0} a_n X^n$, $p' = \sum_{n\geq 1} n a_n x^{n-1}$

Wiederholung:

- R faktoriell $:\Leftrightarrow \forall u \in R\backslash\{R^* \cap \{0\}\}\ \exists a_1, ..., a_r$ prim: $u = a_1 \cdot ... \cdot a_r$, wobei
- $a \in R$ prim $:\Leftrightarrow (a) \subset R$ Primideal
- Primelemente sind irreduzibel.
- R faktoriell $\Rightarrow$ jedes $u \in R\backslash\{R^* \cap \{0\}\}$ ist bis auf Reihenfolge und Einheiten eindeutiges Produkt von irreduziblen Elementen.

  Zu Bemerkung 11.7 c):
  hier gilt sogar Äquivalenz, hier aber nicht bewiesen. Beweisidee:

$$\begin{aligned} u = a_1 \cdot ... \cdot a_r = b_1 \cdot ... \cdot b_s &\Rightarrow b_1 \cdot ... \cdot b_s \in (a_1) \\ &\Rightarrow \exists i : b_i \in (a_1) \\ &\Rightarrow a_1 | b_i \end{aligned}$$

  da aber b_i irreduzibel folgt $\exists c_i \in R^* : b_i = c_i a_1$ Induktion nach $\min\{r, s\}$

Wir wollen zeigen:
R Euklidisch $\Rightarrow$ R Hauptidealring ($\leftrightarrow$ Teilen mit Rest)$\Rightarrow$ R faktoriell.

11.12 Satz:

Jeder Euklidische Ring R ist ein Hauptidealring.
Beweis:
Für $I \subset R$ ein Ideal $\neq (0)$. Wähle $a \in I\backslash\{0\}$ mit $\nu(a) = \min\{\nu(b) \mid b \in I\backslash\{0\}\}$,

$$\nu : R\backslash\{0\} \to \mathbb{N}$$

die Gradfunktion. Dann ist zu zeigen: $I = (a)$:
Sei $b \in I$, dann $b = qa + r$ und $r \neq 0$ oder $\nu(r) < \nu(a)$.

$\underline{r = 0}$: $b = qa \Rightarrow b \in (a)$

$\underline{r \neq 0}$: $r = b - qa \in I$, da schon $b, qa \in I$

Dies ist ein Widerspruch zur Wahl von a.

□

11.13 Lemma

Sei R ein Integrit"atsbereich, $u \in R\backslash\{0\}$ Nichteinheit,

a) Es gilt: $(u) \subset R$ maximal $\Rightarrow$ (u) Primideal $\Rightarrow$ u irreduzibel

b) Ist R ein Hauptidealring, so gelten in a) auch die Umkehrung. Insbesondere sind die irreduziblen Elemente genau die Primelemente

Beweis:

a) bekannt:

   (i) (u) maximal $\Leftrightarrow$ $R/_{(u)}$ Körper $\Rightarrow$ $R/_{(u)}$ Integrit"atsbereich$\Leftrightarrow$ (u) Primideal

   (ii) $u = ab \Rightarrow ab \in (u) \overset{(u)\text{Primideal}}{\Rightarrow} a \in (u)$ oder $b \in (u) \Rightarrow a \in R^*$ oder $b \in R^*$

b) Wir zeigen: u irreduzibel $\Rightarrow (u) \subset R$ maximal, also:
zz. $v \in R \Rightarrow (u,v) = R$ oder $(u,v) = (u)$:

$$\begin{aligned} \text{Sei } R \text{ Hauptidealring } &\Rightarrow \exists a \in R : (u,v) = (a) \\ &\Rightarrow \exists f,g \in R : u = fa,\ v = ga \end{aligned}$$

Da u irreduzibel folgt mit $u = fa$ entweder $a \in R^* \Rightarrow (u,v) = (a) = R$
oder $f \in R^* \Rightarrow (u,v) = (a) = (u)$.

□

Korollar:

- In $R[X], f \in R$ gilt: $K[X]/(f)$ ist ein Körper genau denn wenn f irreduzibel ist.

Bemerkung: Rechnen in diesen Körpern Explizit: $g \in K[X] \backslash (f)$ also kein Vielfaches von f, so läßt sich das Inverse $\bar{g} \in K[X]/_{(f)}$ wie folgt bestimmen:

i) Mit Euklidischem Algorithmus: angewendet auf f, g liefert $p, q \in K[X]$, so dass $pf + qg = 1$
Daraus folgt: $\bar{q}\bar{g} = 1$ in $K[X]/_{(f)}$, d.h. $\bar{q} = \bar{g}^{-1}$.

ii) Mit Lineare Algebra: $deg(f) = r \Rightarrow 1, X, ..., X^{r-1}$ ist $K-$Basis von $K[X]/_{(f)}$. Das heißt für g gibt es Koeffizienten $a_0, ..., a_m \in K \quad (m \leq r)$:

$$(0 \equiv a_0 + a_1\bar{g} + ... + a_m\bar{g}^m)\ mod\ f$$

Wähle m minimal mit $a_m \neq 0$ (also breche ab wenn erste lineare Abhängigkeit gefunden wird)
Dann gilt: $a_0 \neq 0$:

$$0 \equiv a_1\bar{g} + ... + a_m\bar{g}^m = \bar{g}(\underbrace{a_1 + ... + a_m\bar{g}^{m-1}}_{=0})$$

im Integrit"atsbereich$K[X]/_{(f)}$, also ein Widerspruch zur Minimalität von m.

$\Rightarrow \bar{g}(-\frac{a_1}{a_0} - \frac{a_2}{a_0}\bar{g} - ... - \frac{a_m}{a_0}\bar{g}^{m-1}) = 1$

und damit

$$(-\frac{a_1}{a_0} - \frac{a_2}{a_0}\bar{g} - ... - \frac{a_m}{a_0}\bar{g}^{m-1}) = (\bar{g})^{-1}$$

allerdings ist die erste Variante viel Einfacher!

11.14 Satz Jeder Hauptidealring ist faktoriell

(d.h. jedes $u \in R\backslash(\{0\} \cap \mathbb{R}^x)$ ist Produkt von Primelementen)
Beweis:
Jedes irreduzible Element ist prim (nach Satz 11.13)
nach Satz 11.4 gilt dann:
Für Ringe mit aufsteigender Kettenbedingung für Hauptideal gilt eine Zerlegung in irreduzible Elemente. D.h. zu zeigen bleibt noch das wir eine aufsteigende Kettenbedingung (hier äquiv. R ist Noetersch).
Sei $(a_0) \subsetneq (a_1) \subsetneq ...$ aufsteigende Kette von Idealen
$\Rightarrow I := \bigcup_{i \geq 0} (a_i)$ ist ein Ideal:
sei $b \in I, r \in R \Rightarrow rb \in I$, denn $\exists n : b \in (a_n) \Rightarrow rb \in (a_n) \subset I$

R HIR $\Rightarrow \exists a \in R : I = (a) \Rightarrow \exists N : a \in (a_n)\ \forall n \geq N \Rightarrow (a) = (a_n)$

□

11.15 Korollar

$\mathbb{Z}, \mathbb{Z}[i], K[X]$ sind faktoriell

11.16 Zur Untersuchung der Primzerlegung

Zur Untersuchung der Primzerlegung in $\mathbb{Z}[X]$ und $K[X_1, ..., X_n] = K[X_1, ..., X_{n-1}][X_n]$ $(n > 1)$, die keine Hauptidealringe sind, verallgemeinern wir wie folgt:

Satz: Ist R faktoriell, so ist auch $R[X]$ faktoriell. Die Primelemente (=irreduziblen Elemente) von $R[X]$ sind genau:

a) die irreduziblen Elemente von R (als Polynome von Grad 0)

b) $f \in R[X]$ mit

(i) f ist irreduzibel in $K[X]$, $K = Quot(R)$.

(ii) $a \mid f, a \in R \Rightarrow a \in R^x$ (In HIR äquiv zu $f = \sum_{i=0}^{d} a_i X^i$, dann $(a_0, ..., a_d) = R$)
f heißt dann primitiv.

Beweis: 11.18

11.17 Vorbereitung: Gauß-Lemma

Lemma: Sei R faktoriell und $P, Q \in R[X]$ primitiv, dann ist $PQ \in R$ primitiv.
Beweis:
Angenommen $a|PQ, a \notin R^x$.
Da R faktoriell ist gilt:
$\exists$ Primelement $p \in R$ mit $p|a \Rightarrow \overline{PQ} = \overline{P} \cdot \overline{Q} = 0$ in $(R/_p)[X]$.
Ferner ist $(p) \subset R$ Primideal, also $R/_p$ Integrit"atsbereich.

$\Rightarrow \overline{P} = 0$ oder $\overline{Q} = 0$

$\Rightarrow p|P$ oder $p|Q$

$\Rightarrow P$ oder Q ist nicht primitiv, also Widerspruch

11.18 Beweis von 11.16

Die Irreduzibilität der Elemente ist in a), b) ist klar:

a): f in $K[X]$ konstantes Polynom, also nicht reduzibel, wenn nicht schon in R

b): $f = g \cdot h$ in $R[X]$.

- $deg(g) > 0, deg(h) > 0 \Rightarrow f = g \cdot h$ in $K[X]$ nichttriviale Zerleg. in $K[X]$ verboten nach (i)
- $deg(g) = 0$ oder $deg(h) = 0 \Rightarrow a := g$ teilt $f \overset{(ii)}{\Rightarrow} g \in R^x$

Zerlege $P \in R[X]$ zunächst in $K[X] : P = Q_1 \cdot ... \cdot Q_r, Q_i \in K[X]$:

Da R faktoriell ist, können wir $Q_i = c_i \cdot Q_i'$ schreiben mit $Q_i' \in R[X]$ primitiv, $c_i \in K$.

$$\Rightarrow P = Q_1' \cdot ... \cdot Q_r' \quad , \quad c = \prod c_i = a/b \in K$$

mit $a, b \in R$ teilerfremd. Nach dem Gauß-Lemma folgt: $Q_1', ..., Q_r'$ primitiv.
Aber $1/(b \cdot Q_1' \cdot ... \cdot Q_r')$ in $R[X]$
also folgt:

$$b \in R^x \Rightarrow c \in R$$

Zerlege nun noch c in R in Primelemente.
Dies liefert die Existenz der Zerlegung in Elemente aus a), b) und die Vollständigkeit unserer Liste der irreduziblen Elemente.
Es bleibt noch zu zeigen: dies irreduziblen Elemente in $R[X]$ sind prim.

Gelte: $P|Q_1Q_2$ $(\overset{!}{\Rightarrow} P|Q_1$ oder $P|Q_2) \Rightarrow P$ teilt Q_1Q_2 in $K[X]$
Entweder ist $P \in R\backslash\{0\}$ oder P prim in $K[X] \Rightarrow P$ teilt Q_1 oder Q_2 in $K[X]$,

o.E gelte: $P|Q_1$ in $K[X]$

Schreibe: $Q_1 = TP, \;\; T \in K[X]$. Sei $a \in R$ mit $T' := aT \in R[X]$, dann gilt:

$$aQ_1 = T'P \text{ in } R[X]$$

Ist $u \in R$ Primfaktor von a, so folgt $u|T'$, denn P primitiv (Gauß-Lemma)
Nach Kürzen der Primfaktoren dürfen wir also $a \in R^x$ annehmen. ($\Rightarrow T \in R[X]$)
$\Rightarrow P$ teilt Q_1 in $R[X]$.

11.19 Korollar:

$K[X_1, ..., X_n], \mathbb{Z}[X_1, ..., X_n]$ sind faktoriell. Aber dies sind keine HIR für $n > 1, bzw. n > 0$!
für $n > 1$ ist $K[X_1, ..., X_n]/(f)$ nie ein Körper. man braucht mindestens $K[X_1, ..., X_n]/I$ und I hat mind. n Erzeuger

12 Irreduzibilitätskriterien für Polynome

In der Körpertheorie werden wir vor allem Körper der Form

$$\mathbb{Q}[X]/_{(f)}$$

untersuchen. Nach Lemma 11.13 gilt das dies ist ein Körper gdw $f \in \mathbb{Q}[X]$ irreduzibel ist.
Es ist daher wichtig, Irreduzibilitätskriterien für Polynome zu kennen.

