Algebra für Lehramt WiSe 2017/18

Vorlesungen Mo 11:30 - 13:00 V57.05
Di 8:00 - 9:30 V57.06.

Übungen Mo 15:45 - 17:15, Di 15:45 - 17:15 beide 7.331

Assistenz: Eirini Chavli

In der Linearen Algebra haben sie sicherlich die Definitionen der grundlegenden algebraischen Strukturen gesehen:
Gruppen, Ringe, Körper und natürlich Vektorraum.
Wir beginnen mit einigen Erinnerungen und Beispielen.

§1 Algebraische Strukturen

Gruppen Beisp.: Symmetrische Gruppe S_n
alle Permutationen von $1,\dots,n$ mit $\circ$ als Verknüpfung.

z.B. $n=3$

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \qquad \tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

$$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$GL_n(K)$: invertierbare $n \times n$-Matrizen mit Einträgen in einem Körper K. und Matrixmult. als Verknüpfung.

Def. 1.1 Eine Gruppe heißt abelsch (zu Ehren des Mathematikers H. N. Abel) wenn die Multiplikation kommutativ ist.
In diesem Fall wird oft die Verknüpfung mit $+$ bezeichnet, das neutrale Element mit 0 und das Inverse mit $-$.

Beisp: $(\mathbb{Z}, +)$ ist abelsch.

Für $n \geq 3$ ist S_n nicht abelsch; s.o. $n=3$:

$$\sigma \circ \tau + \tau \circ \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

Für $n \geq 2$ ist $GL_n(K)$ nicht abelsch.

Ring abelsche Gruppe + Multiplikation, die assoziativ ist und Distributivregeln gelten, also $x \cdot (a+b) = x \cdot a + x \cdot b$ etc.

Ein Ring heißt kommutativ, wenn die Multiplikation kommutativ ist.

Def. 1.2 Sei R ein Ring, der ein neutrales Element 1_R bzgl. Multiplikation besitzt ("Ring mit 1", manchmal bezeichnet man einen Ring ohne 1_R auch als "Rng".)

~~Ganze Zahlen sind Körper~~

Ein Element $0 \neq a \in R$ heißt Einheit, wenn a bzgl. der Multiplikation ein Inverses besitzt, es ex. also $b \in R$ mit $1_R = a \cdot b = b a$.

$R^\times := \{ a \in R \mid a \text{ Einheit} \}$ heißt Einheitengruppe von R (Dies ist tatsächlich ein Gruppe bzgl. Multiplikation)

Beachte: Ist $1_R = 0$, so $a = a \cdot 1_R = a \cdot 0 = 0$ für alle $a \in R$, also $R = \{0\}$.

Beisp. $\mathbb{Z}$ ganze Zahlen mit üblicher Addition und Multiplikation, kommutativ, $\mathbb{Z}^\times = \{+1, -1\}$.

$M_n(K)$ $n \times n$-Matrizen mit Einträgen in Körper K und üblicher Matrix-Addition und Multiplikation nicht kommutativ für $n \geq 2$, $M_n(K)^\times = \{\text{invertierbare Matrizen}\} = GL_n(K)$.

Einselement $I_n = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$

$K[X]$ Polynome in Unbestimmter X und Koeffizienten in Körper K, kommutativ, $K[X]^\times = K^\times$ (konstante Polynome $\neq 0$).

Körper kommutativer Ring K mit $1 \neq 0$ so daß $K^\times = K \setminus \{0\}$.

Beisp.: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ $\mathbb{F}_p$ = endlicher Körper mit p Elementen, p Primzahl

Insbesondere $p=2$ $\quad \mathbb{F}_2 = \{\bar{0}, \bar{1}\}$.

$+$	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$

$\cdot$	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$

genaue Konstruktion siehe §2.

Konstruktion von $\mathbb{Q}$ aus $\mathbb{Z}$, von $\mathbb{R}$ aus $\mathbb{Q}$, siehe §2

Wie erhält man $\mathbb{C}$ aus $\mathbb{R}$?

a) $\mathbb{C} = \mathbb{R}^2 = \{(a,b) \mid a,b \in \mathbb{R}\}$ $\mathbb{R}$- Vektorraum

Def. Produkt $(a,b)\cdot(c,d) := (ac-bd, ad+bc)$.

Setze $1 := (1,0)$, $i := (0,1)$ Dann $i^2 = -1$

und $\mathbb{C} = \{a+bi \mid a,b \in \mathbb{R}\}$ prüfe alle Körperaxiome.

b) $\mathbb{C} := \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a,b \in \mathbb{R} \right\}$ mit üblicher Matrix-Addition und Multiplikation.

Setze $1 := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $i := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ Dann $i^2 = -1$

und $\mathbb{C} = \{a+bi \mid a,b \in \mathbb{R}\}$.

Können jeweils $\mathbb{R}$ als Teilmenge von $\mathbb{C}$ auffassen

Im Fall a): $\mathbb{R} \to \mathbb{C}$, $a \mapsto (a,0) = a \cdot 1$

b) $\mathbb{R} \to \mathbb{C}$, $a \mapsto \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} = a \cdot \mathbb{1}$.

