Algebra I

Dr. K.-P. Podewski

WS 1998/99

Gewidmet allen,
die sich durch die Algebra beißen müssen.

Dieses Dokument ist meine Mitschrift der Vorlesung "Algebra I" von Dr. K.-P.Podewski im Wintersemester 98/99.
Die Nummerierung der Lemmata, Sätze, etc. habe ich etwas den allgemeinen Normen angepaßt.
Bezüglich Rechtschreibung und Satzstellung habe ich stellenweise ebenfalls die Podewski-Norm an die deutschen Rechtschreibregeln angepaßt.
Sorry, Herr Podewski ! (☺)
Für eventuelle Fehler aller Art übernehme ich keine Verantwortung !
Tobias Müller

Inhaltsverzeichnis

1 Der Ring der ganzen Zahlen

Sei $(\mathbb{Z}, +, *, 0, 1)$ der Ring der ganzen Zahlen.

Lemma 1.0.1 *(Euklid)*
Seien $n, m \geq 0$ ganze Zahlen mit $m \neq 0$, dann gibt es q, r mit:
$n = q * m + r$ *und* $0 \leq r \leq n$
q, r sind eindeutig bestimmt.

Beweis:
Existenz:(Induktion über n)
I.Fall: $n < m$
Sei $q = 0$ und $r = n$
II.Fall: sonst
Dann ist $0 \leq n - m$ und somit gibt es nach Induktionsvoraussetzung q_1 und r mit $m - n = q_1 * m + r$
Sei $q = q_1 + 1$
Eindeutigkeit:
Sei $n = q_1 * m + r_1$ und $n = q_2 * m + r_2$ mit $r_1, r_2 < m$
o.B.d.A. sei $r_1 \leq r_2$
$\succ (q_1 - q_2) * m = r_2 - r_1$ und
$0 \leq r_2 - r_1 < m$
$\succ r_2 - r_1 = 0$
$\succ r_1 = r_2$ und $q_1 = q_2$

Sei $d > 0$. d heißt Teiler von n, wenn es ein e gibt, mit $d * e = n$ (geschrieben $d|n$)
Seien $n, m \in \mathbb{Z}$. d heißt gemeinsamer Teiler, wenn $d|n$ und $d|m$. Ein gemeinsamer Teiler d heißt größter gemeinsamer Teiler, wenn für alle gemeinsamen Teiler e von n, m gilt: $e|d$ (geschrieben: $ggt(n, m)$).

Lemma 1.0.2 *Seien $n, m > 0$, dann gibt es höchstens einen größten gemeinsamen Teiler von n und m.*

Beweis:
Seien d, e größte gemeinsame Teiler.
$\succ e|d$ und $d|e$
$\succ d = m_1 * e$ und $e = m_2 * d$
$\succ d = m_1 * m_2 * d$
$\succ m_1 * m_2 = 1$
Da $e, d > 0 \succ m_1, m_2 > 0 \succ m_1 = m_2 = 1$
$\succ e = d$

Satz 1.0.1 *(euklidischer Algorithmus)*
Seien $n, m > 0$, dann gibt es einen größten gemeinsamen Teiler.
Mehr noch: es gibt x, y mit $ggT(n, m) = x * n + y * m$

Beweis:

Wir definieren eine Folge (n_j) mit $j \in \mathbb{N}$ wie folgt:
Sei $n_1 = n$ und $n_2 = m$
Sei $j > 2$ und $n_1, \cdots, n_{j-1}$ bereits definiert.
I.Fall: $n_{j-1} = 0$, dann sei $n_j = 0$
II.Fall: $n_{j-1} > 0$, dann gibt es
genau ein q_{j-1} und ein n_j mit
$$n_{j-2} = q_{j-1} * n_{j-1} + n_j$$
mit $n_j < n_{j-1}$.

Beispiel: Gesucht ist der $ggt(150, 35)$

$n_1 = 150$
$n_2 = 35$
$n_3 = n_1 - q_2 * n_2 = 150 - 4 * 35 = 10$ mit $n_3 < n_2$
$n_4 = n_2 - q_3 * n_3 = 35 - 3 * 10 = 5 = n_k$ mit $n_4 < n_3$
$n_5 = n_3 - q_4 * n_4 = 10 - 2 * 5 = 0 = n_j$ mit $n_5 < n_4$

$q_2 = 4 \quad q_3 = 3 \quad q_4 = 2$

$x_1 = 1 \quad x_2 = 0 \quad x_3 = 1 \quad x_4 = -3$
$y_1 = 0 \quad y_2 = 1 \quad y_3 = -4 \quad y_4 = 13$

Behauptung 1.0.1 *(Abbruch des euklidischen Algorithmus)*
Es gibt ein k mit $n_k \neq 0$ und $n_{k+1} = 0$

Beweis:

$\{n_k | k \in \mathbb{N}, n_k \neq 0\}$ besitzt ein kleinstes Element n_k.
Da $n_{k+1} < n_k \succ n_{k+1} = 0$
Wir wollen zeigen:
$n_k = ggT(n, m)$

Behauptung 1.0.2 *$n_k | n_j$ mit $1 \leq j \leq k$*

Beweis:

Durch vollständige Induktion zeigen wir $n_k | n_j$ mit $k - 1 \leq j \leq k$
Ist $i = 1$, dann $n_j = n_k \qquad \surd$
oder $n_j = n_{k-1} = q_k * n_k + \underbrace{n_{k+1}}_{=0} \qquad \surd$
Sei $i > 1$
$\succ n_k | n_j$ für $(k - i) + 1 \leq j \leq k$
nach Induktionsvoraussetzung und
$n_{k-i+2} = q_{k-i+1} * n_{k-i+1} + n_{k-i}$
$\succ n_{k-i} = n_{k-i+2} - q_{k-i+1} * n_{k-i+1}$

Da $n_k | n_{k-i+2}$ und $n_k | n_{k-i+1}$
$\succ n_k | n_{k-i}$

Behauptung 2 sagt, ein n_k ist ein gemeinsamer Teiler von $n = n_1$ und $m = n_2$.

Behauptung 1.0.3 *Ist $1 \leq j \leq k$ dann gibt es x_j und y_j mit $n_j = x_j * n + y_j * m$*

Beweis:(Induktion über j)

$j = 1$, sei $x_1 = 1$ und $y_1 = 0$
$j = 2$, sei $x_2 = 0$ und $y_2 = 1$
Sei $j > 2$
Wir setzen:

$$\boxed{\begin{array}{c} X_j = X_{j-2} - q_{j-1} * X_{j-1} \\ Y_j = Y_{j-2} - q_{j-1} * Y_{j-1} \end{array}}$$

$X_j * n + Y_j * m = (X_{j-2} - q_{j-1} * X_{j-1}) * n + (Y_{j-2} - q_{j-1} * Y_{j-1}) * m$
$= (X_{j-2} * n + Y_{j-2} * m) - q_{j-1} * (X_{j-1} * n + Y_{j-1} * m)$
$= m_{j-2} - q_{j-1} * m_{j-1}$
$= m_j$

In unserem Beispiel von Seite 10:

$X_1 = 1$
$Y_1 = 0$
$X_2 = 0$
$Y_2 = 1$
$X_3 = X_1 - q_2 * X_2 = 1 - 4 * 0 = 1$
$Y_3 = Y_1 - q_2 * Y_2 = 0 - 4 * 1 = -4$
$X_4 = X_2 - q_3 * X_3 = 0 - 3 * 1 = -3$
$Y_4 = Y_2 - q_3 * Y_3 = 1 - 3 * (-4) = 13$

Probe: $n_4 = X_4 * n + Y_4 * m = -3 * 150 + 13 * 35 = 5$ $\surd$

Behauptung 1.0.4 *(ggt aus dem euklidischen Algorithmus ablesen)*
$n_k = ggT(n, m)$

Beweis:

Nach Behauptung 2 von Seite 10 ist n_k gemeinsamer Teiler.
Sei e ein gemeinsamer Teiler von n, m.
$\succ$ Es gibt r, s mit
$n = r * e$ und $m = s * e$
Nach Behauptung 3 von Seite 11 ist
$n_k = X_k * n + Y_k * m$
$\succ n_k = X_k * (r * e) + Y_k * (s * e) = e * (X_k * r + Y_k * s)$
$\succ e | n_k$
$\succ n_k$ ist größter gemeinsamer Teiler von n, m

Eine Teilmenge I von $\mathbb{Z}$ heißt Ideal, wenn gilt:

1. $0 \in I$
2. $a, b \in I \succ a + b \in I$
3. $a \in I, b \in \mathbb{Z} \succ a * b \in I$

Beispiele:

1. $\mathbb{Z}$ ist ein Ideal.
2. $\{0\}$ ist ein Ideal.
3. Seien $a_1, \cdots, a_n \in \mathbb{Z}$, dann sei $(a_1, \cdots, a_n) := \{x_1a_1 + x_2a_2 + \cdots + x_na_n | x_1, \cdots, x_n \in \mathbb{Z}\}$.
   Dann ist $(a_1, \cdots, a_n)$ ein Ideal.
   $(a1, \cdots, a_n)$ heißt das von $a_1, \cdots, a_n$ erzeugte Ideal.

$(1) = \mathbb{Z}$ heißt Eins-Ideal
$(0) = \{0\}$ heißt Null-Ideal

Satz 1.0.2 *Ist I ein Ideal in $\mathbb{Z}$, dann gibt es $d \geq 0, d \in \mathbb{Z}$ mit $I = (d)$*

Beweis:
Behauptung 1: Ist $I \neq \{0\}$, dann gibt es $d > 0, d \in I$
Beweis: Sei $x \in I \setminus \{0\}$. $x > 0$. Sei $d = x$. Ist $x < 0$, dann sei $d = (1) * x$.
Sei d das kleinste Element aus $\{x \in I | x > 0\}$.
z.z.:$I = (d)$.
Behauptung 2: $(d) \subseteq I$ $\surd$
Behauptung 3: $I \subseteq (d)$
Beweis: Sei $a \in I$. Dann gibt es q, r mit:

$$a = q * d + r \text{ und } 0 \leq r < d \succ r = \underbrace{\underbrace{a}_{\in I} + \underbrace{(-q) * \underbrace{d}_{\in I}}_{\in I}}_{\in I} \succ r \in I$$

$\succ r = 0$ nach Wahl von d und r.
$\succ a = q * d \in (d)$.

Satz 1.0.3 *Seien $m, n, d \in \mathbb{Z}$ mit $m, n, d > 0$. Ist $(m, n) = (d)$, dann ist d der größte gemeinsame Teiler von n, m*

Beweis:
Behauptung 1: d ist gemeinsamer Teiler
Beweis: Da $m, n \in (d) \succ m = x * d$ und $n = y * d \succ d | m, d | n$.
Behauptung 2: d ist größter gemeinsamer Teiler
Beweis: $e > 0, e \in \mathbb{Z}$ mit $e | m$ und $e | n \succ m = x * e, n = y * e$
Da $d \in (m, n)$, gibt es r, s mit $d = r * m + s * n$
$\succ d = r * x * e + s * y * e = e * (r * x + s * y)$

$\succ e|d$

$p \in \mathbb{Z}$, $p > 1$, heißt Primzahl,
wenn für alle $n, m > 0$ mit $p = m * n$ folgt: $m = 1$ oder $n = 1$.

Lemma 1.0.3 *Sei p eine Primzahl und $m, n > 0$ mit $p|m * n \succ p|m$ oder $p|n$.*

Beweis:
I.Fall: $p|m$ $\surd$
II.Fall: sonst
Dann ist $ggT(p, m) = 1$ $(1) = (p, m)$
$\succ 1 = x * p + y * m \succ n = n * x * p + y * n * m$
Sei $z \in \mathbb{Z}$ mit $z * p = n * m$
$\succ n = n * x * p + y * z * p = p * (n * x + y * z) \succ p|n$

Folgerung 1.0.1 *Sei $m_i > 0$ für $i = 1, \cdots, l$ und p eine Primzahl mit $p| \prod_{i=1}^{l} m_i$. Dann gibt es ein i mit $p|m_i$.*

Beweis:(Induktion über i

Satz 1.0.4 *Ist $n \geq 2$ eine ganze Zahl, dann gibt es Primzahlen $p_1, \cdots, p_l$ mit*
$p_1 \leq p_2 \leq \cdots \leq p_l$ *und* $n = \prod_{i=1}^{l} p_i$
Mehr noch: Die Darstellung ist eindeutig.

Beweis:
Existenz:(Induktion über n)
$n = 2$ $\surd$
Sei $n > 2$
I.Fall: n ist eine Primzahl $\surd$
II.Fall: sonst
Dann gibt es $l \leq n_1, n_2 < m$ mit $m = n_1 * n_2$
Nach Induktionsvoraussetzung ist
$n_1 = \prod_{i=1}^{l} p_i$ $n_2 = \prod_{j=1}^{k} q_j$
mit $p_1 * p_2 * \cdots * p_l$ und $q_1 * \cdots * q_l$ Primzahlen.
Da die Multiplikation kommutativ ist, folgt die Behauptung.
Eindeutigkeit: (Induktion über l)
Sei $\prod_{i=1}^{l} p_i = \prod_{i=1}^{l} q_i$ mit $p_1 \leq \cdots \leq p_l$ und $q_1 \leq q_2 \leq \cdots \leq q_k$ Primzahlen.
Ist $l = 1$ $\surd$
Sei $l > 1$. $\succ p_l| \prod_{i=1}^{k} q_i$
$\succ$ Es gibt q_i mit $p_l|q_i \succ p_l \leq q_k$
$q_k| \prod_{i=1}^{l} p_i \succ$ Es gibt i mit $q_k|p_i$
$\succ q_k \leq p_l \succ q_k = p_l \succ \prod_{i=1}^{l-1} p_i = \prod_{i=1}^{k-1} q_i$
Nach Induktionsvoraussetzung ist $k-1 = l-1$ und $p_i = q_i$ für $i = 1, \cdots, l-1$

Sei I ein Ideal und $a, b \in \mathbb{Z}$. a heißt kongruent b modulo I, wenn $a - b \in I$.
Geschrieben: $a \equiv b \ mod \ I$

Ist $I = (n)$, dann schreibt man für $a \equiv b \ mod \ (n)$ auch $a \equiv b \ mod \ n$

Lemma 1.0.4 *' $\equiv$ ' ist eine Äquivalenzrelation, d.h.*

1. $a \equiv a \ mod \ I$
2. $a \equiv b \ mod \ I \succ b \equiv a \ mod \ I$
3. $a \equiv b \ mod \ I$ *und* $b \equiv c \ mod \ I \succ a \equiv c \ mod \ I$

Beweis:

zu 1: Da $a - a = 0 \in I \succ a \equiv a \ mod \ I$

zu 2: $a \equiv b \ mod \ I \succ a - b \in I \succ b - a = (-1) * (a - b) \in I \succ b \equiv a \ mod \ I$

zu 3: $a \equiv b \ mod \ I$ und $b \equiv c \ mod \ I$

$\succ a - b \in I$ und $b - c \in I$

$\succ a - c = \underbrace{(a - b)}_{\in I} + \underbrace{(b - c)}_{\in I} \in I$

$\succ a \equiv c \ mod \ I$

Lemma 1.0.5 *Sei $a \equiv b \ mod \ I$ und $c \equiv d \ mod \ I$, dann gilt:*

1. $a + c \equiv b + d \ mod \ I$
2. $a * c \equiv b * d \ mod \ I$

Beweis: $(a - b) \in I$ und $(c - d) \in I$

zu 1: Wir wollen zeigen: $(a + c) - (b + d) \in I$

$(a + c) - (b + d) = \underbrace{(a - b)}_{\in I} + \underbrace{(c - d)}_{\in I} \in I$

zu 2: Wir wollen zeigen: $a * c - b * d \in I$

$I \ni (a-b)*(c-d) = a*c-b*c-a*d+b*d = (a*c-b*d)-(b*c-b*d)-(a*d-b*d)$

$\succ (a * c - b * d) = \underbrace{(a - b) * (c - d)}_{\in I} + \underbrace{b * (c - d)}_{\in I} + \underbrace{d * (a - b)}_{\in I} \in I$

Beispiel: Gesucht ist r mit $0 \leq r < 7$ und $9^{10} = 5 * 7 + r$

Behauptung: $r = 2$

$9 \equiv 2 \ mod \ 7$

$9^3 \equiv 2 * 2 * 2 \ mod \ 7 \equiv 1 \ mod \ 7$

$9^9 \equiv 1 * 1 * 1 \ mod \ 7 \succ 9^9 \equiv 1 \ mod \ 7 \succ 9^{10} = 9 \ mod \ 7 \succ 9^{10} \equiv 2 \ mod \ 7$

2 Gruppen

Sei $G \neq \emptyset$ und
$* : G \times G \to G$
$e \in G$
G heißt Gruppe, wenn gilt:

1. $(a * b) * c = a * (b * c)$
2. $a * e = a$
3. Es gibt ein $d \in G$ mit $a * d = e$

Eine Gruppe $(G, *, e)$ heißt kommutativ, wenn für alle $a, b \in G$ gilt:
$$a * b = b * a$$
Ist $(G, *, e)$ kommuttativ, dann schreibt man auch $+$ für $*$ und 0 für e.
Häufig schreibt man G für(G,*,e)

Lemma 2.0.6 *"rechtsinvers gleich linksinvers"*
Ist $a * d = e$, dann ist $d * a = e$

Beweis: Sei $c \in G$ mit $d * c = e$
Nach Voraussetzung gilt:
$a * d = e$
$\overset{*d}{\succ} d * (a * d) = d$
$\overset{*c}{\succ} d * (a * d) * c = d * c$
$\overset{(1)}{\succ} (d * a) * (d * c) = d * c$
$\overset{Wahl\ von\ c}{\succ} (d * a) * e = e$
$\overset{(2)}{\succ} d * a = e$

Lemma 2.0.7 *"e ist auch Links-Eins"*
$d = e * d$

Beweis:
Sei $a \in G$ mit $d * a = e \overset{L1}{\succ} a * d = e$
$d \overset{(2)}{=} d * e \overset{Einsetzen}{=} d * (a * d) \overset{(1)}{=} (d * a) * d \overset{Wahl\ a}{=} e * d$

Lemma 2.0.8 *Ist $a * d = e = a * c \succ d = c$*

Beweis:
$a * d = e \overset{L1}{\succ} d * a = e$
$d \overset{(2)}{=} d * e \overset{Voraussetzung}{=} d * (a * c) \overset{(1)}{=} (d * a) * c \overset{Einsetzen}{=} e * c \overset{L2}{=} c$

Das eindeutig bestimmte Element c mit $a * c = e$ schreibt man auch a^{-1}.

Bemerkung 2.0.1

$$(a^{-1})^{-1} = a$$
$$\overset{(a^{-1})^{-1} * a^{-1} = e}{\underset{a * a^{-1} = e}{\succ}} a = (a^{-1})^{-1}$$

Lemma 2.0.9 $a * b = a \succ b = e$

Beweis:

$$\begin{aligned} & a * b = a \\ \overset{a^{-1}}{\succ} \; & (a^{-1} * a) * b = a^{-1} * a \\ \succ \; & e * b = e \\ \overset{L2}{\succ} \; & b = e \end{aligned}$$

Beispiele:

1. $(\mathbb{Z}, +, 0)$ ist eine Gruppe
2. $(\mathbb{Q}, +, 0)$
3. $(\mathbb{R}, +, 0)$
4. $(\mathbb{C}, +, 0)$
5. $(\mathbb{Q}\backslash\{0\}, *, 1)$ ist eine Gruppe
6. $(\mathbb{Z}\backslash\{0\}, *, 1)$ ist keine Gruppe
7. $(\{1, -1\}, *, 1)$ ist eine Gruppe
8. $(\{1, -1, i, -1\}, *, 1)$ iste eine Gruppe
9. $(\{r \in \mathbb{R} | r > 0\}, *, 1)$ ist Gruppe

Beispiel:

Seien G_1 und G_2 Gruppen.
Sei $G_1 \times G_2 = \{(a, b) | a \in G_1, b \in G_2\}$

$$(a_1, b_1) * (a_2, b_2) := (a_1 * a_2, b_1 * b_2)$$
$$e = (e_1, e_2)$$

Dann ist $G_1 \times G_2$ eine Gruppe.

Beispiel:

Sei M eine Menge.

$$G_M = \{f | f : M \overset{1-1}{\underset{auf}{\longrightarrow}} M\}$$

$$f \circ g : \begin{cases} M & \to & M \\ a & \mapsto & f(g(a)) \end{cases}$$

$$id_M : \begin{cases} M & \to & M \\ a & \mapsto & a \end{cases}$$

Dann ist $(G_M, \circ, id_M)$ eine Gruppe.

Beweis:

Man zeigt:

(i) $f, g \in G_M \succ f \circ g \in G_M$

(ii) $id_M \in G_M)$

und es gilt:

(1) $(f \circ g) \circ h = f \circ (g \circ h)$

(2) $f \circ id_M = f$

(3) Es gibt g mit $f \circ g = id_M$

Behauptung: Ist $|M| \geq 3$, dann ist G_M nicht kommutativ.

Beweis: Sei oBdA $1, 2, 3, 4 \in M$

Sei $f : M \xrightarrow[auf]{1-1} M mit$

$$f(a) = \begin{cases} 2 & \text{für} \quad a = 1 \\ 1 & \text{für} \quad a = 2 \\ a & \text{sonst} \end{cases}$$

Sei $g : M \xrightarrow[auf]{1-1} M$

$$g(a) = \begin{cases} 3 & \text{für} \quad a = 1 \\ 1 & \text{für} \quad a = 3 \\ a & \text{sonst} \end{cases}$$

$$g \circ f(a) = \begin{cases} 2 & \text{für} \quad a = 1 \\ 3 & \text{für} \quad a = 2 \\ 1 & \text{für} \quad a = 3 \\ a & \text{sonst} \end{cases}$$

$$f \circ g(a) = \begin{cases} 3 & \text{für} \quad a = 1 \\ 1 & \text{für} \quad a = 2 \\ 2 & \text{für} \quad a = 3 \\ a & \text{sonst} \end{cases}$$

$g \circ f \neq f \circ g$

Ist $M = \{1, \cdots, n\}$, dann heißt G_M auch Permutationsgruppe der Zahlen $1, \cdots, n$. Man schreibt dann auch S_n für G_M.

Sei G eine Gruppe. $H \subseteq G$, $H \neq \emptyset$, heißt Untergruppe von G, wenn für alle $a, b \in H \succ b * a^{-1} \in H$

Lemma 2.0.10 *Ist H eine Untergruppe von G, dann ist $(H, *, e)$ eine Guppe.*

Beweis:

(i) Sei $a \in H. \succ a * a^{-1} = e \in H$

(ii) Sei $a \in H \succ e * a^{-1} = a^{-1} \in H$

(iii) Sei $a, b \in H \succ a * (b^{-1})^{-1} = a * b \in H$

Es gilt ferner für $a, b, c \in H$:

1) $(a * b) * c = a * (b * c)$
2) $a * e = a$
3) Es gibt $d \in H$ mit $a * d = e$

Ist H eine Untergruppe von G, dann schreibt man auch $H < G$

Sei $H < G$ und $a \in G$, dann sei:
$a * H = \{a * x | x \in H\}$
$H * a = \{x * a | x \in H\}$
$a * H$ heißt Links-Nebenklasse
$H * a$ heißt Rechts-Nebenklasse

Lemma 2.0.11 *Sei H Untergruppe von G* $\hookleftarrow$

1. $a * H \cap b * H \neq \emptyset$
2. $a * H = b * H$
3. $b^{-1} * a \in H$

Beweis:
(1)$\succ$(2)
Sei $a * H \cap b * H \neq \emptyset$ z.z. $a * H = b * H$
Nach Voraussetzung gibt es x und $y \in H$
mit $a * x = b * y \succ a = b * y * \underbrace{x^{-1}}_{\in H}$
"$\subseteq$" Sei $z \in H$, z.z. $a * z \in b * H$
$a * z = b * y * \underbrace{x^{-1} * z}_{\in H} \in b * H$
"$\supseteq$" ebenso
(2)$\succ$(3)
$a = a * e \in a * H = b * H$
$\succ$ Es gibt $z \in H$ mit $a = b * z$
$\succ b^{-1} * a = z \in H$
(3)$\succ$(1)
$a \in a * H$, da $b^{-1} * a \in H$
$\succ a = b * (b^{-1} * a) \in b * H$
$\succ a \in a * H \cap b * H$

Sei G eine Gruppe, $M \subseteq G, M \neq \emptyset$, heißt Untergruppe, wenn für alle $a, b \in H$ gilt: $a * b^{-1} \in H$(geschrieben $H < G$)
Sei $H < G$ und sei $a \in G$, dann ist $a * H = \{a * x | x \in H\}$
Wir hatten gezeigt:

1. $a * H \cap b * H \neq \emptyset$ $\qquad$ G $\overset{eH}{\square}$ $\overset{a_1H}{\square}$ $\overset{a_2H}{\square}$ $\square$ $\square$ $\square$

2. $a * H = b * H$

Lemma 2.0.12 *Sei G Gruppe, $H < G$ und $a \in H$, dann ist $|a * H| = |H|$*

Beweis:

Sei $f : \begin{cases} H & \to & G \\ x & \mapsto & a * x \end{cases}$

Wir zeigen $f : H \xrightarrow[auf]{1-1} a * H$

Behauptung 1: Ist $x \in H \succ a * x \in a * H$

$f : H \to a * H$

Behauptung 2: $f : H \xrightarrow{1-1} a * H$

$f(x) = f(y)$ z.Z. $x = y$

$f(x) = a * x = a * y = f(y) \succ a^{-1} * a * x = a^{-1} * a * y \succ x = y$

Behauptung 3: $f : H \xrightarrow[auf]{} a * H$

Beweis: Sei $c \in a * H \succ$Es gibt $x \in H$ mit $c = a * x \succ f(x) = c$

Sei $H < G$, dann $|G : H|$ gleich die Anzahl der Elemente von $\{a * H, a \in G\}$
$|G : H|$ wird auch Index genannt.

Folgerung 2.0.2 *Ist $H < G$, dann ist $|G : H| * |H| = |G|$*

Beweis:

Seien $A_1, \cdots, A_k$ die Links-Nebenklassen. Dann gilt:

1. $A_i \cap A_j = \emptyset$
2. $A_1 \cup A_2 \cup \cdots \cup A_k = G$

Beweis:

Sei $a \in G$, da $e \in H \succ a = a * e \in a * H \succ a \in A_1 \cup \cdots \cup A_k$

$|G| = |A_1| + |A_2| + \cdots + |A_k| = \underbrace{|H| + |H| + \cdots + |H|}_{|G:H|} = |F : H| * |H|$

Beispiel:

Sei $G = S_n = \{f | f : \{1, \cdots, n\} \xrightarrow[auf]{1-1} \{1, \cdots, n\}\}$

Sei $H_n = \{\sigma \in S_n | \sigma(n) = n\}$

Behauptung 1:$H_n < S_n$

Beweis: Seien $\sigma_1, \sigma_2 \in H_n$. z.z.: $\sigma_1 * \sigma_2^{-1} \in H_n$

$\sigma_1(n) = n, \sigma_2(n) = n$

$\sigma_2^{-1}(n) = n \succ \sigma_1 \circ \sigma_2^{-1}(n) = \sigma_1(n) = n$

$\sigma_1 \circ \sigma_2^{-1} \in H_n$

Behauptung 2:$|H_n| = |S_{n-1}|$ für $n \geq 1$

Beweis:

Sei $f : \begin{cases} H_n & \to & S_{n-1} \\ \sigma & \mapsto & \sigma \restriction \{1, \cdots, n-1\} \end{cases}$

Dann $f : H_n \xrightarrow[auf]{1-1} S_{n-1}$

Behauptung 3: $|S_n : H_n| = n$

Sei $\tau_i \in S_n$ mit

$$\tau_i(k) = \begin{cases} n & \text{für} \quad k = 1 \\ i & \text{für} \quad k = n \\ k & \text{sonst} \end{cases}$$

Dann $\tau_i \circ \tau_i = id_{\{1,\cdots,n\}}$. Also ist $\tau_i^{-1} = \tau_i$

a) $|S_1 : H_n| \geq n$

Es genügt z.z. $\tau_i * H \neq \tau_k * H$ für $i \neq k$

$\tau_k^{-1} \circ \tau_i(n) = \tau_k \circ \tau_i(n) = \tau_k(i) \neq n$ für $i = k$.

$\succ \tau_k^{-1} \circ \tau_i \notin H_n \succ \tau_k * H_n \neq \tau_i * H_n$ b) $|S_n : H_n| \leq n$.

Beweis: Sei A eine Links-Nebenklasse, es genügt ein τ_i zu finden mit

$A \cap \tau_i * H \neq \emptyset$.

Sei $\sigma \in A$. Wir setzen $i = \sigma(n).\tau_i \circ \sigma(n) = \tau_i(i) = n$

$\succ \tau_i \circ \sigma \in H_n \succ \underbrace{\tau_i \circ \tau_i \circ \sigma}_{=\sigma} \in \tau_i * H$

$\succ A \cap \tau_i * H \neq \emptyset$.

Behauptung 4: $|S_n| = n!$

Beweis: (Induktion über n)

$n = 0$ $\quad S_0 = \{\emptyset\} \succ |S_0| = 1 = 0!$

$n = 1$ $\quad S_1 = \{\sigma | \sigma : \{1\} \xrightarrow[auf]{1-1} \{1\}\} \succ |S_1| = 1 = 1!$

$|S_n| = |Sn : H_n| * |H_n| = n * |S_{n-1}| \overset{Induktionsvoraussetzung}{=} n * (n-1)! = n!$

$H_n = \tau_n H_n$	$\tau_{n-1} H_n$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\tau_1 H_n$

Seien $(G, *, e)$ und $(H, *, e)$ Gruppen.
Eine Abbildung $\phi : G \to H$ heißt Homomorphismus, wenn $\phi(a * b) = \phi(a) * \phi(b)$

Beispiel:

Sei G eine kommutative Gruppe.

$$\phi : \begin{cases} G & \to & G \\ a & \mapsto & a^{-1} \end{cases}$$

Dann ist ϕ ein Homomorphismus.

Beweis:

$\phi(a * b) = (a * b)^{-1} = b^{-1} * a^{-1} \overset{kommutativ}{=} a^{-1} * b^{-1} = \phi(a) * \phi(b)$

Beispiel:

$$\phi : \begin{cases} \mathbb{C} & \to & \mathbb{R} \\ c & \mapsto & |c| \end{cases}$$

Dann ist ϕ ein Homomorphismus von $(\mathbb{C}\backslash\{0\}, *, 1)$ in $(\mathbb{R}\backslash\{0\}, *, 1)$

Beispiel:

$$\phi : \begin{cases} \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & e^x \end{cases}$$

Dann ist ϕ ein Homomorphismus von $(\mathbb{R}, +, 0)$ in $(\{x \in \mathbb{R} | x > 0\}, *, 1)$
Beweis:
$\phi(x+y) = e^{x+y} = e^x * e^y = \phi(x) * \phi(y)$

Lemma 2.0.13
1. $\phi(e) = e$
2. $\phi(a^{-1}) = \phi(a)^{-1}$

Beweis:
zu 1: $\phi(e) = \phi(e * e) = \phi(e) * \phi(e)$
$e = \phi(e)^{-1} * \phi(e) = \phi(e)^{-1} * \phi(e) * \phi(e) = \phi(e)$
zu 2: $e^{(1)} = \phi(e) = \phi(a * a^{-1}) = \phi(a) * \phi(a^{-1})$
$\phi(a)^{-1} = \phi(a^{-1})$

Lemma 2.0.14 *Seien $\phi : G \to G'$ und $\psi : G' \to G''$ Homomorphismen. Dann ist $\psi \circ \phi : G \to G''$ ein Homomorphismus.*

Beweis:
$\psi \circ \phi(a * b) = \psi(\phi(a * b)) = \psi(\phi(a)) * \psi(\phi(b)) = \psi \circ \phi(a) * \psi \circ \phi(b)$

Sei $\phi : G \to G'$ ein Homomorphismus, dann ist $Kern(\phi) = \{a | \phi(a) = e\}$

Lemma 2.0.15 $Kern(\phi) < G$

Beweis
Sei $a, b \in Kern(\phi)$ z.z. $a * b^{-1} \in Kern(\phi)$
$a, b \in Kern(\phi)$
$\succ \phi(a) = e$ und $\phi(b) = e$
$\succ \phi(a * b^{-1}) = \phi(a) * \phi(b^{-1}) = \phi(a) * \phi(b)^{-1} = e * e^{-1} = e$
$\succ a * b^{-1} \in Kern(\phi)$

Lemma 2.0.16 *Ist $\phi : G \to G'$ ein Homomorphismus mit $Kern(\phi) = \{e\}$, dann ist ϕ injektiv.*

Beweis:
Seien $a, b \in G$ mit $\phi(a) = \phi(b)$ z.z. $a = b$
$\phi(a) = \phi(b)$
$\succ \phi(a) * \phi(b)^{-1} = e$
$\succ \phi(a * b^{-1}) = e$
$\succ a * b^{-1} \in Kern(\phi) = \{e\}$
$\succ a * b^{-1} = e$
$\succ b^{-1} = a^{-1}$

Seien G und G' Gruppen und $\phi : G \to G'$ ein Homomorphismus, d.h. $\phi(a*b) = \phi(a)*\phi(b)$
Wir hatten definiert:
$Kern(\phi) := \{a | \phi(a) = e\}$

Wir hatten gezeigt:
$$Kern(\phi) < G$$

Wir nennen ϕ einen Monomorphismus, wenn ϕ injektiv ist.