12.1 Korollar zu Satz 11.16

Sei R faktoriell, $K = Quot(R), f \in R[X]$ primitives Polynom, dann gilt:

$$f \in R[X] \text{ irreduzibel} \Leftrightarrow f \in K[X] \text{ irreduzibel}$$

□

Bemerkung

- Dies ist eine wichtige Aussage, also sollte man sich den Beweis nochmal klar machen! Der entscheidende Punkt dabei ist das Gauß-Lemma .
- Für $f \in \mathbb{Z}[X]$ ist die Irreduzibilität über $\mathbb{Z}$ einfacher zu verifizieren als über $\mathbb{Q}$, wie wir sehen werden.

12.2 Kriterium I (Methode der unbestimmten Koeffizienten)

Sei $f \in R[X]$, R Integrit"atsbereich. Setzte an:

$$f = (b_0 + b_1X + ... + b_mX^m) \cdot (c_0 + c_1X + ... + c_nX^n)$$

mit $n, m \geq 1$, $m + n = deg(f)$, $(m \leq n)$. Finde b_i, c_i?
Zeige dann die Unlößbarkeit des entstehenden GLS in den b_i, c_j

Beispiel: $f = X^3 + X^2 + 2X + 1 \in \mathbb{Z}[X]$. die einzige Möglichkeit ist $m = 1, n = 2$.
Ansatz:

$$\begin{aligned}(X^3 + X^2 + 2X + 1) &= (b_0 + b_1X) \cdot (c_0 + c_1X + c_2X^2) \\ &= b_0c_0 + (b_0c_1 + b_1c_0)X + (b_0c_2 + b_1c_1)X^2 + b_1c_2X^3\end{aligned}$$

$$b_1c_2 = 1 \Rightarrow b_1 = \pm 1, c_2 \pm 1 \quad \text{o.E } b_1 = 1 = c_2 \quad (b_i \leftrightarrow -b_i, c_j \leftrightarrow -c_j)$$

Passiert stets falls f normiert. Das Übrige GLS:

$$\begin{aligned} c_1 + b_0 &= 1 \qquad (I) \\ c_0 + b_0 c_1 &= 2 \qquad (II) \\ b_0 c_0 &= 1 \qquad (III) \Rightarrow b_0 = \pm 1 \end{aligned}$$

Fall 1: $b_0 = 1 \overset{(III)}{\Rightarrow} c_0 = 1 \overset{(I)}{\Rightarrow} c_1 = 0$ Widerspruch zu (II)

Fall 2: $b_0 = -1 \Rightarrow c_0 = -1, c_1 = 2$ Widerspruch zu (II)

Also nicht lösbar!

12.3 Abspaltung von Linearfaktoren

Für $m = 1$ ist die folgende Beobachtung nützlich:

Satz: Sei R ein faktorieller Ring, $k = Quot(R)$ und $f = \sum a_i X^i \in R[X]$, $n = deg(f)$. Seien $\alpha, \beta \in R$ teilerfremd, dann gilt:

α/β ist eine Nullstelle von f in $K[X] \Leftrightarrow (\beta X - \alpha) | f$ in $R[X]$.

Ferner gilt dann: $\beta | a_n, \alpha | a_0$. Kein Beweis, aber einfach nachrechnen.

Beispiel:

a) Sei wieder $f = X^3 + X^2 + 2X + 1 \in \mathbb{Z}[X]$
Die möglichen α, β sind dann: $\beta = \pm 1, \alpha = \pm 1$
d.h $\alpha/\beta = \pm 1 : \quad f(1) = 5 \neq 0, \quad f(-1) = -1 \neq 0$

b) $f = 2X^3 - 11X + 5 \in \mathbb{Z}[X]$
$\beta = 1, \pm 2$, $\alpha = \pm 1, \pm 5 \quad \Rightarrow \alpha/\beta \in \{\pm 1, \pm \frac{1}{2}, \pm 5, \pm \frac{5}{2}\}$
Nachrechnen ergibt:

$$f(\alpha/\beta) \neq 0$$

also f irreduzibel

Beweis 12.3:
" $\Leftarrow$ " : okay
" $\Rightarrow$ " : Teilen mit Rest in $K[X]$: $f(\beta X - \alpha) \cdot q + r$ mit $deg(r) = 0$ oder $r = 0$ d.h $r \in K$.
Daraus folgt:

$$0 = f(\alpha/\beta) = 0 \cdot q + r \Rightarrow r = 0$$

Argumentiere mit dem Gauß-Lemma wie in Satz 11.16, um mit $q \in R[X]$ zu zeigen.

$$\alpha, \beta \text{ teilerfremd} \Rightarrow \beta X - \alpha \text{ primitiv}$$

□

Bemerkung: Wenn man bei diesem Verfahren herausfindet das f reduziebel ist erhält man auch gleich die Zerlegung. Weiter ist 12.3 eine Hilfe um das Kriterium schneller zu verifizieren.

12.4 Kriterium II (Reduktion modulo eines Primideals)

Ist R Integrit"atsbereich, $f \in R[X]$ und $I \subset R$ Primideal mit $\bar{f} \in (R/I)[X]$ irreduzibel und $deg(f) = deg(\bar{f})$ (also höchster Koeffizient liegt nicht in I), so ist auch f irreduzibel:

Sei $f = gh$ Zerlegung in $R[X]$ mit $deg(g), deg(h) > 0$, dann folgt:

$$\Rightarrow \bar{f} = \bar{g}\bar{h} \text{ und } deg(\bar{f}) = deg(f) \Rightarrow deg(\bar{g}) = deg(g) > 0, deg(\bar{h}) = deg(h) > 0$$

besonders nützlich in Verbindung mit Kriterium I für $\bar{f}$, falls R/I endlich.

Beispiel:
Sei $f = X^5 + X^2 + 1 \in \mathbb{Z}[X]$

Betrachte *mod* 2: $\bar{f}$ hat keine Nullstellen (also kein Linearfak abspaltbar):

$$1 + 1 + 1 \neq 0 \ mod\ 2 \quad , \quad 0 + 0 + 1 \neq 0 \ mod\ 2$$

Demnach $\bar{f} = \bar{g}\bar{h}$ nichttrivial und

$$deg(\bar{g}) \leq deg(\bar{h}) \Rightarrow deg(\bar{g}) = 2, deg(\bar{h}) = 3$$

Polynome vom Grad 2 über $\mathbb{F}_2 = \mathbb{Z}/_2$:

$X^2 = X \cdot X, X^2 + 1 = (X + 1)^2, X^2 + X = X(X + 1)$ irreduzibel, $X^2 + X + 1$ irreduzibel.

Aber $X^2 + X + 1 \nmid X^5 + X^2 + 1$:

$$(X^5 + X^2 + 1) : (X^2 + X + 1) = X^3 + X^2 + \text{ Rest1}$$

12.5 Kriterium III (Eisensteinkriterium)

Satz: Sei R faktoriell und $f = \sum a_i X^i \in R[X]$ primitiv und $n = ged(f) \geq 1$. Es gebe ein Primelement $u \in R$, so dass:

i) $u | a_i$ für $i = 0, ..., n - 1$ [f primitiv $\Rightarrow u \nmid a_n$]

ii) $u^2 \nmid a_0$

Dann ist f irreduzibel und heißt dann Eisensteinpolynom.

Beweis:
Angenommen $f = gh$ mit:

$$g = b_0 + ... + b_r X^r \quad , \quad h = c_0 + ... + c_s X^s, r, s > 0$$

wobei $b_i = 0$für $i > r$ und $c_j = 0$ für $j > s$

Da $u | a_0$ und $a_0 = b_0 c_0 \overset{u\ prim}{\Rightarrow} u | b_0$ oder $u | c_0$ sagen wir $u | b_0$
Da f primitiv $\overset{\text{Gauß-Lemma}}{\Rightarrow}$ g, h primitiv $\Rightarrow \exists k : u \nmid b_k$. Sei k minimal mit dieser Eigenschaft

$$u \nmid b_k (\Rightarrow u | b_i, i = 0, ..., k - 1)$$

Betrachte

$$a_k = b_0 c_k + b_1 c_{k-1} + ... + b_k c_0$$

$(k \leq r \leq n)$ $\quad u | a_k$ und $u | b_i c_k$ für $i = 0, ..., k - 1$

Daraus folgt $u | b_k c_0$.

aber $u \nmid b_k$, also $u | c_0 \Rightarrow u^2 | a_0 = b_0 c_0$ Widerspruch.

12.6 Beispiele:

a) $f = X^4 + 6X^3 + 2X^2 + 2 \in \mathbb{Z}[X]$ setzte $u = 2$

b) $a \in \mathbb{Z}$ sei kein Quadrat, dann sind $X^n + a, X^n = a$ irreduzibel.

f irrdeuzibel in einem Ring, dann auch in einem Isomorphen. Also suchen wir einen geeigneten in dem wir das Kriterium anwenden können

12.7 Bemerkung zum Eisensteinkriterium

Manchmal hilft eine Substitution $X \mapsto X + \lambda, \lambda \in R$ um die Anwendbarkeit des Eisensteinkriteriums zu erreichen: Klassisches Beispiel: $p-$tes Kreisteilungspolynom

$$f = (X^p - 1)/(X - 1) = 1 + X + ... + X^{p-1} \quad p \text{ prim}$$

Betrachte $f(X + 1) = ((X + 1)^p - 1)/X = \sum_{k=1}^{p} \binom{p}{k} X^{k-1} = \binom{p}{1} + \binom{p}{2} X + ... + \binom{p}{p} X^{p-1}$
Hier ist das Eisensteinkriterium anwendbar für $u = p$, dies zeigt: f irreduzibel!

13 Symmetrische Polynome

13.1 Definition:

Wirkt eine Gruppe G auf einem Ring R durch Ringhomomorphismen (d.h. $\Phi : G \to Aut(R)$ Gruppenhom.), dann heißt die Fixpunktmenge $R^G := \{r \in R \mid g.r = r \forall g \in G\}$ der Invariantenring der $G-$Wirkung (R^G ist wirklich ein Ring!).

13.2 Beispiel:

Klassifikation der Wirkung von $G = \mathbb{Z}/_2$ auf $R := K[X]$ mit einem Körper K

a) triviale Wirkung $R^G = R$

b) sei $\tau \in G\backslash\{e\}$ das nicht triviale Element ($\tau \neq e, \quad \tau^2 = e$). Sei weiter

$$\Phi_{tau}(X) := -X, \quad \Phi\tau(Y) = -Y$$

dann ist:

$$\Phi_\tau(\underbrace{\sum a_{ij}X^iY^j}_{f}) = \sum(-1)^{i+j}a_{ij}X^iY^j$$

($\Rightarrow \Phi_\tau(f) = f \Leftrightarrow a_{ij} = 0$ für alle i, j mit $i + j$ ungerade)
$\Updownarrow$
$f \in R^G$

Damit läßt sich jedes Monom in R^G als Produkt schreiben:

$$X^{2a}Y^{2b}(YX)^c, l \qquad a, b, c \geq 0$$

$\rightsquigarrow$ Definiere Ringhom $K[U, V, W] \xrightarrow{\psi} R^G$ via $\begin{cases} U \mapsto X^2 \\ V \to Y^2 \\ W \to XY \end{cases}$

Behauptung ψ induziert einen Ringisomorphismus:

$$\tilde{\psi} : K[U, V, W]/_{(UV-W^2)} \xrightarrow{\sim} R^G$$

Beweis:
z.z.: $(UV - W^2) = ker(\psi)$:
" $\subset$ " klar
" $\supset$ " $K[U, V, W]/_{(UV-W^2)}$ hat eine lineare $k-$Basis

$$(U^aV^b, U^aV^bW \mid a, b \geq 0)$$

Die von $\tilde{\psi}$ auf $(X^{2a}Y^{2b}, X^{2a+1}Y^{2b+1} \mid a, b \geq 0)$ abgebildet wird. Dies ist Basis von R^G. Daraus folgt $ker(\tilde{\psi}) = 0$ und damit $ker(\psi) = (UV - W^2)$

c) $\Phi_\tau(X) = Y, \Phi_\tau(Y) = X$ für $\tau \in G\backslash\{e\}$

$$f := \sum_{i,j} a_{ij}X^iY^j \overset{!}{\in} R^G \Leftrightarrow a_{ij} = a_{ji}$$

f heißt symmetrisch $\rightsquigarrow$ Def 13

Bemerkung

- lineare Wirkung, ist eine Wirkung die Linear auf den Koordinaten Wirkt
- Allgemeiner gilt für jede Lineare $G-$Wirkung auf K^n, dass $K[X_1, ..., X_n]^G$ ein Quotient eines Polynomrings über K ist ($= K-$Algebra)
- Minimale Erzeugendensysteme von R^G sind nicht eindeutig!

13.3 Definition: Symmetrische Polynome

Wirke die Permutationsgruppe S_n auf dem Ring $R[X_1, ..., X_n]$ durch Permutation der Variablen:

$$\sigma. \sum a_{i_1,....,i_n} X_1^{i_1}, ..., X_n^{i_n} := \sum a_{i_1,....,i_n} X_{\sigma 1}^{i_1}, ..., X_{\sigma n}^{i_n}$$

$\forall \sigma \in S_n$.
$R[X_1, ..., X_n]^{S_n}$ heißt Ring der symmetrischen Polynome.

13.4 Familien symmetrischer Polynome

a) Das $d-$te elementarsymmetrische Polynom $s_d \in R[X_1, ..., X_n]^{S_n}$:

$$\begin{aligned} s_1 &= X_1 + X_2 + ... + X_n \\ s_2 &= X_1X_2 + X_1X_3 + ... + X_1X_n + X_2X_3 + ... \end{aligned}$$

allgemein:

$$s_d = \sum_{1 \le i_1 < ... < i_d} X_{i_1} \cdot ... \cdot X_{i_d}$$

b) Das $d-$te totalsymmetrische Polynom t_d:

$$t_d = \sum_{1 \le i_1 \le ... \le i_d} X_{i_1} \cdot ... \cdot X_{i_d}$$

Also:

$$\begin{aligned} t_1 &= S_1 \\ t_2 &= S_2 + \sum_{i=1}^{n} X_i^2 \end{aligned}$$

etc.

c) Das $d-$te Newtonpolynom

$$N_d := \sum_{i=1}^{n} X_i^d$$

Bemerkung

1) All diese Polynome s_d, t_d, N_d sind homogen, d.h. alle Monome des Polynoms haben gleichen Grad.

2) Jede dieser Familien erzeugt $\mathbb{Q}[X_1, ..., X_n]^{S_n}$! d.h.

$$\mathbb{Q}[s_1, ..., s_n] \stackrel{!}{=} \mathbb{Q}[t_1, ..., t_n] \stackrel{!}{=} \mathbb{Q}[N_1, ..., N_n]$$

und der nächste Satz sagt noch aus, dass:

$$\mathbb{Q}[s_1, ..., s_n] \stackrel{13.5}{=} \mathbb{Q}[X_1, ..., X_n]^{S_n}$$

13.5 Hauptsatz über Symmetrische Polynome

Sei R ein Ring, dann ist Φ mit:

$$\Phi : R[Y_1, ..., Y_n] \stackrel{\sim}{\to} R[X_1, ..., X_n]^{S_n}, \quad Y_d \mapsto S_d(X_1, ..., X_n)$$

ist ein Isomorphismus.
Beweis: folgt noch

13.6 Zum Beweis

Zum Beweis benötigen wir den Begriff der Ordnung auf Monomen. Definiere lexigraphische Ordnung auf Monomen durch:

$$X_1^{i_1}.....X_n^{i_n} > X_1^{j_1}....X_1^{j_n}$$

genau dann wenn für das kleinste k mit $i_k \neq j_k$ gilt $i_k > j_k$
zum Beispiel:

$$X_1^5 X_2^8 > X_1^5 X_3^{10} = X_1^5 X_2^0 X_3^{10}$$

Eigenschaften:

1) Jede fallende Folge von Monomen ist endlich.

2) Ordnung ist verträglich mit der Multiplikation.

Definition: Das Leitmonom $LM\left(\sum_{I\in\mathbb{N}^n} a_I X^I\right) := \begin{cases} max\{X^I \mid a_I \neq 0\} & \text{,falls } \exists I : A_I \neq 0 \\ 0 & \text{,sonst} \end{cases}$

13.7 Beweis von 13.5

1) Φ ist injektiv:

$$\begin{aligned} LM(S_1^{i_1}....S_n^{i_n}) = & \quad LM(S_1)^{i_1}....LM(S_n)^{i_n} \\ = & \quad X_1^{i_1} \cdot (X_1X_2)^{i_2} \cdot ... \cdot (X_1...X_n)^{i_n} \\ = & \quad X_1^{i_1+...+i_n} \cdot X_2^{i_2+...+i_n} \cdot ... \cdot X_n^{i_n} \end{aligned}$$

$\Rightarrow LM(S^I) = LM(S^J) \Leftrightarrow I = J$
also genau dann wenn:

$$\begin{aligned} i_1 + ... + i_n &= j_1 + ... + j_n \\ \vdots &= \vdots \\ i_n &= j_n \end{aligned}$$

$\Rightarrow LM\left(\sum_{I\in\mathbb{N}^n} a_I S^I\right) = max\{X_1^{i_1+...+i_n} \cdot X_2^{i_2+...+i_n} \cdot ... \cdot X_n^{i_n} \mid a_{i_1...,i_n} \neq 0\}$

$\Rightarrow \left(\sum a_I T^I \neq 0 \Rightarrow \sum a_I S^I \neq 0\right)$, also Φ injektiv

2) Φ ist surjektiv:

Sei $f = \sum a_I X^I$ symmetrisch, dann ist:

$$\begin{aligned} LM(f) &= X_1^{j_1}...X_n^{j_n} \text{ mit } j_1 \geq j_2 \geq ... \geq j_n \text{ (da } f \text{ symmetrisch)} \\ &= X_1^{j_1-j_2}(X_1X_2)^{j_2-j_3}...(X_1...X_n)^{j_n} \\ &= LM(S_1^{j_1-j_2}) \cdot LM(S_2^{j_2-j_3})....LM(S_n^{j_n}) \\ &\Rightarrow LM(f - a_{ii_1...i_n} S_1^{j_1-j_2}...S_n^{j_n}) < LM(f) \\ &\Rightarrow \text{Fertig durch Induktion nach } LM-\text{Ordnung.} \end{aligned}$$

□

Die Diskriminante

13.8 13.8 Beispiele (zur Entwicklung symmetrischer Polynome in die S_d via LM)

a) $\Delta_2 = (X_1 - X_2)^2 = X_1^2 - 2X_1X_2 + X_2^2$

$$LM(\Delta_2) = X_1^2 = LM(s_1^2) \qquad (s_1 = X_1 + X_2)$$

$\Rightarrow \Delta_2 - s_1^2 = -4X_1X_2 = -4s_2$

$\Rightarrow \Delta_2 = s_1^2 - 4s_2$

b)
$$\begin{aligned}\Delta_3 &= \prod_{i\neq j;i,j\in\underline{3}} (X_i - X_j)\\ &= -(X_1 - X_2)^2 \cdot (X_2 - X_3)^2(X_1 - X_3)^2\\ &...\\ &= 4s_2^3 + 27s_3^2 - 18s_1s_2s_3 + 4s_1^2s_3 - s_1^2s_2^2\end{aligned}$$

13.9 13.9 Definition:

a) Wir definieren die Diskriminante D_n (in n Variablen) durch:

$$\prod_{i\neq j;i,j\in\underline{n}} (X_i - X_j) = (-1)^{\binom{n}{2}} \prod_{i<j} (X_i - X_j)^2 =: D_n(s_1, ..., s_n)$$

b) Die Diskriminante von

$$f = X^n + a_1X^{n-1} + ... + a_n \in R[X]$$

ist $D_n(f) := D_n(a_1, ..., a_n)$

Bemerkung: (zu 13.9) Eigenschafte von $D_n(f)$:
Zerfällt f in Linearfaktoren

$$f = \prod_{i=1}^{n} (X + \lambda_i)$$

Dann folgt: $a_n = s_d(\lambda_1, ..., \lambda_n) \ \ \forall d \in \{0, ..., n\}$ und damit

$$D_n(f) = \prod_{i\neq j} (\lambda_i - \lambda_j) \qquad (*)$$

13.10 Mehrfache Nullstellen

Aus $(*)$ erhalten wir das folgende Korollar:

Korollar: Sei R ein Integrit"atsbereichund $f \in R[T]$ zerfalle in einen Oberring S von R ($R \hookrightarrow S$), also R ins Unterring von S, dann gilt:

$$f \text{ hat mehrfache Nullstelle } \Leftrightarrow D_n(f) = 0$$

Bemerkung Ein solches S gibt es immer (siehe Kapitel 14)

13.11 Bemerkung

Eine Möglichkeit, mehrfache Nullstellen zu finden:

$$f = (X_j - \lambda)^2 \cdot g \Rightarrow f, f' \in (X_j - \lambda)$$

$\rightsquigarrow$ bestimme $ggT(f, f')$ via euklidischem Algorithmus.

3 III Körper

Jeder nichttriviale Ringhomomorphismus $i : K \to L$ zwischen zwei Körpern K und L ist injektiv, da $\{0\}$ das einzige echte Ideal von K ist.
Daraus folgt: i ist eine Inklusion und heißt Körpererweiterung von K, notiert als L/K

14 14 Algebraische Körpererweiterungen

14.1 Definition:

Ist L/K eine Körpererweiterung und $\alpha_1, ..., \alpha_n \in L$, so bezeichnet $K(\alpha_1, ..., \alpha_n)$ den kleinsten Unterkörper von L der K und $\alpha_1, ...\alpha_n$ enthält.
L heißt endlich erzeugt, falls $L = K(\alpha_1, ..., \alpha_n)$ für Erzeuger $\alpha_1, ..., \alpha_n \in L$

Bemerkung: VORSICHT!:
$K(X) := Quot(K[X])$ muss unterschieden werden von dem durch X und K in $Quot(K[X])$ erzeugten Unterkörper.
Zur Klarheit benutze kleine Buchstaben für Elemente einer Körpererweiterung und große für unabhängige Variablen.

14.2

Sei L/K Körpererweiterung. Definiere:

a) $[L : K] := dim_K(L)$ heißt Grad von L/K (L ist K-Vektorraum)
L/K heißt endlich, falls $[L : K]$ endlich

b) $deg_K(\alpha) := [K(\alpha) : K]$ heißt Grad von $\alpha \in L$ über K

Bemerkung (zu b) α heißt algebraisch über K, falls $deg_K(\alpha) < \infty$, andernfalls transzendent.

Beispiele:

- $[\mathbb{C} : \mathbb{R}] = dim_{\mathbb{R}}(\mathbb{C}) = 2$ ($\mathbb{R}-$Basis $(1, i) \Rightarrow i$ algebraisch)
- $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ ($\mathbb{Q}-$Basis $(1, \sqrt{2})$
- $[\mathbb{R} : \mathbb{Q}] = \infty$ da $\mathbb{Q}^n$ abzählbar aber $\mathbb{R}$ nicht
- $[K(X) : K] = \infty$

14.3 Charakterisierung algebraischer Elemente

Satz: Sei L/K eine Körpererweiterung. Für $\alpha \in L \backslash K$ sind äquivalent:

1. α ist algebraisch über K
2. $\exists f \in K[X]$ mit $f(\alpha) = 0$
3. Es existiert ein Zwischenkörper L', mit $K \subset L' \subset L$ mit $\alpha \in L'$, $[L' : K] < \infty$

Beweis:

1) $\Rightarrow$ 2) $dim_K(K(\alpha)) < \infty$
$\Rightarrow \exists n \in \mathbb{N}$, so dass die Potenzen $1 = \alpha^0, ..., \alpha^n$ über K linear abhängig sind , d.h.

$$\exists c_0, ..., c_n \in K\backslash\{0\} \text{ mit } c_0 + c_1\alpha^1 + ... + c_n\alpha^n = 0$$

$\Rightarrow$ setze:

$$f := c_nX^n + ... + c_1X + c_0$$

dann ist $f(\alpha) = 0$

2) $\Rightarrow$3) o.E. sei f irreduzibel in $K[X]$, dann gilt: (f) ist maximal, da $K[X]$ HIR. Nach 11.13 folgt dann: $L' := K[X]/_{(f)}$ ist ein Körper.

Behauptung:

$$K[X]/_{(f)} \xrightarrow{\sim} K(\alpha), \quad X \mapsto \alpha$$

ist Isomorphismus.