Wir hatten gezeigt: $\hookleftarrow$

1. ϕ ist ein Monomorphismus
2. $Kern(\phi) = \{e\}$

Sei ϕ ein Homomorphismus $\phi : G \to G'$. Dann heißt
$$Bild(\phi) := \phi[G] = \{\phi(a) | a \in G\}$$
Bild von ϕ.

Lemma 2.0.17 $Bild(\phi) < G'$

Beweis:
Sei $\phi(a), \phi(b) \in Bild(\phi)$ z.z. $\phi(a) * \phi(b)^{-1} \in Bild(\phi)$
$\phi(a) * \phi(b)^{-1} = \phi(a) * \phi(b^{-1}) = \phi(a * b^{-1}) \in Bild(\phi)$

Ein Monomorphismus $\phi : G \to G'$ heißt Isomorphismus, wenn er surjektiv ist.

Sei $\phi : G \to G'$ ein Homomorphismus: $\hookleftarrow$

1. ϕ ist ein Isomorphismus
2. $Bild(\phi) = G'$ und $Kern(\phi) = \{e\}$

Sei $G = \mathbb{R}$ und $G' = \{r \in \mathbb{R} | r > 0\}$.
Dann sind
$$(G, +, 0) \text{ und } (G', *, 1)$$
Gruppen.

Beispiel:
$$\phi : \left\{ \begin{array}{ccc} G & \to & G' \\ a & \mapsto & e^a \end{array} \right.$$
Dann ist ϕ ein Homomorphismus.
$$Kern(\phi) = \{a | \phi(a) = 1\} = \{0\}$$
$$Bild(\phi) = G'$$
Also ist ϕ ein Isomorphismus von $(G, +, 0)$ auf $(G', *, 1)$

Lemma 2.0.18 *Ist $\phi : G \to G'$ ein Homomorphismus, dann gilt für alle $a \in G$:*
$\{a * x | x \in Kern(\phi)\} = a * Kern(\phi) = Kern(\phi) * a = \{x * a | x \in Kern(\phi)\}$

Beweis:
"$\subseteq$" Sei $b \in a * Kern(\phi)$

$\succ a^{-1} * b \in Kern(\phi)$
$\succ e = \phi(a^{-1} * b) = \phi(a^{-1}) * \phi(b) \overset{L1}{=} \phi(b) * \phi(a^{-1}) = \phi(b * a^{-1})$
$\succ b * a^{-1} \in Kern(\phi)$
$\succ b \in Kern(\phi) * a$
"$\supseteq$" Ebenso

$H < G$ heißt Normalteiler, wenn für alle $a \in G$ gilt:
$a * H = H * a$

Beispiel: Nicht jede Untergruppe ist Normalteiler.
Sei $G = S_n = \{\sigma | \sigma : \{1, \cdots, n\} \xrightarrow[auf]{1-1} \{1, \cdots, n\}\}$ mit $n \geq 3$.
Sei $H = \{\sigma \in S_n | \sigma(n) = n\}$
Dann ist $H < G$
Wir wollen zeigen: H ist kein Normalteiler.

$$\text{Sei } \tau(k) = \begin{cases} 1 & \text{für} \quad k = n \\ n & \text{für} \quad k = 1 \\ k & \text{sonst} \end{cases}$$

Behauptung: $\tau * H \neq H * \tau$

$$\sigma(k) = \begin{cases} 1 & \text{für} \quad k = 2 \\ 2 & \text{für} \quad k = 1 \\ k & \text{sonst} \end{cases}$$

$\succ \sigma(n) = n \succ \sigma \in H \succ \tau \circ \sigma \in \tau * H$
Behauptung: $\tau \circ \sigma \notin H * \tau$
Nach Definition von τ und σ ist $\tau \circ \sigma(2) = \tau(1) = n$
Sei $\rho \in H$
$\rho \circ \tau(2) = \rho(2) \neq \rho(n) = n$
$\succ$ Für alle $\rho \in H$ ist $\rho \circ \tau(2) \neq n$
$\succ \tau \circ \sigma \notin H * \tau$

Ist H ein Normalteiler von G, dann schreibt man auch
$H \lhd G$

Beispiel:
Sei $(G, *, e)$ kommutativ und $H < G \succ H \lhd G$

Beweis:
Sei $a \in G \succ a * H = \{a * x | x \in H\} \overset{kommutativ}{=} \{x * a | x \in H\} = H * a$

Satz 2.0.5 *Sei G eine Gruppe und $H \lhd G$.*
Dann gibt es eine Gruppe G/H und einen Homomorphismus $\phi : G \to G/H$ mit $Kern(\phi) = H$ und $Bild(\phi) = G/H$.

Beweis:
$G/H = \{a * H | a \in G\}$

G	$H = eH$		aH		bH	

Seien $S_1, S_2 \subseteq G$, dann sei $S_1 * S_2 = \{x * y | x \in S_1, y \in S_2\}$
Behauptung 1: $(a * H) * (b * H) = (a * b) * H$

Beweis:

"$\subseteq$" Sei $c \in a * H$ und $d \in b * H$ z.z. $c * d \in (a * b) * H$

Seien $x, y \in H$ mit $c = a * x$ und $d = b * y$

$x * b \in H * b = b * H$

$\succ$ Es gibt $z \in H$ mit $x * b = b * z$

$\succ c * d = a * x * b * y = a * b * \underbrace{z * y}_{\in H} = a * b * H$

"$\supseteq$" Sei $c \in a * b * H$ z.z. $c \in (a * H) * (b * H)$

$c \in a*b*H \succ$ Es gibt $z \in H$ mit $c = a*b*z = \underbrace{a * e}_{\in a*H} * \underbrace{b * z}_{\in b*H} \in (a*H)*(b*H)$

Behauptung 2: $(G/H, *, H)$ ist eine Gruppe.

Beweis:

$H = e * H \in G/H$

Sei $a \in H, b * H \in G/H \succ (a * H) * (b * H) = (a * b) * H \in G/H$

1. Seien $a * H, b * H, c * H \in G/H$

   $a * H * (b * H * c * H)$

   $= (a * H)(b * c * H)$

   $= (a * (b * c)) * H$

   $= ((a * b) * c) * H$

   $= (a * H * b * H) * c * H$

2. Sei $a \in a * H$

   $\succ a * H * H = a * H * e * H = (a * e) * H = a * H$

3. $a * H * a^{-1} * H = (a * a^{-1}) * H = e * H = H$

   Sei $\phi : \begin{cases} G & \to & G/H \\ a & \mapsto & a * H \end{cases}$

Behauptung 3: ϕ ist ein Homomorphismus

Beweis: $\phi(a) * \phi(b) = a * H * b * H \overset{Behauptung 1}{=} a * b * H = \phi(a * b)$

Behauptung 4: $Kern(\phi) = H$

Beweis:

"$\subseteq$" $a \in Kern(\phi) \succ \phi(a) = H \succ a * H = H \succ a = a * e \in a * H = H$

"$\supseteq$" Sei $a \in H \succ a * H \cap H \neq \emptyset \succ a * H = H \succ \phi(a) = a * H = H$

$\succ a \in Kern(\phi)$

Behauptung 5: $Bild(\phi) = G/H$

Beweis: Sei $a * H \in G/H \succ \phi(a) = a * H \succ a * H \in Bild(\phi)$

Beispiel:

Sei $(G, *, e) = (\mathbb{Z}, +, 0)$

Sei $n \in \mathbb{Z}$ und sei

$H = (n) = \{z * n | z \in \mathbb{Z}\}$

Dann ist:

1. $a + H = \{a + z * n | n \in \mathbb{Z}\} = \{b | b \equiv a \ mod \ n\} =: \overline{a}$
2. $G/H = \{a + H | a \in \mathbb{Z}\} = \{\overline{a} | a \in \mathbb{Z}\} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \cdots, \overline{n-1}\} =: \mathbb{Z}_n$

3. Seien $\overline{a}, \overline{b} \in \mathbb{Z}_n$. Dann gilt:
   $\overline{a} + \overline{b} = (a + H) + (b + H) = (a + b) + H = \overline{a + b}$

Sei G eine Gruppe und $N \lhd G$. ($N \lhd G$, d.h. für alle $a \in G$ ist $a * N = N * a$)
Sei $G/N = \{a * N | a \in G\}$
a*N*b*N=a*b*N
Dann ist $(G/N, *, N)$ ist eine Gruppe.
G/N heißt auch Faktorgruppe von G nach N.
Wir hatten gezeigt:

$$\phi : \begin{cases} G & \to & G/N \\ a & \mapsto & a * N \end{cases}$$

ist ein Homomorphismus mit $Kern(\phi) = N$ und $Bild(\phi) = G/N$.

Folgerung 2.0.3 *Ist $\phi : G \to G'$ ein Homomorphismus, dann sind $G/Kern(\phi)$ und $Bild(\phi)$ isomorph.*

Beweis:

Sei $N = Kern(\phi)$. Dann ist $N \lhd G$.

Sei $\overline{\phi} : \begin{cases} G/N & \to & Bild(\phi) \\ a * N & \mapsto & \phi(a) \end{cases}$

Behauptung 1: $\overline{\phi}$ ist "wohldefiniert" z.z. $a * N = b * N \succ \phi(a) = \phi(b)$
(meint: ϕ ist Abbildung, Anm. des Schreiberlings)

Beweis:

$a * N = b * N$
gdw. $a * b^{-1} \in N = Kern(\phi)$
gdw. $\phi(a * b^{-1}) = e$
gdw. $\phi(a) * \phi(b)^{-1} = e$
gdw. $\phi(a) = \phi(b)$

Behauptung 2: $\overline{\phi}$ ist injektiv.

Beweis:

Es genügt z.z. $Kern(\phi) = \{N\}$
Sei $a * N \in Kern(\overline{\phi})$
$\succ \overline{\phi}(a * N) = \phi(a) = e$
$\succ a \in Kern(\phi) = N$
$\succ a * N = N$
$\succ Kern(\phi) = \{N\}$

Behauptung 3: $\overline{\phi}$ ist surjektiv

Beweis:

Sei $\phi(a) \in Bild(\phi)$
Dann ist $\overline{\phi}(a * N) = \phi(a)$ und somit hat $\phi(a)$ ein Urbild.

3 Spezielle Gruppen

3.1 Zyklische Gruppen

Eine Gruppe G heißt zyklisch, wenn es einen Homomorphismus ϕ von $(\mathbb{Z}, +, 0)$ auf G gibt.

Beispiel: $(\mathbb{Z}, +, 0)$ ist eine zyklische Gruppe.
Beweis: $id_z : \left\{ \begin{array}{ccc} \mathbb{Z} & \to & \mathbb{Z} \\ a & \mapsto & a \end{array} \right.$ ist Homomorphismus auf $\mathbb{Z}$

Beispiel:
Sei $n \in \mathbb{Z}, n \geq 0$
Sei $(n) = \{x * n | x \in \mathbb{Z}\}$.
Dann ist $\phi : \left\{ \begin{array}{ccc} \mathbb{Z} & \to & \mathbb{Z}_n \\ a & \mapsto & \overline{a} = \{b | a \equiv b \ mod \ n\} \end{array} \right.$ ein Homomorphismus von $\mathbb{Z}$ auf $\mathbb{Z}_n$.
Also ist $\mathbb{Z}_n$ zyklisch.

Satz 3.1.1 *Ist $\phi : \mathbb{Z} \to G$ ein Homomorphismus. Dann ist $Kern(\phi)$ ein Ideal in $\mathbb{Z}$.*

Beweis:
$Kern(\phi)$ ist eine Untergruppe von $(\mathbb{Z}, +, 0) \succ$
(1) $0 \in Kern(\phi)$
(2) $a, b \in Kern(\phi) \succ a + b \in Kern(\phi)$
Bleibt z.z:
(3) $x \in \mathbb{Z}$ und $a \in Kern(\phi) \succ x * a \in Kern(\phi)$
Beweis:
I.Fall: $x \geq 0$
$x * a = \underbrace{a + a + \cdots + a}_{x-mal} \in Kern(\phi)$
II.Fall: $x < 0 \succ -x > 0 \succ -x * a \in Kern(\phi)$
$\overset{Kern(\phi) Gruppe}{\succ} x * a = -(-x * n) \in Kern(\phi)$

Folgerung 3.1.1 *Ist G eine zyklische Gruppe, dann gibt es $n \geq 0$ und G ist isomorph zu $\mathbb{Z}_n$.*

Beweis:
Sei $\phi : \mathbb{Z} \underset{auf}{\longrightarrow} G$ ein Homomorphismus. Dann ist
$G = Bild(\phi) \approx \mathbb{Z}/Kern(\phi)$.
$Kern(\phi)$ ist ein Ideal $\succ$ Es gibt $n \geq 0$ mit $Kern(\phi) = (n) \succ G \approx \mathbb{Z}/(n) = \mathbb{Z}_n$.

Bemerkung 3.1.1 *Jede zyklische Gruppe ist kommutativ.*

Beweis:
Sei $\phi : (\mathbb{Z}, +, 0) := \mathbb{Z} \underset{auf}{\longrightarrow} G := (G, *, e)$ ein Homomorphismus.
Seien $\phi(n), \phi(m) \in G$
$\succ \phi(n) * \phi(m) \overset{homomorph}{=} \phi(n + m) = \phi(m + n) \overset{homomorph}{=} \phi(m) * \phi(n)$

Lemma 3.1.1 *Sei G eine Gruppe und $a \in G$. Dann gibt es genau einen Homomorphismus von $(\mathbb{Z}, +, 0)$ in $(G, *, e)$ mit $\phi(1) = a$.*

Beweis:

"Existenz:"

Wir definieren ϕ wie folgt:

$\phi(0) = e$

$\phi(n+1) = \phi(n) * a$ für $n \geq 0$

$\phi(-n) = -\phi(n)$ für $n < 0$

Man rechnet nach: ϕ ist Homomorphismus.

"Eindeutigkeit"

I.Fall: $n = 0 \succ \phi(0) = e = \psi(0)$

II.Fall: $n > 0$.

$\succ \phi(n) = \phi((n-1)+1) \overset{homomorph}{=} \phi(n-1) * \phi(1)$

$= \phi(n-1) * a \overset{Induktionsvoraussetzung}{=} \psi(n-1) * a = \cdots = \psi(n)$

III.Fall: $n < 0$

$\succ -n > 0 \succ \phi(-n) = \psi(-n)$

$\succ \phi(n) = \phi(-(-n)) = \phi(-n)^{-1} = \psi(-n)^{-1} * \cdots = \psi(n)$

Sei G eine Gruppe, $a \in G$ und $\phi : \mathbb{Z} \to G$ ein Homomorphismus mit $\phi(1) = a$, dann schreibt man a^n für $\phi(n)$. Statt $Bild(\phi)$ schreibt man auch $< a >$.

2 Fälle können eintreten:

I.Fall: $Kern(\phi) = \{0\}$

Dann ist $< a > \approx \mathbb{Z}$. Man sagt a hat unendliche Ordnung.

(geschrieben: $ord(a) = \infty$)

Beispiel: $G = (\mathbb{Q} \setminus \{0\}, *, 1)$ Sei $a = \frac{1}{2}$.

Dann ist $\mathbb{Z} \approx < a > = \{\cdots 4, 2, 1, \frac{1}{2}, \frac{1}{4} \cdots\}$

II.Fall: $Kern(\phi) \neq \{0\}$

Dann gibt es ein $n > 0$ mit $Kern(\phi) = n$. Dann ist $< a > \approx \mathbb{Z}_n$.

Man sagt dann: a hat die Ordnung n (geschrieben: $ord(a) = n$)

Folgerung 3.1.2 *Ist G eine endliche Gruppe und $a \in G$.*
Dann gilt: $ord(a) \mid |G|$.

Beweis:

Sei $\phi : \mathbb{Z} \to G$ der Homomorphismus mit $\phi(1) = a$.

Da $Bild(\phi) = < a >$ eine Untergruppe von $G \succ |G : < a > | * | < a > = G$

$\succ < a > \mid |G|$. Es gilt: $ord(a) = | < a > | \succ ord(a) \mid G$.

Wir hatten gezeigt:

Ist G eine endliche Gruppe und $a \in G$, dann gilt:

$ord(a)$ *teilt* $|G|$.

Folgerung 3.1.3 *Ist p eine Primzahl und $|G| = p$, dann ist $G \approx \mathbb{Z}_p$.*

Beweis:

Sei $a \in G \setminus \{e\} \succ ord(a) > 1$
$ord(a)$ teilt $|G| = p \succ ord(a) = p$
$\succ | < a > | = p \succ < a > \approx \mathbb{Z}_p$
$| < a > | \subseteq G$ und $|G| = p \succ < a > = G$

3.2 Abelsche Gruppen

Eine Gruppe G heißt abelsch, wenn für alle a, b gilt:

$$a * b = b * a$$

Lemma 3.2.1 *Sei G eine endliche Gruppe und $N \lhd G$.*
Besitzt G/N ein Element mit Ordnung p, p Primzahl, so auch G.

Beweis:

Sei $\phi : \begin{cases} G & \to & G/N \\ a & \mapsto & a * N \end{cases}$

Nach Voraussetzung gibt es ein $a * N \in G/N$ mit $ord(a * N) = p$

Da G endlich ist, ist $ord(a) = n \in \mathbb{N}$

Beh: $p|n$

Bew:

$p \nmid n \succ ggT(p, n) = 1 \succ 1 = x * p + y * n$

$\succ a = a^1 = a^{x*p+y*n} = (a^p)^x * (\underbrace{a^n}_{=e})^y$

$\succ a = a^{p*x}$

$\succ \phi(a) = \phi(a^{p*x}) = \phi(a)^{p*x} = e^x = e$

$\succ ord(\phi(a)) = 1 \quad \lightning$

Sei $n = l * p$. Sei $b = a^l . \succ b^p = a^{l*p} = a^n = e \succ ord(b) = p$

Satz 3.2.1 *Ist G eine endliche abelsche Gruppe und p eine Primzahl mit $p|\ |G|$, dann gibt es ein $a \in G$ mit $ord(a) = p$*

Beweis:(volständige Induktion über $|G|$)

Ist $|G| = 1 \quad \surd$

Sei $|G| > 1$. Sei $a \in G \setminus \{e\}$ und $K = ord(a)$.

I. Fall: $p|k$

$\succ k = l * p$

Sei $b = a^l \succ ord(b) = p$

II. Fall: $p \nmid k$

Sei $< a >$ die von a erzeugte Untergruppe. Da G abelsch ist, ist $< a > \lhd G$

$\succ |G/ < a > | < |G|$

Es gilt: $|G| = |G/ < a > | * | < a > |$

Da $p \nmid | < a > | = ord(a) \succ p$ teilt $|G/ < a > |$

$\overset{Induktionsvoraussetzung}{\succ}$ $|G/ < a > |$ besitzt ein Element der Ordnung p.

Nach dem Lemma von Seite 29 besitzt G ein Element der Ordnung p.

Sei G eine abelsche Gruppe und $r \in \mathbb{N}$, dann sei

$$G_r = \{a | a^r = e\}$$

Satz 3.2.2 *Sei G endlich und abelsch mit $G = r * s$.*
Ist $ggT(r, s) = 1$, dann gilt:

1. $G_r \cap G_s = \{e\}$
2. $G = G_r * G_s$

Beweis:

zu 1: Sei $a \in G_r \cap G_s$

Da $ggt(r,s) = 1$, gibt es $x, y \in \mathbb{Z}$ mit $1 = x * r + y * s$

$a = a^1 = a^{x*r+y*s} = \underbrace{(a^r)^x}_{=e} * \underbrace{(a^s)^y}_{=e} = e$

$\succ G_r \cap G_s = \{e\}$

zu 2: Sei $a \in G$.

Da $ggT(r,s) = 1$

$\succ 1 = x * r + y * s$

$a = a^{x*r+y*s} = a^{r*x} * a^{s*y}$

Sei $a_1 = a^{r*x}$ und $a_2 = a^{s*y}$

Da $a_1^s = a^{r*x*s} = e \succ a_1 \in G_s$

Da $a_2^r = e \succ a_2 \in G_r$

Folgerung 3.2.1 *Sei G eine abelsche Gruppe mit $|G| = r * s$ und $ggT(r,s) = 1$, dann ist*

$$G \approx G_r \times G_s$$

Beweis:

$G_r \times G_s = \{(a,b) | a \in G_r \text{ und } b \in G_s\}$

$(a,b) * (c,d) = (a * c, b * d)$

Dann ist $(G_r \times G_s, *, (e,e))$ eine Gruppe.

Sei $\phi := \begin{cases} G_r \times G_s & \to & G \\ (a,b) & \mapsto & a * b \end{cases}$

1. ϕ ist Homomorphismus

$\phi((a,b) * (c,d)) = \phi((a * c, b * d)) = a * c * b * d$

$\overset{abelsch}{=} a * b * c * d = \phi((a,b)) * \phi((c,d))$

2. ϕ ist injektiv

z.Z. $Kern(\phi) = \{(e,e)\}$

Beweis:

$\phi((a,b)) = e$

$\succ a * b = e$

$\succ \underbrace{a}_{\in G_r} = \underbrace{b^{-1}}_{\in G_s} \in G_s \cap G_r = \{e\}$

$\succ (a,b) = (e,e)$

3. ϕ ist surjektiv

Beweis:

$G_r * G_s = G$

Folgerung 3.2.2 *Ist G eine abelsche Gruppe mit $|G| = r * s$ mit $ggT(r,s) = 1$, dann $|G_r| = r$ und $|G_s| = s$*

Beweis:

$r * s = |G| = |G_r \times G_s| = |G_r| * |G_s|$

Es genügt zu zeigen:

Ist p eine Primzahl, mit $p|r \succ p \nmid |G_s|$

Angenommen $p|\ |G_s|$. Dann gibt es ein $a \in G_s \setminus \{e\}$ mit $ord(a) = p \succ a^p = e$.

Da $p|r \succ a^r = e \succ a \in G_r \succ a \in G_r \cap G_s \succ a = e$ $\sharp$

Beispiel:

Ist G eine abelsche Gruppe mit $|G| = 15 \succ G \approx \mathbb{Z}_3 \times \mathbb{Z}_5$

Beweis:

$15 = 3 * 5$ mit $ggT(3,5) = 1$

Also gibt es G_3 und G_5 mit $G \approx G_3 \times G_5$ (Folgerung von Seite 30)

$|G_3| = 3$ und $|G_5| = 5$ (Folgerung von Seite 30)

Nach der Folgerung von Seite 27 $\succ G_3 \approx \mathbb{Z}_3$ $G_5 \approx \mathbb{Z}_5$

$\succ G \approx \mathbb{Z}_3 \times \mathbb{Z}_5$

3.3 Klassengleichungen

Sei G eine Gruppe, dann heißt

$$Z(G) := \{a | \text{Für alle } x \in G \text{ ist } a * x = x * a\}$$

Zentrum von G.

Bemerkung 3.3.1

1. $Z(G) \lhd G$

2. $Z(G)$ *ist abelsch*

Sei $a \in G$, dann heißt

$$C(a) := \{x | x * a = a * x\}$$

Zentralisator von a.

Bemerkung 3.3.2

1. $C(a) < G$

2. $C(a) = G$ *gdw* $a \in Z(G)$

Seien $s, b \in G$, dann heißt a konjugiert zu b, wenn es ein $x \in G$ gibt, mit $b = x * a * x^{-1}$(geschrieben: $a \sim b$)

Lemma 3.3.1 $\sim$ *ist eine Äquivalenzrelation.*

Beweis:

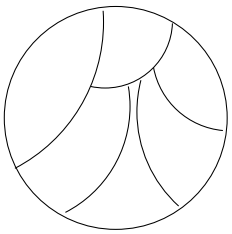
1. $a \sim a$, da $a = e * a * e^{-1}$
2. $a \sim b \succ b \sim a$
   $a \sim b \succ$ Es gibt x mit $b = x * a * x^{-1} \succ a = x^{-1} * b * (x^{-1})^{-1} \succ b \sim a$
3. $a \sim b$ und $b \sim c$, dann ist $a \sim c$
   $b = x * a * x^{-1}$
   $c = y * b * y^{-1} = y * x * a * x^{-1} * y^{-1} = (y * x) * a * (y * x)^{-1} \succ a \sim c$

Seien $a, b \in G$. a und b heißen konjugiert, wenn es ein x gibt mit:

$$b = x * a * x^{-1}$$

(geschrieben: $a \sim b$)

Wir hatten gezeigt $\sim$ ist Äquivalenzrelation.
$\tilde{a} = \{b | b \sim a\}$



$Z(G) = \{a |\ |\tilde{a}| = 1\}$

Wir hatten

$$C(a) := \{x | x * a = a * x\}$$

den Zentralisator von a genannt.

Lemma 3.3.2 *Sei $a \in G$, dann ist*
$|\{x * a * x^{-1} | x \in G\}| = |\tilde{a}| = |G : C(a)| = |\{x * C(a) | x \in G\}|$

Beweis:

Sei $f : \begin{cases} \{x * C(a) | x \in G\} & \to & \{x * a * x^{-1} | x \in G\} \\ x * C(a) & \mapsto & x * a * x^{-1} \end{cases}$

Behauptung 1: f ist wohldefiniert

$x * C(a) = y * C(a)$, z.Z. $x * a * x^{-1} = y * a * y^{-1}$

Da $x * C(a) = y * C(a)$

$\succ x^{-1} * y \in C(a)$

$\succ a * x^{-1} * y = x^{-1} * y * a$

$\succ x * a * x^{-1} = y * a * y^{-1}$

Behautpung 2: f ist injektiv

$f(x * C(a)) = f(y * C(a))$, z.Z. $x * C(a) = y * C(a)$

$f(x * C(a)) = f(y * C(a))$

$\succ x * a * x^{-1} = y * a * y^{-1}$

$\succ x^{-1} * y * a = a * x^{-1} * y$

$\succ x^{-1} * y \in C(a)$

$\succ x * C(a) = y * C(a)$

Behauptung 3: f ist surjektiv

Sei $b \in \tilde{a}$. Dann gibt es x mit $b = x * a * x^{-1}$

$\succ f(x * C(a)) = x * a * x^{-1} = b$

Satz 3.3.1 *(Klassengleichung)*
Sei G eine endliche Gruppe, dann gibt es $S \subseteq G$ mit $S \cap Z(G) = \emptyset$ und

$$|G| = |Z(G)| + \sum_{a \in S} |G : C(a)|$$

Beweis:

$G = \bigcup_{a \in G} \tilde{a}$

Sei $T \subseteq G$ mit:

1. $\bigcup_{a \in T} \tilde{a} = G$
2. $a, b \in T$ und $a \neq b \succ \tilde{a} \cup \tilde{b} = \emptyset$

Dann $|G| = \sum_{a \in T} |\tilde{a}|$

Sei $S = \{a | a \in T \text{ mit } |\tilde{a}| > 1\}$

$\succ |G| = |Z(G)| + \sum_{a \in S} |\tilde{a}|$

$\succ |G| = |Z(G)| + \sum_{a \in S} |G : C(a)|$

Satz 3.3.2 *Ist G eine endliche Gruppe und p eine Primzahl mit $p \mid |G|$, dann gibt es ein $a \in G$ mit $ord(a) = p$.*

Beweis:(Induktion über $|G|$)

1. $|G| = 1$ $\quad \surd$

2. Sei $|G| > 1$

   I.Fall: $p| \ |Z(G)|$. Da $Z(G)$ eine abelsche Gruppe ist,
   gibt es ein $a \in Z(G) \subseteq G$ mit $ord(a) = p$

   II.Fall: $p \nmid |Z(G)|$. Es gibt $S \subseteq G$ mit $|G| = |Z(G)| + \sum_{a \in S} |G : C(a)|$.
   Da $p| \ |Z(G)| \succ$ Es gibt ein $a \in S$ mit $p \nmid |G : C(a)|$
   Da $|G| = |G : C(a)| * |C(a)| \succ p| \ |C(a)|$.
   Da $|C(a)| < |G|$ gibt es nach Induktionsvoraussetzung
   ein $b \in C(a)$ mit $ord(b) = p$.

3.4 p-Gruppen

Sei p eine Primzahl. G heißt p-Gruppe, wenn es ein n gibt mit
$$|G| = p^n$$

Beispiel für 2-Gruppen:
$\mathbb{Z}_1$, $\mathbb{Z}_2$, $\mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, D_4

Lemma 3.4.1 *Ist G eine p-Gruppe, dann ist*
$$Z(G) \neq \{e\}$$

Beweis:
Sei $S \subseteq G$ mit $S \cap Z(G) = \emptyset$
$|G| = |Z(G)| + \sum_{a \in S} |G : C(a)|$

Behauptung 3.4.1 *Ist $a \in S \succ p|\ |G : C(a)|$*

Beweis:
$p^n = |G| = |G : C(a)| * |C(a)|$
Da $a \notin Z(G) \succ |C(a)| < |G| = p^n \succ p|\ |G : C(a)|$

Satz 3.4.1 *Ist $|G| = p^2$, dann ist $G \approx \mathbb{Z}_{p^2}$ oder $G \approx \mathbb{Z}_p \times \mathbb{Z}_p$*

Beweis:
I. Fall: Es gibt $a \in G$ mit $ord(a) = p^2$
Dann $G \approx \mathbb{Z}_{p^2}$
II. Fall: sonst
Sei $a \in Z(G) \setminus \{e\}$
$\succ ord(a)|\ |G| = p^2$
$\succ ord(a) = p$.
Sei $< a >= \{e, a, \cdots, a^{p-1}\}$
Da $< a > \subseteq Z(G) \succ < a > \lhd G$
Da $|G| = \underbrace{|G :< a > |}_{= G/<a>} * < a > \succ p = |G :< a > | = |G/ < a > |$
$\succ G/ < a > \approx \mathbb{Z}_p$. Sei $b * < a > \in G/ < a >$ mit $< b < a >> = G/ < a >$
Gesucht ist $f : G \xrightarrow[auf]{1-1} \mathbb{Z}_p \times \mathbb{Z}_p$,f Homomorphismus
Sei $c \in G$, dann gibt es genau ein i_c mit
$$c * < a >= b^{i_c} * < a >$$
Da $c \in b^{i_c} * < a >$, gibt es genau ein k_c mit $c = b^{i_c} * a^{k_c}$
Sei $f : \begin{cases} G & \to & \mathbb{Z}_p \times \mathbb{Z}_p \\ c & \mapsto & (\overline{i_c}, \overline{k_c}) \end{cases}$

Wir wollen zeigen:
Ist G eine Gruppe mit $|G| = p^n$, dann gibt es ein $H \lhd G$ mit $|H| = p^{n-1}$

Lemma 3.4.2 *Ist $N \lhd G$ und $H \lhd G/N$. Dann ist $\bigcup H \lhd G$ und $|\bigcup H| = |H| * |N|$*

Behauptung 1: $a \in \bigcup H$ gdw. $a * N \in H$

Beweis: $a \in \bigcup H$

gdw. Es gibt $b * N \in H$ mit $a \in b * H$

gdw. Es gibt ein $b * N \in H$ mit $a * N = b * N$

gdw. $a * N \in H$

Behauptung 2: $\bigcup H \subset G$

Beweis:

$e \in N \in H \succ e \in \bigcup H$

$a, b \in \bigcup H \succ a * N, b * N \in H$

$a * b^{-1} * N = a * N * b^{-1} * N \in H$

$a * b^{-1} \in a * b^{-1} * N \in H \succ a * b^{-1} \in \bigcup H$

Behautpung 3: $\bigcup H \lhd G$

"Ich hab´ keine Lust mehr das Nachzurechen !" (Podewski)

Behauptung 4: $|\bigcup H| = |H| * |N|$

Satz 3.4.2 *Sei G eine p-Gruppe mit $|G| = p^n$ mit $n \geq 1$. Dann gibt es ein $H \lhd G$ und $|H| = p^{n-1}$.*

Beweis: (Induktion über n)

Da G eine p-Gruppe ist, ist $Z(G) \neq \{e\}$. Da $p|G \succ p|Z(G)$.

Also gibt es $a \in Z(G)$ mit $ord(a) = p$. Dann $| < a > | = p$.

Da $< a >< Z(G) \succ < a > \lhd G$.

$n = 1$: Dann sei $H = \{e\}$.

$n > 1$: Dann ist $|G/ < a > | = p^{n-1}$.

Also gibt es ein $H \lhd G/ < a >$ mit $|H| = p^{n-2}$.(Induktionsvoraussetzung)

$\succ |\bigcup H| = |H| * | < a > | = p^{n-1}$ und $\bigcup H \lhd G$

Eine Gruppe G heißt auflösbar, wenn es Gruppen $H_0, \cdots, H_n$ gibt mit:

1. $H_0 = G$, $H_2 = \{e\}$
2. $H_{i+1} \lhd H_i$
3. H_{i+1}/H_i ist zyklisch

Folgerung 3.4.1 *Jede p-Gruppe ist auflösbar.*

Beweis: (Induktion über n)

Sei $|G| = p^n$.

$n = 0$: $H_0 = G = \{e\}$.

$n = 1$: $H_1 = G$ und $H_0 = \{e\}$.

Da $|G| = p$, ist $G/H_0 \approx G \approx \mathbb{Z}_p$.

$n > 1$: Dann gibt es nach dem Satz von Seite 36 einen

Normalteiler $H_1 \lhd G$ mit $|H_1| = p^{n-1}$

$\succ G/H_1 = H_0/H_1$, $H_0 = G$.

$\succ G/H_1 = H_0/H_1 \approx \mathbb{Z}_p$.

Nach Induktionsvoraussetzung gibt es $H_2, \cdots, H_n$ mit $H_{i+1} \lhd H_i$ für $i \geq 1$ und H_i/H_{i+1} ist zyklisch.

3.5 Permutationsgruppen

$S_n := \{\sigma | \sigma : \{1, \cdots, n\} \xrightarrow[auf]{1-1} \{1, \cdots, n\}\}$.
Ziel: S_n ist nicht auflösbar für $n \geq 5$.

Lemma 3.5.1 *Sei $n \geq 2$ und $H < S_n$. Enthält H alle Transpositionen, dann $H = S_n$.*

Beweis: (siehe Lineare Algebra)

Lemma 3.5.2 *Sei $n \geq 5$ und $H < S_n$, die alle Dreier-Zykeln enthält.*
Ist $N \lhd H$ und H/N abelsch, dann enthält N alle Dreier-Zykeln.

Beweis:

Da H/N kommutativ ist, gilt σ,$\tau \in H$: $\sigma N \tau N = \tau N \sigma N$
$\succ \sigma\tau N = \tau\sigma N \succ \sigma\tau(\tau\sigma)^{-1} \in N \succ \sigma\tau\sigma^{-1}\tau^{-1} \in N$.
Sei (i, j, k) ein Dreier-Zyklus. Wir wollen zeigen:
$(i, j, k) = N$.
Da $n \geq 5$, gibt es r, s; $r \neq s$; $r, s \in \{1, \cdots, n\} \setminus \{i, j, k\}$.
Sei $\sigma = (k, r, j)$ und sei $\tau = (j, i, s)$.
$\sigma\tau\sigma^{-1}\tau^{-1} \in N$.

Behauptung 3.5.1 $(i, j, k) = \sigma\tau\sigma^{-1}\tau^{-1}$

Beweis:

$\sigma\tau\sigma^{-1}\tau^{-1} = (k, r, j) * (j, i, s) * (j, r, k) * (s, i, j)$
$j \xrightarrow{\tau^{-1}} s \xrightarrow{\sigma^{-1}} s \xrightarrow{\tau} j \xrightarrow{\sigma} k$
$k \to k \to j \to i \to i$
$i \to j \to r \to r \to j$
$s \to i \to i \to s \to s$
$r \to r \to k \to k \to r$

Satz 3.5.1 *Ist $n \geq 5$, dann ist S_n nicht auflösbar.*

Beweis:

Angenommen S_n ist auflösbar, dann gibt es $H_0, \cdots, H_n$:
1. $H_0 = S_n$, $H_n = \{id\}$
2. $H_{i+1} \lhd H_i$
3. H_i/H_{i+1} ist zyklisch und damit abelsch.

Wir zeigen durch Induktion über i:
H_i enthält alle Dreier-Zykeln.
$n = 0 : \succ H_o = S_n$ $\surd$
Nach Induktionsvoraussetzung enthält H_i alle Dreier-Zykeln.
Da $H_{i+1} \lhd H_i$ und H_i/H_{i+1} abelsch ist, enthält H_{i+1} alle Dreier-Zykeln nach dem +Lemma von Seite 37.
$\succ H_n$ enthält alle Dreier-Zykeln. $\sharp$

Wir werden zeigen: $x^5 - 80 * x + 2 = 0$ oder $2 * x^5 - 10 * x + 5 = 0$ ist nicht durch Wurzelziehen lösbar.

Dazu werden wir benutzen:

Ist $H < S_5$ mit:

1. H enthält alle Transpositionen
2. $5| \ |H|$

Dann ist $H = S_5$.

Lemma 3.5.3

Ist $H \lhd S_n$ und $(i_1, \cdots, i_n)$ n-Zyklus mit:

1. $(i_1, \cdots, i_n) \in H$

2. $(i_1, i_2) \in H$

Dann ist $H = S_n$.

Beweis:

Behauptung 1: $(i_k, i_{k+1}) \in H$ für $1 \leq k < n$

Beweis: (Induktion über k)

$k = 1$ $\surd$

Induktionsvoraussetzung: Sei $(i_{k-1}, i_k) \in H \succ \sigma(i_{k-1}, i_k) * \sigma^{-1} \in H$

$\succ \sigma(i_{k-1}, i_k) * \sigma^{-1} = (i_1, \cdots, i_n) * (i_{k-1}, i_k) * (i_n, \cdots, i_1) = (i_k, i_{k+1})$

Behauptung 2: $(i_k, i_l) \in H$ für $1 \leq k \leq l \leq n$.

Beweis: (induktion über $l - k$)

Ist $l - k = 1 \succ$ Behauptung 1 $\surd$

Sei $l - k > 0$. Nach Induktionsvoraussetzung ist $(i_k, i_{l-1}) \in H$

Nach Behauptung 1 ist $(i_{l-1}, i_l) \in H$

$\succ H \ni (i_{l-1}, i_l) * (i_k, i_{l-1}) = (i_k, i_l)$.

Also ist nach dem Lemma von Seite 37: $H = S_n$

Wir wollen zeigen:

Sei p Primzahl und $H < S_p$, und gilt:

1. H enthält eine Transposition
2. $p| \ |H|$

Dann gilt $H = S_p$.

Wir hatten gezeigt:

Ist $H < S_n$ und $(i_1, i_2, \cdots, i_n)$ ein n-Zyklus mit

1. $(i_1, \cdots, i_n) \in H$
2. $(i_1, i_2) \in H$

Dann $H = S_n$.

Lemma 3.5.4 *Sei $\sigma \in S_p$ mit $ord(\sigma) = p$ und sei $1 \leq i \leq p$.*
Dann ist $\{\sigma^l(i) | 0 \leq l < p\} = \{1, \cdots, p\}$.

Beweis:

Behauptung 1: Ist $1 \leq i \leq p$ und $0 \leq l < p$ mit $\sigma^l(i) = i$, dann ist $\sigma(i) = i$

Beweis:

Da $ggT(l,p) = 1$, gibt es x und y mit $1 = x * l + y * p$
$\sigma(i) = \sigma^1(i) = \sigma^{x*l+y*p}(i) = \sigma^{x*l} \circ \sigma^{y*p}(i)$
$= \sigma^{x*l} * (\sigma^p(i))^y = (\sigma^l(i))^x = i$

Behauptung 2: $|\{\sigma^l(i)|0 \leq l < p\}| < p$, dann gibt es ein i mit $\sigma(i) = i$.

Beweis:

Seien $l \neq k$ mit $0 \leq l < k < p$ mit $\sigma^l(i) = \sigma^k(i)$
$\succ \sigma^{l-k}(i) = i \overset{Behauptung1}{\succ} \sigma(i) = i.$

Behauptung 3: $|\{\sigma^k(i)|0 \leq l < p\}| = p$

Beweis:

Angenommen nicht. Dann gibt es ein i mit $\sigma(i) = i$.
Dann gibt es für jedes l $\sigma^l(i) = i$.
Dann ist für jedes j mit $1 \leq j \leq p$
$|\{\sigma^l(j)|o \leq j < p\}| < |p|$
$\overset{Behauptung2}{\succ}$ $\sigma(j) = j$ für alle j, $1 \leq j \leq p$
$\succ \sigma = id \succ ord(\sigma) = 1$ $\sharp ord(\sigma) = p$

Satz 3.5.2 *Sei p eine Primzahl und $H < S_p$ mit:*

1. H enthält eine Transposition

2. $p|\ |H|$

Dann $H = S_P$

Beweis:

Sei $(i_1, i_2) \in H$ eine Transposition.
Da $p|\ |H|$ gibt es ein σ mit $ord(\sigma) = p$.
Dann ist $\{\sigma^l(i_1)|0 \leq l < p\} = \{1, \cdots, p\}$.
Also gibt es ein l mit
$\sigma^l(i_1) = i_2$ mit $0 < l < p$
Da $ggT(l,p) = 1 \succ ord(\sigma^l) = p$
Also ist $\{\sigma^{l*x}(i_1)|0 \leq x < p\} = \{1, \cdots, p\}$
Sei $i_{x+1} = \sigma^{l*x}(i_1)$ für $2 \leq x < p$ dann $\sigma^l = (i_1, i_2, \cdots, i_p) \in H$
Also ist nach dem Lemma von Seite 38 $H = S_p$

4 Ringe

4.1 Definitionen

$(R, +, *, 0, e)$ heißt (kommutativer) Ring, wenn gilt:

1. $+ : R \times R \to R$
2. $* : R \times R \to R$
3. $0, e \in R$ mit $0 \neq e$

mit folgenden Eigenschaften:

1. $(R, +, 0)$ ist abelsche Gruppe
2. $a * (b * c) = (a * b) * c$
3. $e * a = a$
4. $a * b = b * a$
5. $a * (b + c) = a * b + a * c$

Ein Ring $(R, +, *, 0, e)$ heißt Körper, wenn gilt:

6. Ist $a \neq 0$, dann gibt es ein d mit $a * d = e$

Beispiele:

1. $(\mathbb{Z}, +, *, 0, 1)$ ist ein Ring
2. $(\mathbb{R}, +, *, 0, 1)$ ist ein Körper
3. $(\mathbb{Q}, +, *, 0, 1)$ ist ein Körper
4. $(\mathbb{C}, +, *, 0, 1)$ ist ein Körper
5. Sei $R = \{f | f * [a, b] \to \mathbb{R}$ und f ist stetig$\}$

   Sei $f + g : \left\{ \begin{array}{ccc} [a,b] & \to & \mathbb{R} \\ x & \mapsto & f(x) + g(x) \end{array} \right.$

   Sei $f * g : \left\{ \begin{array}{ccc} [a,b] & \to & \mathbb{R} \\ x & \mapsto & f(x) * g(x) \end{array} \right.$

   Sei $0 : \left\{ \begin{array}{ccc} [a,b] & \to & \mathbb{R} \\ x & \mapsto & 0 \end{array} \right.$

   Sei $e : \left\{ \begin{array}{ccc} [a,b] & \to & \mathbb{R} \\ x & \mapsto & 1 \end{array} \right.$

   Dann ist $(R, +, *, 0, e)$ ein Ring.

6. Seien $(R_1, +, *, 0_1, e_1)$ und $(R_2, +, *, 0_2, e_2)$ Ringe, dann sei
   $R = R_1 \times R_2 = \{a, b | a \in R_1, b \in R_2\}$
   $(a, b) + (c, d) = (a + c, b + d)$
   $(a, b) * (c, d) = (a * c, b * d)$
   $0 := (0_1, 0_2)$
   $e := (e_1, e_2)$
   Dann ist $(R_1 \times R_2, +, *, 0, e)$ ein Ring.

Lemma 4.1.1 *(weitere Rechenregeln)*

1. $0 * a = 0$
2. $(-e) * a = -a$
3. $(-e) * (-e) = e$
4. $(-x) * y = -x * y$
5. $(-x) * (-y) = x * y$

Beweis:

zu 1:
$0 * x + x = 0 * x + e * x = (0 + e) * x = e * x = x$
$\succ (0 * x + x) - x = x - x$
$\succ 0 * x = 0$

zu 2:
$(-e) * x + x = (-e) * x + e * x = (-e + e) * x = 0 * x = 0$
$\succ ((-e) * x + x) - x = 0 - x$
$\succ (-e) * x = -x$

zu 3:
$e + (-e) = 0$
$\succ (-e) * (e + (-e)) = (-e) * 0 = 0$
$\succ (-e) * e + (-e) * (-e) = 0$
$\succ (-e) + (-e) * (-e) = 0$
$\succ e - e + (-e) * (-e) = e + 0$
$\succ (-e) * (-e) = e$

zu 4:
$(-x) * y \overset{(2)}{=} ((-e) * x) * y = (-e) * (x * y) = -x * y$

zu 5:
$(-x) * (-y) = ((-e) * x) * ((-e) * y) = ((-e) * (-e)) * (x * y) \overset{(3)}{=} e * (x * y) = x * y$

Lemma 4.1.2 *Sei $(R, +, *, 0, e)$ ein Ring und $R' \subset R$ mit folgenden Eigenschaften: Sind $a, b \in R'$, dann gilt:*

1. *$-a \in R'$ und $a + b \in R'$*
2. *$e \in R'$ und $a * b \in R'$*

Dann $(R', +, *, 0, e)$ ein Ring.

Beweis:

Da $e \in R'$ ist $-e \in R' \succ 0 = e + (-e) \in R'$

Aus 1. folgt:

$(R, +, 0)$ ist eine abelsche Gruppe.

Die zusätzlichen Regeln $1, \cdots, 5$ gelten in $(R', +, *, 0, e)$, da sie in $(R, +, *, 0, e)$ gelten.

Man nennt R' Unterring von R.

Beispiele:

1. $\mathbb{Z}$ ist ein Unterring von $\mathbb{R}$
2. Sei R der Ring der stetigen Funktionen von $[a, b]$ in $\mathbb{R}$. Sei R' die Menge der differenzierbaren Funktionen aus R. Dann ist R' ein Ring.

4.2 (Ring-)homomorphismen

$(R, +, *, 0, e)$
Seien R, R' Ringe.

$\phi : R \to R'$ heißt Homomorphismus, wenn gilt:

1. $\phi(a + b) = \phi(a) + \phi(b)$
2. $\phi(a * b) = \phi(a) * \phi(b)$
3. $\phi(e) = e$

Beispiele:
Sei R der Ring der stetigen Funktionen auf $[0, 1]$
Dann ist

1. $\phi : \left\{ \begin{array}{lcl} R & \to & \mathbb{R} \\ f & \mapsto & f(\frac{1}{2}) \end{array} \right.$
2. $\phi : \left\{ \begin{array}{lcl} R_{[0,1]} & \to & R_{[0,\frac{1}{2}]} \\ f & \mapsto & f|[0,\frac{1}{2}] \end{array} \right.$

ein Ring-Homomorphismus.

Lemma 4.2.1 *Seien $\psi : R \to R'$ und $\phi : R' \to R''$ Homomorphismen.*
Dann ist $\phi \circ \psi$ ein Homomorphismus.

Beweis:
zu 2:
$$\phi\circ\psi(a*b) = \phi(\psi(a*b)) = \phi(\psi(a)*\psi(b)) = \phi(\psi(a))*\phi(\psi(b)) = \phi\circ\psi(a)*\phi\circ\psi(b)$$

Sei $\phi : R \to R'$ ein Homomorphismus, dann ist
$Bild(\phi) = \phi[R] = \{\phi(a) | a \in R\}$
$Kern(\phi) = \{a | \phi(a) = 0\}$

Lemma 4.2.2 *$Bild(\phi)$ ist Unterring von R'*

Beweis:
z.Z. ist: Seien $a, b \in Bild(\phi)$
1. $-a \in Bild(\phi)$ und $a + b \in Bild(\phi)$
2. $e \in Bild(\phi)$ und $a * b \in Bild(\phi)$

zu 2:
Da $\phi(e) = e \succ e \in Bild(\phi)$
Da $a, b \in Bild(\phi)$, gibt es $c, d \in R$ mit $\phi(c) = a$ und $\phi(d) = b$
$\succ \phi(c * d) = \phi(c) * \phi(b) = a * b$
$\succ a * b \in Bild(\phi)$

Bemerkung 4.2.1 *Ist $Kern(\phi) = \{0\}$, dann ist ϕ injektiv.*
$\phi : (R, +, 0) \to (R', +, 0)$ ist ein (Gruppen-)Homomorphismus.
Also ist ϕ injektiv.

Lemma 4.2.3 *Ist $\phi : R \to R'$ ein Homomorphismus, dann gilt:*

1. *Sind $a, b \in Kern(\phi) \succ a + b \in Kern(\phi)$*
2. *Ist $a \in R$ und $b \in Kern(\phi) \succ a * b \in Kern(\phi)$*

Beweis:

zu 1:

$b, a \in Kern(\phi)$. Dann ist $\phi(b) = 0$ und $\phi(a) = 0$

$\phi(a + b) = \phi(a) + \phi(b) = 0 + 0 = 0 \succ a + b \in Kern(\phi)$

zu 2:

Da $b \in Kern(\phi) \succ \phi(b) = 0$

$\phi(a * b) = \phi(a) * \phi(b) = \phi(a) * 0 = 0$

$\succ a * b \in Kern(\phi)$

Beispiele:

1. $\mathbb{Z}$ ist ein Unterring von $\mathbb{R}$
2. Sei R der Ring der stetigen Funktionen von $[a, b]$ in $\mathbb{R}$.
   Sei R' die Menge der differenzierbarenm Funktionen aus R.
   Dann ist R' ein Ring.

4.3 Ideale und Kongruenzen

Sei R ein Ring. $J \subseteq R$ heißt Ideal, wenn gilt:

1. $a, b \in J \succ a + b \in J$
2. $a \in J, b \in R \succ a * b \in J$
3. $0 \in J$

Beispiel:

Sei $R_{[0,1]}|f(\frac{1}{2}) = 0\}$
Sei $J = \{f \in R_{[0,1]}|f(\frac{1}{2} = 0\}$
Dann ist J ein Ideal.

Beispiel:

$\{n \in\mathbb{Z}|n$ ist gerade$\}$ ist ein Ideal in $\mathbb{Z}$

Beispiel:

Sei $n \in\mathbb{Z}$ und $(n) = \{x * n|x \in\mathbb{Z}\}$
Dann ist (n) ein Ideal in $\mathbb{Z}$.

Beispiel:

Sei R ein Ring und $a \in R$.
Dann ist $(a) = \{x * a|x \in R\}$ ein Ideal.

Beispiel:

Sei R ein Ring und $a_1, \cdots, a_n \in R$. Dann sei
$(a_1, \cdots, a_n) = \{\sum_{i=1}^{n} x_i * a_i|x_1, \cdots, x_n \in R\}$
Dann ist $(a_1, \cdots, a_n)$ ein Ideal.

Sei $J \subseteq R$ ein Ideal in R.
a heißt Kongruent b modulo J, wenn $a - b \in J$. (geschrieben: $a \equiv b \bmod J$).

Lemma 4.3.1 $\equiv$ *ist Äquivalenzrelation.*

Beweis:

1. $a \equiv a \bmod J$.
Beweis:
$a - a = 0 \in J$
2. $a \equiv b \bmod J \succ b \equiv a \bmod J$.
Beweis:
$a - b \in J \succ (-e) * a - b \in J \succ b - q \in J \succ b \equiv a \bmod J$.
3. $a \equiv b \bmod J$ und $b \equiv c \bmod J$, z.Z.: $a \equiv c \bmod J$.
Beweis:
$a - b \in J$ und $b - c \in J \succ a - c = \underbrace{(a - b)}_{\in J} + \underbrace{(b - c)}_{\in J} \in J$

Lemma 4.3.2 *Sei $a \equiv b \ mod \ J$ und $c \equiv d \ mod \ J$.*
Dann gilt:

1. $a + c \equiv b + d \ mod \ J$
2. $a * c \equiv b * d \ mod \ J$

Beweis:

zu 1:

$a - b \in J$, $c - d \in J$

$$(a + c) - (b + d) = \underbrace{(a - b)}_{\in J} + \underbrace{(c - d)}_{\in J} \in J$$

$a + c \equiv b + d \bmod J$

zu 2:

$$\begin{aligned}
&(a - b) * (c - d) \\
&= a * c - b * c - a * d + b * d \\
&= (a * c - b * d) + (b * d - a * d) + (b * d - b * c) \\
&= (a * c - b * d) + d * (b - a) + b * (d - c)
\end{aligned}$$

$$(a * c - b * d) = \underbrace{(a - b)}_{} \in J * \underbrace{(c - d)}_{\in J} + \underbrace{d * \underbrace{(a - b)}_{\in J}}_{\in J} + \underbrace{b * \underbrace{(c - d)}_{\in J}}_{\in J} \in J$$

$a * c \equiv b * d \bmod J$

Diese Seite wurde aus Versehen frei gelassen
und ist NICHT für Notizen gedacht !

...oder was dachtest Du, was Du hier findest ?

4.4 Faktorstrukturen

Sei R ein Ring und $J \subseteq R$ ein Ideal.
Sei $a \in R$, dann sei

$$a/J = \{b | b \equiv \text{mod } J\} = \{b | a - b \in J\}$$

Lemma 4.4.1 $\hookrightarrow$

1. $a/J = b/J$
2. $a/J \cap b/J \neq \emptyset$
3. $a \equiv b \ mod \ J$
4. $a - b \in J$

Beweis:

$1 \succ 2$ $\surd$

$2 \succ 3$

Sei $c \in a/J \cap b/J$
$c \equiv a \text{ mod } J$ und $c \equiv b \text{ mod } J$
$\succ a \equiv b \text{ mod } J$

$3 \succ 4$ $\surd$

$4 \succ 1$

Behauptung: $a/J \subseteq b/J$
Sei $c \in a/J \succ a - c \in J$
Da $a - b \in J \succ b - c = (a - c) + (-1) * (a - b) \in J$
$\succ c \in b/J$

Behauptung: $b/J \subseteq a/J$
ebenso.

Sei $R/J = \{a/J | a \in R\}$

$$a/J + b/J := (a + b)/J$$
$$a/J * b/J := (a * b)/J$$

Lemma 4.4.2 $+$ *und* $*$ *sind "wohldefiniert"*

Beweis:

zu *:

$a/J = c/J$ und $b/J = d/J$, z.Z.: $(a * b)/J = (c * d)/J$
Da $a/J = c/J$ und $b/J = d/J$
$\succ a \equiv c \text{ mod } J$ und $b \equiv d \text{ mod } J$.
$\succ a * b \equiv c * d \text{ mod } J$
$\succ a * b/J = c * d/J$

Satz 4.4.1 $(R/J, +, *, 0/J, 1/J)$ *ist ein Ring.*

Beweis:

Da $J \neq R \succ 1 \notin J$. Also $0/J \neq 1/J$

1. $(R/J, +, 0/J)$ ist eine abelsche Gruppe
2. Man rechnet nach:
   a) $1/J * a/J = a/J$
   b) $(a/J * b/J) * c/J = a/J * (b/J * c/J)$
   c) $a/J * b/J = b/J * a/J$
   Beweis:
   $$a/J * b/J \overset{Definition}{=} (a * b)/J \overset{RRing}{=} (b * a)/J \overset{Definition}{=} b/J * a/J$$
   d) $(a/J + b/J) * c/J = a/J * c/J + b/J * c/J$

R/J heißt Faktorstruktur von R/J

Beispiel:

$(\mathbb{Z}/(n), +, *, 0/n, 1/n)$ mit $n > 1$ ist ein Ring.
Statt $K/(n)$ schreibt man auch $\overline{K}$.
Statt $\mathbb{Z}/(n)$ schreibt man auch $\mathbb{Z}_n$.
Satt $(\mathbb{Z}_n, +, *, \overline{0}, \overline{1})$ schreibt man auch $\mathbb{Z}_n$.

Sei $\phi : \left\{ \begin{array}{lcl} R & \to & R/J \\ a & \mapsto & a/J \end{array} \right.$

Lemma 4.4.3 *ϕ ist ein Homomorphismus von R nach R/J mit $Kern(\phi) = J$ und $Bild(\phi) = R/J$*

Beweis:

1. $\phi(a + b) \overset{Definition\phi}{=} (a + b)/J \overset{Definition+}{=} a/J + b/J \overset{Definition\phi}{=} \phi(a) + \phi(b)$
2. $\phi(a * b) \overset{Definition\phi}{=} (a * b)/J \overset{Definition*}{=} a/J * b/J \overset{Definition\phi}{=} \phi(a) * \phi(b)$
3. $\phi(1) = 1/J$

   Also ist ϕ ein Homomorphismus.

4. $a \in Kern(\phi)$
   gdw. $\phi(a) = 0/J$
   gdw. $a/J = 0/J$
   gdw. $a = a - 0 \in J$

ϕ heißt kanonischer Homomorphismus von R auf R/J.

Satz 4.4.2 *Ist $\phi : R \to R'$ ein Homomorphismus, dann sind $Bild(\phi)$ und $R/Kern(\phi)$ isomorph.*

Beweis:

$J = Kern(\phi)$ ist ein Ideal.
Sei $\overline{\phi} : \left\{ \begin{array}{lcl} R/J & \to & Bild(\phi) \\ a/J & \mapsto & \phi(a) \end{array} \right.$

1. $\overline{\phi}$ ist wohldefiniert und injektiv
   Beweis:
   $a/J = b/J$
   gdw. $a - b \in J = Kern(\phi)$
   gdw. $\phi(a - b) = 0$
   gdw. $\phi(a) - \phi(b) = 0$
   gdw. $\phi(a) = \phi(b)$

2. $\overline{\phi}$ ist surjektiv. $\surd$

3. $\overline{\phi}$ ist Homomorphismus.
   a) $\overline{\phi}(a/J + b/J) = \overline{\phi}(a/J) + \overline{\phi}(b/J)$
   b) $\overline{\phi}(a/J * b/J) = \overline{\phi}(a/J) * \overline{\phi}(b/J)$
   Beweis:
   $\overline{\phi}(a/J * b/J)$
   $\overset{Definition*}{=} \overline{\phi}((a * b)/J)$
   $\overset{Definition\overline{\phi}}{=} \phi(a * b)$
   $\overset{\phi homomorph}{=} \phi(a) * \phi(b)$
   $\overset{Definition\overline{\phi}}{=} \overline{\phi}(a/J) * \overline{phi}(b(J)$

4. $\overline{\phi}(a/J) = 1$

4.5 Nullteiler und Einheiten

$a \in R$ mit $a \neq 0$ heißt Nullteiler,
wenn es ein $b \in R$ gibt, mit $b \neq 0$ und $a * b = 0$

Beispiel:
Sei $R = \mathbb{Z}_6$.
Dann ist $\overline{2} \neq 0$ und $\overline{3} \neq 0$ und $\overline{2} * \overline{3} = \overline{6} = \overline{0}$.
Also sind $\overline{2}$ und $\overline{3}$ Nullteiler, $\overline{4}$ ist Nullteiler.

$a \in R$ heißt Einheit, wenn es ein b gibt mit $a * b = 1$

Beispiel:
$R = \mathbb{Z}_6$.
Dann ist $\overline{1}$ Einheit, da $\overline{1} * \overline{1} = \overline{1}$
$\overline{5}$ ist Einheit, denn $\overline{5} * \overline{5} = \overline{25} = \overline{1}$

Lemma 4.5.1 *Ist a Nullteiler, dann ist a keine Einheit.*

Beweis:
Sei $a \neq 0$ und a Nullteiler, dann gibt es $b \neq 0$, $a * b = 0$.
Angenommen, a ist Einheit $\succ$ Es gibt c mit $a * c = 1$.
$\succ b = 1 * b = a * c * b = c * 0 = 0$ $\quad\quad$ ♯Da $b \neq 0$.

R heißt Integritätsring, wenn es keine Nullteiler in R gibt.

Beispiel:
$\mathbb{Z}$ ist eine Integritätsring.

R heißt Körper, wenn es zu jedem $a \in R \setminus \{0\}$ ein $b \in R$ gibt, mit $a * b = 1$.

Bemerkung 4.5.1 *Jeder Körper ist Integritätsring.*

Lemma 4.5.2 *Sei p eine Primzahl, dann ist $\mathbb{Z}_p$ ein Körper.*

Beweis:
Sei $\overline{a} \in \mathbb{Z}_p \setminus \{\overline{0}\}$. Dann ist $ggT(a, p) = 1$.
Also gibt es b und y mit $1 = a * b + y * p$.
$\overline{1} = \overline{a * b + y * p} = \overline{a} * \overline{b} + \overline{y} * \overline{p} = \overline{a} * \overline{b} + \overline{y} * \overline{0} = \overline{a} * \overline{b}$

Guten Tag Frau Vogel, ich möchte Ihre Tochter zum Fischen abholen !

Lemma 4.5.3 *Sei p Primzahl.*
Ist R ein Ring mit $|R| = p$, dann ist $R \approx \mathbb{Z}_p$.

Beweis:
$(R, +, 0)$ ist eine abelsche Gruppe.

$ord(1) \neq 1 \succ ord(1) = p$
$(R, +, 0) \approx (\mathbb{Z}, +, 0)$
$\phi : \begin{cases} R & \to & \mathbb{Z}_p \\ n * 1 & \mapsto & \overline{n} \end{cases}$
Bleibt z.Z.: ϕ ist ein Ring-Homomorphismus.
$\phi(n * 1; m * 1) = \phi(n * m * 1) = \overline{n * m} = \overline{n} * \overline{m} = \phi(n * 1) * \phi(m * 1)$
$(R, +, *, 0, 1)$ ist R $\qquad\qquad$ $n * 1 = \underbrace{1 + 1 + \cdots + 1}_{n-mal}$

Satz 4.5.1 *(Fermat)*
Ist p eine Primzahl und $p > k > 1$
$k^{p-1} \equiv 1 \ mod \ p$

Beweis:
$\overline{K} \in \mathbb{Z}_p$ und $\overline{K} \neq \overline{0}$.
Da $(\mathbb{Z}_p \setminus \{\overline{0}\}, *, \overline{1})$ eine Gruppe ist
$\succ ord(\overline{K})$ teilt $|\mathbb{Z}_p \setminus \{\overline{0}\}| = p^{-1}$
$\succ \overline{K}^{p-1} = \overline{1}$
$\succ \overline{K^{p-1}} = \overline{1}$
$\succ K^{p-1} \equiv 1 \bmod p$

Sei R ein Ring und $s \in \mathbb{N} \setminus \{0\}$. Dann sei $R_s = \{a | s * a = \underbrace{a + a + \cdots + a}_{s-mal}\}$

Satz 4.5.2 *Ist $ggT(n, m) = 1$, dann ist*
$\phi : \begin{cases} \mathbb{Z}_{n*m} & \to & \mathbb{Z}_n \times \mathbb{Z}_m \\ a/(n*m) & \mapsto & (a/(n), a/(m)) \end{cases}$
ein Isomorphismus.

Beweis:
Sei $k = n * m$

1. ϕ ist wohldefiniert: $a/(k) = b/(k)$
   z.Z.: $a/(n) = b(n)$ und $a/(m) = b/(m)$
   $a/(k) = b/(k)$
   $\succ a - b \in (k) \succ k | (a - b) \succ n | (a - b)$ und $m | (a - b)$
   $\succ a/(n) = b/(n)$ und $a/(m) = b/(m)$

2. ϕ ist Homomorphismus
   1. $\phi(a/(k) + b/(k)) = \phi((a + b)/k) = ((a + b)/(n), (a + b)/(m))$
      $= (a/(n) + b(n), a/(m) + b/(m)) = (a/(n), b/(n)) + (a/(m), b/(m))$
      $= \phi(a/(k)) + \phi(b/(k))$
   2. $\phi((a * b)/(k)) = \phi(a/(k)) * \phi(b/(k))$
   3. $\phi(1/(k)) = (1/(n), 1/(m))$

3. ϕ ist Monomorphismus (injekiv)
   z.Z.: $kern(\phi) = \{0/(k)\}$

$a/(n) = 0/(n)$ und $a/(m) = 0/(m)$
$\succ n|a$ und $m|a$
$\succ a = l * n$ und $a = j * m$
Da $ggT(n, m) = 1$
$\succ 1 = x * n + y * m$
$\succ a = a * x * n + a * y * m$
$\succ a = j * m * x * n + l * n * y * m$
$\succ k = m * n|a$
$\succ 0/(k) = a/(k)$

4. ϕ ist Epimorphismus (surjektiv)
   $|\mathbb{Z}_{n*m}| = n * m = |\mathbb{Z}_n \times \mathbb{Z}_m|$
   $\phi : \mathbb{Z}_{n*m} \xrightarrow{1-1} \mathbb{Z}_n \times \mathbb{Z}_m$.
   Da $\mathbb{Z}_{n*m}$ endlich, ist ϕ surjektiv.