Beweis:
Sei $g(\alpha) = 0$
$\Rightarrow (f, g) = (h)$, da $K[X]$ HIR
$\Rightarrow h | f, g$
$\Rightarrow$ o.E. $h = f$, da f irreduzibel. $\surd$

3) $\Rightarrow$1) Aus $K(\alpha) \subset L' \Rightarrow [K(\alpha) : K] \leq [L' : K] < \infty$

□

14.4 Das Minimalpolynom

Sei L/K Körpererweiterung und $\alpha \in L$ algebraisch über K. Sei $d \in \mathbb{N}$ die kleinste Zahl, so dass $(\alpha^0, ..., \alpha^d)$ linear abhängig sind. Dann folgt:

$$\exists c_0, ..., c_{d-1} \in K : \alpha^d + c_{d-1}\alpha^{d-1} + ... + c_0 = 0$$

Definition: $Irr(\alpha, K) := X^d + c_{d-1}X^{d-1} + ... + c_0$ heißt Minimalpolynom von α über K wdh: $K \subset L$ oder L/K, $\alpha \in L$ heißt alagebraisch $\Leftrightarrow$ $\exists\, f \in K[T] : f(\alpha) = 0 \in L$.
Grad von L/K:

$$[L : K] := dim_K(L)$$

die anderen Elemente heißen transzendent (z.B. e eulersche Zahl, π).
Weiter hatten wir, dass α algebraisch $\Leftrightarrow [K(\alpha) : K] < \infty$
Minimalpolynom:
gegeben L/K, $\alpha \in L$ algebraisch über K. dann sei:

$$Irr(\alpha, K) := \text{ das normierte Polynom } f \neq 0 \text{ kleinsten Grades mit } f(\alpha) = 0$$

14.5 14.5 Eigenschaften des Minimalpolynoms $Irr(\alpha, K)$

Satz:

a) $Irr(\alpha, K)$ ist irreduzibel

b) $f \in K[T]\backslash\{0\},\ f(\alpha) = 0 \Rightarrow Irr(\alpha, K) | f$

c) $deg_K(\alpha) (:= [K(\alpha) : K]) = degIrr(\alpha, K) =: d$ und $1, \alpha, \alpha^2, ..., \alpha^{d-1}$ ist eine $K-$Basis von $K(\alpha)$

d) $K[T]/(Irr(\alpha, K)) \to K(\alpha),\ \ g \mapsto g(\alpha)$ ist ein Isomorphismus

Beweis:

a) $Irr(\alpha, K) = g \cdot h \Rightarrow g(\alpha) = 0$ oder $h(\alpha) = 0$

$$\overset{degIrr(\alpha,K)\ min}{\Rightarrow} deg(h) = 0 \text{ oder } deg(g) = 0$$

b),d) wie im Beweis von Satz 14.3 (2)$\Rightarrow$(3):

$$\left| \begin{array}{c} L/K, \alpha \in L,\ f \in K[T], f(\alpha) \overset{(2)}{=} 0 \\ \Rightarrow \exists L' :\ K \subset L' \subset L, [L' : K] < \infty,\ \ \alpha \in L' \end{array} \right|$$

c) $K[T]/(Irr(\alpha, K)) \simeq K(\alpha)$:

$$Irr(\alpha, K) = T^d + c_1 T^{d-1} + ... + c_d \Rightarrow \alpha^d = -(c_1\alpha^{d-1} + ... + c_d)$$

Demnach: $1, \alpha, \alpha^2, ..., \alpha^d$ erzeugt $K(\alpha)$ und sind linear unabhängig/K nach Def von $Irr(\alpha, K)$

□

Bemerkung:

- Umgekehrt tritt jedes irreduzible $f \in K[T]$ als Minimalpolynom eines Elementes $\alpha \in L$ auf, mit L/K eine Körpererweiterung, nämlich von $\alpha := T$ in $L := K[T]/_{(f)}$.
- zu c): setze $f := Irr(\alpha, K)$, dann stimmt die folgerung genau dann wenn $f(\alpha) = 0$

14.6 14.6 Multiplikativität der Grades

Satz: Für $K \subset L \subset M$ Körper gilt:

$$[M : K] = [M : L] \cdot [L : K]$$
$$H_1 < H_2 < G \Rightarrow [G : H_1] = [G : H_2] \cdot [H_2 : H_1]$$

Beweis 14.6:
$[M : K] = \infty \Leftrightarrow [M : L] = \infty$ oder $[L : K] = \infty$ $\surd$

Sei also: $\mu_1, ..., \mu_r \in M$ Basis von M als $L-$VR und

$\lambda_1, ..., \lambda_s \in L$ Basis von L als $K-$VR.

Wir zeigen:
$\mu_i\lambda_j$ ist eine Basis von M als $K-$VR, wobei $i = 1, ..., r, \quad j = 1, ..., s$

Erzeugendensystem:

$L = K \cdot \lambda_1 + ... + K \cdot \lambda_s$ und damit:

$M = L\mu_1 + ... + L\mu_r$

$= (K \cdot \lambda_1 + ... + K \cdot \lambda_s)\mu_1 + ... + (K \cdot \lambda_1 + ... + K \cdot \lambda_s)\mu_r = \sum\limits_{i,j} K\lambda_i\mu_j$

Lineare Unabhängigkeit:

$\sum\limits_{i,j} \alpha_{ij}\lambda_i\mu_j = 0$ mit $\alpha_{ij} \in K$.

Dies ist aber gerade:

$$\sum_{j=1}^{r} \left(\sum_{i=1}^{s} \alpha_{ij}\lambda_i \right) \mu_j$$

Da μ_j unabhängig/$L \Rightarrow \forall j : \sum\limits_{i=1}^{s} \alpha_{ij}\lambda_i = 0$
λ_i unabhängig/$K \Rightarrow \forall i, j : \alpha_{ij} = 0$

□

14.7 Definition:

Eine Körpererweiterung L/K heißt algebraisch, falls jedes $\alpha \in L$ algebraisch ist.

Korollar zu S.14.6 Endliche Körpererweiterungen L/K sind algebraisch und es gilt $\forall \alpha \in L$:

$$deg_K(\alpha) | [L : K]$$

Beweis:
$\alpha \in L$, dann $K \subset K(\alpha) \subset L$ und $[L : K] = [L : K(\alpha)] \cdot deg_K(\alpha)$

□

Beispiel von L/K algebraisch mit $[L : K] = \infty$:

$$K(\sqrt{2}) \subset K(\sqrt{2}, \sqrt{3}) \subset ... \subset K(...., \sqrt{p})$$

setze:

$$L = \bigcup_{p_1,...,p_r} K(\sqrt{p_1}, ..., \sqrt{p_r})$$

14.8 Satz

1) Jede endlich erzeugte, algebraische Körpererweiterung ist endlich (algebraisch wichtig, vgl. $K(T) = Quot(K[T])$ überabzählbar wenn K unendlich)

2) Für L/K Körpererweiterung ist

$$\{\alpha \in L \mid \alpha \text{ algebraisch } \} \subset L \quad \text{Unterkörper}$$

(und ist algebraische Körpererweiterung von K).

3) Seien $K \subset L \subset M$ Körper mit M/L, L/K algebraisch, so ist auch M/K algebraisch.

Beweis:

1) Für $L = K(\alpha_1, ..., \alpha_n)$ betrachte $K \subset K(\alpha_1) \subset K(\alpha_1, \alpha_2) \subset ... \subset K(\alpha_1, ..., \alpha_n) = L$
$\overset{14.6}{\Rightarrow} [L : K] = \prod_{i=1}^{n} \underbrace{deg_{K(\alpha_1,...,\alpha_n)}(\alpha_i)}_{\leq deg_K \alpha_i} < \infty$

2) z.z.: α, β algebr./$K \Rightarrow \alpha - \beta, \quad \alpha\beta^{-1}$ algebraisch/K korrekt, denn:

$$\alpha - \beta, \alpha\beta^{-1} \in [K(\alpha, \beta) : K] = \underbrace{[K(\alpha, \beta) : K(\alpha)]}_{=deg_{K(\alpha)}\beta \leq deg_K \beta < \infty} \cdot \underbrace{[K(\alpha) : K]}_{<\infty} < \infty$$

3) Sei $\alpha \in M$. z.z. α ist algeb/K:
M/L algeb. $\Rightarrow \exists\ f = \sum_{i=0}^{d} \beta_i X^i, \quad \beta_i \in L : \quad f(\alpha) = 0 \in M$
Insbesondere ist α auch algebraisch über $K(\beta_0, ..., \beta_d, d)$
Fertig mit Korollar 14.7, denn $K(\alpha) \subset K(\beta_0, ..., \beta_d, d)$

□

Turm endlicher Körpererweiterung

Anwendung von (2)**:**
$\overline{\mathbb{Q}} := \{c \in \mathbb{C} \mid \alpha \text{ algebraisch}/\mathbb{Q}\}$ ist eine algebraische Körpererweiterung von $\mathbb{Q}$.
$\overline{\mathbb{Q}}$ heißt algebraischer Abschluss von $\mathbb{Q}$.

15 15 Konstruktion mit Zirkel und Lineal

Dieses Kapitel hängen wir hinten an.
Es behandelt u.a. Quadratische Körpererweiterung

16 16 Endliche Körper

Ziel: zu jeder Primzahlpotenz $q = p^r$ existiert ein bis auf Isomorphie eindeutiger Körper mit q Elementen.
Notation: $\mathbb{F}_q$ oder $GF(q)$ ("Galois field")
Wir kennen schon: $\mathbb{F}_p = (\mathbb{Z}/_p, +, \cdot)$

16.1 Sei $K^x = (K\backslash\{0\}, \cdot)$

Satz: Für einen beliebigen Körper K ist jede endliche Untergruppe $G \subset K^x$ zyklisch.
Beweis:
Wäre G nicht zyklisch, dann gäbe es ein $n < |G|$ mit $a^n = 1$ für alle $a \in G$. (siehe Struktursatz endlicher abelscher Gruppen, setze $n = d_r$)
$\Rightarrow a \in G$ ist Nullstelle von $X^n - 1$. aber $X^n - 1$ hat aber höchstens n Nullstellen, also Widerspruch

$$\prod_{a \in G} (X - a) | X^n - 1$$

16.2 Satz

Sei K ein endlicher Körper , $char(K) = p$. dann gilt:

1) $q = \#K$ ist eine Primpotenz

2) $K^x \simeq \mathbb{Z}/_{(q-1)}$

3) $\forall a \in K\backslash\{0\} : a^{q-1} = 1$ ($K = \mathbb{F}_p$: kleiner Fermat)

Bemerkung:

1. K ist ein $\mathbb{F}_p-$VR $\Rightarrow K \simeq \mathbb{F}_p^r \Rightarrow \#K = p^r$
2. $\#K = q - 1$ udn K^x zyklisch nach Satz 16.1
3. $ord_{K^x} a || K^x| = q - 1$

Wiederholung:
$G \subset K^x$, G endlich $\Rightarrow G$ zyklisch
$|K| = q = p^r, \alpha \in K$, $\alpha^{q-1} = 1 \Rightarrow \alpha$ ist Nullstelle von $X^\alpha - X$

16.3 Satz

Für jede Primzahlpotenz $q = p^r$ existiert ein bis auf Isomorphie eindeutiger Körper mit q Elementen.
Beweis:

Schritt 1: Es existiert eine Körpererweiterung $L/\mathbb{F}_q$, in der $X^q - X$ in Linearfaktoren zerfällt:

$$X^q - X = \prod_{i=1}^{q}(X - \alpha_i) \quad \alpha_i \in L \text{ in } L[X]$$

(Satz 16.4)

Schritt 2: $K := \{\alpha_1, ..., \alpha_q\} \subset L$ ist ein Körper, denn K ist die Fixpunktmenge des Körperautomorphismus

$$\Phi : L \to L \quad x \mapsto x^q$$

(hier muss gelten: $(x + y)^q \stackrel{!}{=} x^q + y^q$, da $char(L) = p$, $p \mid q$

Schritt 3: $\#K = q$, denn $\forall i \neq j : \ \alpha_i \neq \alpha_j$ (Lemma 16.5)
$\Rightarrow$ Existenz $\surd$

Schritt 4: Eindeutigkeit: Sei K' gegeben mit $\#K' = q$.
Ist $\alpha \in K\backslash\{0\}$ Erzeuger von $(K')^x$ Satz (16.2), so gilt:

$$K' = \mathbb{F}_p(\alpha) \qquad (\text{denn } 1, \alpha, \alpha^2, ..., \alpha^{q-1} \in \mathbb{F}_p(\alpha))$$

und $P = Irr(\mathbb{F}_p, \alpha)$ ist ein $\mathbb{F}_p-$irreduzibler Faktor von $X^q - X$ vom Grad r.
(r ist der maximal mögliche Grad eines $\mathbb{F}_p-$irreduziblen Faktors von $X^q - X$, siehe 16.7)

$\Rightarrow \mathbb{F}_p(\alpha) = K \simeq \mathbb{F}_p[X]/(P')$ für einen (jeden) $\mathbb{F}_p-$irreduziblen Faktor P von $X^q - X$ mit $deg(P) = r$.