Bemerkung 4.5.2 *Sei $s, r \in \mathbb{N}\backslash\{0, 1\}$ mit $ggT(r, s) = 1$ und R ein Ring mit $|R| = r * s$ Dann sind R_1, R_s Ringe mit $|R_r| = r$ und $|R_s| = s$ und*

$$R \cong R_r \times R_s$$

Beweis:

Da $(R, +, 0)$ ein Gruppe ist, gibt es einen Gruppenhomomorphismus mit

$$\phi : \begin{cases} R_r \times R_s & \to & R \\ (a, b) & \mapsto & a + b \end{cases}$$

und $|R_s| = s$ und $|R_r| = r$
Da $ggT(r, s) = 1$, gibt es x, y mit $1 = x * r + y * s$.
Sei e das Einselement aus R.
Wir setzen $e_s = x * r * e$ und $e_r = y * s * e$
Behauptung: $(R, +, *, 0, e_s)$ ist ein Ring.
...to be continued !

Beispiel:

Seien p und q Primzahlen mit $p \neq q$. Dann ist der Ring $\mathbb{Z}_{p*q}$ isomorp zu $\mathbb{Z}_p \times \mathbb{Z}_q$.

Beweis:

Da $ggT(p, q) = 1 \succ \mathbb{Z}_{p*q} \approx R_p \times R_q$ mit $|R_p| = p$ und $|R_q| = q$.
$\succ R_p \approx \mathbb{Z}_p$ und $R_p \approx \mathbb{Z}_q$.

Folgerung 4.5.1 *(Chinesischer Restsatz)*
Sei $ggT(n, m) = 1$ und $r_1, r_2 \in \mathbb{Z}$.
Dann gibt es ein $r \in \mathbb{Z}$ mit:

$$r \equiv r_1 \ mod \ n$$
$$r \equiv r_2 \ mod \ m$$

Beweis:

$r_1/(n) \in \mathbb{Z}_n$ und $r_2/(m) \in \mathbb{Z}_m$.

$$\phi : \begin{cases} \mathbb{Z}_{n*m} & \to & \mathbb{Z}_n \times \mathbb{Z}_m \\ a/(n * m) & \mapsto & (a/(n), a/(m)) \end{cases}$$

ist surjektiv.
Also gibt es ein $r \in \mathbb{Z}$ mit
$(r/(n), r/(m)) = \phi(n/(n * m)) = (r_1/(n), r_2/(m))$
$\succ r/(n) = r1(n)$ und $r/(m) = r_2/(m)$
$\succ r - r_1 = l * n$, $r - r_2 = k * m$
$\succ r \equiv r_1 \bmod n$ und $r \equiv r_2 \bmod m$.

5 Polynomringe

5.1 Definitionen und Einführung

Sei $(R, +, *, 0, e)$ ein Ring.
Eine Folge $(a_i), i \in \mathbb{N}$ von Elementen aus R heißt Polynom,
wenn es ein n gibt mit $a_i = 0$ für $i > n$.
Sei $R[x] = \{f; f \text{ ist Polynom}\}$
Sei $f = (a_i) \in R[x]$ mit $i \in \mathbb{N}$

1. Ist $a_i = 0$ für alle $i \in \mathbb{N}$, dann heißt $(a_i), i \in \mathbb{N}$ Nullpolynom.
   (i.Z.: $0'$). Wir setzen $grad(0') = \infty$.

2. Ist $a_i \neq 0$ für ein $i \in \mathbb{N}$,
   dann sei $grad(f)$ die größte natürliche Zahl k mit $a_k \neq 0$.
   f heißt normiert, wenn $a_{grad(f)} = 1$.

3. Sei $a \in R$ und sei $a_c = a$ und $a_i = 0$ für $i > 0$,
   dann heißt f konstantes Polynom. Statt f schreibt man auch a'.

Wir setzen:

$$-\infty + -\infty = -\infty$$
$$-\infty + n = n - \infty = -\infty$$
$$-\infty < n \text{ für alle } n \in \mathbb{N}.$$

Sei $f = (a_i), i \in \mathbb{N}$ und $g = (b_i), i \in \mathbb{N}$
Wir setzen:

$$f + g := (a_i + b_i), i \in \mathbb{N}$$

Lemma 5.1.1 *Sind $f, g \in R[x]$, dann ist*

$$grad(f) + grad(g) \geq grad(f + g)$$

Es gilt sogar:

$$max(grad(f), grad(g)) \geq grad(f + g)$$

Beweis:

Sei $f = (a_i), i \in \mathbb{N}$ und $g = (b_i), i \in \mathbb{N}$.
Sei $n = max(grad(f), grad(g))$. Dann ist $a_i = 0$ und $b_i = 0$ für $i > n$.
$\succ$ $a_i + b_i = 0$ für $i > n$.
$\succ$ $grad(f + g) \leq n$

Sei $f = (a_i), i \in \mathbb{N}$ und $g = (b_i), \in \mathbb{N}$. Dann sei

$$f * g = (c_i), i \in \mathbb{N} \text{ mit } c_i = \sum_{l+k=i} a_l * b_k$$

Lemma 5.1.2 *Sei $f, g \in R[x], dannist$*

$$grad(f * g) \leq grad(f) * grad(g)$$

Beweis:

Sei $f = (a_i), i \in \mathbb{N}$ und $g = (b_i), i \in \mathbb{N}$ und $n = grad(f) * grad(g)$.

Dann ist für $l + k > n$ $a_l = 0$ oder $b_k = 0$.
Also ist $\sum_{l+k=i} a_l * b_k = 0$ für $i > n$.
Also ist $grad(f * g) \leq n$.

Lemma 5.1.3 *Ist R ein Integritätsring, dann gilt:*
$$grad(f * g) = grad(f) + grad(g)$$

Beweis:
Sei $f = (a_i), i \in \mathbb{N}$ und $g = (b_i), i \in \mathbb{N}$.
Sei $c_j = \sum_{l+k=i} a_l * b_k$
I. Fall: $grad(f) = -\infty$ oder $grad(g) = -\infty$
$\succ c_j = 0 \ \forall i \in \mathbb{N}$
$grad(f * g) = -\infty = -\infty - \infty = grad(f) + grad(g)$
II. Fall: $grad(f) = n \geq 0$ und $grad(g) = m \geq 0$
$\succ c_{n*m} = \sum_{l+k=n*m} a_l * b_k = a_n * b_m$
$grad(f) = n \succ a_n \neq 0$
$grad(g) = m \succ b_m \neq 0$
Da a_n, b_m keine Nullteiler sind $\succ a_n * b_m \neq 0$

Satz 5.1.1 $(R[x], +, *, 0', 1')$ *ist ein Ring.*

Beweis:

1. $0' \neq 1' \in R[x]$
2. $(R[x], +, 0')$ ist eine abelsche Gruppe
3. $(f * g) * h = f * (g * h)$
4. $f * 1' = f$
5. $f * g = g * f$
6. $f * (g + h) = f * g + f * h$

Lemma 5.1.4 *Ist R ein Integritätsring, dann ist $R[x]$ ein Integritätsring.*

Beweis:
Sei $f \neq 0'$ und $g \neq 0'$
$\succ grad(f * g) = grad(f) + grad(g) > -\infty + -\infty = -\infty$
$\succ f * g \neq 0'$

Lemma 5.1.5 *Sei R ein Ring und $R[x]$ der Polynomring über R.*
Dann ist
$$\phi : \begin{cases} R & \to & R[x] \\ a & \mapsto & a' = (a, 0, 0, \cdots) \end{cases}$$
ein Monomorphismus. (d.h. injektiver Homomorphismus)

Beweis:

ϕ ist injektiv $\surd$
$\phi(1) = 1'$ $\surd$
$\phi(a+b) = \phi(a) + \phi(b)$ $\surd$
$\phi(a*b) = \phi(a) * \phi(b)$ $\surd$

Man schreibt deshalb auch a für a'. Man identifiziert a mit $(a, 0, \cdots)$.
Man bettet R in $R[x]$ ein.

Bemerkung 5.1.1 *Sei*

$x := (0, 1, 0, \cdots)$
$x^0 := (1, 0, \cdots)$
$x^{i+1} := x^i * x$
Dann ist $x^i := (0, \cdots, 0, \underbrace{1}_{i-te-Stelle}, 0, \cdots)$

Sei $f \in R[x]$, $f = (a_i), i \in \mathbb{N}$ mit $grad(f) = n$.
Dann ist $f = \sum_{i=0}^{n} a_i' * x^i = \sum_{i=0}^{n} a_i x^i$
da a und a' identifiziert werden.

5.2 Ideale im Polynomring

Bemerkung 5.2.1 *Sei K ein Körper und $K[x]$ der Polynomring über K.*
Sei $f = (a_i) \in K[x]$ und $g = (b_i) \in K[x]$ mit $i \in \mathbb{N}$

$f + g := (a_i + b_i), i \in \mathbb{N}$
$f * g := (c_i), i \in \mathbb{N}$ *mit* $c_i = \sum_{l+k=i} a_l * b_k$
$e' := (1, 0, \cdots, 0, \cdots)$
$0' := (0, 0, \cdots, 0, 0)$

Dann ist $(K[x], +, *, 0', e')$ ein Ring.

Satz 5.2.1 *Seien $f, g \in K[x]$ mit $g \neq 0$.*
Dann gibt es genau ein q und genau ein r mit

$f = q * g + r$

und

$grad(r) < grad(g)$

Beweis:

Existenz: (Induktion über $grad(f)$)

A) Ist $grad(f) < grad(g)$, dann sei $\phi = 0$ und $r = f$.
B) Sei $grad(f) = n$ und $grad(g) = m$
und $f = \sum_{i=0}^{n} a_i x^i$ und $g = \sum_{i=0}^{m} b_i x^i$.
Dann ist $n > m$.
Sei $f_1 = f - a_n * b_m^{-1} * x^{n-m} * g = \sum_{i=1}^{n} a_i x^i - a_n b_m^{-1} * x^{n-m} * \sum_{i=0}^{m} b_i x^i$.
Dann ist $grad(f_1) < grad(f)$
Nach Induktionsvoraussetzung gibt es q_1 und r mit
$f_1 = q_1 * g - r$ mit $grad(r) < grad(g)$
Sei $q = (q_1 + a_n * b_m^{-1} * x^{n-m})$
Dann ist $f = q * g + r$

Eindeutigkeit :

$f = q_1 * g + r_1$, $f = q_2 * g + r_2$ mit $grad(r_1), grad(r_2) < grad(g)$
$\succ (r_1 - r_2) = (q_2 - q_1) * g$
$\succ grad(g) > grad(r_1 - r_2) = grad(q_2 - q_1) + grad(q)$
$\succ grad(q_2 - q_1) = -\infty$
$\succ q_1 = q_2$
$\succ r_1 = r_2$

Satz 5.2.2 *Ist J ein Ideal in $K[x]$, dann gibt es ein Polynom $g \in J$ mit $J = (g)$*

Beweis:

$(g) = \{f * g | f \in K[x]\}$
I. Fall: $J = \{0\}$
Sei $g = 0$
II. Fall: Sei $g \in J \setminus \{0\}$ mit $grad(g)$ minimal.
Behauptung:$(g) = (J)$
Da $g \in J \succ (g) \subseteq J$, bleibt z.Z.: $h \subseteq (g)$

Sei $f \in J$. Dann gibt es q, r mit
$f = q * g + r$
mit $grad(r) < grad(g)$
$\succ r = \underbrace{f}_{\in J} - \underbrace{q * \underbrace{g}_{\in J}}_{\in J} \in J$
Da $grad(r) < grad(g) \succ r = 0$ nach Wahl von g
$\succ f = q * g$
$\succ f \in (g)$

Folgerung 5.2.1 *Ist J ein Ideal in $K[x]$, dann gibt es genau ein normiertes Polynom g mit $J = (g)$.*

Beweis:
Existenz:
Sei $g \in K[x]$ mit $J = (g)$.
Sei $grad(g) = m$ und $g = \sum_{i=0}^{m} b_i x^i$.
Sei $g' = b_m^{-1} * g$
$\succ J = (g')$
Eindeutigkeit:
$J = (g_1) = (g_2)$
$\succ g_1 = h_1 * g_2$ und $g_2 = h_2 * g_1$, $grad(g_1) \leq grad(g_2)$, $grad(g_2) \leq grad(g_1)$
$\succ grad(g_1) = grad(g_2)$
$\succ grad(h_1) = 0$ und $grad(h_2) = 0$
Sei $h_1 = c \succ g_1 = c * g_2$
Da g_1, g_2 normiert sind, ist $c = 1$.
Also ist $g_1 = g_2$.

Seien f und g Polynome mit $f = h * g$, dann sagt man, daß g ein Teiler von f ist.
geschrieben: $g|f$
g heißt gemeinsamer Teiler von f_1 und f_2, wenn $g|f_1$ und $g|f_2$.
Ein gemeinsamer Teiler g von f_1 und f_2 heißt größter gemeinsamer Teiler von f_1 und f_2, wenn für alle gemeinsamen Teiler h von f_1 und f_2 gilt:
$h|g$
Ist g normiert, dann schreibt man
$g.g.T.(f_1, f_2)$
für g.

Satz 5.2.3 *Seien f_1, f_2 und g Polynome mit $(g) = (f_1, f_2)$. Dann ist g ein größter gemeinsamer Teiler.*

Beweis:
Da $f_1, f_2 \in (g) \succ$ Es gibt h_1, h_2 mit $f_1 = h_1 * g$ und $f_2 = h_2 * g$.
$\succ g$ ist gemeinsamer Teiler.
Sei h ein Teiler von f_1, f_2, z.Z.: $g|h$

Da h ein Teiler von f_1, f_2, gibt es h_1, h_2 mit $f_1 = h_1 * h$ und $f_2 = h_2 * h$
Da $g \in (f_1, f_2)$, gibt es g_1, g_2 mit $g = g_1 * f_1 + g_2 * f_2$
$\succ g = g_1 * h_1 * h + g_2 * h_2 * h = h(g_1 * h_1 + g_2 * h_2)$
$\succ h|g$

Folgerung 5.2.2 *Sind f_1, f_2 Polynome mit $f_1 \neq 0$ und $f_2 \neq 0$, dann existiert $ggT(f_1, f_2)$*

Ein normiertes Polynom p mit $grad(p) \geq 1$ heißt irreduzibel, wenn für alle f und g mit $p = f * g$ gilt:

$grad(f) = 0$ oder $grad(g) = 0$

Lemma 5.2.1 *Seien $f_1, \cdots, f_k$ Polynome und p ein irreduzibles Polynom mit:*
$p| \prod_{i=1}^{k} f_i$
Dann gibt es ein i mit $p|f_i$.

Beweis:(Induktion über k)
$k = 1$ $\surd$
$p| \prod_{i=1}^{k+1} f_i$
I. Fall: $p|f_{n+1}$ $\surd$
II. Fall: sonst
Sei $g = ggT(f_{n+1}, p)$
Da p irreduzibel ist, ist $g = 1$.
Da $(g) = (f_{k+1}, p)$
$\succ g = 1 = h_1 * f_{k+1} + h_2 * p$
$\succ \prod_{i=1}^{k} f_i = h_1 * \prod_{i=1}^{k+1} f_i + h_2 * p * \prod_{i=1}^{k} f_i$
Da $p| \prod_{i=1}^{k+1} f_i \succ p| \prod_{i=1}^{k} f_i$
Nach Induktionsvoraussetzung gibt es ein i mit $p|f_i$

Satz 5.2.4 *Sei f ein Polynom mit $grad(f) \geq 1$.*
Dann gibt es irreduzible Polynome $p_1, \cdots, p_k$ und $c \in K$ mit $f = c * p_1 * \cdots * p_k$
Bis auf die Reihenfolge von $p_1, \cdots, p_k$ und $c \in K$ ist diese Darstellung eindeutig.

Beweis:
I. Existenz: (Induktion über den $grad(f)$)
$grad(f) = 1$, $f = a_1 * x + a_0$
Sei $c = a_1$ und $p = x + \frac{a_0}{a_1}$.
Sei $grad(f) = n > 1$
Sei $f = c * g$ mit g ist normiert.
I. Fall: g ist irreduzibel $\surd$
II. Fall: sonst
Dann sei $p_1 = g$.
Sonst gibt es Polynome h_1, h_2 mit $g = h_1 * h_2$
und $grad(h_1) < grad(g)$ und $grad(h_2) < grad(g)$
Nach Induktionsvoraussetzung gibt es $p_1, \cdots, p_l$ und $q_1, \cdots, q_k$ mit
$h_1 = p_1, \cdots, p_l$ und $h_2 = q_1 * \cdots * q_k$
$\succ f = c * p_1 * \cdots * p_l * q_1 * \cdots * q_k$

II. Eindeutigkeit:

Durch Induktion über n zeigen wir:

Ist $a * p_1 * \cdots * p_n = b * q_1 * \cdots * q_n$ mit:

1) $p_1 \cdots p_n$ irreduzibel
2) $a, b \in K$

Dann gilt:

3) $a = b$
4) $n = m$
5) $q_1, \cdots, q_n$ ist eine Permutation $p_1, \cdots, p_n$.

$n = 1$:

$p | b * q_1 * \cdots * q_m$

Also gibt es ein i mit $p | q_i$. oBdA sei $i = m$

Da q_m und p_1 irreduzibel sind

$\succ q_m = p_i$

$\succ a = b * \prod_{i=1}^{m-1} q_i$

$\succ m = 1$

$\succ a * p_1 = b * q_1 = b * p_1$

$a = b$

$n > 1$:

Ebenso.

5.3 Nullstellen von Polynomen

Sei L ein Körper. Ein Unterring K von L heißt Unterkörper, wenn gilt:

$a \in K$ und $a \neq 0 \succ a^{-1} \in K$

Sei K ein Unterkörper von L.

Sei $\alpha \in L$.

$$\phi_\alpha : \begin{cases} K[x] & \to & L \\ f = (a_i), i \in \mathbb{N} & \mapsto & f(\alpha) := \sum_{i=0}^{n} a_i \alpha^i \end{cases}$$

Lemma 5.3.1 *$\phi(\alpha)$ ist ein Homomorphismus von $K[x]$ in L.*

Beweis:

Sei $f = (a_i), i \in \mathbb{N} = \sum_{i=0}^{n} a_i x^i$ und $g = (b_i), i \in \mathbb{N} = \sum_{i=0}^{m} b_i x^i$ mit $n \geq grad(f), grad(g)$

(i) $\phi_\alpha(f) + \phi_\alpha(g) = \phi_\alpha(f+g)$

Beweis:

$\phi_\alpha(f+g)$
$= \phi_\alpha(\sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{n} b_i x^i)$
$= \phi_\alpha(\sum_{i=0}^{n} (a_i + b_i) * x^i)$
$= \sum_{i=0}^{n} (a_i + b_i) * \alpha^i$
$= \sum_{i=0}^{n} a_i * \alpha^i + \sum_{i=0}^{n} b_i * \alpha^i$
$\phi_\alpha(f) + \phi_\alpha(g)$

(ii) $\phi_\alpha(f * g) = \phi_\alpha(f) * \phi_\alpha(g)$

Beweis:

$\phi_\alpha(f * g)$
$= \phi_\alpha(\sum_{i=0}^{n+n} (\sum_{l+k=i} a_l * b_k) * x^i)$
$= \sum_{i=0}^{n+n} (\sum_{l+k=i} a_l * b_k) * \alpha^i$
$= (\sum_{i=0}^{n} a_i * \alpha^i) * (\sum_{i=0}^{n} b_i * \alpha^i)$
$= \phi_\alpha(f) * \phi_\alpha(g)$

$\phi_\alpha(e') = e$

Sei $f \in K[x]$. $\alpha \in K$ heißt Nullstelle von f, wenn $\phi_\alpha(f) = f(\alpha) = 0$

Lemma 5.3.2 *Ist α eine Nullstelle von f, dann gibt es $h \in K[x]$ mit $f = h * (x - \alpha)$.*

Beweis:

Nach dem Lemma von Euklid (Seite 9) gibt es h und r mit:

$f = h * (x - \alpha) + r$, $grad(r) < 1$

Da α Nullstelle von f ist

$\succ 0 = \phi_\alpha(f) = \phi_\alpha(h * (x - \alpha) + r) = \underbrace{\phi_\alpha(h)}_{=0} * \underbrace{\phi_\alpha(x - \alpha)}_{=0} + \phi_\alpha(r) = \phi_\alpha(r)$

$\succ r = 0$

$\succ f = h * (x - \alpha)$

Satz 5.3.1 *Ist $f \in K[x]$ mit $grad(f) \geq 0$.*
Dann besitzt f höchstens $grad(f)$-viele Nullstellen.

Beweis: (Induktion über $grad(f)$)
$grad(f) = 0 \succ f$ besitzt keine Nullstelle.
Sei $grad(f) = n > 0$.
Angenommen es gibt $n+1$-viele paarweise verschiedene Nullstellen $\alpha_1, \cdots, \alpha_{n+1}$
$\succ grad(h) < n$
$0 = f(\alpha_i) = \phi_{\alpha_i}(f) = \phi_{\alpha_i}(h) * \phi_{\alpha_i}(x - \alpha_{n+1})$
$= \phi_{\alpha}(h) * (\alpha_i - \alpha_{n+1})$
Ist $i \leq n$, dann ist $(\alpha_i - \alpha_{n+1}) \neq 0$.
$\phi_{\alpha_i}(h) = 0$ für $i = 1, \cdots, n$
h besitzt n-Nullstellen. $grad(h) < n$.
Dies ist ein Widerspruch zur Induktionsvoraussetzung.

Folgerung 5.3.1 *Seien $f, g \in K[x]$ mit $grad(f) \leq n$ und $grad(g) \leq n$.*
Gibt es $n+1$-viele paarweise verschiedene $\alpha_1, \cdots, \alpha_{n+1}$ mit:
$$f(\alpha_i) = g(\alpha_i)$$
Dann ist $f = g$.

Beweis:
Sei $h = f - g$. Dann ist $grad(h) \leq n$.
$\phi_{\alpha_i} = \phi_{\alpha_i}(f - g) = \phi_{\alpha_i}(f) - \phi_{\alpha_i}(g) = f(\alpha_i) - g(\alpha_i) = 0$
$\succ \alpha_1, \cdots, \alpha_{n+1}$ sind Nullstellen von $f - g$
$\succ g - f = 0$
$\succ g = f$

Ein Körper K heißt algebraisch abgeschlossen, wenn jedes Polynom f mit $grad(f) \geq 1$ eine Nullstelle besitzt.
Der Körper der komplexen Zahlen $\mathbb{C}$ ist algebraisch abgeschlossen.

Satz 5.3.2 *Sei K ein algebraisch abgeschlossener Körper*
und $f \in K[x]$ mit $grad(f) \geq 1$.
Dann gibt es $\alpha_1, \cdots, \alpha_n$ und $c \in K$ mit:
$$f = c * (x - \alpha_1) * \cdots * (x - \alpha_n)$$

Beweis: (Induktion über $n = grad(f)$)
Ist $n = 1 \succ f = a_1 * x + a_0$
Sei $c = a_1$, $\alpha_1 = -\frac{a_0}{a_1}$
$\succ f = c * (x - \alpha_1)$
$n = grad(f) > 1$. Dann besitzt f eine Nullstelle α_n in K.
$\succ f = h * (x - \alpha_n)$
Da $grad(h) = grad(f) - 1$ gibt es nach Induktionsvorausetzung $\alpha_1, \cdots, \alpha_{n-1}$
und $c \in K$ mit:
$$h = c * (x - \alpha_1) * \cdots * (x - \alpha_{n-1})$$
$\succ f = c * (x - \alpha_1) * \cdots * (x - \alpha_n)$

Seien $f, g \in K[x]$ mit g irreduzibel.

Die Vielfachheit von g in f ist dasjenige m mit
$$g^m | f \text{ und } g^{m+1} \nmid f$$
Ist α eine Nullstelle von f, dann ist die Vielfachheit von α die Vielfachheit von $(x-\alpha)$ in f.
Gesucht ist eine Kriterium für die Vielfachheit einer Nullstelle in f.
Sei $f = \sum_{i=0}^{n} a_i x^i$, dann sei $f' = \sum_{i=0}^{n-1} (i+1) * a_{i+1} x^i$

Lemma 5.3.3

1. $f' + g' = (f+g)'$
2. $(f*g)' = f'*g + g'*f$
3. $(f^m)' = m * f^{m-1} * f'$

Beweis:
(Nachrechen)

Satz 5.3.3 *Sei $grad(f) \geq 1$ und α eine Nullstelle von f* $\hookleftarrow$
1) Die Vielfachheit der Nullstelle α ist größer als 1.
2) α ist Nullstelle von f'.

Beweis:
Sei m die Vielfachheit von α, dann ist $f = (x-\alpha)^m * h$ mit $h(\alpha) \neq 0$
"1 $\succ$ 2"
Sei $m > 1 \succ f' = ((x-\alpha)^m)' * h + h' * (x-\alpha)^m = m * (x-\alpha)^{m-1} + h' * (x-\alpha)^m$
Da $m > 1 \succ f'(\alpha) = 0$
"2 $\succ$ 1"
d.h. nicht-1 $\succ$nicht-2.
Sei $m = 1$.
$f = (x-\alpha) * h$ mit $h(\alpha) \neq 0$
$f' = h + (x-\alpha) * h'$
$\succ f'(\alpha) = h(\alpha) + 0 \neq 0$
$\succ \alpha$ ist keine Nullstelle von f'

Satz 5.3.4 *Sei K ein Unterkörper von $\mathbb{C}$.*
Sei $g \in K[x]$ irreduzibel in $K[x]$ mit $grad(g) = n$.
Dann besitzt g n paarweise verschiedene Nullstellen in $\mathbb{C}$

Beweis:
Da $\mathbb{C}$ algebraisch abgeschlossen ist, gibt es $\alpha_1, \cdots, \alpha_n \in \mathbb{C}$ mit:
$$g = (x-\alpha_1) * \cdots * (x-\alpha_n)$$
Es ist z.Z.:
Die Vielfachheit von α_i ist 1.
$\phi_{\alpha_i} : \begin{cases} K[x] & \to & \mathbb{C} \\ f & \mapsto & f(\alpha_i) \end{cases}$ ist Homomorphismus.
Der $Kern(\phi_{\alpha_i})$ ist ein Ideal in $K[x]$.

Dann gibt es ein normiertes Polynom h mit $Kern(\phi_{\alpha_i}) = (h)$.
Da $g \in (h)$ und g irreduzibel $\succ g = h$.
Angenommen, die Vielfachheit von α_i ist größer als 1.
$\succ \alpha_i$ ist Nullstelle von g'.
$g' \in (h) = (g)$
$\succ g' = f * g$
$\succ grad(g') \geq (g)$ oder $grad(g') = -\infty$
$grad(g') < grad(g)$
$\succ grad(g') = -\infty$
$\succ g' = 0$
$\succ grad(g) \leq 0$
Da g irreduzibel ist $\succ grad(g) \geq 1$ ♯

5.4 Polynome von Einheitsformen

Ziel: Wir wollen zeigen:
$x^5 - 10 * x - 2$ ist irreduzibel in $\mathbb{Q}[x]$.

Ein Polynom $f = (a_i) \in \mathbb{Z}[x]$, mit $i \in \mathbb{N}$ mit $grad(f) = n$ hat Einheitsform,
wenn $ggT(a_0, \cdots, a_n) = 1$

Lemma 5.4.1 *Ist $f \in \mathbb{Q}[x]$ mit $grad(f) \geq 0$, dann gibt es ein $r \in \mathbb{Q}$ mit $r * f$ ist von Einheitsform.*

Beweis:
Sei $f = (a_i), i \in \mathbb{N}$ mit $grad(f) = n$. Sei $a = \frac{b_i}{c_i}$ mit $ggT(b_i, c_i) = 1$
Sei $c = \prod_{i=0}^{n} c_i$. Dann ist $c * f \in \mathbb{Z}[x]$. Sei $b = ggT(c * a_0, \cdots, c * a_n)$
Sei $r = \frac{c}{b}$. Dann ist $r * f \in \mathbb{Z}[x]$ von Einheitsform.

Lemma 5.4.2 *Sind f und g von Einheitsform, dann ist $f * g$ von Einheitsform.*

Beweis:
Sei $f = (a_i), i \in \mathbb{N}$,$g = (b_i), i \in \mathbb{N}$. Dann ist
$f * g = (c_i), i \in \mathbb{N}$ mit $c_i = \sum_{l+k=1} a_l * b_k$.
Da $f, g \in \mathbb{Z}[x]$, genügt es z.Z.:
Ist p eine Primzahl, dann gibt es ein c_i mit $p \nmid c_i$.
Da f und g von Einheitsform sind, gibt es ein größeres l_0
mit $p \nmid a_{l_0}$ und ein größtes k_0 mit $p \nmid b_{k_0}$.
Sei $i_0 = l_0 + k_0$.
$c_{i_0} = \sum_{\substack{l+k=i_0 \\ k>k_0}} a_l * b_k$
$\succ p | (c_{i_0} - a_{l_0} * b_{k_0})$
Da $p \nmid a_{l_0} * b_{k_0} \succ p \nmid c_{i_0}$

Satz 5.4.1 *(Gauß)*
Sei $f \in \mathbb{Z}[x]$ von Einheitsform und reduzibel in $\mathbb{Q}[x]$.
Dann gibt es $g, h \in \mathbb{Z}[x]$ von Einheitsform mit $grad(g) \geq 1$,
$grad(h) \geq 1$ und $f = g * h$. Sei $grad(f) = n$.

Beweis:
Da f reduzibel in $\mathbb{Q}[x]$, gibt es g_1, h_1 mit $grad(g_1) = m \geq 1$
und $grad(h_1) = n - m \geq 1$. Dann gibt es $r, s \in \mathbb{Q}$ mit $r * g_1$ ist von
Einheitsform und $s * h_1$ ist von Einheitsform.
Sei $h = s * h_1$ und $g = r * g_1$. Dann ist $f = \frac{1}{r*s} * g * h$
$\frac{1}{r*s} = \frac{a}{b}$ mit $ggT(a, b) = 1 \succ b * f = a * h * g$.
Da f von Einheitsform, ist $a = \pm 1$.
Da $g * h$ von Einheitsform, ist $b = \pm 1 \succ f = h * g$ oder $f = (-h) * g$

Satz 5.4.2 *(Eisenstein)*
Ist $f \in \mathbb{Z}[x]$ mit $grad(f) = n$, $f = (a_i), i \in \mathbb{N}$.
Gibt es eine Primzahl p mit:

1. $p \nmid a_n$
2. $p | a_i,\ i = 0, \cdots, n-1$
3. $p^2 \nmid a_0,$

dann ist f irreduzibel in $\mathbb{Q}[x]$.

Beweis:

oBdA sei f von Einheitsform. Angenommen f ist reduzibel.
Dann gibt es $g = (b_i), i \in \mathbb{N}$ und $h = (c_i), i \in \mathbb{N}$ von Einheitsform.
$grad(g) = m \geq 1$ und $grad(h) = n - m$ und $f = g * h$
Somit ist $a_i = \sum_{l+k=i} b_l * c_k$
$p^2 \nmid a_0 = b_0 * c_0 \succ p \nmid b_0$ oder $p \nmid c_0$
oBdA gelte $p \nmid b_0$
Da $p \nmid a_n = b_m * c_{n-m} \succ p \nmid c_{n-m}$
Also gibt es ein kleinstes $i_0 \leq n - m$ mit $p \nmid c_{i_0}$
$a_{i_0} = \sum_{l+k=i_0} b_l * c_k = b_0 * c_{i_0} + \sum_{\substack{l+k=i_0 \\ k<i_0}} b_l * c_k$
$p | a_{i_0}$ und $p | \sum_{\substack{l+k=i_0 \\ k<i_0}} b_l * c_k \succ p | b_0 * c_{i_0}$
$\nexists$, da $p \nmid b_0$ und $p \nmid c_{i_0}$.

Beispiel: $x^5 - 10 * x - 2$ ist irreduzibel in $\mathbb{Q}[x]$.
$a_0 = -2,\ a_1 = -10,\ a_5 = 1\ (a_2 = a_3 = a_4 = 0)$
$\succ 2 | a_0 \succ 2 | a_1 \succ \alpha | a_2, a_3, a_4,\ 2 \nmid a_5$ und $4 \nmid a_0$.

5.5 Fundamentalsatz der Algebra

Sei $f \in \mathbb{C}[x]$ mit $grad(f) \geq 1$, dann besitzt f eine Nullstelle in $\mathbb{C}$.
$\mathbb{C}$ ist der $\mathbb{R}^2$ mit der zusätzlichen Multiplikation

$$(a,b) * (c,d) = (a*c - b*d, b*c + a*d)$$

Mit der Multiplikation kann man zusätzliche Funktonen definieren, z.B.:
Sei $f = (a_i) \in \mathbb{C}[x]$ mit $i \in \mathbb{N}$, ein Polynom mit $grad(f) = n$.
Dann sei $F_f : \begin{cases} \mathbb{R}^2 & \to & \mathbb{R}^2 \\ z & \mapsto & \sum_{i=0}^{n} a_i * z^i \end{cases}$
Man nennt F_f ebenfalls Polynom und schreibt auch f für F_f.
Der Beweis des Fundamentalsatzes zerfällt in drei Teile.
Sei $f \in \mathbb{C}[x]$ mit $grad(f) \geq 1$

1. f ist stetig
2. $|f|$ besitzt ein lokales Minimum.
3. Ist $f(z) \neq 0$, dann besitzt $|f|$ an der Stelle z kein lokales Minimum.

zu 1)

Lemma 5.5.1 $|z_1| * |z_2| = |z_1 * z_2|$

Beweis:

Sei $z_1 = (a,b)$ und $z_2 = (c,d)$.
$|z_1 * z_2|^2 = |(a*c - b*d, a*d + b*c)|^2$
$= (a*c - b*d)^2 + (c*d + b*c)^2$
$= a^2*c^2 - 2*a*b*c*d + b^2*d^2 + a^2*d^2 + 2*a*b*c*d + b^2*c^2$
$= (a^2 + b^2) * (c^2 + d^2)$
$= |z_1|^2 * |z_2|^2$

Lemma 5.5.2 *Sind f und g stetig an der Stelle z_0, so ist*
$f * g : \begin{cases} \mathbb{R}^2 & \to & \mathbb{Z}^2 \\ z & \mapsto & g(z) * f(z) \end{cases}$ *stetig an der Stelle z_0.*

Beweis:

Sei $a = f(z_0)$, $b = g(z_0)$. Sei $\epsilon > 0$. Wir wählen $\epsilon' > 0$ mit
$(\epsilon'^2) + |a| * \epsilon' + |b| * \epsilon' < \epsilon$.
Da f und g stetig an der Stelle z_0, gibt es ein $\delta > 0$, so
daß $|f(z) - a| < \epsilon'$ und $|g(z) - b| < \epsilon'$ für $|z - z_0| < \delta$.
Sei $|z - z_0| < \delta$. Dann gilt
$|f(z) * s(z) - a * b|$
$= |(f(z) - a) * (g(z) - b) + a * (g(z) - b) + b * (f(z) - a)|$
$\leq |f(z) - a| * |g(z) - b| + |a| * |g(z) - b| + |b| * |f(z)|$
$< \epsilon'^2 + |a| * \epsilon' + |b| * \epsilon'$
$< \epsilon$

Folgerung 5.5.1 *Sei $f \in \mathbb{C}[x]$, dann ist f stetig.*

Beweis:

Sei $f = \sum_{i=0}^{n} a_i * x^i$, $a_i : \begin{cases} \mathbb{R}^2 & \to & \mathbb{R}^2 \\ z & \mapsto & a_i \end{cases}$ ist stetig.

$x : \begin{cases} \mathbb{R}^2 & \to & \mathbb{R}^2 \\ z & \mapsto & z \end{cases}$ ist stetig.

Mit dem Lemma von Seite 68 und durch Induktion folgt:

$x^i : \begin{cases} \mathbb{R}^2 & \to & \mathbb{R}^2 \\ z & \mapsto & z^i \end{cases}$ ist stetig.

Aus dem Lemma von Seite 68 folgt:

$a_i x^i : \begin{cases} \mathbb{R}^2 & \to & \mathbb{R}^2 \\ z & \mapsto & a_i z^i \end{cases}$ ist stetig.

Induktion über n und Induktionsannahme:

$\sum_{i=0}^{m} a_i x^i : \begin{cases} \mathbb{R}^2 & \to & \mathbb{R}^2 \\ z & \mapsto & \sum_{i=0}^{m} a_i z^i \end{cases}$ ist stetig.

Ist $f = (a_i) \in \mathbb{C}[x]$ mit $i \in \mathbb{N}$ mit $grad(f) = n$, dann ist

$$f : \begin{cases} \mathbb{R}^2 & \to & \mathbb{R}^2 \\ z & \mapsto & \sum_{i=0}^{n} a_i z^i \end{cases}$$

stetig.

zu 2)

Satz 5.5.1 *Ist $f \in \mathbb{C}[x]$ ein normiertes Polynom mit $grad(f) = n \geq 2$, dann besitzt $|f|$ ein lokales Minimum.*

Beweis:

Sei $f = (a_i), i \in \mathbb{N}$

Sei $r = \sum_{i=0}^{n} |a_i| \succ |r| > a_0$ und $|r| > 1$

Sei $K = \{z| \ |z| \leq r\}$

Dann ist K kompakt.

$$|f| = \begin{cases} \mathbb{R}^2 & \to & \mathbb{R}^2 \\ z & \mapsto & |f(z)| \end{cases}$$

Dann ist f stetig.

Also gibt es ein $z_0 \in K$ mit $|f(z_0)| \leq |f(z)|$ für $z \in K$.

Dann $|f(z_0)| \leq |f(0)| = |a_0| < r$

Um zu zeigen, daß $|z_0| < r$ genügt es zu zeigen:

$|f(z)| \geq r$ für $|z| = r$

$|f(z)| = |\sum_{i=0}^{n} a_i z^i| \geq |z^n| - (\sum_{i=0}^{n-1} |a_i * z^i|)$

$= |z|^n - \sum_{i=0}^{n-1} |a_i| * |z^i|$

$= r^n - \sum_{i=0}^{n-1} |a_i| * r^i$

$\geq r^n - r^{n-1} * \sum_{i=0}^{n-1} |a_i|$

$= r^n - r^{m-1} * (r-1)$

r^{n-1}

$\geq r$

zu 3)

Wir wollen zu 3) zeigen:

Ist f ein Polynom mit $f(z_0) \neq 0$ und $grad(f) \geq 2$, dann besitzt f an der Stelle z_0 kein lokales Minimum.

Lemma 5.5.3 *Sei* $r(x) \in \mathbb{C}[x]$ *mit* $r(0) = 0$.
Sei $h = 1 - x^k + x^k * r(x)$.
Dann besitzt h *an der Stelle* 0 *kein lokales Minimum.*

Beweis:

Sei $\epsilon > 0$. Es genügt ein $t \in (0, \epsilon)$ zu finden, mit:
$|h(t)| < |h(0)| = 1$
Da $|r(0)| = 0$ und $|r|$ stetig ist, gibt es ein $t \in (0, \epsilon)$
mit $t < 1$ und $|r(t) < 1$
$|h(t)|$
$= |1 - t^k + t^k * r(t)|$
$\leq |1 - t^k| + |t^k * r(t)|$
$= 1 - t^k + |t^k| * |r(t)|$
$= 1 - t^k + t^k * |r(t)|$
$= 1 - t^k * (1 - \underbrace{|r(t)|}_{>0})$
$< 1 = h(0)|$

Satz 5.5.2 *Sei* $g \in \mathbb{C}[x]$ *mit* $grad(g) \geq 1$ *und* $g(0) \neq 0$.
Dann besitzt $|g|$ *an der Stelle* 0 *kein lokales Minimum.*

Beweis:

Sei $\epsilon > 0$. Es genügt ein z mit $|z| < \epsilon$ zu finden,
mit $|g(z)| < |g(0)|$.
Sei $k > 0$ mit $b_k \neq 0$ und $g = b_0 + b_k * x^k + \sum_{i=k+1}^{n} b_i * x^i$
Dann ist $g(0) = b(0) \neq 0$
$-\frac{b_0}{b_k} = r * e^{i*\nu}$
Sei $\alpha = \sqrt[k]{r} * e^{i\frac{\nu}{k}}$
$\frac{b_k}{b_0} * \alpha^k = -1$
$h(x) = \frac{g(\alpha * x)}{b_0}$
$= \frac{b_0}{b_0} + \frac{b_k}{b_0} * \alpha^k * x^k + \sum_{i=k+1}^{n} \frac{b_i}{b_0} * \alpha^i * x^i$
Sei $r(x) = \sum_{i=k+1}^{n} \frac{b_i}{b_0} \alpha^i * x^{i-k}$
Dann ist $h(x) = 1 - x^k + x^k * r(x)$
Da $r(0) = 0$ ist, besitzt $|h(x)|$ kein lokales Minimum
$\succ$Es gibt ein z_1 mit $|z_1| < \frac{\epsilon}{|\alpha|}$ und $|h(z_1)| < |h(0)|$
Sei $z = z_1 * \alpha \succ |z| = |z_1| * |\alpha| < \epsilon$
$|g(z)| = |g(z_1 * \alpha)| = |b_0| * |h(z_1)| < |g(0)| * |h(0)| = |g(0)|$

Folgerung 5.5.2 *Sei* $f \in \mathbb{C}[x]$ *mit* $grad(f) > 0$.
Sei $z_0 \in \mathbb{C}$ *mit* $f(z_0) \neq 0$.
Dann besitzt $|f|$ *an der Stelle* z_0 *kein lokales Minimum.*

Beweis:

Sei $\epsilon > 0$

Es genügt ein z zu finden, mit

$|z - z_0| < \epsilon$ und $|f(z)| < |f(z_0)|$

Sei $g(x) = f(x + z_0)$

Dann ist $g(0) = f(z_0) \neq 0$

Also gibt es z_1 mit $|z_1| < \epsilon$ und $|g(z_1)| < |g(0)|$

Sei $z = z_0 + z_1 \succ |z - z_0| < \epsilon$

$|f(z)| = |f(z_0 + z_1)| = |g(z_1)| < |g(0)| = |f(z_0)|$

Folgerung 5.5.3 *(Fundamentalsatz der Algebra)*
Ist $f \in \mathbb{C}[x]$ mit $grad(f) > 0$, dann besitzt f eine Nullstelle.

Beweis:

oBdA sei f normiert.

I.Fall: $grad(f) = 1$

$\succ f = x + a_0$

$\succ -a_0$ ist Nullstelle.

II. Fall: $grad(f) \geq 2$.

Dann besitzt f ein lokales Minimum an der Stelle z_0.

$\succ f(z_0) = 0$.

6 Körpertheorie

6.1 transzendente und algebraische Elemente

Sei $K \subseteq \mathbb{C}$, K heißt Unterkörper, wenn gilt:

1. $a, b \in K \succ a + b \in K$
2. $0, 1 \in K$
3. $a, b \in K \succ a * b \in K$
4. $a \in K, a \neq 0 \succ a^{-1} \in K$

Sei K ein Unterkörper von $\mathbb{C}$ und sei $\alpha \in \mathbb{C}$.
Wir hatten gezeigt:

$$\phi_\alpha : \begin{cases} K[x] & \to & \mathbb{C} \\ (a_i), i \in \mathbb{N} & \mapsto & \sum a_i * \alpha^i \end{cases}$$

ist ein Homomorphismus.
Man unterscheidet 2 Fälle:
I. Fall: $Kern(\phi) = \{0\}$
Dann heißt α transzendent über K.
II. Fall: sonst
Dann heißt α algebraisch über K.
Da $Kern(\phi_\alpha)$ ein Ideal ist, gibt es ein normiertes Polynom g
mit $Kern(\phi_\alpha) = (g_\alpha)$.

Lemma 6.1.1 *g_α ist irreduzibel.*

Beweis:
Angenommen g_α ist reduzibel. Dann gibt es f und h, mit $grad(f) < grad(g_\alpha)$ und $grad(h) < grad(g_\alpha)$ und $g_\alpha = f * h$.
$0 = \phi_\alpha(g_\alpha) = \phi_\alpha(f * h) = \phi_\alpha(f) * \phi_\alpha(h)$
$\succ \phi_\alpha(f) = 0$ oder $\phi_\alpha(h) = 0$
Sei oBdA $\phi_\alpha(f) = 0$
$\succ f \in Kern(\phi_\alpha) = (g_\alpha)$
$\succ f = r * g_\alpha$
$\succ grad(f) = grad(r) + grad(g_\alpha)$
Da $grad(f) < grad(g_\alpha)$
$\succ r = 0$
$\succ f = 0$
$\succ g_\alpha = 0$ ♯

g_α heißt Minimalpolynom von α.

Lemma 6.1.2 *Ist α algebraisch über K, dann ist*
$Bild(\phi_\alpha) := K(\alpha)$
ein Körper.

Beweis:

Sei $a \in K(\alpha), a \neq 0$, z.Z.: $a^{-1} \in K(\alpha)$
Sei $f \in K[x]$ mit $\phi_\alpha(f) = f(\alpha) = a \neq 0 \succ f \notin Kern(\phi_\alpha)$
Sei g_α das Minimalpolynom von α
$(g_\alpha) = Kern(\phi_\alpha) \succ g_\alpha \nmid f$
Da g_α irreduzibel ist, folgt $ggT(f, g_\alpha) = 1$
$\succ 1 = r * f + g_\alpha * s$, $r, s \in K[x]$
$\succ 1 = \phi_\alpha(1) = \phi_\alpha(r * f + g_\alpha * s) = \phi_\alpha(r) * \underbrace{\phi_\alpha(f)}_{=a} + \underbrace{\phi_\alpha(g_\alpha)}_{=0} * \phi_\alpha(s)$
$\succ 1 = \phi_\alpha(r) * a$
$a^{-1} = \phi_\alpha(r)$

Bemerkung 6.1.1 *Sei K ein Unterkörper von $\mathbb{C}$ und sein $\alpha \in \mathbb{C}$*

1. $\phi_\alpha : \left\{ \begin{array}{ccc} K[x] & \to & \mathbb{C} \\ (a_i), i \in \mathbb{N} & \mapsto & \sum a_i * \alpha^i \end{array} \right.$
   Sei α algebraisch über K, das heißt:
   $Kern(\phi_\alpha) \neq \{0\}$

2. *Es gibt ein irreduzibles Polynom g_α mit $Kern(\phi_\alpha) = (g_\alpha)$*
   g_α heißt Minimalpolynom von a

3. *$K(\alpha) := Bild(\phi_\alpha)$ ist ein Körper.*

Lemma 6.1.3 *Sei α algebraisch über K, dann ist $K(\alpha)$ der kleinste Unterkörper L von $\mathbb{C}$ mit $K \subseteq L$ und $\alpha \in L$*

Beweis:

Da $\phi_\alpha(x) = \alpha \succ \alpha \in K(\alpha)$
Da $\phi_\alpha(a) = a \succ a \in K(\alpha)$ für $a \in K$.
Sei L Unterkörper von $\mathbb{C}$ mit $K \subseteq L$ und $\alpha \in L$.
Sei $b \in K(\alpha)$. Sei $f = (a_i), i \in \mathbb{N} \in K[x]$ mit $\phi_\alpha(f) = \sum a_i * \alpha^i = b$
Da $\alpha \in L \succ \alpha^i \in L$.
Da $K \subseteq L \succ a_i * \alpha^i \in L$
$b = a_i * \alpha^i \in L$.

6.2 endliche Körpererweiterung

Bemerkung 6.2.1 *Sei L ein Unterkörper von $\mathbb{C}$ und K ein Unterkörper von L.*
Wir können L als Vektorraum über K auffassen,
denn $(L, +, 0)$ ist eine abelsche Gruppe und es gibt
für $a, b \in K$ und $\alpha, \beta \in L$

1. $1 * \alpha = \alpha$
2. $a * (\alpha + \beta) = a * \alpha + a * \beta$
3. $(a + b) * \alpha = a * \alpha + b * \alpha$
4. $(a * b) * \alpha = a * (b * \alpha)$

Beispiel:

1. $K = \mathbb{Q}$ und $L = \mathbb{R}$. Dann sind $1, \pi, \pi^2, \pi^3, \cdots$ linear unabhängig.
2. $K = \mathbb{R}$ und $L = \mathbb{C}$. Dann ist $\{1, i\}$ eine Basis von L über K.

Man nennt L eine endliche Körpererweiterung von K,
wenn die Dimension von L über K endlich.
Bezeichne $[L : K]$ die Dimension von L über K.

Satz 6.2.1 *Ist α algebraisch über K und g_α das Minimalpolynom von α, dann ist*
$[K(\alpha) : K] = grad(g_\alpha)$

Beweis:

Sei $grad(g_\alpha) = n$
Es genügt z.Z.: $1, \alpha, \alpha^2, \cdots, \alpha^{n-1}$ ist eine
Basis von $K(\alpha = L$ über K.
1) $1, \alpha, \cdots, \alpha^{n-1}$ erzeugen L.
Sei $b \in K(\alpha) \succ f \in K[x]$ mit $b = \phi_\alpha(f)$.
Dann gibt es $q, r \in K[x]$ mit:
$f = q * g_\alpha + r$ mit $grad(r) < grad(g_\alpha)$
Sei $r = (b_i), i \in \mathbb{N}$
$\succ b = \phi_\alpha(f) = \phi_\alpha(f) = \phi_\alpha(q * g_\alpha + r)$
$\overset{\phi_\alpha homomorph}{=} \phi_\alpha(q) * \phi_\alpha(g_\alpha) + \phi_\alpha(r)$
$= \phi_\alpha(r) = \sum_{i=0}^{n-1} b_i * \alpha^i$
$\succ \alpha^0 = 1, \alpha, \cdots, \alpha^{n-1}$ ist ein erzeugendes System.
2) $1, \alpha, \cdots, \alpha^{n-1}$ sind linear unabhängig.
Sei $0 = \sum_{i=0}^{n-1} c_i * \alpha^i \succ c_i = 0$ für $i = 0, \cdots, n-1$
Sei $f = \sum_{i=0}^{n-1} c_i * x^i \succ \phi_\alpha(f) = 0$
$\succ f \in kern(\phi_\alpha) = (g_\alpha)$.
Da $grad(f) < grad(g_\alpha) = n$
$\succ f = 0$
$\succ c_i = 0$ für $i = 0, \cdots$.

Satz 6.2.2 *Ist $[L:K]$ endlich und $\beta \in L$, dann ist β algebraisch über K.*

Beweis:

Sei $n = [L:K]$
Dann sind $1, \beta, \beta^2, \cdots, \beta^n$ linear abhängig.
Also gibt es $c_0, \cdots, c_n$ mit $c_i \neq 0$ für ein i mit $0 = \sum_{i=0}^{n} c_i * \beta^i$
Sei $f = \sum_{i=0}^{n} c_i * x^i$. Dann ist $f \neq 0$ und $\phi_\beta(f) = 0$
$\succ f \in Kern(\phi_\beta)$
$\succ Kern(\phi_\beta) \neq \{0\}$
$\succ \beta$ ist algebraisch über K.

Satz 6.2.3 *(Gradformel)*
Sei M Unterkörper von $\mathbb{C}$.
Sei L Unterkörper von M.
Sei K Unterkörper von L.
Sind $[L:K]$ und $[M:L]$ endlich, dann ist

$$[M:K] = [M:L] * [L:K]$$

Beweis:

Sei $[M:L] = m$ und $[L:K] = n$.
Sei $\{\alpha_1, \cdots, \alpha_n\}$ eine Basis von L über K
und sei $\{\beta_1, \cdots, \beta_m\}$ eine Basis von M über L.
Sei $B = \{\alpha_i * \beta_k | 1 \leq i \leq n \text{ und } 1 \leq k \leq m\}$
Es genügt z.Z. das B ein Basis von M über K ist.
Behauptung 1: B ist ein erzeugendes System.
Beweis:
Sei $\gamma = \sum_{i=1}^{n} c_i * \beta_i$
Da $c_i \in L$ gibt es $b_{i,k} \in K$ mit $c_i = \sum_{k=1}^{n} b_{i,k} * \alpha_k$
$\succ \gamma = \sum_{i=1}^{m} (\sum_{k=1}^{n} b_{i,k} * \alpha_k) * \beta_i = \sum_{i=1}^{m} \sum_{k=1}^{n} b_{ik} * (\alpha_k * \beta_i)$
Behauptung 2: B ist linear unabhängig.
Beweis:
$0 = \sum_{i=1}^{m} \sum_{k=1}^{n} b_i * \alpha * (\alpha_k * \beta_i)$
z.Z.: $b_{ik} = 0$ für $1 \leq i \leq m$ und $1 \leq k \leq n$
$0 = \sum_{i=1}^{m} \sum_{k=1}^{n} b_{ik} * (\alpha_k * \beta_k)$

$$= \sum_{i=1}^{m} (\underbrace{\sum_{k=1}^{n} b_{ik} * \alpha_k}_{\in L}) * \beta_k$$

$\{\beta_1, \cdots, \beta_m\}$ sind linear unabhängig.
$\succ \sum_{k=1}^{n} b_{ik} * \alpha_k = 0$ für $i = 1, \cdots, m$
$\{\alpha_1, \cdots, \alpha_n\}$ sind linear unabhängig.
$\succ b_{ik}$ für $1 \leq k \leq n$ und $1 \leq i \leq m$.

6.3 Einbettungen

Sei K ein Unterkörper von $\mathbb{C}$. Ein Ringhomomorphismus $\sigma : K \to \mathbb{C}$ heißt Einbettung.

Beispiel:

Sei $K = \mathbb{C}$.

Sei $id_C : \begin{cases} \mathbb{C} & \to & \mathbb{C} \\ z & \mapsto & z \end{cases}$ eine Einbettung.

Sei $\sigma : \begin{cases} \mathbb{C} & \to & \mathbb{C} \\ z & \mapsto & \overline{z} \end{cases}$ eine Einbettung.

Es gilt: $\sigma|\mathbb{R} = id\mathbb{R}$ und $id_C|\mathbb{R} = id_R$

$|\{\sigma, id_C\}| = [\mathbb{C}:\mathbb{R}]$

Lemma 6.3.1 *Ist $\sigma : K \to \mathbb{C}$ eine Einbettung, dann σ injektiv.*

Beweis:

Sei $a \in K$ mit $a \neq 0$

$1 = a^{-1} * a$

$\succ 1 = \sigma(1) = \sigma(a^{-1}) * \sigma(a)$

$\succ \sigma(a) \neq 0$

$\succ a \notin Kern(\sigma)$

$\succ Kern(\sigma) = \{0\}$

Sei $Bild(\sigma) = \sigma[K] =: K_\sigma$.

Folgerung 6.3.1 *$\sigma : H \to K_\sigma$ ist ein Isomorphismus und K_σ ist ein Körper.*
Sei $\sigma : K \to \mathbb{C}$ eine Einbettung.
Sei $\sigma^* : \begin{cases} K[x] & \to & K_\sigma[x] \\ (a_i), i \in \mathbb{N} & \mapsto & (\sigma(a_i)), i \in \mathbb{N} \end{cases}$

Lemma 6.3.2 *Seien $f, g \in K[x]$, dann gilt:*

1. $(f + g)_\sigma = f_\sigma + g_\sigma$
2. $(f * g)_\sigma = f_\sigma * g_\sigma$
3. $grad(f) = grad(f_\sigma)$

Also ist $\sigma^* : K[x] \to K_2[x]$ ein Isomorphismus.

Beweis:

zu 3)

Sei $f = (a_i), i \in \mathbb{N}$

$grad(f) = n \succ a_n \neq 0$ und $a_i = 0$ für $i > n$

$\succ \sigma(a_n) \neq 0$ und $\sigma(a_i) = 0$ für $i > n$

$\succ grad(f_\sigma) = grad(f)$

Lemma 6.3.3 *Ist $p \in K[x]$ irreduzibel , dann ist $p_\sigma \in K_\sigma[x]$ irreduzibel.*

Beweis:

Sei $p_\sigma = h_1 * g_1$ mit $h_1, g_1 \in K_\sigma[x]$.
z.Z.: $grad(h_1) = 0$ oder $grad(g_1) = 0$
Seien $h_2, g_2 \in K[x]$ mit $(h_2)_\sigma = h_1$ und $(g_2)_\sigma = g_1$
Dann ist $p_\sigma = (h_2)_\sigma * (g_2)_\sigma = (h_2 * g_2)_\sigma$
$\succ p = h_2 * g_2$
Da p irreduzibel ist, ist $grad(h_2) = 0$ oder $grad(g_2) = 0$
$\succ h_1 = (h_2)_\sigma = 0$ oder $g_1 = (g_2)_\sigma = 0$

Sei L ein Unterkörper von $\mathbb{C}$ mit $L \supseteq K$ und $[L : K] = n$ endlich.
τ heißt Fortsetzung von σ auf L, wenn $\tau \restriction K = \sigma$.
Ziel: $|\{\tau | \tau \text{ ist Fortsetzung von } \sigma \text{ auf } L\}| = [L : K]$.

Lemma 6.3.4 *Sei $\tau : L \to \mathbb{C}$ eine Fortsetzung von $\sigma : H \to \mathbb{C}$.*
Ist $f \in K[x]$ und $\alpha \in L$, dann gilt:

1. $\tau(f(\alpha)) = f_\sigma(\tau(\alpha))$

Insbesondere:

2. Ist α eine Nullstelle von f, dann $\tau(\alpha)$ Nullstelle von f_σ

Beweis:

1. Sei $f = \sum_{i=0}^n a_i * x^i$.
$\tau(f(\alpha)) = \tau(\sum_{i=0}^n a_i * \alpha^i) = \sum_{i=0}^n \tau(a_i) * \tau(\alpha^i)$
$\overset{homomorph}{=} \sum_{i=0}^n \tau(a_i) * \tau(\alpha)^i$
$\overset{\tau \restriction K = \sigma}{=} \sum_{i=0}^n \sigma(a_i) * \tau(\alpha)^i$
$= f_\sigma(\tau(\alpha))$.
2. $0 = \tau(0) = \tau(f(\alpha)) \overset{(1)}{=} f_\sigma(\tau(\alpha))$

Satz 6.3.1 *Sei p ein irreduzibles Polynom in $K[x]$.*
Sei α Nullstelle von p in $\mathbb{C}$ und
sei β Nullstelle von p_σ in $\mathbb{C}$
Dann gibt es genau eine Einbettung τ von $K(\alpha)$ in $\mathbb{C}$ mit:

1. τ setzt σ auf $K(\alpha)$ fort.

2. $\tau(\alpha) = \beta$.

Beweis:

Existenz:

Sei $\tau : \left\{ \begin{array}{ccc} K(\alpha) & \to & \mathbb{C} \\ f(\alpha) & \mapsto & f_\sigma(\beta) \end{array} \right.$

1. τ ist "wohldefiniert"

Sei $f(\alpha) = g(\alpha)$ z.Z. $f_\sigma(\beta) = g_\sigma(\beta)$.

Beweis:

Sei $I = \{h | h(\alpha) = 0\} = Kern(\phi_\alpha)$. Dann ist $I = (g_\alpha)$.
Da $p(\alpha) = 0 \succ p \in I$. Wenn p irreduzibel ist, dann ist $p = g_\alpha$.
Sei $f(\alpha) = g(\alpha) \succ (f - g)(\alpha) = 0$
$\succ f - g \in I \succ$ Es existiert h mit $p * h = f - g$.

$\succ f = g + p * h \succ f_\sigma + p_\sigma * h_\sigma$
$\succ f_\sigma(\beta) = g_\sigma(\beta) + \underbrace{p_\sigma(\beta)}_{=0} * h_\sigma(\beta)$
$\succ f_\sigma(\beta) = g_\sigma(\beta)$

2. τ ist Homomorphismus.
Beweis:
(1) Sei $f(\alpha), g(\alpha) \in K(\alpha)$
$\succ \tau(f(\alpha) + g(\alpha)) = \tau((f+g)(\alpha))$
$= (f+g)_\sigma(\beta) = f_\sigma(\beta) + g_\sigma(\beta)$
$= \tau(f(\alpha)) + \tau(g(\alpha))$
(2) $\tau(f(\alpha) * g(\alpha)) = \tau(f(\alpha))$.
$\tau(g(\alpha))$ ebenso.
(3) $\tau(1) = \sigma(1) = 1$.

Eindeutigkeit:
Seien τ_1, τ_2 Fortsetzungen von σ mit $\tau_1(\alpha) = \beta$ und $\tau_2(\alpha) = \beta$. z.Z.: $\tau_1 = \tau_2$
Sei $a = f(\alpha) \in K(\alpha)$. Sei $f = \sum_{i=0}^{n} a_i * x^i$
$\succ \tau_1(f(\alpha)) \overset{Lemma,S.\ 77}{=} f_\sigma(\tau_1(\alpha)) = f_\sigma(\beta)$
$= f_\sigma(\tau_2(\alpha)) \overset{Lemma,S.\ 77}{=} \tau_2(f(\alpha))$
$\succ \tau_1(a) = \tau_2(a)$ für alle $a \in K(\alpha)$.
Also $\tau_1 = \tau_2$.

Beispiel:
Sei $K = \mathbb{Q}$. Sei $\sigma = id_Q$. Sei $L = K(\sqrt[3]{2})$.
Wir wollen die Einbettung von L in $\mathbb{C}$ bestimmen, die σ fortsetzen.
Sei $p = x^3 - 2$. Dann ist p nach Eisenstein irreduzibel
und $\alpha_1 = \sqrt[3]{2}$ ist Nullstelle von p.
Die weiteren Nullstellen von $p_\sigma = p$ sind
$\alpha_2 = \sqrt[3]{2} * e^{\frac{2*\pi}{3}*i}$, $\alpha_2 = \sqrt[3]{2} * e^{\frac{4*\pi}{3}*i}$
Also gibt es drei Einbettungen von $\mathbb{Q}(\sqrt[3]{2})$ in $\mathbb{C}$, die id_Q fortsetzen:
1. $\tau_1 : \mathbb{Q}(\sqrt[3]{2}) \to \mathbb{C}$ mit $\tau_1(\sqrt[3]{2}) = \sqrt[3]{2}$
2. $\tau_1 : \mathbb{Q}(\sqrt[3]{2}) \to \mathbb{C}$ mit $\tau_1(\sqrt[3]{2}) = \alpha_2 = \sqrt[3]{2} * e^{\frac{2*\pi}{3}*i}$
3. $\tau_1 : \mathbb{Q}(\sqrt[3]{2}) \to \mathbb{C}$ mit $\tau_1(\sqrt[3]{2}) = \alpha_2 = \sqrt[3]{2} * e^{\frac{4*\pi}{3}*i}$

Folgerung 6.3.2 *Sei $\sigma : K \to \mathbb{C}$ eine Einbettung und α algebraisch über K.*
Dann gibt es genau $[K(\alpha) : K]$ viele Einbettungen von $K(\alpha)$ in $\mathbb{C}$, die σ fortsetzen.

Beweis:
Sei p das Minimalpolynom von α über K. Dann ist $[K(\alpha) : K] = grad(p) = n$.
Da p irreduzibel über K ist, ist p_σ irreduzibel über K_σ mit $grad(p_\sigma) = grad(p)$.
1. Es gibt $[K(\alpha) : K]$ viele Einbettungen von $K(\alpha)$ in $\mathbb{C}$.
Beweis:
Da p_σ irreduzibel ist, besitzt p_σ n-viele verschiedene
Nullstellen in $\mathbb{C}$. Diese seien $\beta_1, \cdots, \beta_n$.
Dann gibt es Einbettungen $\tau_i, 1 \leq i \leq n$ mit $\tau_i(\alpha) = \beta_i$

für $i = 1, \cdots, n$, die σ fortsetzen.

2. Es gibt genau $[K(\alpha) : K]$ viele Fortsetzungen von σ.

Beweis:

Sei $\tau_K(\alpha) \to \mathbb{C}$ eine Einbettung die σ fortsetzt.

Aus dem Lemma von Seite 77$\succ$ Es gibt ein i mit $\tau(\alpha) = \beta(i)$

Aus dem Satz von Seite 77$\succ$ $\tau = \tau_i$.

Folgerung 6.3.3 *Sei $\sigma : K \to \mathbb{C}$ ein Einbettung.*
Ist $[L : K] = n$ endlich, dann ist
$|\{\tau | \tau$ *setzt σ auf L fort*$\}| = [L : K]$

Beweis: (Induktion über $n = [L : K]$)

Sei $n = 1$. Dann ist $L = K$.

Sei $n > 1$. Sei $\alpha \in L \setminus K$. Dann ist

$[L : K] = [L : K(\alpha)] * [K(\alpha) : L]$

Nach der Folgerung von Seite 78 ist

$|\{\tau | \tau$ setzt σ auf $K(\alpha)$ fort$\}| = [K(\alpha) : K]$

Sei τ eine Fortsetzung von σ auf $K(\alpha)$.

Da $[L : K(\alpha)] < m$ ist, ist nach Induktionsvoraussetzung

$|\{\delta | \delta$ ist eine Fortsetzung von τ auf $L\}| = [L : K(\alpha)]$

$\succ |\{\delta | \delta$ ist eine Fortsetzung von σ auf $L\}| = |K(\alpha) : K] * [L : K(\alpha)] = [L : K]$

Satz 6.3.2 *(Satz von primitiven Elementen)*
Sei L eine endliche Körpererweiterung von K, dann gibt es ein $\gamma \in L$ mit $L = K(\gamma)$.
$K(\alpha_1, \alpha_2) = (K(\alpha_1)) * (\alpha_2)$
$K(\alpha_1, \cdots, \alpha_n) = K(\alpha_i, \cdots, \alpha_{n-1}) * (\alpha_n)$

Beweis:(Induktion über $[L : K] = n$)

$n = 1 \succ K = K(a)$

Sei $n > 1$. Sei $\alpha \in L \setminus K$.