Dies zeigt zunächst, dass $\mathbb{F}_p[X]/(P) \simeq \mathbb{F}_p[X]/(P')$ für verschiedene $\mathbb{F}_p-$irred. Faktoren P, P' von $X^q - X$.

$$\mathbb{F}_p[X]/(P) \to \mathbb{F}_p[X]/(P'), \quad X \mapsto X^s, \quad 1 \leq s < r$$

Demnach gilt auch $K \simeq K'$ für jedes K, K' mit $\#K = \#K' = q$.

□

Bemerkung: der Beweis war in der Vorlesung nicht ganz klar, also gut reflektieren!

16.4 Zerfällung

Wir haben im Beweis benutzt:

Satz: Zerfällung von Polynomen in Körpererweiterungen
Zu $P \in K[X]$, K Körper, gibt es eine endliche Körpererweiterung

$$\iota : K \to L \quad (\tilde{\iota} : K[X] \to L[X] \text{ die induzierte Abbildung})$$

so dass $\tilde{\iota}(P) \in L[X]$ in Linearfaktoren zerfällt.
Beweis:
Mit Induktion nach $\deg(P)$ reicht es L so zu Konstruieren, dass $\tilde{\iota}(P)$ eine Nullstelle hat.
o.E. sei P irreduzibel, sonst fertig mit Induktionsvoraussetzung angewendet auf einen irreduziblen Faktor.

$$L := K[X]/(P), \quad \iota : K \hookrightarrow L$$

Zur Klarheit ersetze die freie Variable X in $K[X]$ durch T, und schreibe $\alpha := \overline{X}$ (Restklasse von X in $K[X]/(P)$).
ι induziert $\tilde{\iota} : K[T] \hookrightarrow L[T]$.
$\tilde{\iota}(P(T)) = \iota(a_n)T^n + ... + \iota(a_0) \in L[T]$, wobei $P = a_nX^n + ... + a_0$ mit $a_i \in K$.

$$\tilde{\iota}(P(T))(\alpha) = \underbrace{\iota(a_n)\overline{X}^n + ... + \iota(a_0)}_{\in L} = \text{Restklasse von } P \text{ in } L = K[X]/(P)$$
$$= 0$$

□

16.5 Lemma:

In jeder Körpererweiterung $L/\mathbb{F}_p$ hat $X^q - X$ nur einfache Nullstellen, wobei $q = p^r$ für ein r.
Beweis:
Für $\alpha \in L$ Nullstelle von $X^q - X$ gilt $\alpha^q - \alpha = 0$, und damit:

$$X^q - X = (X^q - \alpha^q) - (X - \alpha) \overset{charL=p, p|q}{=} (X-\alpha)^q - (X-\alpha) = (X-\alpha)(\underbrace{(X-\alpha)^{q-1} - 1}_{\text{hat keine NST in } \alpha})$$

□

16.6 Praktischer Umgang mit $\mathbb{F}_q$

$q = p^r$. Finde $\mathbb{F}_p$ irreduziblen Teiler von $X^q - X$, von maximalem Grad r. Dann gilt $\mathbb{F}_q \simeq \mathbb{F}_p[X]/(P)$ und $\alpha := \overline{X}$ ist ein Erzeuger vom $\mathbb{F}_q^x$ (Satz 16.7,3)

Beispiel: Betrachte das Polynom:

$$X^8 - X = X(X-1)(X^3 + X + 1)(X^3 + X^2 + 1)$$

Wähle $P := X^3 + X + 1$ (alternativ $P = X^3 + X^2 + 1$). In $K := \mathbb{F}_2[X]/(X^3 + X + 1) \simeq \mathbb{F}_8$ gilt:

$$\alpha^3 = \alpha + 1 (\Leftrightarrow \alpha^3 + \alpha + 1 = 0)$$

Die Elemente von $\mathbb{F}_8$:

exponentielle Schreibweise ($\leftrightarrow \mathbb{F}_8^x =< \alpha >$)	oder polynomiale Schreibweise: ($\mathbb{F}_8$ als $\mathbb{F}_2-$VR mit Basis $1, \alpha, \alpha^2$)
0	0
$1 = \alpha^0$	1
α^1	α
α^2	α^2
α^3	$\alpha + 1$
α^4	$\alpha^2 + \alpha$
α^5	$\alpha^3 + \alpha^2 = \alpha^2 + \alpha + 1$
α^6	$\alpha^2 + 1$
α^7	$\alpha^3 + \alpha = 1$

Zerlegung von $X^8 - X$ in Linearfaktoren, als Polynom über $\mathbb{F}_8$:

$X^3 + X + 1 = (X - \alpha)(X - \alpha^2)(X - \alpha^4)$
$X^3 + X^2 + 1 = (X - \alpha^3)(X - \alpha^6)(X - \alpha^{12})$ stimmt hier X^2?

Bedenke $\mathbb{F}_8^x \simeq \mathbb{Z}/_7$ und $\alpha^{12} = \alpha^5$

Beobachtung:
Die $\mathbb{F}_8-$irred. Faktoren von X^8-X stehen in Bijektion zu den Bahnen des Frobenius-Automorphismus

$$F : \mathbb{F}_8 \to \mathbb{F}_8, \quad a \mapsto a^2$$

Bahnen:
$\{0\}, \{1\}, \{\alpha, \alpha^2, \alpha^4\}, \{\alpha^3, \alpha^6, \alpha^5\}$

16.7 Allgemein: Automorphismen von $\mathbb{F}_p$ und $\mathbb{F}_p-$irred. Faktoren von $X^q - X$

Notation: $q = p^r$
$F : \mathbb{F}_q \to \mathbb{F}_p$, $a \mapsto a^p$ der Frobeniusautomorphismus.
$Aut(\mathbb{F}_q) = \{\Phi : \mathbb{F}_q \to \mathbb{F}_q$ Isom. von Körpern$\}$

Satz:

1) $\mathbb{F}_p = \mathbb{F}_q^{Aut(\mathbb{F}_q)} = \{a \in \mathbb{F}_q \mid a^p = a\}$

2) $Aut(\mathbb{F}_q) =< F >\simeq \mathbb{Z}/_r$ ($< F >$ von F erzeugte Untergruppe)

3) Jeder Erzeuger $\alpha \in \mathbb{F}_q^x$ ist eine Nullstelle eines $\mathbb{F}_p-$irreduziblen Polynoms von Grad r (und umgekehrt).

4) Jeder $\mathbb{F}_p-$irreduzible normierte Teiler von $X^q - X$ hat die Form:

$$\prod_{i=0}^{s-1}(X - F^j(\alpha)) = \prod_{i=0}^{s-1}(X - \alpha^{p^j})$$

für $\alpha \in \mathbb{F}_q$ mit $s = min\{j \mid F^j(\alpha) = \alpha\}$.
Ferner gilt $s|r$.

5) $X^q - X$ ist das Produkt aller $\mathbb{F}_p-$irred., normierten Polynome, deren Grad r teilt.

Nachtrag zu 16.3 (Beweis der Eindeutigkeit):
K Körper mit $\#K = q = p^r$ ($\Rightarrow K^x \simeq \mathbb{Z}/_{q-1}$)
Wir hatten gesehen:
$\forall \alpha \in K,\ K^x =< \alpha >:\ Irr(\mathbb{F}_p, \alpha) \mid X^q - X$, da $deg(\mathbb{F}_q) = r$
und damit :

$$\forall \alpha \in K,\ K^x =< \alpha >: K \simeq \mathbb{F}_p[X]/_{Irr(\mathbb{F}_p, \alpha)}$$

Ferner $X^q - X = \prod_{\alpha_i \in K} (X - \alpha_i)$.

Umgekehrt: $g \mid X^q - X$, g normiert. $\Rightarrow \exists \alpha_{i_1}, ..., \alpha_{i_s} : g = \prod_{\mu=1}^{s} (X - \alpha_{i_\mu})$

K $\xleftarrow{\varphi}$ $\mathbb{F}_p[X]/(g)$ mit $x \mapsto \alpha_{i_1}$. gilt $deg = r \Rightarrow \varphi$ ist Isomorphismus.
Seien g_1, g_2 Teiler mit $deg(g_i) = r \Rightarrow \mathbb{F}_p[X]/(g_1) \simeq K \simeq \mathbb{F}_p[X]/(g_2)$
und $\psi : \mathbb{F}_p[X]/(g_2) \to \mathbb{F}_p[X]/(g_1)$ □

Bemerkung: ψ explizit: $g_2 \leftrightarrow \alpha$, $g_1 \leftrightarrow \alpha^l$
$\mathbb{F}_p[X]/(g_2) \to \mathbb{F}_p[X]/(g_1)$, $X \mapsto X^l$
Dies ist Wohldefiniert!

Beweis (zu 16):

1) Sei $\Phi \in Aut(\mathbb{F}_q) \Rightarrow \Phi(1) = 1 \Rightarrow \Phi|_{\mathbb{F}_p} = Id_{\mathbb{F}_p}$

   Dies Zeigt: $\mathbb{F}_p \subset \mathbb{F}_q^{Aut(\mathbb{F}_q)}$

   Umgekehrt: $a \in \mathbb{F}_q^{Aut(\mathbb{F}_q)} \Rightarrow a^p = F(a) = a \qquad (F \text{ Frobenius})$

   $\Rightarrow a$ ist Nullstelle von $X^p - X = \prod_{\lambda \in \mathbb{F}_p} (X - \lambda)$

   $\Rightarrow a \in \mathbb{F}_p$.

4) Sei P ein $\mathbb{F}_p$ irred., normierter Teiler von $X^q - X$. $X^q - X$ zerfällt über $\mathbb{F}_q$ in Linearfaktoren (Satz 16.3 Schritt 1)
   $\Rightarrow P$ zerfällt über $\mathbb{F}_q$ in Linearfaktoren .
   Sei $\alpha \in \mathbb{F}_q$ eine NST von P. Da $F|\mathbb{F}_p = id$ gilt: $F(P) = P$ und damit:

$$\forall j: \ P(F^j(\alpha)) = F^j(P(\alpha)) = 0$$

   Sei $\alpha_1, ..., \alpha_s$ die Bahn der Frobeniuswirkung durch α, d.h.

$$\alpha_1 = \alpha, \ \alpha_2 = F(\alpha), ..., \ \alpha_{i+1} = F(\alpha_i) = \alpha_i^p, ..., \ \alpha_s^p = \alpha_1$$

   Dann ist:

$$Q := \prod_{i=1}^{s} (X - \alpha_i) \in \mathbb{F}_q[X]$$

   wendet man F an erhält man:

$$F(Q) = Q \Rightarrow Q \in \mathbb{F}_p[X]$$

   $Q|P, \quad Q, P$ normiert, P irred $\Rightarrow Q = P$
   Ferner gilt: $\alpha^{p^s} = \alpha \Rightarrow \exists t : q = (p^s)^t = p^{st} \Rightarrow a \mid r$

5 Die Invarianz unter F zeigt auch, dass für jede $F-$Bahn $\alpha_1, ..., \alpha_s$ in $\mathbb{F}_q$ das Polynom

$$Q = \prod_{i=1}^{s} (X - \alpha_i)$$

   Koeffizienten in $\mathbb{F}_q$ hat und irreduzibel über $\mathbb{F}_p$ ist.
   Sei umgekehrt $P \in \mathbb{F}_p[X]$ irreduzibel, $s = deg(P) \mid r$, dann folgt:

$$\mathbb{F}_p[X]/_{(P)} \simeq \mathbb{F}_{p^s} \simeq \{a \in \mathbb{F}_q \mid a^{p^s = a}\} \subset \mathbb{F}_q$$

   $\Rightarrow P$ zerfällt in $\mathbb{F}_q$ in Linearfaktoren, $\Rightarrow P \mid X^q - X$.