Dann $[K(\alpha) : K] \geq 2$ und $[L : K(\alpha)] * [K(\alpha) : K] = n$

$\succ [L : K(\alpha)] < n$.

Also gibt es nach Induktionsvoraussetzung ein $\beta \in L$ mit $L = K(\alpha, \beta)$.

Es genügt ein c zu finden, mit

$[K(\alpha + c * \beta) : K] = n = [L : K]$

Nach der Folgerung von Seite 79 ist

$|\{\sigma_1, \cdots, \sigma_n\}| = |\{\sigma | \sigma$ ist K-Einbettung von $L\}| = [L : K] = n$

Sei $f = \prod_{i=1}^{n} * \prod_{\substack{j=1 \\ j \neq i}}^{n} [(\sigma_i(\alpha) - \sigma_j(\alpha)) + x * (\sigma_i(\beta) - \sigma_j(\beta)]$

Behauptung: $f \neq 0$

Beweis:

Angenommen $f = 0$. Dann gibt es $i \neq j$ mit

$\sigma_i(\alpha) = \sigma_j(\alpha)$ und $\sigma_i(\beta) = \sigma_j(\beta)$

Da $\sigma_i(\alpha) = \sigma_j(\alpha) \succ \sigma_i \restriction K(\alpha) = \sigma_j \restriction K(\alpha)$

Da $\sigma_i(\beta) = \sigma_j(\beta) \succ \sigma_i = \sigma_i \restriction K(\alpha, \beta) = \sigma_j \restriction K(\alpha.\beta) = \sigma_j$

$\succ \sigma_j = \sigma_j$ $\quad \sharp$zur Wahl von σ_i und σ_j.

Da K unendlich ist, gibt es ein $c \in K$ mit $f(c) \neq 0$.
Dann ist für $i \neq j$:

$\sigma_i(\alpha) = \sigma_j(\alpha) + c * (\sigma_i(\beta)) \neq 0$
$\sigma_i(\alpha + c * \beta) = \sigma_i(\alpha) + c * \sigma_i(\beta)$
$\neq \sigma_j(\alpha) + c * \sigma_j(\beta) = \sigma_j(\alpha + c * \beta)$

Sei $\gamma = \alpha + c * \beta$, dann ist $\sigma_i(\gamma) \neq \sigma_j(\gamma)$ für $i \neq j$.
Also gibt es n-viele K-Einbettungen von $K(\gamma)$ in $\mathbb{C}$.
$\succ [K(\gamma) : K] \geq n$. Da $K(\gamma) \subseteq L \succ K(\gamma) = L$

Seien L, K Unterkörper von $\mathbb{C}$ mit $K \subseteq L$ und $[L : K]$ endlich.
Wir nennen eine Einbettung σ von L eine K-Einteilung, wenn $\sigma \restriction K = id_K$.

Folgerung 6.3.4 $[L : K] = |\{\sigma | \sigma$ *ist K-Einbettung von* L *in* $\mathbb{C}\}|$

6.4 Zerfällungskörper

Sei σ eine Einbettung von L in $\mathbb{C}$. σ heißt Automorphismus, wenn $L_\sigma = L$

Beispiel:

Nicht jede K-Einbettung ist ein K-Automorphismus.
$K = \mathbb{Q}$ $L = \mathbb{Q}(\sqrt[3]{2})$
$p = x^3 - 2$ ist das Minimalpolynom von $\sqrt[3]{2}$
Die Nullstellen von p sind $\sqrt[3]{2}$, $\sqrt[3]{2} * e^{i*\frac{2*\pi}{3}}$, $\sqrt[3]{2} * e^{i*\frac{4*\pi}{3}}$.
Dann ist σ_1 mit $\sigma_1(\sqrt[3]{2}) = \sqrt[3]{2}$ ein K-Automorphismus.
Aber σ_2 mit $\sigma_2(\sqrt[3]{2}) = \sqrt[3]{2} * e^{i*\frac{2*\pi}{3}}$ ist kein K-Automorphismus,
da $L_\sigma \not\subseteq \mathbb{R}$ und $L \subseteq \mathbb{R}$

Eine endliche Körpererweiterung L von K heißt Galois-Erweiterung, wenn jede K-Einbettung von L in $\mathbb{C}$ ein K-Automorphismus ist.

Beispiel: $\mathbb{Q}[\sqrt[3]{2}]$ ist keine Galois-Erweiterung.

L heißt Zerfällungskörper über K, wenn es ein Polynom f gibt, mit $L = K(\alpha_1, \cdots, \alpha_n)$, wobei $\alpha_1, \cdots, \alpha_n$ Nullstellen von f sind.

Beispiel:

$\mathbb{Q}(\sqrt[3]{2}, e^{i*\frac{2*\pi}{3}}) = Q(\sqrt[3]{2}, \sqrt[3]{2} * e^{i*\frac{2*\pi}{3}}, \sqrt[3]{2} * e^{i*\frac{4*\pi}{3}})$
ist ein Zerfällungskörper. Dabei ist $f = x^3 - 2$.

Satz 6.4.1 *Sei L ein endliche Erweiterung von K $\hookleftarrow$*
1) L ist Galoiserweiterung von K
2) L ist Zerfällungskörper über K

Beweis:

$1 \succ 2$

Da $[L : K]$ endlich, gibt es ein γ mit $L = K(\gamma)$. Sei p das Minimalpolynom von γ über K. Seien $\alpha_1, \cdots, \alpha_n$ die Nullstellen von p.
Dann ist $K(\alpha_1, \cdots, \alpha_n)$ ein Zerfällungskörper.
$L = K(\gamma) = K(\alpha_1, \cdots, \alpha_n)$
Da $\gamma \in \{\alpha_1, \cdots, \alpha_n\}$ ist $K(\gamma) \subseteq K(\alpha_1, \cdots, \alpha_n)$
"$\supseteq$" Da p irreduzibel ist, gibt es zu jedem α_i eine K-Einbettung σ von $K(\gamma)$ in $\mathbb{C}$ mit $\sigma(\gamma) = \alpha_i$
Da L eine Galoiserweiterung ist, ist $L_\sigma = L$
$\sigma(\gamma) = \alpha_i \in L \succ \alpha_1, \cdots, \alpha_n \in L$
$K(\gamma) = L \supseteq K(\alpha_1, \cdots, \alpha_n)$

$2 \succ 1$

Sei f ein Polynom und $\alpha_1, \cdots, \alpha_n$ die Nullstellen von f mit $L = K(\alpha_1, \cdots, \alpha_n)$
Sei σ eine K-Einbettung. z.Z.: $L_\sigma = L$.
Da α_i Nullstelle von f ist, ist $\sigma(\alpha_i)$ Nullstelle von f.

Da σ injektiv ist, ist $\{\sigma(\alpha_1), \cdots, \sigma(\alpha_n)\} = \{\alpha_1, \cdots, \alpha_n\}$
Also $L_\sigma = K(\sigma(\alpha_1), \cdots, \sigma(\alpha_n)) = K(\alpha_1, \cdots, \alpha_n) = L$

Folgerung 6.4.1 *Ist L eine Galoiserweiterung von K und p ein irreduzibles Polynom aus $K[x]$, besitzt p eine Nullstelle von L, so sind alle Nullstellen von p aus L.*

Beweis:

Sei $\alpha \in$ Nullstellen von p mit $\alpha \in L$.
Sei β eine Nullstelle von p in $\mathbb{C}$. Dann gibt es eine
K-Einbettung σ von $K(\alpha)$ in $\mathbb{C}$ mit $\sigma(\alpha) = \beta$
Sei τ eine Fortsetzung von σ auf L. Da L galloisch ist,
ist $L_\tau = L \succ \tau(\alpha) = \sigma(\alpha) = \beta \in L$.

Sei L eine endliche Erweiterung von K, dann sei

$$G_{L:K} = \{\sigma | \sigma \text{ ist K-Automorphismus } L\}$$

Dann ist $(G_{L:K}, \circ, id_L)$ eine Gruppe.
$G_{L:K}$ heißt Galoisgruppe von L über K.

Ein Körper M heißt Zwischenkörper von L und K, wenn $L \subseteq M \subseteq K$.

Lemma 6.4.1 *Ist M ein Zwischenkörper von K und L. Dann ist $G_{L:M} \subseteq G_{L:K}$.*

Beweis:

Sei $\sigma \in G_{L:M} \succ$ Für alle $a \in M$ ist $\sigma(a) = a$
$\succ$ Für alle $a \in K \subseteq M$ ist $\sigma(a) = a$
$\succ \sigma \in G_{L:K} \succ G_{L:M} \subseteq G_{L:K}$.
Da $G_{L:M}$ eine Gruppe ist, ist $G_L : M \subseteq G_{L:K}$

Sei $H \subset G_{L:K}$. Dann sei $L^H := \{a \in L | \sigma(a) = a \text{ für alle } \sigma \in H\}$.

Ich sollte doch Schluß machen, aber ich muß das noch machen ! (Podewski)

Satz 6.4.2 *Ist $H < G_{L:K}$, dann L^H Zwischenkörper von L und K.*

Beweis:

$a \in L^H$ gdw $\sigma(a) = a$ für alle $\sigma \in H$.
1) $a, b \in L^H \succ a + b \in L^H$
Beweis:

$\sigma(a + b) = \sigma(a) + \sigma(b) = a + b$ für alle $\sigma \in H \succ a + b \in L^H$

2) $a, b \in L^H \succ a * b \in L^H$
Beweis:

wie 1)

3) Sei $a \in L^H$ und $a \neq 0 \succ a^{-1} \in L^H$
Beweis:

$\sigma(a^{-1} = \sigma(a)^{-1} = a^{-1}$ für alle $\sigma \in H \succ a^{-1} \in L^H$.

Seien L, K Unterkörper von $\mathbb{C}$ mit $K \subseteq L$.
Sei $G_{L:K} = \{\sigma | \sigma \text{ ist Automorphismus von } L \text{ mit } \sigma \restriction K = ig_K\}$

Wir hatten gezeigt:

1. Ist M ein Zwischenkörper von K und L, dann ist $G_{L:M} < G_{L:K}$
2. Ist $H < G_{L:K}$, dann ist $L^H = \{a \in L | \sigma(a) = a \text{ für all } \sigma \in H\}$
   ein Zwischenkörper von L und L^H und heißt auch Fixkörper von H.

L heißt Galois-Erweiterung von K, wenn jede K-Einbettung von L in $\mathbb{C}$ ein K-Automorphismus ist, d.h.:

Für jeden injektiven Homomorphismus σ von L in $\mathbb{C}$ mit $\sigma \restriction K = id_K$
ist $\sigma[L] \subseteq L$

Satz 6.4.3 *Sei L eine Galois-Erweiterung von K*
und M ein Zwischenkörper von L und K.
Sei $H = G_{M:K}$, dann ist $M = L^H$.

Beweis:

"$\subseteq$"

Sei $a \in M$ und $\sigma \in H = G_{M:K}$
$\succ \sigma(a) = a$
$\succ a \in L^H$

"$\supseteq$"

Angenommen $L^H \setminus M$. Sei $p \in M[x]$ das Minimalpolynom von α über M.
Da $\alpha \neq M$ ist $grad(p) \geq 2$
Also gibt es eine Nullstelle β von p mit $\beta \neq \alpha$.
(Da L eine Galois-Erweiterung von K ist, ist $\beta \in L$).
Dann gibt es eine M-Einbettung τ von $M(\alpha)$ in $\mathbb{C}$ mit $\tau(\alpha) = \beta$.
Da $[L : K]$ endlich ist, ist $[L : M(\alpha)]$ endlich. Also gibt es eine
K-Einbettung σ von L in $\mathbb{C}$ mit $\sigma \restriction M(\alpha) = \tau$.
Da L eine Galois-Erweiterung von K ist, ist $\sigma \in G_{L:M}$.
Da $\sigma \restriction M = id_M$ ist $\sigma \in G_{L:K}$.
Da $\sigma(a) = \beta \neq \alpha \succ \alpha \in L^H$ ♯

Satz 6.4.4 *Sei L eine Galois-Erweiterung von K und $H < G_{L:K}$.*
Sei $M = L^H$, dann ist $G_{L:M} = H$.

Beweis:

Nach Definition von M ist $H \subseteq G_{L:M}$.
Es genügt zu zeigen: $|G_{L:M}| \leq |H|$.
Da $[L : M]$ endlich ist, gibt es ein $\gamma \in L$ mit $L = M(\gamma)$
(Satz vom primitiven Element, S. 79).
Sei $f = \prod_{\sigma \in H}(x - \sigma(\gamma))$
Dann gilt:

1. $f(\gamma) = 0$
2. $grad(f) = |H|$
3. $f \in M[x]$

zu 3)

Sei $\tau \in H$

$f_\tau = \prod_{\sigma \in H}(x - \tau(\sigma(\gamma)) = \prod_{\sigma \in H}(x - \sigma(\gamma)) = f$

Also sind alle Koeffizienten von f aus M, somit ist $f \in M[x]$.

Sei p das Minimalpolynom von γ über M. Dann ist
$grad(p) < grad(f) = |H|$ und $[L : M] = |M(\alpha) : M] = grad(p) \leq |H|$.
$|G_{L:M}| = |G_{M(\alpha):M}| \leq grad(p) \leq |H|$.

Satz 6.4.5 *(Fundamentalsatz der Galois-Theorie)*
Sei L eine Galois-Erweiterung von K. Dan ist die Zuordnung $M \mapsto G_{L:M}$, wobei M ein Zwischenkörper von L und K ist, eine bijektive Abbildung der Menge aller Zwischenkörper auf die Menge aller Untergruppen von $G_L : K$
Ferner gilt:

Der Fixkörper von $G_{L:M}$ ist M

Beweis:

1. injektiv:

   Sei $G_{L:M_1} = G_{L:M_2} = H \overset{Seite\ 83}{\succ} M_1 = L^H = M_2$

2. surjektiv:

   Sei $H < G_{L:K}$. Sei $M = L^H \overset{Seite\ 84}{\succ} G_{L:M} = H$

   Sei $H = G_{L:K}$. Nach dem Satz von Seite 83 ist $L^H = M$.

Lemma 6.4.2 *Sei L eine Galois-Erweiterung von K und sei M ein Zwischenkörper von L und K.*
Ist M eine Galois-Erweiterung von K, dann ist $G_{L:M} \lhd G_{L:K}$ und $G_{L:K}/G_{L:M} \approx G_{M:K}$

Beweis:

Sei $\sigma \in G_{L:K}$. Dann ist $\sigma \restriction M$ eine K-Einbettung von M in $\mathbb{C}$.
Da M über K eine Galois-Erweiterung ist, ist $\sigma \restriction M \in G_{M:K}$
Sei $\phi : \left\{ \begin{array}{ccc} G_{L:K} & \to & G_{M:K} \\ \sigma & \mapsto & \sigma \restriction M \end{array} \right.$.
Dann ist ϕ ein Homomorphismus, da $\sigma \circ \tau \restriction M = \sigma \restriction M \circ \tau \restriction M$
Behauptung: $Kern(\phi) = G_{L:M}$
Beweis:

$\sigma \in G_{L:M}$, gdw. $\sigma \restriction M = id_M$, gdw. $\sigma \in Kern(\phi)$.

Behauptung: $Bild(\phi) = G_{M:K}$
Beweis:

Sei $\tau \in G_{M:K}$. Dann gibt es eine K-Einbettung σ von L in $\mathbb{C}$,
die τ fortsetzt. Da L über K eine Galois-Erweiterung ist, ist $\sigma \in G_{L:K}$
Da $\sigma \restriction M = \tau$, ist $\tau \in Bild(\phi)$
$G_{M:K} = Bild(\phi) \approx G_{L:K}/Kern(\phi) = G_{L:K}/G_{L:M}$.

7 Lösbarkeit von Gleichungen durch Radikale

7.1 Definitionen

ZIEL: Sei K ein Körper und $f \in K[x]$.
Gesucht sind die Lösungen von $f(x) = 0$.

Beispiel:
$x^2 + a * x + b = 0$
$x_{1,2} = -\frac{a}{2} \pm \sqrt{\frac{a^2}{4} - b}$

$f(x) = 0$ heißt durch Radikale lösbar, wenn man die Lösung mit den sechs Grundrechenarten finden kann, d.h. mit Hilfe von:

1. der Addition
2. der Subtraktion
3. der Multiplikation
4. der Division
5. potenzieren
6. n-te Wurzel ziehen

Ein Oberkörper L von K heißt Radikalerweiterung von K, wenn es $\alpha_1, \cdots, \alpha_n$ gibt, mit $m_1, \cdots, m_n$ und:

1. $L = K(\alpha_1, \cdots, \alpha_n)$
2. $\alpha_i^{m_i} \in K(\alpha_1, \cdots, \alpha_{i-1})$

$f(x) = 0$ ist durch Radikale lösbar,wenn es eine Radikalerweiterung L von K gibt, die alle Nullstellen von f enthält.
Wir hatten einen Oberkörper L von K eine Radikalerweiterung genannt, wenn es $\alpha_1, \cdots, \alpha_n$ und $m_1, \cdots, m_n$ gibt, mit:

1. $L = K(\alpha_1, \cdots, \alpha_n)$
2. $\alpha_i^{m_i} \in K(\alpha_1, \cdots, \alpha_{i-1})$

Sei $f(x) \in K[x]$, $\beta_1, \cdots, \beta_n$ die Nullstellen von $f(x)$ und $N = K(\beta_1, \cdots, \beta_n)$.
$f(x) = 0$ ist durch Radikale lösbar,
wenn es eine Radikalerweiterung L von K gibt mit $N \subseteq L$.
Man sagt dann auch $f(x) = 0$ ist auflösbar.

ZIEL:

1. Ist $f(x) = 0$ auflösbar, dann ist $G_{N:K}$ auflösbar.
2. Ist $f(x) = x^5 - r * x + 3$, dann ist $G_{N:K} \approx S_5$ und somit ist $G_{N:K}$ nicht auflösbar.

7.2 Radikalerweiterungen

ZIEL:
Ist L eine Radikalerweiterung von K, dann gibt es $M_0 \subseteq M_1 \subseteq \cdots \subseteq M_l$ mit

1. $M_0 = K$, $L \subseteq M_l$ und M_l ist Galois-Erweiterung von K
2. M_{i+1} ist Galois-Erweiterung von M_i und $G_{M_{i+1}:M_i}$ ist abelsch.

ξ heißt n-te Einheitswurzel, wenn $\xi^n = 1$.
ξ heißt n-te primitive Einheitswurzel, wenn $\xi, \xi^2, \cdots, \xi^n$ alle n-ten Einheitswurzeln sind.

Beispiel:
$e^{\frac{2*k*\pi*i}{n}} = cos(\frac{2*k*\pi}{n}) + i * sin(\frac{2*k*\pi}{n})$ ist eine n-te Einheitswurzel.
$e^{\frac{2*\pi*i}{n}}$ ist n-te primitive Einheitswurzel.

Lemma 7.2.1 *Sei L eine Galois-Erweiterung von K und ξ eine n-te primitive Einheitswurzel, dann gilt:*

1. *$L(\xi)$ ist eine Galois-Erweiterung von K.*
2. *$G_{L(\xi):L}$ ist abelsch.*

Beweis:

Behauptung:
Ist G eine K-Einbettung von $L(\xi)$ in $\mathbb{C}$,
dann ist $\sigma(\xi) = \xi^k$ für ein k mit $0 \leq k \leq n$.

Beweis:
ξ ist Nullstelle von $x^n - 1 = f(x)$.
Da $f_\sigma = f$, ist $\sigma(\xi)$ eine Nullstelle von $x^n - 1$
$\succ$ $\sigma(\xi)$ Einheitswurzel.
$\succ$ Es gibt ein k mit $\sigma(\xi) = \xi^k$

zu 1:
Sei σ eine K-Einbettung von $L(\xi)$ in $\mathbb{C}$.
$\sigma[L(\xi)] = L(\sigma(\xi)) = L(\xi^k) \subseteq L(\xi)$
$\succ$ σ ist ein L-Automorphismus
$\succ$ $L(\xi)$ ist eine Galois-Erweiterung.

zu 2:
Seien $\tau, \sigma \in G_{L(\xi):L}$
$\succ$ Es gibt k, l mit $\sigma(\xi) = \xi^k$, $\tau(\xi) = \xi^l$
$\succ$ $\sigma \circ \tau(\xi) = \sigma(\xi^l) = \sigma(\xi)^l = (\xi^k)^l = \xi^{k*l}$
$\tau \circ \sigma(\xi) = \tau(\xi^k) = \tau(\xi)^k = (\xi^l)^k = \xi^{k*l}$
Da es nur eine Einbettung σ gibt, mit $\sigma(\xi) = \xi^{l*k}$
$\succ$ $\tau \circ \sigma = \sigma \circ \tau$

Lemma 7.2.2 *Sei L eine Erweiterung von K, die eine n-te primitive Einheitswurzel enthält.*
Ist $\alpha^n \in L$, dann gilt:

1. *$L(\alpha)$ ist eine Galois-Erweiterung von L.*
2. *$G_{L(\alpha):L}$ ist abelsch.*

Beweis:

Sei $\xi \in L$ eine n-te primitive Einheitswurzel.
Behauptung:
Ist σ eine L-Einbettung von $L(\alpha)$ in $\mathbb{C}$.
Dann gibt es ein k mit $\sigma(\alpha) = \alpha * \xi^k$
Beweis:
Sei $a = \alpha^n \in L$. Da α Nullstelle von $x^n - a$ ist,
ist auch $\sigma(\alpha)$ Nullstelle von $x^n - a$.
Somit ist $(\frac{\sigma(\alpha)}{\alpha})^n = \frac{\sigma(\alpha^n)}{\alpha^n} = \frac{\sigma(\alpha)^n}{\alpha^n} = \frac{a}{a} = 1$.
Also ist $\frac{\sigma(\alpha)}{\alpha}$ eine n-te primitive Einheitswurzel,
also gibt es ein k mit $\frac{\sigma(\alpha)}{\alpha} = \xi^k \succ \sigma(\alpha) = \xi^k * \alpha$.
zu 1:
Sei σ eine L-Einbettung von $L(\xi)$ in $\mathbb{C}$
$\succ G[L(\alpha)] = L(G(\alpha)) = L(\alpha * \xi^k) = L(\alpha)$.
Also ist σ ein L-Automorphismus.
zu 2:
$\sigma, \tau \in G_{L(\alpha):L}$.
Dann gibt es l und k mit $\sigma(\alpha) = \alpha * \xi^k$ und $\tau(\alpha) = \alpha * \xi^l$.
$\tau \circ \sigma(\alpha) = \alpha * \xi^{l+k}$, $\sigma \circ \tau(\alpha) = \alpha * \xi^{l+k}$
Da es nur ein σ mit $\sigma(\alpha) = \alpha^{l+k}$ gibt
$\succ \tau \circ \sigma = \sigma \circ \tau$.

Frage:

Sei L eine Galois-Erweiterung von K und N eine Galois-Erweiterung von L.
Ist N eine Galois-Erweiterung von K ?

Anzwort:

Nein: nicht immer. Sei $K = \mathbb{Q}$. Sei $L = \mathbb{Q}(\sqrt{2})$.
Sei N der Zerfällungskörper $x^3 - \sqrt{2}$. Aber N ist keine Galois-Erweiterung von K.

Satz 7.2.1 *Sei L eine Galois-Erweiterung von K und $\alpha^n \in L$. Dann gibt es $\alpha_1, \cdots, \alpha_m \in \mathbb{C}$ mit:*

1. *$\alpha \in \{\alpha_1, \cdots, \alpha_n\}$*
2. *$\alpha_i^n \in L$*
3. *$L(\alpha_1, \cdots, \alpha_n)$ ist Galois-Erweiterung von K.*

Beweis:

Sei $a = \alpha^n \in L$.
Sei $g = \prod_{\alpha \in G_{L:K}} (x^n - \sigma(a))$.
Seien $\alpha_1, \cdots, \alpha_n$ die Nullstellen von g und $M = L(\alpha_1, \cdots, \alpha_m)$.
Dann gilt:

zu 1:

$\alpha \in \{\alpha_1, \cdots, \alpha_n\}$, da $id_L \in G_{L:K}$.

zu 2:

Da α_i Nullstelle von g ist, gibt es ein σ mit α_i ist
Nullstelle von $x^n - \sigma(a)$.
$\succ \alpha_i^n = \sigma(a)$.
Da L eine Galois-Erweiterung von K
$\succ \sigma(a) \in L$.

zu 3:

Sei τ eine Einbettung von $M = L(\alpha_1, \cdots, \alpha_n)$ in $\mathbb{C}$
$\succ \tau[M] = L(\tau(\alpha_1), \cdots, \tau(\alpha_m))$
Es genügt z.Z.: $\tau(\alpha_i) \in \{\alpha_1, \cdots, \alpha_m\}$, denn
dann ist $\tau[M] \subseteq M$.
Da L eine Galois-Erweiterung von K, ist $\tau \restriction L \in G_{L:K}$.
Da α_i Nullstelle von g ist, gibt es $\sigma \in G_{L:K}$
mit α_i ist Nullstelle von $x^n - \sigma(a)$.
$\succ \tau(\alpha_i)$ ist Nullstelle von $x^n - \tau(\sigma(a))$.
Da $\tau \circ \sigma \in G_{L:K} \succ \tau(\alpha_i)$ ist Nullstelle von g.

Satz 7.2.2 *Sei L eine Galois-Erweiterung von K und $\alpha \in \mathbb{C}$ mit $\alpha^n \in L$. Dann gibt es eine Kette*

$$M_0 \subseteq M_1 \subseteq \cdots \subseteq M_l$$

mit

1. *$L = M_0$, $L(\alpha) \subseteq M_l$ und M_l ist Galois-Erweiterung von K.*
2. *M_{i+1} ist Galois-Erweiterung von M_i und $G_{M_{i+1}:M_i}$ ist abelsch.*

Beweis:

Sei $M_0 = L$.
Sei $M_1 = M_0(\xi)$ mit ξ ist n-te primitive Einheitswurzel.
1. M_1 ist eine Galois-Erweiterung von K
2. M_1 ist eine Galois-Erweiterung von M_0 und $G_{M_1:M_0}$ ist abelsch.
Da $\alpha^n \in M_1$, gibt es $\alpha_1, \cdots, \alpha_m \in \mathbb{C}$ mit
$\alpha \in \{\alpha_1, \cdots, \alpha_m\}$, $\alpha_i^n \in M_1$ und $M_1(\alpha_1, \cdots, \alpha_n)$ ist Galois-Erweiterung von K.
$M_{i+1} = M_i(\alpha_i)$ für $i \geq 1$.
Dann ist $\alpha \in M_{m+1}$ und somit $L(\alpha) \subseteq M_{m+1}$
und M_{i+1} ist Galois-Erweiterung von M_i mit $G_{M_{i+1}:M_i}$ abelsch
nach dem Lemma von Seite 87.

Folgerung 7.2.1 *Sei L eine Radikalerweiterung von K.*
Dann gibt es eine Körperkette

$$M_0 \subseteq \cdots \subseteq M_k$$

mit

1. $M_0 = K$, $L \subseteq M_k$.
2. M_{i+1} *ist eine Galois-Erweiterung von* M_i *mit* $G_{M_{i+1}:M_i}$ *abelsch.*
3. M_k *ist Galois-Erweiterung von* K.

Sei $f \in K[x]$ und F der Zerfällungskörper von F.
Wir wollen zeigen:

Ist $f(x) = 0$ auflösbar, dann ist $G_{F:K}$ auflösbar.

7.3 Mehr über auflösbare Gruppen

Lemma 7.3.1 *Ist G auflösbar und ϕ ein Homomorphismus von G, dann ist $\phi[G]$ auflösbar.*

Beweis:

G auflösbar, d.h. Es gibt eine Kette von Gruppen

$G_0 \supseteq G_1 \supseteq \cdots G_l$.

mit:

1. $G_0 = G_1, \cdots, G_l = \{e\}$
2. $G_{i+1} \lhd G_i$
3. G_i/G_{i+1} ist zyklisch.

Sei $H_i = \phi[G_i]$. Dann gilt:

$H_0 \supseteq H_1 \supseteq \cdots \supseteq H_l$.

und

1. $H_0 = \phi[G]$, $H_l = \{e\}$
2. $H_{i+1} \lhd H_i$

Beweis:

Sei $\phi(a) \in H_i$. Dann gilt:

$$\begin{aligned}
&\phi(a) * H_{i+1} \\
&= \phi(a) * \phi[G_{i+1}] \\
&= \phi[a * G_{i+1}] \\
&= \phi[G_{i+1} * a] \\
&= \phi[G_{i+1}] * \phi(a) \\
&= H_{i+1} * \phi(a)
\end{aligned}$$

3. H_i/H_{i+1} ist zyklisch.

Beweis:

$$\overline{\phi} : \left\{ \begin{array}{lcl} G_i/G_{i+1} & \rightarrow & H_i/H_{i+1} \\ a * G_{i+1} & \mapsto & \phi(a) * H_{i+1} \end{array} \right.$$

Behauptung 1: $\overline{\phi}$ ist wohldefiniert.

Beweis:

$$\begin{aligned}
&a * G_{i+1} = b * G_{i+1} \\
&\succ \phi(a) * H_{i+1} = \phi(a) * \phi[G_{i+1}] = \phi[a * G_{i+1}] \\
&\phi[b * G_{i+1}] = \cdots = \phi(b) * H_{i+1}
\end{aligned}$$

Behauptung 2: $\overline{\phi}$ ist Homomorphismus.

Behauptung 3: $\overline{\phi}$ ist surjektiv.

Da das homomorphe Bild einer zyklischen Gruppe zyklisch ist, ist H_i/H_{i+1} zyklisch.

Lemma 7.3.2 *Sei ϕ ein Homomorphismus von G.*
$H_1 \lhd \phi[G] =: H$. Dann gilt:

1. $G_1 = \{a | \phi(a) \in H_1\} \lhd G$
2. $G/G_1 \approx H/H_1$

Beweis:

Sei $\psi : \left\{ \begin{array}{lcl} H & \rightarrow & H/H_1 \\ a & \mapsto & a * H_1 \end{array} \right.$

Sei $\overline{\phi} = \psi \circ \phi$. Dann ist $\overline{\phi}$ ein Homomorphismus von G auf H/H_1.

Behauptung: $Kern(\phi) = G_1$

Beweis:

"$\supseteq$"

Sei $a \in G_1$
$\succ \phi(a) \in H_1$
$\succ \phi(a) * H_1 = H_1$
$\succ \overline{\phi}(a) = H_1$
$\succ a \in kern(\overline{\phi})$

"$\subseteq$"

Ist $a \in kern(\overline{\phi})$
$\succ \phi(a) * H_1 = H_1$
$\succ \phi(a) \in H_1$
$\succ a \in G_1$

Es gilt: $G/Kern(\overline{\phi}) \approx Bild(\overline{\phi}) \succ G/G_1 \approx H/H_1$

Satz 7.3.1 *Sei ϕ ein Homomorphismus von G. Ist $Bild(\phi)$ auflösbar und $Kern(\phi)$ auflösbar, dann ist G auflösbar.*

Beweis:

Da $\phi(b)$ auflösbar ist, gibt es

$H_0 \supseteq \cdots \supseteq H_m$

mit

1. $H_0 = Bild(\phi)$, $H_M = \{e\}$
2. $H_{i+1} \lhd H_i$
3. H_i/H_{i+1} zyklisch

Sei $G_i = \{a | \phi(a) \in H_i\}$

Dann ist:

$G_0 \subseteq G_1 \subseteq \cdots \subseteq G_m$

1. $G_0 = G$, $G_m = kern(\phi)$
2. $G_{i+1} \lhd G_i$
3. G_i/G_{i+1} ist zyklisch

Beweis:

$\phi_i = \phi \restriction G_i$.

Dann $\phi[G_i] = H_i$ und $H_{i+1} \lhd H_i$.

Also $G_{i+1} \lhd G_i$ und $G_{i+1}/G_i \approx H_{i+1}/H_i$ nach dem Lemma von Seite 90.

Da $Kern(\phi)$ auflösbar ist, gibt es

$G_m \supseteq G_{m+1} \supseteq \cdots G_k$

mit

1. $G_m = Kern(\phi)$
2. $G_{i+1} \lhd G_i$
3. G_i/G_{i+1} ist zyklisch.

Lemma 7.3.3 *Ist G abelsch, dann ist G auflösbar.*

Beweis: (Induktion über $|G|$)

$|G| = 1$ $\surd$

Sei $|G > |1$.

Sei p Primzahl mit $p|\ |G|$.

Also gibt es ein $a \in G$ mit $ord(a) = p$.

Sei $H =< a >$. Dann ist H zyklisch und somit auflösbar.

Da G abelsch ist, ist $H \lhd G$.

$$\phi : \begin{cases} G & \to & G/H \\ a & \mapsto & a * H \end{cases}$$

$\phi[a]$ ist abelsch und $|\phi[G]| < |G|$ nach dem Satz von Lagrange.

Nach Induktionsvoraussetzung ist $\phi[G]$ auflösbar.

Da $Kern(\phi) = H$ auflösbar ist $\succ G$ ist auflösbar.

Folgerung 7.3.1 *Sei G eine Gruppe. Gibt es*

$$G_0 \supseteq G_1 \supseteq \cdots \supseteq G_l$$

mit

1. $G_0 = G, \cdots, G_l = \{e\}$
2. $G_{i+1} \lhd G_i$
3. G_i/G_{i+1} *ist abelsch*

Dann ist G auflösbar.

Beweis:

Durch Induktion über i zeigen wir:

G_{l-i} ist auflösbar

$i = 0 \succ G_{l-i} = G_l = \{e\}$ $\surd$

Sei $i > 0$. Dann ist

$G_{l-(i-1)} \lhd G_{l-1}$

Sei $\phi : \begin{cases} G_{l-1} & \to & G_{l-i}/G_{l-(i-1)} \\ a & \mapsto & a * G_{l-(i-1)} \end{cases}$

Dann ist $\phi[G_{l-i}]$ abelsch nach 3.

Also ist nach dem Lemma von Seite 92 $\phi[G_{l-i}]$ auflösbar.

$Kern(\phi) = G_{l-(i-1)}$ ist nach Induktionsvoraussetzung auflösbar.

Also ist G_{i-1} auflösbar.

Da $G = G_{e-l}$ ist G auflösbar.

7.4 Auflösbare Gleichungen

Sei $f(x) \in K[x]$ mit $grad(f) \geq 1$.
Sei $\alpha_1, \cdots, \alpha_n$ die Nullstellen von f.
$F = K(\alpha_1, \cdots, \alpha_n)$.

Satz 7.4.1 *Ist $f(x) = 0$ auflösbar, dann ist $G_{F:K}$ auflösbar.*

Beweis:

Wir hatten gezeigt:

Ist $f(x) = 0$ auflösbar, dann gibt es eine Kette von Körpern

$M_0 \subseteq M_1 \subseteq \cdots \subseteq M_l$

mit

1. $M_0 = K$, $\alpha_1, \cdots, \alpha_n \in M_l$
2. $L := M_L$ ist Galois-Erweiterung von K
3. M_{i+1} ist Galois-Erweiterung von M_i
4. $G_{M_{i+1}:M_i}$ ist abelsch

Sei $G_i = G_{L:M_i}$. Dann gilt:

$G_0 \supseteq G_1 \supseteq \cdots \supseteq G_l$

mit:

1. $G_0 = G_{L:K}$, $G_l = M_{L:L} = \{id_L\}$
2. $G_{i+1} \lhd G_i$
3. G_i/G_{i+1} ist abelsch

Beweis:

Da M_{i+1} eine Galois-Ereiterung von M_i und L eine Galois-Erweiterung von M_i ist
$\succ G_{L:M_{i+1}} \lhd G_{L:M_i}$ und $G_{L:M_i}/G_{L:M_{i+1}} \approx G_{M_{i+1}:M_i}$
Da $G_{i+1} = G_{L:M_{i+1}}$, $G_i = G_{L:M_i}$ ist und $G_{M_{i+1}:M_i}$ abelsch ist
$\succ G_i/G_{i+1}$ ist abelsch.

Also ist nach der Folgerung von Seite 92 $G_{L:K}$ auflösbar.
Da F der Zerfällungskörper von f über K ist,
ist F eine Galois-Erweiterung von K.
Da $\alpha_1, \cdots, \alpha_n \in L$, ist F Zwischenkörper von K und L.
Also ist $G_{L:F} \lhd G_{L:K}$ und $G_{L:K}/G_{L:F} \approx G_{F:K}$
Sei $\phi : G_{L:K} \to G_{F:K}$ ein Homomorphismus auf $G_{F:K}$.
Da $G_{L:K}$ auflösbar, ist $Bild(\phi) = G_{F:K}$ auflösbar.

Satz 7.4.2 *$f(x) = x^5 - 6 * x + 3$ ist nicht auflösbar über $\mathbb{Q}$*

Beweis:

Behautpung 1: f ist irreduzibel

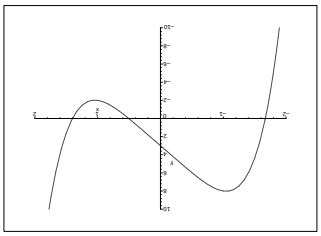
Beweis:

$3 \nmid 1$ $3|6$ $3|3$ und $3^2 \nmid 3$
Also ist nach Eisenstein f irreduzibel über $\mathbb{Q}$.
Somit besitzt f 5 Nullstellen $\alpha_1, \cdots, \alpha_5$

Behautpung 2: f besitzt genau 3 reelle Nullstellen

Beweis: (Kurvendiskussion)

$$f'(x) = 5 * x^4 - 6 = 5 * (x^2 + \sqrt{\tfrac{6}{5}}) * (x + \sqrt[4]{\tfrac{6}{5}}) * (x - \sqrt[4]{\tfrac{6}{5}})$$



oBdA Seien α_1, α_2 die nichtreellen Nullstellen.

$f(x) = x^5 - 6 * x + 3$

Wir hatten gezeigt: f hat 5 Nullstellen $\alpha_1, \cdots, \alpha_5 \in \mathbb{R}$ und $\alpha_1, \alpha_2 \notin \mathbb{R}$

$F = K(\alpha_1, \cdots, \alpha_5)$ ist der Zerfällungkörper von f über K.

Wir wollen zeigen:

$$G_{F:Q} \cong S_5$$

Sei $\sigma \in G_{F:Q}$. Sei α_i eine Nullstelle

$\succ \sigma(\alpha_i) \in \{\alpha_1, \cdots, \alpha_5\}$.

Da σ injektiv ist, gibt es genau eine Permutation π_σ mit

$$\sigma(\alpha_i) = \alpha_{\pi_\sigma}(i)$$

Sei $\pi : \begin{cases} G_{F:Q} & \to & S_5 \\ \sigma & \mapsto & \pi\sigma \end{cases}$

Behauptung 3: π ist Monomorphismus

Beweis:

$\sigma, \tau \in G_{F:Q}$ z.Z. $\pi_{\sigma\circ\tau} = \pi_\sigma \circ \pi_\tau$.

$\sigma \circ \tau(\alpha_i) = \sigma(\tau(\alpha_i)) = \sigma(\alpha_{\pi_\tau}(i))$

$\succ \pi_{\sigma\circ\tau} = \pi_\sigma \circ \pi_\tau(i) = \alpha_{\pi_\sigma}(\pi_\sigma(i))$

$\succ \pi_{\sigma\circ\tau} = \pi_{\sigma\circ\tau} = \pi_\sigma \circ \pi_\tau$.

$Kern(\pi) = \{id_F\}$

$\pi_\sigma = id_{\{1,\cdots,5\}} \succ \sigma(\alpha_i) = \alpha_i \succ \sigma = id_F$

Sei $H = \pi[G_{F:Q}] \leq S_5$.

Wir wollen zeigen: $H = S_5$.

Behauptung 4: 5 teilt $|H|$

Beweis:

Da f irreduzibel ist, ist

$$[\mathbb{Q}(\alpha_1) : \mathbb{Q}] = grad(f) = 5$$

$\succ$ Da $[F : \mathbb{Q}] = [F : \mathbb{Q}(\alpha_1)] * [\mathbb{Q}(\alpha_1) : \mathbb{Q}]$

$\succ$ 5 teilt $[F : \mathbb{Q}]$

Da F eine Galois-Erweiterung ist, ist $[F : \mathbb{Q}] = |F_{F:Q}|$

$\succ$ 5 teilt $|G_{F:Q}|$

π Monomorphismus $\succ$ 5 teilt $|H|$.

Behauptung 5: H entält den Zweierzyklus $(0,1)$
Beweis:

Sei $\sigma : F \to \mathbb{C}$ mit $\sigma(a) = \overline{a}$.
Da F eine Galois-Erweiterung von $\mathbb{Q} \succ \sigma \in G_{F:Q}$
Da $\alpha_1 \notin \mathbb{R} \succ \sigma(\alpha_1) \neq \alpha_1 \succ \sigma(\alpha_1) = \alpha_2$
$\alpha \notin \mathbb{R} \succ \sigma(\alpha_2) \neq \alpha_2 \succ \sigma(\alpha_2) = \alpha_1$
$\sigma(\alpha_i) = \alpha_i$ für $i > 2$
$\succ \pi_\sigma = (0,1) \in H$
Aus Behautpung 4 und Behauptung 5 $\succ H = S_5$

8 Konstruktion mit Zirkel und Lineal

8.1 Definitionen

Sei M ein Menge von Punkten mit $|M| \geq 2$.
Folgende Konstruktionen sind erlaubt:

1. Durch zwei verschiedene Punkte aus M eine Gerade zeichnen.
   G heißt dann M-Gerade.

2. Die Strecke $\overline{Q_1Q_2}$ zwischen zwei Punkten aus M in den Zirkel nehmen und den Kreis K um einen Punkt $P \in M$ zeichen.
   K nennt man auch M-Kreis.

Wir nennen einen Punkt P in einem Schritt aus M konstruierbar, wenn gilt:

1. $P \in M$

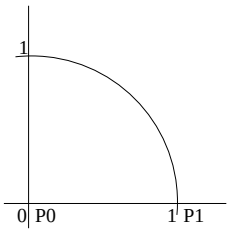
2. P ist der Schnittpunkt zweier nicht paralleler M-Geraden

3. P ist ein Schnittpunkt einer M-Geraden und eines M-Kreises

4. P ist Schnittpunkt zweier M-Kreise mit verschiedenen Mittelpunkten

Eine Menge N von Punkten ist in n Schritten aus M konstruierbar, wenn gilt:
Ist $M = N$, dann ist N in 0-Schritten konstruierbar.
Ist N in n Schritten aus M konstruierbar und P in einem Schritt aus N konstruierbar, dann ist $N \cup \{P\}$ in n+1 Schritten konstruierbar.
N heißt konstruierbar, wenn es ein n gibt, mit N ist in n Schritten konstruierbar.
P ist konstruierbar, wenn es ein konstruierbares N gibt mit $P \in N$.
Wir wählen $P_0, P_1 \in M$ mit $P_0 \neq P_1$.
Wir legen ein Achsenkreuz so in die Ebene, daß

$$P_0 = \binom{0}{0} \text{ und } P_1 = \binom{1}{0}$$



Dann wird jedem Punkt ein Paar (r_1, r_2) zugeordnet.
Faßt man $\mathbb{R}^2$ als $\mathbb{C}$ auf, dann ist $P_0 = 0$ und $P_1 = 1$.
Sei $N \subseteq \mathbb{C}$. Sind $P_0, P_1 \in N$ mit $P_0 \neq P_1$, dann ist

$$G = \{P_0 + t * (P_1 - P_0) | t \in \mathbb{R}\}$$

eine N-Gerade.
Sind $Q_0, Q_1, Q_2 \in N$, dann ist

$$\{Q| \ |Q - Q_0| = |Q_1 - Q_2|\}$$

ein N-Kreis.

8.2 Ein notwendiges Kriterium für die Konstruierbarkeit

Sei $M \subseteq \mathbb{C}$, dann bezeichne K_M den kleinsten Körper mit:

$a + b * i \in M \succ a, b \in K$

$K_{\{0,1\}} = \mathbb{Q}$

Wir werden zeigen:

Ist P aus M konstruierbar, dann ist $[K_M(P) : K_M] = 2^l$ für ein l.

Wir nennen einen Unterkörper K von $\mathbb{C}$ zulässig,
wenn für $a, b \in \mathbb{R}$ mit $a + i * b \in K \succ a, b \in K$.

Beispiel:

1. K_M ist zulässig, da $K_M \subseteq \mathbb{R}$
2. $\mathbb{Q}(i)$ ist zulässig
3. Ist K zulässig und $\alpha \in \mathbb{R}$ mit $\alpha^2 \in K$, dann ist $K(\alpha)$ zulässig

Beweis: zu 3:

I. Fall: $\alpha \in K$

$\succ K(\alpha) = K$ $\surd$

II. Fall: sonst

Da $\alpha^2 \in K$ ist, sind 1 und α eine Basis von $K(\alpha)$ über K.

Sei $z = a + b * i \in K(\alpha)$ mit $a, b \in \mathbb{R}$

Dann gibt es $z_1 = a_1 + b_1 * i$ und $z_2 = a_2 + b_2 * i \in K$ mit:

$z = z_1 * 1 + z_2 * \alpha$

$\succ z = a_1 + b_1 * i + \alpha(a_2 + b_2 * i) = (a_1 + \alpha * a_2) + (b_1 + \alpha * b_2) * i$

Da K zulässig ist, sind $a_1, a_2, b_1, b_2 \in K$

$b_1 + \alpha * b_2 = b \in K(\alpha)$

Satz 8.2.1 *Ist K zulässig und ist P in einem Schritt aus K konstruierbar, dann gibt es ein $\alpha \in \mathbb{R}$ mit $\alpha^2 \in K$ und $P \in K(\alpha)$*

Beweis:

I.Fall: $P \in K$

Sei $\alpha = 1$ $\surd$

II. Fall: P ist der Schnittpunkt zweier nicht paralleler K-Geraden G und H.

Dann gibt es $P_0, P_1, Q_0, Q_1 \in K$ mit

1. $G = \{P_0 + t * (P_1 - P_0) | t \in \mathbb{R}\}$
2. $H = \{Q_0 + t * (Q_1 - Q_0 | t \in \mathbb{R}\}$
3. $(P_1 - P_0)$ und $(Q_1 - Q_0)$ sind linear unabhängig
4. $P \in H \cap G$

Seien $a, b, c, d, e, f \in \mathbb{R}$ mit

$(P_1 - P_0) = a + b * i \in K$

$(Q_0 - Q_1) = c + d * i \in K$

$(Q_0 - P_0) = e + f * i \in K$

Da K zulässig $\succ a, b, c, d, e, f \in K$

Da $P \in G \cap H \succ$ Es gibt $t, s \in R$ mit

$P_0 + t * (P_1 - P_0) = P = Q_0 + s * (Q_1 - Q_0)$

$t * (P_1 - P_0) + s * (Q_0 - Q_1) = Q_0 - P_0$

$t * a + s * c = e$

$t * b + s * d = f$

Da $(P_1 - P_0)$ und $(Q_0 - Q_1)$ linear abhängig sind, folgt

$$\begin{vmatrix} a & c \\ b & d \end{vmatrix} \neq 0$$

Dann ist $\begin{vmatrix} a & c \\ b & d \end{vmatrix} \in K$ und $\begin{vmatrix} e & c \\ f & d \end{vmatrix} \in K$

$$\succ t = \frac{\begin{vmatrix} e & c \\ f & d \end{vmatrix}}{\begin{vmatrix} a & c \\ b & d \end{vmatrix}} \in K$$

$P = P_0 + t * (P_1 - P_0) \in K$

$\alpha = 1$

III. Fall: P ist ein Schnittpunkt eines K-Kreises H und einer K-Geraden G

Dann gibt es: $P_0 \neq P_1$ und Q_0, Q_1, Q_2 mit:

1. $G = \{P_0 + t * (P_1 - P_0) | t \in \mathbb{R}\}$
2. $H = \{Q | \ |Q - Q_0| = |Q_2 - Q_1|\}$
3. $P \in H \cap G$

$\succ |P_0 + t * (P_1 - P_0) - Q_0| = |Q_2 - Q_1|$

Seien $a, b, c, d, e, f \in \mathbb{R}$, so daß :

$a + b * i = P_1 - P_0 \in K$

$c + d * i = P_0 - Q_0 \in K$

$e + f * i = Q_1 - Q_2 \in K$

$\succ a, b, c, d, e, f \in K$

$P_1 \neq P_0 \succ a^2 + b^2 \neq 0 \succ p = \frac{a*c+b*d}{a^2+b^2} \in K$

$\succ q = \frac{c^2+d^2-e^2-f^2}{a^2+b^2} \in K$

Es gibt:

$e^2 + f^2$

$= |Q_2 - Q_1|$

$= |t * (P_1 - P_0) + (P_0 - Q_0)|$

$= t^2 * (a^2) + (c)^2 + 2 * t * a * c + (t * b + a)^2$

$= t^2 * a^2 + c^2 + 2 * t * a * c + t^2 * b^2 + d^2 + 2 * t * b * a$

$= t^2 * (a^2 + b^2) + 2 * t * (a * c + b * a) + c^2 + d^2$

$\succ t^2 + 2 * t * \frac{a*c+b*d}{a^2+b^2} + \frac{c^2+d^2-e^2-f^2}{a^2+b^2} = 0$

$\succ t^2 + 2 * t * p + q = 0$

$\succ t = -p \pm \sqrt{p^2 - q}$

Sei $\alpha = \sqrt{p^2 - q} \succ \alpha^2 = p^2 - q \in K \succ t \in K(\alpha)$

$\succ P = P_0 + t * (P_1 - P_0) \succ P \in K(\alpha)$

Da $P \in \mathbb{R}$ und $t \in \mathbb{R} \succ \alpha = t - p \in \mathbb{R}$

IV. Fall: Sei P der Schnittpunkt zweier K-Kreise G und H,
die nicht denselben Mittelpunkt haben

Dann gibt es $P_0, P_1, P_2, Q_0, Q_1, Q_2$ mit:

1. $H = \{Q|\ |Q - P_0| = |P_1 - P_2|\}$
2. $G = \{Q|\ |Q - Q_0| = |Q_1 - Q_2|\}$
3. $P \in G \cap H$
4. $P_0 \neq Q_0$

$\succ$ Es gibt $a, b, c, d, e, f, g, h \in \mathbb{R}$ mit:

$a + b * i = Q_0 \in K$
$c + d * i = P_0 \in K$
$e + f * i = P_2 - P_1 \in K$
$g + h * i = Q_2 - Q_1 \in K$

$\succ a, b, c, d, e, f, g, h \in K$

$\succ r = \frac{1}{2} * (-a^2 - b^2 + c^2 + a^2 + e^2 + f^2 - g^2 - h^2) \in K$

$c - q \in K \qquad d - b \in K$

Behauptung 1: Die Lösungsmenge von $(c - a) * x + (d - b) * y = r$
ist eine K-Gerade F

Beweis:

Da $P_0 \neq Q_0 \succ c - a \neq 0$ oder $d - b \neq 0$
Also ist $R_0 = r/(c - a)$ eine Lösung oder $R_0 = r/(d - b)$
eine Lösung der Gleichung.
Eine Lösung R_2 des Gleichungssystems $(c - a) * x + (d - b) * y = 0$
ist $R_2 = (d - b) + i * (a - c)$.
Dann sind $R_0, R_1 = R_0 + R_2 \in K$ und die Lösungsmenge
der Gleichung ist $F = \{R_0 + t * (R_1 - R_0) | t \in \mathbb{R}\}$.

Behauptung 2: Ist $P \in G \cap H$,
dann ist P eine Lösung von $(c - a) * x + (d - b) * y = r$

Beweis:

Sei $P = x + i * y \in H \cap G \succ |P - P_0| = |P_1 - P_2|$.
$|P - Q_0| = |Q_1 - Q_2|$
$(x - a)^2 + (y - b)^2 = e^2 + f^2$
$(x - c)^2 + (y - d)^2 = g^2 + h^2$
$x^2 - 2 * a * x + a^2 + y^2 - 2 * b * y + b^2 = e^2 + f^2$
$x^2 - 2 * c * x + c^2 + y^2 - 2 * d * y + d^2 = g^2 + h^2$
$2 * (c - a) * x + 2 * (d - b) * y = -a^2 + c^2 - b^2 + d^2 + e^2 + f^2 - g^2 - h^2$
$\succ (c - a) * x + (d - b) * y = r,$
wobei $r = \frac{1}{2} * (-a^2 + c^2 - b^2 + d^2 + e^2 + f^2 - g^2 - h^2)$
Also $P \in G \cap F$. Nach Fall 3 gibt es dann ein $\alpha \in \mathbb{R}$, mit:
$a, b \in \mathbb{R}$ und $a + b * i \in M \succ a, b \in K$

Bemerkung 8.2.1 *Ist* $M = \{0, 1\}$, *dann ist* $K_M = \mathbb{Q}$.

Satz 8.2.2 *Ist $N \subseteq \mathbb{C}$ in n-Schritten aus M konstruierbar, dann gibt es eine Kette von zulässigen Körpern mit:*

$$L_0 \subseteq L_1 \subseteq \cdots \subseteq L_m$$

mit:

1. $L_0 = K_M$, $L_1 = L_0(i), \cdots N \subseteq L_n$
2. *Es gibt ein* $\alpha_i \in \mathbb{R}$ *mit* $\alpha_i^2 \in L_i$ *und* $L_{i+1} = L_i(\alpha_i)$.

Beweis: (Induktion über n)

Ist $n = 0$, dann ist $N = M$. $L_0 = K_M$ ist zuläsig.
$\succ L_0(i) = L_1$ ist zulässig und $M \subseteq L_1$.
Sei N in n+1-Schritten aus M konstruierbar.
Dann gibt es ein $p \in N$, so daß :
$N \setminus \{P\}$ ist in n-Schritten konstruierbar
P ist in einem Schritt aus $N \setminus \{0\}$ konstruierbar
Also gibt es nach Induktionsvoraussetzung eine Kette von zulässigen Körpern $L_0 \subseteq L_1 \subseteq \cdots \subseteq L_m$ mit:
1. $L_0 = K_M$, $L_1 = K_M(i), \cdots N \setminus \{P\} \subseteq L_M$
2. Es gibt $\alpha_i \in \mathbb{R}$ mit $\alpha^2 \in L_i$ und $L_{i+1} = L_i(\alpha_i)$

Dann ist $N \setminus \{P\} \subseteq L_m$ und P ist in einem Schritt aus L_M konstruierbar.
Nach dem Satz von Seite 97 gibt es ein $\alpha_m \in \mathbb{R}$ mit $\alpha_m^2 \in L_m$
$P \in L_m(\alpha_m) =: L_{m+1} \succ N \subseteq L_{m+1}$.

Folgerung 8.2.1 *Ist P aus M konstruierbar, dann $[K_M(P) : K_M] = 2^l$ für ein l.*

Beweis:

Da P konstruierbar aus M ist, gibt es eine Kette von Körpern $L_0, \cdots, L_m$ mit:
1. $P \in L_m$
2. $[L_{i+1} : L_i] \leq 2$

$[L_m : K_M] = \prod_{i=0}^{m-1} [L_{i+1} : L_i] = 2^k$ für ein K.
$[L_m : K_M(P)] * [K_M(P) : K_M] = [L_m : K_M]$
$\succ$ Es gibt ein l mit $[K_M(P) : K_M] = 2^l$.

Delisches Problem (Würfelverdopplung)

Gegeben sei ein Würfel W.
Ist aus W ein Würfel V mit doppeltem Volumen konstruierbar ?
Ein Würfel ist gegeben durch zwei Ecken P_0, P_1 und eine Kante mit $P_0 \neq P_1$.
Ein Würfel V ist aus W konstruierbar, wenn zwei Ecken Q_1, Q_2 und eine Kante aus P_0, P_1 konstruierbar sind.
Wir setzen: $P_0 = 0$ und $P_1 = 1$ und erhalten $K_M = \mathbb{Q}$.
Ist Q_1, Q_2 aus $\mathbb{Q}$ konstruierbar $\succ |Q_1 - Q_2| = b$ ist konstruierbar aus $\mathbb{Q}$.
$\succ [\mathbb{Q}: b] = 2^l$ für ein l.
Sei das Volumen von $W = 1$. Sei das Volumen von $V = 2$.

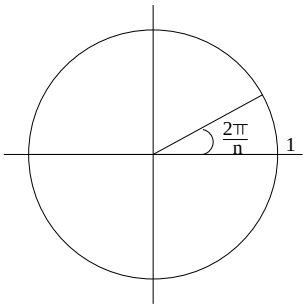
$\succ b^3 = 2 \succ b$ ist Nullstelle von $x^3 - 2 = 0$.
Da $x^3 - 2$ irreduzibel ist, gilt: $[\mathbb{Q}(b) : \mathbb{Q}] = 3$.

Quadratur des Kreises
Gegeben sei ein Kreis K durch P_1 mit dem Mittelpunkt P_0 und $P_0 \neq P_1$.
Ist ein Quadrat konstruierbar aus P_0 und P_1 mit gleichem Flächeninhalt ?
NEIN !
Seien $P_0 = 0$ und $P_1 = 1$.
Angenommen zwei Ecken einer Kante Q_1, Q_2 des Quadrates sind konstruierbar.
$|Q_1 - Q_2| = b$ ist konstruierbar.
$[\mathbb{Q}(b) : \mathbb{Q}] = 2^l$ für ein l.
b ist algebraisch $\succ b^2$ ist algebraisch.
$\succ$ Da $b^2 = 1^2 * \pi = \pi$
$\succ \pi$ ist algebraisch. $\sharp$ Da π transzendent.

8.3 Regelmäßige n-Ecke

Ein regelmäßiges n-Eck heißt konstruierbar,
wenn $e^{i*\frac{2*\pi}{n}}$ konstruierbar ist (aus $\{0,1\}$).
ZIEL: Ist das regelmäßige n-Eck konstruierbar, dann ist $n = 2^\nu * p_1 \cdots p_k$,
wobei $p_1, \cdots, p_k$ paarweise verschiedene Fermatsche Primzahlen sind.

p heißt Fermatsche Primzahl,
wenn es ein k gibt, mit $2^{2^k} + 1 = p$. $(3 = 2^{2^0} + 1,\ 5 = 2^{2^1} + 1,\ 17 = 2^{2^2} + 1 \cdots)$



$$e^{\frac{2*\pi*i}{n}} = cos(\frac{2*\pi}{n}) + i * sin(\frac{2*\pi}{n})$$

Lemma 8.3.1 *Ist $e^{\frac{2*\pi*i}{n}}$ konstruierbar, so auch $e^{\frac{2*\pi*i}{n}*l}$*

Beweis:

$l = 1$: Voraussetzung.
Angenommen: $e^{\frac{2*\pi*i}{n}*l}$ ist konstruierbar.
Sei E der Einheitskreis. Sei K der Kreis um $e^{\frac{2*\pi*i}{n}*l}$ mit
dem Radius $|1 - e^{\frac{2*\pi*i}{n}}|$.
Dann ist $e^{2*\pi*i*(l+1)} \in E \cap K$.

Folgerung 8.3.1 *Ist das regelmäßige n-Eck konstruierbar und $m|n$.
Dann ist das regelmäßige m-Eck konstruierbar.*

Beweis: Sei $l \in \mathbb{N}$ mit $m * l = n$.
Dann ist $e^{\frac{2*\pi*i}{m}} = e^{\frac{2*\pi*i*l}{n}}$ konstruierbar.

ϵ heißt n-te Einheitswurzel, wenn ϵ Nullstelle von $x^n - 1$ ist.

Beispiel: $\epsilon = e^{\frac{2*\pi*i}{n}}$

ϵ heißt n-te primitive Einheitswurzel, wenn $\{\epsilon^k | k \in \mathbb{N}\}$
die Nullstellenmenge von $x^n - 1$ ist. Beispiel: $\epsilon = e^{\frac{2*\pi*i}{n}}$

Lemma 8.3.2 $\hookleftarrow$

1. *$e^{\frac{2*\pi*i}{n}*k}$ ist primitive n-te Einheitswurzel*
2. *$ggT(n,k) = 1$*

Beweis:

1$\succ$2:

Sei $e^{\frac{2*\pi*i}{n}*k}$ primitive n-te Einheitswurzel.
$e^{\frac{2*\pi*i}{n}}$ ist n-te Einheitswurzel.
Also gibt es ein l mit $e^{\frac{2*\pi*i}{n}} = (e^{\frac{2*\pi*i}{n}*k})^l = e^{\frac{2*\pi*i}{n}*k*l}$
$\succ 1 = e^{\frac{2*\pi*i}{n}*(k*l-1)}$
$\succ n|k*l-1 \succ$ Es gibt m mit:
$1 = n*m+k*l \succ ggT(n,k) = 1.$

2$\succ$1:

Sei $ggT(n,k) = 1$. Dann gibt es l und m mit $1 = n*m+k*l$.
$e^{\frac{2*\pi*i}{n}} = e^{\frac{2*\pi*i}{n}*(n*m+k*l)} = \underbrace{(e^{\frac{2*\pi*i}{n}*n})^m}_{(e^{2*\pi*i})^m=1^m=1} *(e^{\frac{2*\pi*i}{n}*k})^l = (e^{\frac{2*\pi*i}{n}*k})^l$
$\succ \{(e^{\frac{2*\pi*i}{n}*k})^l | l \in \mathbb{N}\} = \{(e^{\frac{2*\pi*i}{n}})^l | l \in \mathbb{N}\}$ ist die Nullstellenmenge von $x^n - 1$.

Sei E_n die Menge der n-ten primitiven Einheitswurzeln, dann gilt:
$|E_n| = |\{K | 0 < k < n \text{ mit } ggT(k,n) = 1\}|$.

Beispiel:

Sei p Primzahl, dann ist $|E_p| = p-1$. $|E_{p^2}| = p*(p-1)$

Satz 8.3.1 *Ist p Primzahl, dann $\sum_{i=0}^{p-1} x^i$ irreduzibel über $\mathbb{Q}$ und $x^p - 1 = (x-1)*f_1$.*

Beweis:

siehe Übung !

Lemma 8.3.3 *Ist $p \geq 3$ eine Primzahl und ist das regelmäßige p-Eck konstruierbar, dann ist $p = 2^l + 1$.*

Beweis:

$x^p - 1 = (x-1).\ f_1$ mit $\sum_{i=0}^{p-1} x^i$
$\epsilon = e^{\frac{2*\pi*i}{p}}$ ist p-te primitive Einheitswurzel.
$\succ \epsilon$ ist Nullstelle von f_1. f_1 ist irreduzibel.
$\succ [\mathbb{Q}(\epsilon) : \mathbb{Q}] = grad(f) = p-1.$
Ist ϵ konstruierbar $\succ$ Es gibt ein l mit $p-1 = 2^l$

Folgerung 8.3.2 *Das regelmäßige 7-Eck ist nicht konstruierbar.*

Satz 8.3.2 *Ist $p \geq 3$ eine Primzahl und ist das regelmäßige p-Eck konstruierbar, dann ist p eine Fermatsche Primzahl.*

Beweis:

Es ist nach dem Lemma von Seite 103 $p = 2^l + 1$ für ein l.
Angenommen $l \neq 2^r$ mit r aus $\mathbb{N}$.
Dann gibt es eine Primzahl $q = 3$ mit $l = q*k$.
Es gilt: $(x-1)|x^q - 1$

-2^k eingesetzt $\succ (-2^k-1)|(-2^k)^q-1$
Da q ungerade $\succ (-2^k-1)|-2^{k*q}-1$
$\succ 2^k+1|2^{k*q}+1=2^l+1=p$
$2^k+1>1 \succ 2^k+1=p=2^l+1 \succ k=l \succ q=1$ $\sharp$

Satz 8.3.3 *Ist $p \geq 3$ eine Primzahl, dann*
$f_2=\sum_{j=0}^{p-1} x^{p*j}$
irreduzibel und $x^{p^2}-1=(x^p-1)*f_2$

Beweis:
$(y^p-1)=(y-1)*\sum_{j=0}^{p-1} y^j$. Sei $y=x^p$
$(x^{p^2}-1)=(x^p-1)*f_2$.

Behauptung 8.3.1 *Die Nullstellenmenge von f_2 ist E_{p^2}*

Beweis:
Sei $\epsilon \in E_{p^2} \succ \epsilon$ ist keine Nullstelle von x^p-1.
$\succ \epsilon$ ist Nullstelle von f_2.
$grad(f_2)=p*(p-1)=|E_{p^2}|$
Sei L der Zerfällungskörper von $x^{p^2}-1$ und sei $n=[L:\mathbb{Q}]$.

Behauptung 8.3.2 *$n=(p-1)*l$ mit $l>1$*

Beweis:
Sei ξ eine p-te primitive Einheitswurzel.
Es gilt: $\mathbb{Q}(\xi) \subseteq L$.
Da $\sum_{j=0}^{p-1} x^j$ irreduzibel ist, ist $[\mathbb{Q}(\xi):\mathbb{Q}]=p-1$.
Da $E_{p^2} \cap \mathbb{Q}(\xi)=\emptyset$.
$[L:\mathbb{Q}(\xi)]>1 \succ n=[L:\mathbb{Q}]=[L:\mathbb{Q}(\xi)]*[\mathbb{Q}(\xi):\mathbb{Q}]$.
mit $[L:\mathbb{Q}(\xi)]=e>1$ und $[\mathbb{Q}(\xi):\mathbb{Q}]=(p-1)$.