3 Siehe Satz 16.3 Nachtrag

2 Sei $\Phi \in Aut(\mathbb{F}_q)$. Seien $\alpha \in \mathbb{F}_q^x$ ein Erzeuger und $P = Irr(\mathbb{F}_p, \alpha)$ mit $deg = r$.
   $\Rightarrow \exists s : \Phi(\alpha) = F^s(\alpha)$, denn $P(\Phi(\alpha)) = \Phi(P(\alpha)) = 0$ und jede NST von P ist von der Form $F^s(\Phi(\alpha))$ (nach 4))
   $\Rightarrow \forall n : \Phi(\alpha^n) = \Phi(\alpha)^n = (F^s(\alpha))^n = F^s(\alpha^n)$
   $\Rightarrow \Phi = F^s$

□

16.8 16.8 Galoiskorrespondenz für endliche Körper

Korollar: Sei $q = p^r$. Dann ist
$\{$Undergruppen von $Aut(\mathbb{F}_q) \simeq \mathbb{Z}/_r\} \to \{$ Zwischenkörper $K\mathbb{F}_p \subset K \subset \mathbb{F}_q$
1:1$\updownarrow$
$\{$Teiler s von $r\}$
$< F^s >= H \mapsto \mathbb{F}_q^H = \{a \in \mathbb{F}_q \mid a^{p^s} = a\}$ ist Bijektiv.
Beweis:
surjektiv: $[\mathbb{F}_p : K] = t \Rightarrow K \simeq \mathbb{F}_{p^s}, \quad s = r/t. \Rightarrow \forall a \in K: \ a^{p^s} = a$
$\Rightarrow K = \mathbb{F}_q^H, H =< F^s > \simeq \mathbb{Z}/_5$
injektiv: $s < s \Rightarrow \exists a \in \mathbb{F}_q : a^{p^{s'}} = a$ aber $a^{p^s} \neq a$

□

Beispiel:

17 17. Zerfällungskörper - normale Körpererweiterungen

17.1 Definition: Zerfällungskörper

Sei K ein Körper und $P \in K[X]$ (nicht notwendiger weise irreduzibel!)
Ein Zerfällungskörper von P ist eine Körpererweiterung L/K mit:

(1) P zerfällt über L in Linearfaktoren:

$$P = a_0 \cdot \prod_{i=1}^{d} (X - \alpha_i) \quad \alpha_i \in L$$

(2) $L = K(\alpha_1, ..., \alpha_d)$

Bemerkung: Zerfällungskörper existieren (nach Satz 16.4)

17.2 Beispiel:

1) $\mathbb{C}$ ist ein Zerfällungskörper von $X^2 + 1 \in \mathbb{R}[X]$

2) $\mathbb{Q}(\sqrt[3]{2})$ ist nicht Zerfällungskörper von $X^2 - 2 = Irr(\mathbb{Q}, \sqrt[3]{2}) \in \mathbb{Q}[X]$, denn $(X^3 - 2)/_{(X - \sqrt[3]{2})}$ zerfällt nicht in Linearfaktoren über $\mathbb{Q}(\sqrt[3]{2})$
Bemerkung: Die anderen Nullstellen liegen in $\mathbb{C} \backslash \mathbb{R}$

17.3 Eindeutigkeit von Zerfällungskörpern

Satz: Sei K ein Körper und seinen L/K und L'/K Zerfällungskörper von einem Polynom $P \in K[X]$, dann gibt es einen Isomorphismus

$$\Phi : L \to L' \text{ mit } \Phi \mid_K = Id$$

Beweis:
Nach Vorbereitungen in 17.6

Bemerkung: es ist jetzt zwar gerechtfertigt von dem Zerfällungskörper zu reden, aber der Isomorphismus Φ ist nur eindeutig bis auf Komposition mit $Aut(L/K) = \{\psi : L \to L \mid \psi \mid_K = Id\}$.
Beispiel:

17.4 17.4 Faktorisierung von Körpererweiterungen

Motivation: Wollen $K(\alpha_i)$ und $K(\alpha_j)$ aus 17.1 vergleichen.

Satz: Seien M/K und L/K Körpererweiterungen und sei $\alpha \in L$ ein primitives algebraisches (über K) Element von L, d.h.:
$L = K(\alpha), deg_k(\alpha) < \infty$. Dann gibt es eine kanonische Bijektion

$$Hom_k(L, M) \overset{1:1}{\leftrightarrow} \{\tilde{\alpha} \in M \mid \tilde{\alpha} \text{ ist NST von } Irr(\alpha, K)\}$$

$$\Phi : (\varphi : L \to M) \mapsto \varphi(\alpha)$$
$$(g(\alpha) \mapsto g(\tilde{\alpha})) \leftarrow \tilde{\alpha} : \Psi \text{ mit } g \in K[X]$$

Notation:
$Hom_k(L, M) := \{\varphi : L \to M \mid \varphi \text{ Hom}, \varphi|_K = Id\}$
Beweis:

$\underline{\Psi \text{ ist wohldefiniert:}}$ Sei $g(\alpha) = g'(\alpha) \Rightarrow \alpha$ ist NST von $g' - g$
$\Rightarrow Irr(\alpha, K) \mid g' - g$ in $K[X]$
$\Rightarrow (g' - g)(\tilde{a}) = 0$
$\Rightarrow g'(\tilde{a}) = g(\tilde{\alpha})$. ersetze in letztem Bild $K(\alpha)$ mit $K[X]$.

$\underline{\Psi \circ \Phi = Id_{Hom_k(L,M)}:}$ φ ist der eindeutige Hom. $L \to M$ mit $\alpha \mapsto \varphi(\alpha)$ $(L = K(\alpha)!)$

$$\Psi(\Phi(\varphi)) = \Psi(\varphi(\alpha)) \text{ tut dies auch}$$

$\Rightarrow \Psi(\Phi(\varphi)) = \varphi$

$\underline{\Phi \circ \Psi = Id_{\tilde{a}}:}$ $\Phi(\Psi(\tilde{\alpha}))0\tilde{\alpha}$

□

Beispiel: Körperautomorphismen von $\mathbb{F}_q = \mathbb{F}_p(\alpha) = \mathbb{F}_p[X]/_{(Irr(\alpha,\mathbb{F}_p))}$ $\mathbb{F}_p-$irred. Teiler P von $X^q - X$, $deg = r, q = p^r$
$\alpha, \alpha^p, ..., \alpha^{p^{r-1}}$ sind genau die NSt von $(Irr(\alpha, \mathbb{F}_p))$. $(L = M = \mathbb{F}_q)$

17.5 17.5 Korollar1 (Existenz von Körpereinbettungen)

Sei L/K und M/K Körpererweiterungen, und $[L : K] < \infty$. Existieren dann $\alpha_1, ..., \alpha_r \in L$ s.d. $Irr(\alpha_i, K)$ über M in Linearfaktoren zerfallen, so existiert eine Einbettung

$$\varphi : L \to M, \quad \text{mit } \varphi \mid_K = Id_K$$

Beweis:
Betrachte "den Körperturm" $L = K(\alpha_1, ..., \alpha_r) \supset \alpha_1, ..., \alpha_{r-1} \supset ... \supset K(\alpha_1) \supset K$ und die Abbildungen $\varphi_i : K(\alpha_1, ..., \alpha_i) \to M$.
Betrachte $\beta \in K(\alpha_1, ..., \alpha_i)$, dann teilt:

$$Irr(\beta, K(\alpha_1, ..., \alpha_{i-1}) \mid Irr(\beta, K) \quad \text{in } K(\alpha_1, ..., \alpha_{i-1})[X]$$

Insbesondere für $\beta = \alpha_i$.
Nach 17.4 gilt dann:

$$Hom_{K(\alpha_1,...,\alpha_{i-1})}(K(\alpha_1, ..., \alpha_i), M) \neq \emptyset$$

da $Hom_{K(\alpha_1,...,\alpha_{i-1})}(K(\alpha_1, ..., \alpha_i), M) \subset Hom_K(K(\alpha_1, ..., \alpha_i), M)$

□

17.6 (17.6) Beweis von 17.3

Haben
Nach Korollar 17.5 folgt es existiert ein $\varphi : L \to L', \psi : L' \to L$. Sind beides injektive Abb. endlich dimensionaler K-VR's $\Rightarrow \varphi, \psi$ sind Körperautomorphismen.

□

17.7 (17.7) Bemerkung:

Korollar 1 und sein Beweis lehren auch:

Korollar 2: (Anzahl der Faktorisierungen) Für L/K eine endliche und M/K eine beliebige Körpererweiterung gilt:

$$\#Hom_K(L, M) \leq [L : K] \quad (*)$$

Beweis.
Durch Induktion nach der Anzahl der Erzeuger von L/K (beide Seiten von $(*)$ verhalten sich multiplikativ unter der Körpererw.) dürfen wir $L = K(\alpha)$ annehmen.
Dann folgt nach 17.4, dass $\#Ham_K(K(\alpha), M) = \#$NST'en von $Irr(\alpha, K)$ in $M \leq deg(Irr(\alpha, K)) = [K(\alpha) : K]$.

□

17.8 17.8 Normale Körpererweiterungen

Definition: Eine Körpererweiterung L/K heißt normal, wenn sie algebraisch ist und wenn für jedes irreduzible $P \in K[X]$ gilt: ¶ hat eine NST in $L \Rightarrow P$ zerfällt in $L[X]$ in Linearfaktoren.

Beispiel:
$\mathbb{Q}(\sqrt{2})$ ist normal (siehe 17.9), aber $\mathbb{Q}(\sqrt[3]{2})$ ist nicht normal:
$P = X^3 - 2$ hat in $\mathbb{Q}(\sqrt[3]{2})$ eine Nullstelle, die anderen beiden NST'en liegen jedoch in $\mathbb{C}\backslash\mathbb{R} \subset \mathbb{C}\backslash\mathbb{Q}(\sqrt[3]{2})$. (siehe auch Bsp. 17.2)

17.9 17.9 Charakterisierung endlicher, normaler Erweiterungen

Satz: Für eine endliche Körpererweiterung sind äquivalent:

1) L/K ist normal

2) L/K ist Zerfällungskörper eines Polynoms

3) Sind $\varphi, \psi : L \to M$ zwei Einbettungen über $K(\varphi, \psi \in Hom_K(L, M))$ in eine Körpererweiterung M/K , so gilt dass die Bilder gleich sind, also

$$\varphi(L) = \psi(L)$$

Beispiel zu (3): $\varphi : \sqrt[3]{2} \mapsto \sqrt[3]{2}$
$\psi : \sqrt[3]{2} \mapsto \zeta \cdot \sqrt[3]{2}$, $\zeta = e^{\frac{2\pi i}{3}}$
und $\zeta \cdot \sqrt[3]{2} = \tilde{\alpha}$ ist NST von $Irr(\sqrt[3]{2}, \mathbb{Q}) = X^3 - 2$
also $\varphi(L) \neq \psi(L)$.

Beweis von 17.9

(1)⇒(2) $L = K(\alpha_1, ..., \alpha_r), L$ normal $\Rightarrow L$ ist Zerfällungskörper von $\prod_{i=1}^{r} Irr(\alpha_i, K)$

(2)⇒(3) $\varphi(L), \psi(L) \subset M$ werden erzeugt über K von den Nullstellen von P in M.
$\Rightarrow \varphi(L) = \psi(L)$.

(3)⇒(1) Sei $L = K(\alpha_1, ..., \alpha_r)$ und $P \in K[X]$ irreduzibel habe eine NST $\beta \in L$.
(ist P normiert $\Rightarrow P = Irr(\beta, K)$)
Sei M/L so, dass $Irr(\alpha_i, K)$ und $Irr(\beta, K)$ in Linearfaktoren zerfällt für $i = 1, ..., r$.
Wir zeigen: Für jede Nullstelle $\beta' \in M$ von P gibt es $\varphi \in Hom_K(L, M)$ mit $\beta' \in \varphi(L)$. (**)
Dann folgt: (3) $\Rightarrow \forall \varphi \in Hom_K(L, M) : \varphi(L) = L \subset M$ also insbesondere $\beta' \in L$ Beweis von (**): mit Satz 17.4 sehen wir $\exists$ Hom. $K(\beta) \to M, \quad \beta \mapsto \beta'$.
Nach Satz 17.5 lässt sich erweitern zu $L = K(\alpha_1, ..., \alpha_r) \to M$. mit $K(\beta) \subset K(\alpha_1, ..., \alpha_r)$ folgt die Aussage.