Behauptung 8.3.3 *$f_2=\sum_{j=0}^{p-1} x^{p*j}$ ist irreduzibel.*

Beweis:
Sei $f_2=\prod_{i=1}^{k} h_i$ mit h_i ist irreduzibel.
Sei ϵ Nullstelle von $h_i \succ \mathbb{Q}(\epsilon_i)=L$
Da H_i irreduzibel ist, gilt
$grad(h_i)=[\mathbb{Q}(\epsilon_i):\mathbb{Q}]=[L:\mathbb{Q}]=n$.
$\succ p*(p-1)=grad(f)=\sum_{i=1}^{k} grad(h_i)=k*n=k*(p-1)*l$
Da $l>0 \succ l=p \succ k=1$.

Folgerung 8.3.3 *Ist $p \geq 3$ eine Primzahl, dann ist das regelmäßige p^2-Eck nicht konstruierbar.*

Beweis:
$\epsilon=e^{\frac{2*\pi*i}{p^2}}$. Da $x^{p^2}-1=(x^p-1)*f_2$
$\succ \epsilon$ ist Nullstelle von f_2.

Da f_2 irreduzibel ist, gilt

$[\mathbb{Q}(\epsilon) : \mathbb{Q}] = grad(f_2) = (p-1) * p \neq 2^l$ für alle $l \in \mathbb{N}$

$\succ \epsilon$ ist nicht konstruierbar.

Folgerung 8.3.4 *Das regelmäßige 9-Eck ist nicht konstruierbar.*

Satz 8.3.4 *Ist das regelmäßige n-Eck konstruierbar, dann*

$$n = 2^\nu * p_1 \cdots p_k,$$

wobei $p_1 \cdots p_k$ paarweise verschiedene Fermatsche Primzahlen sind.

Beweis:

Es gibt paarweise verschiedene Primzahlen $p_1 \cdots p_k \geq 3$ mit $n = 2^\nu * p_1^{l_1} \cdots p_k^{l_k}$.

Sei m ein Teiler von n. Dann ist das regelmäßige m-Eck konstruierbar.

$\succ l_i = 1$ und p_i Fermatsche Primzahlen.

8.4 Die Menge der konstruierbaren Punkte

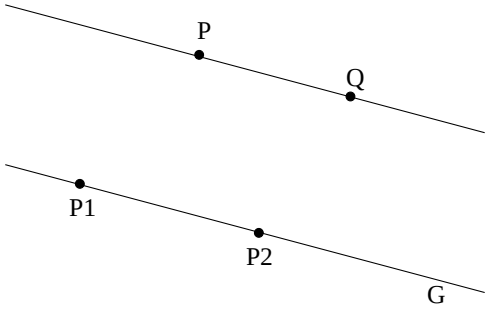
Sei M eine Menge von Punkten mit $1, 0 \in M$.
Dann sei

$$\tilde{M} = \{N | N \text{ ist aus } M \text{ konstruierbar}\}$$

Wir werden zeigen:

1. $\tilde{M}$ ist ein zulässiger Körper
2. $(x - \alpha_1) * (x - \alpha_2) \in \tilde{M}[x] \succ \alpha_1, \alpha_2 \in \tilde{M}$

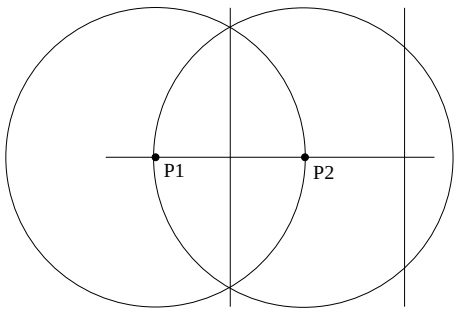
Lemma 8.4.1 *Sei G eine $\tilde{M}$-Gerade und $P \in \tilde{M}$.*
Dann ist die Gerade H durch P parallel zu G einer $\tilde{M}$-Geraden.



Beweis:

Seien $P_1, P_2 \in \tilde{M} \cap G$ und $P_1 \neq P_2$.
Ist $P \in G$. Dann sei $H = G$.
Sei K_1 der Kreis um P mit dem Radius $\overline{P_1 P_2}$.
Sei Sei K_2 der Kreis um P_2 mit dem Radius $\overline{P_1 P}$.
Dann sind die Schnittpunkte $Q_1, Q_2 \in \tilde{M}$.
Also sind die Geraden durch P und Q_i $\tilde{M}$-Geraden.
Eine davon ist parallel zu G.

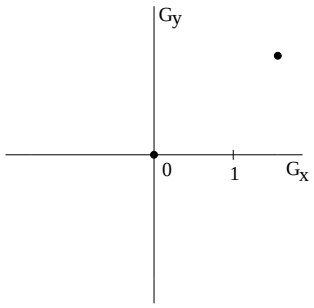
Lemma 8.4.2 *Ist G eine $\tilde{M}$-Gerade und $P \in \tilde{M}$.*
Dann ist die Gerade H durch P senkrecht auf G eine $\tilde{M}$-Gerade.



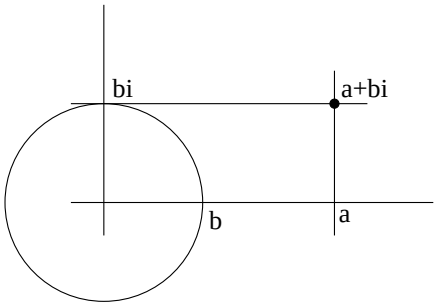
Beweis:

Seien $P_1, P_2 \in \tilde{M} \cap G$ mit $P_1 \neq P_2$.
Sei K_1 der Kreis um P_1 mit dem Radius $\overline{P_1P_2}$.
Sei K_2 der Kreis um P_2 mit dem Radius $\overline{P_1P_2}$.
Seien Q_1, Q_2 die Schnittpunkte von K_1 und K_2.
Dann ist die Gerade H' durch Q_1, Q_2 eine $\tilde{M}$-Gerade.
Sei H die Gerade durch P parallel zu H'.

Sei die Gerade durch $0, 1$ die x-Achse. Dann ist G_x ein $\tilde{M}$-Gerade.
Sei G_y die Gerade durch 0 senkrecht auf G_x.
Dann ist G_y eine $\tilde{M}$-Gerade.
G_y heißt auch y-Achse.



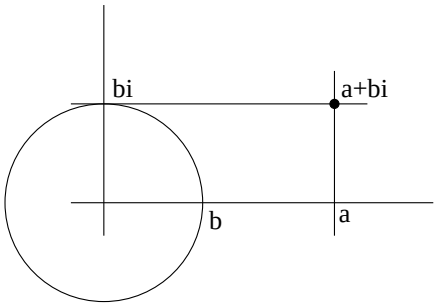
Lemma 8.4.3 *Sind $a, b \in \tilde{M} \cap \mathbb{R}$, dann ist $a + b * i \in \tilde{M}$.*



Beweis:

Sei H_1 die Gerade durch a senkrecht auf G_y.
Sei K_1 der Kreis um 0 mit dem Radius b.
Sei $b * i$ der Schnittpunkt mit G_y.
Sei H_2 die Gerade durch $b * i$ senkrecht auf G_y.
Dann ist der Schnittpunkt von H_1 und $H_2 = a + b * i$.

Lemma 8.4.4 *$\tilde{M}$ ist zulässig.*



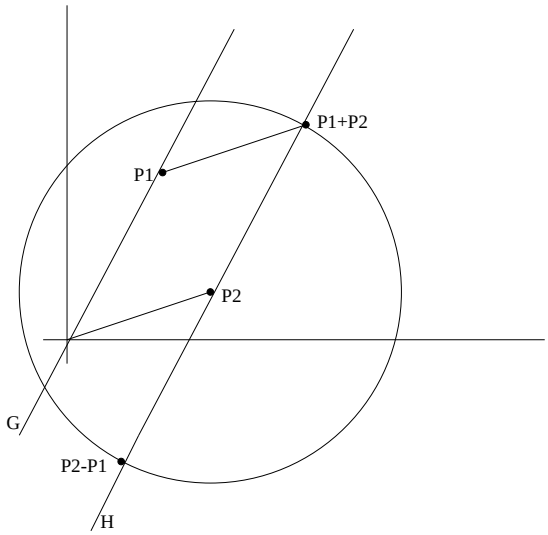
Beweis:

Seien $a, b \in \mathbb{R}$ mit $a + b * i \in \tilde{M}$. z.Z.: $a, b \in \tilde{M}$.

Beweis:

Sei H_1 die Gerade durch $a + b * i$ senkrecht auf G_x.
Dann ist a der Schnittpunkt von H_1 und G_x.
Sei H_2 die Gerade durch $a + b * i$ senkrecht auf G_y.
Dann ist der Schnittpunkt von H_2 und G_y gleich $b * i$.
Sei K der Kreis um 0 mit dem Radius $\overline{0b * i}$, dann
ist ein Schnittpunkt von K und G_x gleich b.

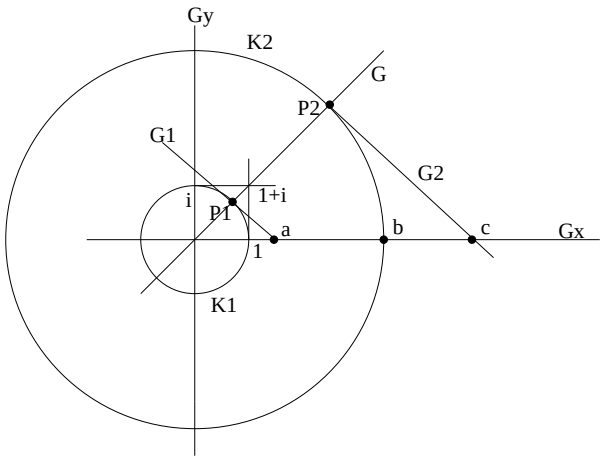
Lemma 8.4.5 *Sind $P_1, P_2 \in \tilde{M}$, dann ist $P_1 + P_2 \in \tilde{M}$ und $P_1 - P_2 \in \tilde{M}$.*



Beweis:

Sei G die Gerade durch P_1 und 0.
Sei H die Gerade durch P_2 parallel zu G.
Sei K der Kreis um P_2 mit dem Radius $\overline{P_1 0}$.
Dann sind die Schnittpunkte $P_1 + P_2$ und $P_2 - P_1$.

Lemma 8.4.6 *Sind $P_1, P_2 \in \tilde{M}$, dann ist $P_1 * P_2 \in \tilde{M}$.*



Beweis:

Behauptung: Sind $a, b \in \mathbb{R} \cap \tilde{M}$, dann ist $a * b \in \tilde{M}$.

Beweis:

$a = 0$ oder $b = 0$ $\surd$

Seien also $a, b \neq 0$.

Sei G die Gerade durch 0 und $1 + i$.

Sei K_1 der Kreis um 0 mit dem Radius 1.

Sei P_1 ein Schnittpunkt von K_1 und G.

Sei K_2 der Kreis um 0 mit dem Radius b.

Sei P_2 der Schnittpunkt von K_2 und G.

Sei G_1 die Gerade durch P_1 und a.

Sei G_2 die Gerade durch P_2 parallel zu G_1.

Sei c der Schnittpunkt von G_2 und der x-Achse.

Dann gilt nach dem Strahlensatz:

$$\frac{1}{b} = \frac{\overline{0P_1}}{\overline{0P_2}} = \frac{a}{c} \succ c = a * b$$

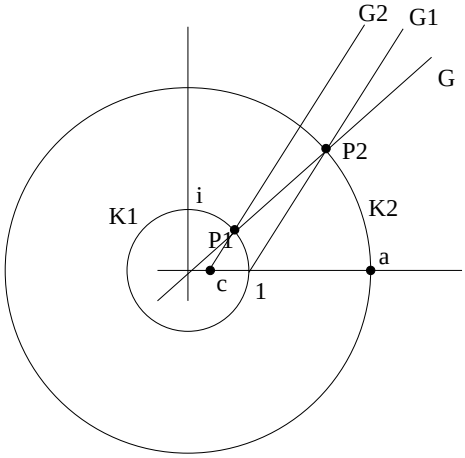
Sei $P = a + b * i$ und $Q = c + i * d \in \tilde{M}$ mit $a, b, c, d \in \mathbb{R}$

$\succ a, b, c, d \in \tilde{M}$

$\succ a * c - b * d \in \tilde{M},\ a * d + b * c \in \tilde{M}$

$\succ P_1 * P_2 = (a * c - b * d) + (a * d + b * c) * i \in \tilde{M}$

Lemma 8.4.7 *Ist* $P \in \tilde{M} \setminus \{0\} \succ \frac{1}{P} \in \tilde{M}$



Beweis:

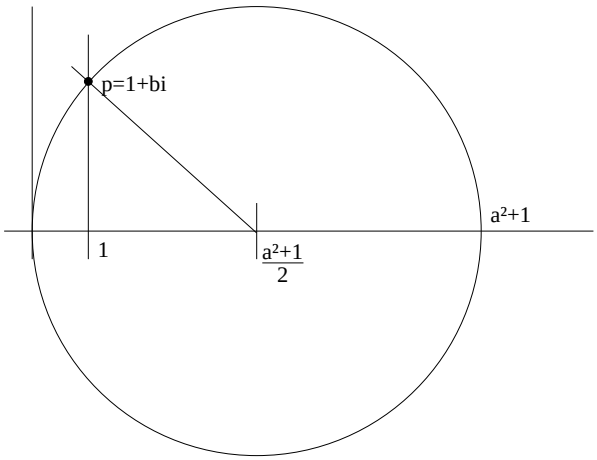
Behauptung: Ist $a \in \mathbb{R} \cap \tilde{M}$ mit $a \neq 0$. Dann ist $\frac{1}{a} \in \tilde{M}$.

Beweis:

Sei G die Gerade durch 0 und $1 + i$.
Sei K_1 der Kreis um 0 mit dem Radius 1.
Sei P_1 der Schnittpunkt von K_1 und G.
Sei K_2 der Kreis um 0 mit dem Radius 1.
Sei P_2 der Schnittpunkt von K_2 und G.
Sei G_1 die Gerade durch P_2 und 1.
Sei G_2 die Gerade durch P_1 parallel zu G_1.
Dann ist der Schnittpunkt von G_2 und der x-Achse $c = \frac{1}{a}$,
da $\frac{c}{1} = \frac{\overline{0P_1}}{\overline{0P_2}} = \frac{1}{a}$.
Sei $P_1 = a + b * i \in \tilde{M} \setminus \{o\}$ mit $a, b \in \mathbb{R}$.
$\succ a, b \in \tilde{M} \succ a^2 + b^2 \neq 0 \in \tilde{M}$
$succ\frac{1}{a^2+b^2} \in \tilde{M} \succ \frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2} \in \tilde{M}$
$\frac{1}{P} = \frac{a}{a^2+b^2} + \frac{-b}{a^2+b^2} * i \in \tilde{M}$.

Folgerung 8.4.1 *$\tilde{M}$ ist ein zulässiger Körper.*

Lemma 8.4.8 *Ist $z^2 \in \tilde{M}$, dann $z \in \tilde{M}$*



Beweis:

Behautpung: Ist $a \in \mathbb{R}$ mit $a^2 \in \tilde{M} \succ a \in \tilde{M}$

Beweis:

Da $a^2 \in \tilde{M} \succ \frac{a^2+1}{2} \in \tilde{M}$.

Sei K der Kreis um $\frac{a^2+1}{2}$ mit dem Radius $\frac{a^2+1}{2}$.

Sei G_1 die Gerade durch 1 senkrecht auf der x-Achse.

Sei $P = 1 + b * i$ der Schnittpunkt von K und G_1.

Dann $b \in \tilde{M}$.

Behauptung: $a = \pm b$

Nach dem Pythagoras gilt:

$b^2 + (\frac{a^2+1}{2} - 1)^2 = (\frac{a^2+1}{2})^2$

$\succ b^2 + (\frac{a^2+1}{2})^2 - (a^2 + 1) + 1 = (\frac{a^2+1}{2})^2$

$b^2 = a^2$

$b = \pm a$.

Sei $P \in a + b * i$ mit $a, b \in \mathbb{R}$ und $P^2 = c + d * i \in \tilde{M}$ mit $c, d \in \mathbb{R}$.

Behauptung: $P \in \tilde{M}$

Beweis:

$P^2 = (a + b * i) * (a + b * i) = c + d * i$

$\succ a^2 - b^2 = c,\ 2 * a * b = d$

$\succ (\frac{d}{2*b})^2 - b^2 = c$

$\succ 4 * b^4 + 4 * b^2 * c - d^2 = 0$

$\succ b^2 = -\frac{1}{2} * c \pm \frac{1}{2} * \sqrt{c^2 + d^2}$

Da $b^2 \in \mathbb{R} \succ \sqrt{c^2 + d^2} \in \mathbb{R} \succ b^2 \in \tilde{M}$

$\succ b \in \tilde{M}$

$\succ a = \frac{d}{2*b} \in \tilde{M}$

$\succ a + b * i \in \tilde{M}$

Folgerung 8.4.2 *Ist* $(x - \alpha_1) * (x - \alpha_2) \in \tilde{M}[x] \succ \alpha_1, \alpha_2 \in \tilde{M}$

Beweis:

$(x - \alpha_1) * (x - \alpha_2) = x^2 + p * x + q$ mit $p, q \in \tilde{M}$

$$\alpha_{1,2} = -\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q}$$
$$\succ \alpha_1, \alpha_2 \in \tilde{M}$$

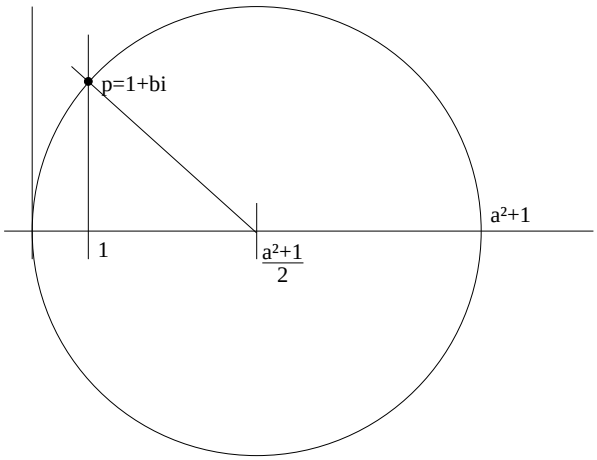
Sei M eine Menge von Punkten mit $0, 1 \in M$.
Dann war
$$\tilde{M} = \bigcup\{N | N \text{ ist aus } M \text{ konstruierbar}\}.$$
Wir hatten gezeigt:

1. $\tilde{M}$ ist ein zulässiger Körper
2. Sind $\alpha, \beta \in \mathbb{C}$ mit $(x - \alpha) * (x - \beta) \in \tilde{M}[x]$, dann sind $\alpha, \beta \in \tilde{M}$.

Satz 8.4.1 *Ist F eine Galois-Erweiterung von K_M mit $[F : K_M] = 2^l$ für ein l, dann ist $F \subseteq \tilde{M}$.*

Beweis:
Da F eine Galois-Erweiterung von K_M ist, ist $|G_{F:K_M}| = [F : K_M]$
Also ist $G_{F:K_M}$ eine p-Gruppe mit p=2.
Wir hatten gezeigt:
Es gibt eine Kette von Gruppen
$$H_0 \supseteq H_1 \supseteq \cdots \supseteq H_k$$
mit:
1. $H_0 = G_{F:K_M} \cdots H_K = \{id_F\}$
2. $H_{i+1} \lhd H_i$
3. $H_i/H_{i+1} \approx \mathbb{Z}_2$

Beweis:
Behauptung: Ist $a \in \mathbb{R}$ mit $a^2 \in \tilde{M} \succ a \in \tilde{M}$
Beweis:
Da $a^2 \in \tilde{M} \succ \frac{a^2+1}{2} \in \tilde{M}$
Sei K der Kreis um $\frac{a^2+1}{2}$ mit dem Radius $\frac{a^2+1}{2}$.
Sei G_1 die Gerade durch 1 senkrecht auf die x-Achse.
Sei $P = 1 + b * i$ der Schnittpunkt von K und G_1.
Dann ist $G \in \tilde{M}$.
Behauptung: $a = \pm b$
Beweis:



Nach Pythagoras gilt:

$b^2 + (\frac{a^2+1}{2} - 1)^2 = (\frac{a^2+1}{2})^2$

$b^2 + (\frac{a^2+1}{2})^2 - (a^2+1)^2 + 1 = (\frac{a^2+1}{2})^2$

$\succ b^2 = a^2$

$\succ b = \pm a$

Sei $P \in a + b * i$ mit $a, b \in \mathbb{R}$ und $P^2 = c + d * i \in \tilde{M}$ mit $c, d \in \mathbb{R}$.

Behauptung: $p \in \tilde{M}$

Beweis:

$p^2 = (a + b * i) * (a + b * i) = c + d * i$

$\succ a^2 - b^2 = c \qquad 2 * a * b = d$

$\succ (\frac{d}{2*b})^2 - b^2 = c$

$\succ 4 * b^4 - 4 * b^2 * c - d^2 = 0$

$\succ b^2 = -\frac{1}{2} * c \pm \frac{1}{2} * \sqrt{c^2 + d^2}$

Da $b^2 \in \mathbb{R} \succ \sqrt{c^2 + d^2} \in \mathbb{R}$.

$\succ b^2 \in \tilde{M} \succ b \in \tilde{M} \succ a = \frac{d}{2*b} \in \tilde{M} \succ a \times b * t \in \tilde{M}$

Sei L_i der Fixkörper von H_i. Dann gilt:

1. $L_0 = K_H \cdots L_K = F$
2. $[L_{i+1} : L_i] \leq 2$

Beweis zu 2:

Da F eine Galois-Erweiterung von K_M ist, gilt:

$G_{F:L_i} = H_i$ und $[F : L_i] = |G_{F:L_i}|$

$G_{F:L_{i+1}} = H_{i+1}$ und $[F : L_{i+1}] = |G_{F:L_{i+1}}|$

Da $[F : L_i] = [F : L_{i+1}] * [L_{i+1} : L_i]$

$\succ |H_i| = |H_{i+1}| * [L_{i+1} : L_i]$

Da $|H_i|/|H_{i+1}| = |H_i/H_{i+1}| = 2 \succ [L_{i+1} : L_i] = 2$

Behauptung: $L_i \subseteq \tilde{M}$

Beweis: (Induktion über i)

Ist $i = 0 \succ L_0 = K_M \subseteq \tilde{M}$

Sei $L_i \subseteq \tilde{M}$.

Da $[L_{i+1} : L_i] \leq 2$ gibt es ein $\alpha \in L_{i+1} \setminus L_i$

mit $\alpha^2 \in L_i$
Dann ist $L_{i+1} = L_i(\alpha)$.
α ist Nullstelle von $x^2 - \alpha^2 \in L_i[x] \subseteq \tilde{M}[x]$
$\succ \alpha \in \tilde{M} \succ L_{i+1} = L_i(\alpha) \subseteq \tilde{M}$

Satz 8.4.2 *Ist $\alpha \in \tilde{M}$, dann gibt es eine Galois-Erweiterung F von K_M mit $[F : K_M] = 2^l$ für ein l und $\alpha \in F$.*

Beweis:

Da $\alpha \in \tilde{M}$ gibt es eine Kette von Körpern
$L_0 \subseteq L_1 \subseteq \cdots \subseteq L_m$
mit:
1. $L_0 = K_M$, $L_1 = K_M(i) \cdot \alpha \in L_M$
2. Es gibt $\alpha_i \in \mathbb{R}$ mit $\alpha_i^2 \in L_i$ und $L_{i+1} = L_i(\alpha_i)$

Wir zeigen durch Induktion über i:
Es gibt eine Kette von Körpern M_i mit:
1. $L_i \subseteq M_i$, $M_0 = K_M$
2. M_i ist eine Galois-Erweiterung von K_M
3. $[M_{i+1} : M_i] = 2^l$ für ein l_i

Sei $i = 0$. Dann sei $M_i = K_M$.
Angenommen wir haben M_i definiert:
Da M_i eine Galois-Erweiterung von K_M ist, gibt es ein Polynom $h_i \in K_M[x]$, dessen Zerfällungskörper M_i ist.
Sei $a_i = a_i^2$.
Dann ist $x^2 - a_i \in L_i[x]$ und α_i ist Nullstelle von $x^2 - a_i$.
Sei $g_i(x) = \prod_{\sigma \in G_{M_i:K_M}} x^2 - \sigma(a_i)$
Dann ist $g_\sigma = g_i \succ g_i \in K_M[x]$.
Sei M_{i+1} der Zerfällungskörper von $h_i * g_i \in K_M[x]$
$\succ$1. M_{i+1} ist eine Galois-Erweiterung von K_M
2. $M_i \subseteq M_{i+1}$ und $\alpha_i \in M_{i+1}$ und somit $L_{i+1} \subseteq M_{i+1}$.

Seien $\beta_1, \cdots, \beta_n$ die Nullstellen von g_i.
Sei $N_0 = M_i \qquad N_{i+1} = N_i(\beta_i)$
Da β_i Nullstelle von $g_i \succ$ Es gibt $\sigma \in G_{M_i:K_M}$
und β_i ist Nullstelle von $x^2 - \sigma(a_i)$
$\succ [N_{i+1} : N_i] \leq 2$
$\succ [M_{i+1} : M_i] = [N_{n+1} : N_0] = \prod_{i=0}^{n} [N_{i+1} : N_i] = 2^{l*i}$ für ein i.

8.5 Regelmäßige n-Ecks

Wir wollen zeigen:
Ist $n = 2^\nu * p_1 \cdots p_k$, wobei $p_1, \cdots, p_k$ paarweise verschiedene Fermat'sche Primzahlen sind, dann ist das regelmäßige n-Eck (aus $\{0,1\}$) konstruierbar.

Lemma 8.5.1 *Sei $ggT(n,m) = 1$.*
*Sind das regelmäßige n-Eck und das regelmäßige m-Eck konstruierbar, so auch das regelmäßige n*m-Eck.*

Beweis:

Nach Voraussetzung ist $\epsilon_1 = e^{\frac{i*2*\pi}{n}} \in \{\tilde{0,1}\}$ und $\epsilon_2 = e^{\frac{i*2*\pi}{m}} \in \{\tilde{0,1}\}$.
$\succ \epsilon_1 * \epsilon_2 = e^{\frac{i*2*\pi}{n}} * e^{\frac{i*2*\pi}{m}} = e^{\frac{i*2*\pi(m+n)}{n*m}} \in \{\tilde{0,1}\}$
Da $ggT(n,m) = 1 \succ ggT(n*m, n+m) = 1$
$\succ \epsilon_1 * \epsilon_2 =$n*m-te primitive Einheitswurzel.
Also gibt es ein l mit $e^{\frac{2*\pi*i}{n*m}} = (\epsilon_1 * \epsilon_2)^l \in \{\tilde{0,1}\}$.

Lemma 8.5.2 *Das regelmäßige 2^ν-Eck ist konstruierbar.*

Beweis: (Induktion über ν)

$\nu = 0 \succ e^{\frac{2*\pi*i}{2^\nu}} = 1 \in \{\tilde{0,1}\}$
$e^{\frac{2*\pi*i}{2^{\nu+1}}} * e^{\frac{2*\pi*i}{2^{\nu+1}}} = e^{\frac{2*\pi*i}{2^\nu}} \overset{Induktionsvoraussetzung}{\in} \{\tilde{0,1}\}$.
$\succ e^{\frac{2*\pi*i}{2^{\nu+1}}} \in \{\tilde{0,1}\}$.

Lemma 8.5.3 *Ist p eine vermatschte Primzahl, dann ist das regelmäßige p-Eck konstruierbar.*

Beweis:

Sei $\epsilon = e^{\frac{2*\pi*i}{p}}$.
Dann ist $[\mathbb{Q}(\epsilon) : \mathbb{Q}] = p - 1 = 2^l$ für ein l.
$\mathbb{Q}(\epsilon)$ ist der Zerfällungskörpervon $x^p - 1$.
$\succ \mathbb{Q}(\epsilon)$ ist Galois-Einheit von $\mathbb{Q}$.
Da $K_M = \mathbb{Q} \succ \epsilon$ ist konstruierbar nach dem Satz von Seite 114.

Sei $\epsilon = 2^{\frac{2*\pi*i}{p}}$ mit p Fermat'sche Primzahl und $F = \mathbb{Q}(\epsilon)$.

Gauss zeigt:
1. $G_{F:Q}$ ist zyklisch der Ordnung z^l
Er bestimmt ein $g \in \mathbb{N}$ mit
$$\sigma(\epsilon) = \epsilon^g$$
so daß $< \sigma >= G_{F:Q}$

Sei $p = 17$ und $g = 3$.
Es sei $H_i =< \sigma^{2^i} >$. Dann gibt es $H_i/H_{i+1} \approx \mathbb{Z}_2$.
Ist $p = 17$, dann ist:
$\sigma_{F:Q} = H_0 =< \sigma >$
$H_1 =< \sigma^2 >$
$H_2 =< \sigma^4 >$
$H_3 =< \sigma^8 >$
$H_4 =< \sigma^{16} >=< id_F >$
Seien L_i die Fixkörper von H_i.
Dann ist $[L_{i+1} : L_i] = 2$.
Also gibt es η_{i+1} mit $L_{i+1} = L_i(\eta_{i+1})$
und es gibt $f \in K_i[x]$ mit $grad(f) \leq 2$ und η_{i+1} ist Nullstelle von f.
Gauss gibt η_i's und Polynome f an:
Er setzt:
$$\epsilon_k = \sigma^k(\epsilon) \text{ und } \eta_{i,k} = \sum_{\tau \in H_i} \tau(\epsilon_k)$$
$\eta_{i,k}$ heißen Gaus'sche Perioden.
Man rechnet nach:

1. $\eta_{0,0} = -1$ $\eta_{l,0} = \epsilon$
2. $\eta_{i,k} = \eta_{i,k+m}$ gdw. $2^i | m$
3. $\eta_{i,k} = \eta_{i+1,k} + \eta_{i+1,k+2^i}$

Behauptung 8.5.1 $L_{i+1} = L_i(\eta_{i+1,k})$

Beweis:
$\eta_{i+1,k} \in L_{i+1}$
Beweis:
Sei $\sigma^n \in H_{i+1} \succ 2^{i+1} | m$
$\succ \sigma^m(\eta_{i+1,k}) = \sigma^m(\sum_{\tau \in H_{i+1}} \tau(\epsilon_k))$
$= \sum_{\tau \in H_{i+1}} \sigma^m \circ \tau(\epsilon_k)$
$= \sum_{\tau \in H_{i+1}} \tau(\sigma^m(\epsilon_k))$
$= \sum_{\tau \in H_{i+1}} \tau(\epsilon_{k+m})$
$= \eta_{i+1,k+m}$
$= \eta_{i+1,k}$ da $2^{i+1}/m$.

Ebenso zeigt man:
Sei $\sigma^{2^i} \in H_i \succ \sigma^{2^i}(\eta_{i+1,k}) \neq \eta_{i+1,k}$
$\succ \eta_{i+1,k} \notin L_i$
$[L_{i+1} : L_i] = 2 \succ L_{i+1} = L_i(\eta_{i,k})$

Behauptung 8.5.2 *Sei* $\alpha = \eta_{i+1,k}$ *und* $\beta = \eta_{i+1,k+2^i}$.
Dann ist $(x - \alpha) * (x - \beta) \in L_i[x]$.

Beweis:
$(x - \alpha) * (x - \beta) = x^2 - (\alpha + \beta) * x + \alpha * \beta$
$\alpha + \beta \overset{(3)}{=} \eta_{i,k} \in L_i$
Da $[L_{i+1} : L_i] = 2 \succ \alpha^2, \beta^2 \in L_i$
$\succ \alpha * \beta = \frac{1}{2} * (\alpha + \beta)^2 . \alpha^2 - \beta^2 \in L_i$

Danach gab Gauss noch einige Polynome an, die leider mangels Zeit hier keine Beachtung mehr finden.

"Und Clarice ? Haben die Lemma aufgehört zu schreien ?"

9 Zeichenerklärung und Schlagwortregister

Erklärung für einige Sonderzeichen:

e	neutrales Element
$\hookleftarrow$	dann sind äquivalent
$\succ$	daraus folgt
($\ddot\smile$)	Das is´n smiley,du ...
$\forall$	für alle
$\subset, \subseteq$	ist Teilmenge von
$<$	ist Untergruppe von
$\mapsto$	wird abgebildet auf
$\rightarrow$	geht über
$\lhd$	ist Normalteiler von
$\cup$	vereinigt
$\cap$	geschnitten
$\mid$	teilt
$\in$	ist Element von
$\notin$	ist kein Element von
$\equiv$	identisch, Kongruent
$\approx$	ist isomorph zu
$\cong$	ist kongruent zu
$\sim$	konjugiert zu
$\sharp$	Widerspruch
$\surd$	logisch, trivial, abgehakt
/	nach
gdw	genau dann wenn
qed	quot erat demonstrandum (oder so ähnlich)
wzbw	was zu beweisen war
oBdA	ohne Beschränkung der Allgemeinheit
z.z.	zu zeigen
i.Z.	in Zeichen
d.h.	das heißt

Index