□

17.10 17.10 Komposition normaler Erweiterungen

Satz: Sind $L/K, L'/K$ normale (endliche) Körpererweiterungen, so gibt es einen bis auf Isomorphie eindeutige Oberkörper M von L, L' mit:

$$M = LL' = \{ \sum_{\text{endlich}} a_i b_i \mid a_i \in L, b_i \in L' \}$$

Ferner respektiert jeder solche Isomorphismus die Inklusionen $L \cap L' \subset M$ und $M/K, (L \cap L')/K$ sind normal Beweis:
L sei der Zerfällungskörper von $P \in K[X]$ und L' der von $P' \in K[X]$ (P, P' sind nicht eindeutig! dies ist aber irrelevant)
Existenz:
Setze $M :=$ Zerfällungskörper von PP'

Eindeutigkeit und Normalität:
(Satz 17.9,(3)) Seien $\psi_1, \psi_2 : M \to N$ Einbettungen über K und $= LL'$, dann gilt:
$\psi_1(L) = \psi_2(L)$ und $\psi_1(L') = \psi_2(L')$ (da $L/K, L'/K$ normal).
$\Rightarrow \psi_1(M) = \psi_1(LL') = \psi_1(L)\psi_1(L') == \psi_2(L)\psi_2(L') = \psi_2(LL') = \psi_2(M)$.
$\overset{17.9,(3)}{\Rightarrow} M/K$ ist normal.
Wenn $N == \psi_1(L)\psi_1(L')$ wende diese Argumente an, das gibt die Eindeutigkeit.
$(L \cap L')/K$ normal nach Definition von Normalität.

□

Bemerkung: Der Satz ist auch richtig für unendliche Erweiterungen, wir zeigen aber ihn aber nur für endliche.

17.11 17.11 Bemerkung

a) Sein M/L und L/K normal, so braucht M/K nicht normal zu sein.
Bsp.: $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2})$

b) Umgekehrt gilt aber: $K \subset L \subset M$ und M/K normal, dann ist M/L auch normal.
Beweis:
Jede Einbettung $\varphi : M \to N$ über L ist auch eine Einbettung über $K \overset{M/K \text{ normal}}{\Rightarrow} \varphi(M) \subset N$ eindeutig.

18 18. Galoiserweiterungen

Wir verallgemeinern nun das bei endlichen Körpern beobachtete Bild und betrachten Körpererweiterungen L/K, so dass $G \subset Aut(L)$ Untergruppe existiert mit:

- $K = L^G$
- $|G| = [L : K]$
- $\forall \alpha \in L$ operiert G transitiv auf den NST'en von $Irr(\alpha, K)$ $\left(= \prod_{\beta \in G.\alpha} (X - \beta) \right)$

18.1 Definition:

Für L/K eine Körpererweiterung heißt :

$$Aut(L/K) := \{\Phi \in Aut(L) \mid \Phi|_K = Id_k\}$$

Automorphismengruppe (oder Galoisgruppe) von L über K.
Alternativ: $(Aut_K(L), Gal(L/K), G(L/K)$

Beispiel: $q = p^s, r \geq 1$, dann ist $Aut(\mathbb{F}_{q^r}/\mathbb{F}_q) \simeq \mathbb{Z}/_r$ erzeugt von $F^s : \mathbb{F}_{q^r} \to \mathbb{F}_{q^r}, \quad a \mapsto a^q$

18.2 18.2 Bemerkung;

Korollar 17.7 über die Anzahl der Einbettungen $L \to M$ mit $M = L$ zeigt:

$$|Aut(L/K)| \leq [L : K]$$

18.3 Satz/ Definition:

Eine endliche Körpererweiterung L/K heißt Galoisch (oder Galoiserweiterung) mit der Galoisgruppe

$$G := Aut(L/K)$$

falls eine der drei folgenden, äquivalenten Bedingungen gilt:

1. $K = L^G$
2. $|G| = [L : K]$
3. $\forall \alpha \in L$ zerfällt $Irr(\alpha, K)$ in L in paarweise verschiedene Linearfaktoren (" L/K seperabel")

Beweis:

(2) $\Rightarrow$ (1): $|G| = [L : K] \overset{(*)}{\geq} [L : L^G] \overset{18.2}{\geq} |G| \Rightarrow K = L^G$
((*) betrachte Körperturm: $L - L^G - K$).

(1) $\Rightarrow$ (3): $f := \prod_{\beta \in G.\alpha} (X - \beta)$ ist $G-$invariant $\Rightarrow f \in L^G[X]$. Mit (1) $\Rightarrow K = L^G$ folgt dann $f \in K[X]$
Ferner $f(\alpha) = 0 \Rightarrow Irr(\alpha, K) \mid f$ und da f normiert, irreduzibel folgt $f = Irr(\alpha, K)$
$\Rightarrow Irr(\alpha, K)$ zerfällt in paarw. verschiedene Linearfaktoren. (3) $\Rightarrow$ (2) am Dienstag.

Verbesserugn von Satz 16.7 (3)
$\mathbb{F}_q$ gegeben mit $q = p^r | F_q^x =< \alpha > \Rightarrow \alpha$ ist Nullstelle eines $\mathbb{F}_q-$irred. Polynoms vom grad r.
Dies gilt aber nicht umgekehrt!:
Beispiel:
$q = 9 (p = 3, r = 2)$
$\mathbb{F}_3-$irreduzible Polynome von grad 2:

$$f = X^2 + 1,\ X^2 + X - 1,\ X^2 - X - 1$$

$\mathbb{F}_q = \mathbb{F}_3[X]/_{(f)}, \mathbb{F}_3 = \{-1, 0, 1\}$

$\underline{f = X^2 + 1:}$ $\alpha = X,\ X^2 = -1, -X, -X^2$
also ist:

$$ord_{\mathbb{F}_9^x} = 4$$

$\underline{f = X^2 - X - 1:}$

$$\alpha = X,\ X^2 = X + 1, X^3 = X^2 + X = -X + 1, -X^2 + X = -1, -X, -X - 1, -X^2 - X, 1$$

also ist:

$$ord_{\mathbb{F}_9^x = 8}$$

Erklärung:
F-Bahnen, $F : a \mapsto a^3$
$\{1\}, \{\alpha, \alpha^3\}, \{\alpha^2, \alpha^6\}, \{\alpha^4\}, \{\alpha^5, \alpha^7\}$ und es gilt: $\alpha = \alpha^9, +\alpha^2 = \alpha^{18}$
Dann gilt: $\{\alpha^5, \alpha^7\}, \{\alpha, \alpha^3\}$ erzeugen $\mathbb{F}_9^x$
aber $\{\alpha^2, \alpha^6\}$ erzeugt nicht $\mathbb{F}_9^x$

$$\mathbb{Z}/_d :< m >\simeq \mathbb{Z}/_d \Leftrightarrow ggT(m, d) = 1$$

$X^2 + 1 \Leftrightarrow \{\alpha^2, \alpha^6\}$

In 16.6: Wähle solche f, die zu $f-$Bahnen gehören, die aus Erzeugern von $\mathbb{F}_q^x$ bestehen.
$\Rightarrow \mathbb{F}_q = \mathbb{F}_p[X]/_{(f)}$, dann in der Tat:

$$\mathbb{F}_q^x =< x >$$

18.4 18.7

Es sei $L =$ Zerfällungskörper von $X^4 - 2 \in \mathbb{Q}[X]$. $G = Aut(L/K), \alpha = \sqrt[4]{2}$.
Betrachte den Automorphismus:

$$\tau : z \mapsto \bar{z},\quad \alpha \mapsto \alpha, ,\ i \mapsto -i$$

$\mathbb{Q}(\alpha) = L^{<\tau>}$
$L/\mathbb{Q}$ Galoisch $\overset{\text{Bem}}{\Rightarrow} L/\mathbb{Q}(i)$ Galoisch , $[L:\mathbb{Q}(i)] = 4$
$\Rightarrow \exists \sigma \in Aut(L/K) : \sigma(\alpha) = i\alpha$, dann ist:

$$\sigma : \left.\begin{array}{c} \alpha \mapsto i\alpha \\ i\alpha \mapsto -\alpha \\ -\alpha \mapsto -i\alpha \\ -i\alpha \mapsto \alpha \end{array}\right\} \Rightarrow ord(\sigma) = 4 \Rightarrow Aut(L/\mathbb{Q}(i)) =< \sigma >$$

$\tau \notin < \sigma > \Rightarrow < \tau > \cap < \sigma >= \{e\} \subset G \Rightarrow G =< \tau, \sigma >$
Es gilt:

$$\tau\sigma = \sigma^{-1}\tau$$

$\Rightarrow G$ ist semidirektes Produkt: $G \simeq D_4$

$$0 \to \mathbb{Z}/_4 \to G \to \mathbb{Z}/_2 \to 0$$

und $G \lhd \mathbb{Z}/_4 \leftrightarrow L/\mathbb{Q}(i)$ Galoisch

$$G = \{e, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau\}$$

Untergruppen:
Körper:
davon normale Untergruppen:
alle vom Index 2:

$$< \sigma^2\tau > \leftrightarrow \mathbb{Q}(\alpha^2)/\mathbb{Q} \text{ Galoisch}$$
$$< \sigma > \leftrightarrow \mathbb{Q}(i)/\mathbb{Q} \text{ Galoisch}$$
$$< \sigma^2, \sigma\tau > \leftrightarrow \mathbb{Q}(i\alpha^2)$$
$$< \sigma^2 > \text{ ist normal: } \tau\sigma^2\tau^{-1} = \sigma^{-2}\tau\tau^{-1} = \sigma^2 \leftrightarrow \mathbb{Q}(\alpha^2, i)$$

nicht nomal sind $< \tau >, < \sigma^2\tau >$ sind nicht normal:

$$< \tau >, < \sigma^2\tau > : \sigma < \tau > \sigma^{-1} =< \sigma\tau\sigma^{-1} >=< \sigma^2\tau >$$
$$< \sigma\tau >, < \sigma^3\tau > : \tau < \sigma\tau > \tau^{-1} = ... =< \sigma^3\tau >$$

19 19 Kreisteilungstheorie:

Zerfällungskörper von $X^n - 1 = \mathbb{Q}(\zeta_n), \zeta_n \in \mathbb{C}$ prim. n-te Einheitswurzel.
$Irr(\zeta_n, \mathbb{Q}) =: \Phi_n$ die $n-$te Kreisteilungspolynom.

$$\Phi_n = \prod_{ord\zeta = n \ \zeta \in U(1) \subset \mathbb{C}} (X - \zeta), \qquad X^n - 1 \prod_{d|n} \Phi_d$$

Satz: $Aut(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq (\mathbb{Z}/_n)^x := \{m \in \{1, .., n-1\} | ggT(m, n) = 1\}$

20 Radikalerweiterungen

Für Polynome vom Grad≤ 4 lassen sich Nullstellen durch Wurzeln darstellen:
$deg = 2$:

$$f = ax^2 + bx + c \Rightarrow x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

$deg = 3$:

$$f \rightsquigarrow x^3 + px + q \Rightarrow x = \sqrt[3]{-\frac{q}{2} + \sqrt{\underbrace{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}_{\Delta}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{...}}$$

Geschichtliches:

1530 Tartaglia für $\Delta > 0$

1545 Cardano allgemein $\Rightarrow \mathbb{C}$

1540 $deg = 4$Ferrari

$deg = 5$: allgemein unmöglich, bewiesen von Ruffini 1799, oder Abel 1826

21 20.1

Definition:

a) L/K heißt Radikalerweiterung, falls L aus K durch sukzessive Adjunktion von Wurzeln aus K entsteh. D.h. $L = K(\alpha_1, ..., \alpha_r)$ und $\forall i \exists m_i \in \mathbb{N}$ mit: $\alpha_i^{m_i} \in K(\alpha_1, ...\alpha_{i-1})$

b) M/K Körpererweiterung, so heißt $\alpha \in M$ durch Radikale darstellbar über K, falls $K(\alpha)/K$ Radikalerweiterung ist.

Das nächste Zeil ist die Verbindung zwischen den Radikalerweiterungen und der Gruppentheorie.

21.1 20.2 Zyklische Erweiterungen

Definition: Eine Galios-Erweiterung L/K heißt zyklisch, falls $Aut(L/K)$ eien zyklische Gruppe ist.

Satz: Sei K ein Körepr, $char(K) = 0$ und K enthalte alle $n-$ten Einheitswurzeln ($X^n - 1$ zerfällt), $n \geq 2$, dann gilt:

1) Das Adjungieren einer $n-$ten Wurzel eines Elements in K liefert eine zyklische Erweiterung L/K mit $[L : K]|n$

2) Jede zyklische Erweiterung von k mit $[L : K]|n$ entsteht auf diese Weise

Beweis:

1. Situation: $L = K(\alpha)/K$, $\alpha^n =: a \in K, G := Aut(K(\alpha)/K)$.
   $K(\alpha)/K$ ist Galoisch, denn:

$$X^n - a = \prod_{\zeta \in \mu_n} (X - \zeta\alpha), \quad \mu_n := \{\zeta \in K \mid \zeta^n = 1\} \subset K^x$$

   Betrachte die Injektion:

$$\varphi : G \to \mu_n, \sigma \mapsto \sigma(\alpha)/\alpha \qquad \text{d.h. } \sigma(\alpha) = \varphi(\sigma) \cdot \alpha$$

   φ ist ein Hom. von Gruppen:

$$(\sigma \circ \sigma')(\alpha) = \sigma(\varphi(\sigma') \cdot \alpha) = p(\sigma') \cdot \varphi(\sigma) \cdot \alpha \Rightarrow \varphi(\sigma \circ \sigma') = \varphi(\sigma) \cdot \varphi(\sigma')$$

   $\Rightarrow G$ ist Untergruppe von $\mu_n \Rightarrow G$ zyklisch, $[L : K] = |G|$ teilt n.

2. Sei L/K zyklisch, $[L : K] = n$, $Aut(L/K) =< \sigma > \simeq \mathbb{Z}/_n$
   Betrachte L als $K-$VR: E$\sigma : L \to L$ ist $K-$linear, $\sigma^2 = id$.
   Lineare Algebra $\Rightarrow H := EW(\sigma) \subset \mu_n$:

$$\sigma(v) = \lambda v \Rightarrow \sigma^n(v) = \lambda^n v \overset{v \neq 0^n}{\lambda} = 1$$

$H \subset \mu_n$ ist Untergruppe:
Sei λ Eigenwert mit Eigenvektor v, und λ' Eigenwert mit Eigenvektor v', dann folgt:

$$\sigma(\underbrace{vv'}_{\in L}) = (\lambda\lambda') \cdot (vv')$$

$\underline{H = \mu_n}$:
$d := |H|$, so hat $\tau := \sigma^d$ nur Eigenwerte 1 und es gilt

$$\tau^{\frac{n}{d}} = \sigma^n = Id$$

und mit der Jordennormalform im Zfkp von χ_τ folgt: $\tau = Id \Rightarrow d = n$
$\Rightarrow \exists v$ EV von σ mit Eigenwert ζ, prim. $n-$te EWrzl: $\mu_n =< \zeta >$

$\underline{\text{Behauptung}}$ $\alpha := v$ ist eine $n-$te Wurzel, die L erzeugt:
α^k ist EV zum Eigenwert $\zeta^k \Rightarrow 1, \alpha, \alpha^2, ..., \alpha^{n-1}$ sind linear unabhängig über K.
$\sigma(\alpha^n) = \zeta^n \cdot \alpha^n = \alpha^n \Rightarrow \alpha^n \in K$
Demnach $K \subset K(\alpha) \subset L$ und $[K(\alpha) : K] = n = [L : K] \Rightarrow L = K(\alpha)$

□

21.2 20.3 Korollar

K Körper, $char(K) = 0$, K enthalte alle $p-$ten Einheitswurzeln , p prim., dann gilt:
L/K Galoiserweiterung mti $[L : K] = p \Leftrightarrow L = K(\sqrt[p]{a}), a \in K \backslash K^p$
Beweis:
$G = Aut(L/K)$ $|G| = p \Rightarrow G$ zyklisch

□

Sei $K \ni \zeta$, ζ prim n-te Einheitswurzel. L/K zyklisch mit $[L : K]|n \Leftrightarrow L = K(\alpha), \alpha^n \in K$

21.3 20.4 Auflösbare Gruppen

$\underline{\text{Erinnerung:}}$ Kompositionsreihe von G:

$$\{1\} = G_0 \subsetneq G_1 \subsetneq ... \subsetneq G_r = G$$

mit $G_{i-1} \lhd G_i$ und G_i/G_{i-1} isteinfach ($\Leftrightarrow r$ maximal)
(d.h. hat keine nichttriv. normalen Untergruppen)
Ferner:

$$\{G_r/G_{r-1} \subsetneq, ..., G_1/G_2\} \qquad \text{ist einfach}$$

Definition: G heißt $\underline{\text{auflösbar}}$:$\Leftrightarrow$ alle G_i/G_{i-1} sind abelsch ($\Leftrightarrow G_i/G_{i-1} \simeq \mathbb{Z}/_{p_i}$)

Beispiele:

a) Endliche abelsche Gruppen sind auflösbar

b) D_n ist auflösbar: $\{1\} \subset \mathbb{Z}/_{p_1} \subset \mathbb{Z}/_{p_2} ... \subset \mathbb{Z}/_{p_n} \subset D_n$

c) S_5 ist nicht auflösbar:

$$\{1\} \subset A_5 \subset S_5$$

und A_5 ist nicht einfach. (das hatten wir nicht bewiesen aber es stimmt.

d) Untergruppen und Quotienten von auflösbaren Gruppen sind auflösbar.

$$\begin{array}{rr} H \subset & G \\ \cup & \cup \\ H \cap G_{r-1} & G_{r-1} \\ \cup & \cup \\ \vdots & \vdots \end{array} \qquad\qquad \begin{array}{rr} G & \xrightarrow{q} Q \\ \cup & \cup \\ G_{r-1} & q(G_{r-1}) \\ \cup & \cup \\ \vdots & \vdots \end{array}$$

21.4 20.5 Hauptsatz

Für eine Körpererweiterung L/K, $char(K) = 0$, sind äquivalent:

1. L lässt sich in eine Radikalenerweiterung von K einbetten
2. L lässt sich in eine Galoiserweiterung L'/K einbetten mit $Aut(L/K)$ auflösbar

Beweis in 20.7

21.5 Translationssatz der Galoistheorie:

Seien $K, L \subset M$ Körper mit M/K und M/L endlich. Ist $K/(K \cap L)$ Galoisch, so auch KL/L und

$$p : Aut(KL/L) \to Aut(K/(K \cap L)), \quad sigma \mapsto \sigma|_K$$

ist ein Isomorphismus.
Beweis: (Für $char(K) = 0$)
$K/(K \cap L)$ ist Zfkp von $f_1, .., f_r \in (K \cap L)[X]$
$\Rightarrow KL/L$ ist Zfkp von $f_1, ..., f_r \in L[X]$
$\overset{charK=0}{\Rightarrow} KL/L$ Galois.

p ist wohldefiniert: $\sigma \in Aut(KL/L) \overset{K/K\cap L \text{ normal}}{\Rightarrow} \sigma(K) = K$

p ist injektiv: $\sigma \in Aut(KL/L)$ wird durch $\sigma|_K$ festgelegt.

p ist surjektiv: $G := p(Aut(KL/L)) \Rightarrow K^G = K \cap L \overset{KL/L \text{ Gal}}{\Rightarrow} G = Aut(K/(K \cap L))$

□

21.6 20.7 Beweis von 20.5

(1) ⇒ (2) o.E. L/K ist eien Radikalerweiterung und L/K Galois:
Konjugierte Elemente von Wurzeln sind Wurzeln (bilde Kompositum der $\sigma(L)$ in einer normalen Erweiterung, σ Körpermonomorphismus). ($\alpha \in L$ Wurz. $\Rightarrow \sigma(\alpha)$ Wurzel)

Daraus folgt wir haben einen Körperturm mit $K_i = K_{i-1}(\sqrt[d_i]{a_1})$, $L = K_r \supset K_{r-1} \supset ... \supset K_0 = K$
O.E. seien die d_i prim., und $n := \prod_{i=0}^{r} d_i$
und $\zeta :=$ primitive Einheitswurzel
Nach Satz 20.2 folgt K_i'/K_{i-1}' Galoissch, $Aut(K_i'/K_{i-1}') \simeq \mathbb{Z}/_{p_i}$
Galois-Körpererweiterung liefert Kompositionsreihe:

$$\{1\} = Aut(K_r'/K_r') \trianglelefteq Aut(K_r'/K_{r-1}') \trianglelefteq ... \trianglelefteq Aut(K_r'/K_0')$$

mit Subquotienten $\simeq \mathbb{Z}/_{p_i}$

$\Rightarrow Aut(K_r'/K_0') = Aut(L(\zeta)/K(\zeta))$ ist auflösbar.
20.6 für zeigt: $Aut(L(\zeta)/K(\zeta)) \simeq Aut(L/K) \Rightarrow Aut(L/K)$ auflösbar.

(2) ⇒ (1) o.E. se $L = L'$
$Aut(L/K)$ auflösbar $\rightsquigarrow Aut(L/K) = G_0 \trianglerighteq G_1 \trianglerighteq ... \trianglerighteq G_r = \{1\}$ mit $G_{i-1}/G_i \simeq \mathbb{Z}/_{p_i}$ mit p_i prim.
Galoiskorrespondenz liefert Folge von Galoiserweiterungen ($K_i = L^{G_i}$)

$$K = K_0 \subsetneq K_1 \subsetneq ... \subsetneq K_r = L$$

Translationssatz 20.6 $\Rightarrow$ auch $K_i(\zeta)/K_{i-1}(\zeta)$ Galoisschmit Gruppe $\mathbb{Z}/_{p_i}$
Kor20.3 $\Rightarrow K_i(\zeta)/K_{i-1}(\zeta)$ ist Radikalerweiterung $\Rightarrow L(\zeta)/K$ ebenso

□

21.7 20.8 Korollar

Für $P \in K[X]$, $char(K) = 0$, gilt:
NST von P sind durch Radikaledarstellbar $\Leftrightarrow Aut(L/K)$ auflösbar, L =Zfkp von P.
Beweis:
$\alpha_1, ..., \alpha_r$ NST von P in L. $\alpha_1, ..., \alpha_r$ durch Radikale darstellbar $\Leftrightarrow L := K(\alpha_1, ..., \alpha_r)$ in Radikalerweiterung einbettbar $\overset{20.5}{\Leftrightarrow} Aut(L/K)$ auflösbar.

□

21.8 Grad = 5

Satz: $P \in \mathbb{Q}[X]$, $deg(P) = 5$, P habe genau drei reelle Nullstellen. $\Rightarrow Aut(L/\mathbb{Q}) \simeq S_5$, wobei L : Zfkp von P.
Insbesondere sind die NSTen von P nicht durch Radikale darstellbar.
Beweis:
$:= Aut(L/\mathbb{Q})$ operiert treu (wie Id) auf den Nullstellen $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{R},\ \alpha_4, \alpha_5 \in \mathbb{C}\backslash\mathbb{R}$
$\Rightarrow G \subset S_5$.
Finde Elemente von G, die S_5 erzeugen: $\tau : z \mapsto \bar{z}$ d.h. $\alpha_i \mapsto \alpha_i, i = 1, 2, 3;\ \alpha_4 \mapsto \alpha_5, \alpha_5 \mapsto \alpha_4 = (4, 5)$
G operiert transitiv auf $\alpha_1, ..., \alpha_5 (\leftrightarrow P$ irred.)
$\Rightarrow 5 || G|$
$\Rightarrow \exists \sigma \in G, ord(\sigma) = 5$
$\Rightarrow \sigma$ ist ein 5-Zykel,
$\Rightarrow G \supset < \sigma, \tau > \overset{(!)}{=} S_5$

Beispiel $P = X^5 - 16X + 2$

22 15. Quadratische Körpererweiterungen -Konstruktion mit Zirkel und Lineal

15.1 Elememtargeom. Konstruktionen Hier nicht mehr Klausurrelevant. mach ich wenn ich mehr Zeit habe.