Bemerkung: $\mathbb{H} := \left\{ \begin{pmatrix} u & v \\ -\bar{v} & \bar{u} \end{pmatrix} \mid u,v \in \mathbb{C} \right\} \subseteq M_2(\mathbb{C})$

↑ komplexe Konjugation ist ein Schiefkörper mit üblicher Matrix Addition und Multiplikation "Hamilton'sche Quaternionen"

d.h. $\mathbb{H}$ Ring mit 1 so daß $\mathbb{H}^\times = \mathbb{H} \setminus \{0\}$ aber Einheitengruppe nicht abelsch.

wg werden wir hier nicht weiter betrachten.

Vektorraum gemischte algebraische Struktur

V abelsche Gruppe (Verknüpfung $+$)

K Körper

plus Abbildung $K \times V \to V$, $(s,v) \mapsto s \cdot v$ skalare Multiplikation

so dass Vektorraumaxiome gelten.

Zusammenfassung: Abelsche Gruppen sind grundlegend in allen obigen Definitionen: Ringe, Körper und Vektorräume sind zunächst abelsche Gruppen plus zusätzliche Operationen

Untersstrukturen

Def. 1.3 Sei G eine Gruppe und $H \subseteq G$ eine Teilmenge. Dann heißt H eine Untergruppe (in Zeichen $H \leq G$) wenn gilt:

$1_G \in H$, $a \cdot b \in H$ und $a^{-1} \in H$
(insbes. $H \neq \emptyset$) für alle $a, b \in H$

$\Rightarrow$ H zusammen mit der Einschränkung der Verknüpfung aus G ist wieder eine Gruppe.

Beisp. $G = GL_n(K)$ K Körper

$SL_n(K) = \{ A \in G \mid \det(A) = 1 \}$ ist eine Untergruppe.

(benutze: $\det(AB) = \det(A) \cdot \det(B)$
A invertierbar $\Leftrightarrow \det(A) \neq 0$ }.

$H := \left\{ \begin{pmatrix} a_1 & & * \\ & \ddots & \\ 0 & & a_n \end{pmatrix} \mid 0 \neq a_i \in K \right\} \subset G$ ist eine Untergruppe.

(benutze: Produkte und Inverse von Dreiecksmatrizen sind wieder Dreiecksmatrizen

$$\begin{pmatrix} a_1 & & * \\ & \ddots & \\ 0 & & a_n \end{pmatrix}^{-1} = \begin{pmatrix} a_1^{-1} & & * \\ & \ddots & \\ 0 & & a_n^{-1} \end{pmatrix}.$$

Analog für Ringe: Sei R ein Ring und $S \subseteq R$ eine Teilmenge. Dann heißt S ein Teilring von R

wenn $(S,+)$ eine Untergruppe von $(R,+)$ ist und $a \cdot b \in S$ für alle $a,b \in S$ gelt.

~~Teilring, Einselement, Verknüpfung~~

Bemerkung: Hat R ein Einselement, so muß dieses nicht zu S gehören. Es kann sogar sein, daß R und S verschiedene Einselemente haben.

Beisp: $R = \mathbb{Z}$ $\quad S = 2\mathbb{Z} = \{$ gerade ganze Zahlen $\} \subseteq R$ Teilring ohne 1.

$R = M_2(\mathbb{Q})$ $\quad S = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \mid a \in \mathbb{Q} \right\} \subseteq R$ Teilring

↑ Einselement $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. ↳ Einselement $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$

Bemerkung: Ist $S \subseteq R$ Teilring und $0 \neq s \in S$ invertierbar in R, so muß nicht unbedingt $s^{-1} \in S$ gelten.

Beisp: $S = \mathbb{Z} \subseteq R = \mathbb{Q}$ $\quad \frac{1}{2} \in \mathbb{Q} \setminus \mathbb{Z}$.

Zusammen mit algebraischen Strukturen betrachten wir auch unter strukturerhaltende Abbildungen (Homomorphismen)

Def. 1.4 Seien G, H Gruppen. Eine Abbildung $f: G \to H$ heißt Gruppenhomomorphismus, wenn gilt:

$$f(x \cdot y) = f(x) \cdot f(y) \quad \text{für alle } x, y \in G.$$

↑ Mult. in G ↑ Mult. in H.

Es folgt dann automatisch (Beweis selbst) $f(1_G) = 1_H$ und $f(x^{-1}) = f(x)^{-1}$ für alle $x \in G$.

Ein Homomorphismus, der bijektiv ist, heißt ein Isomorphismus. Die beteiligten Gruppen heißen dann isomorph, in Zeichen $G \cong H$

Sind zwei Gruppen isomorph, so kann man in G genauso rechnen wie in H, die beiden Gruppen sind also in diesem Sinne "gleich".

Analoge Definitionen für andere algebraische Strukturen.

R, S Ringe $f: R \to S$ heißt Ringhomomorphismus, wenn $f: (R,+) \to (S,+)$ ein Gruppenhom. ist und zusätzlich $f(r_1 \cdot r_2) = f(r_1) \cdot f(r_2)$ für alle $r_1, r_2 \in R$ gelt.

Besitzen R, S 1-Elemente, $1_R, 1_S$, so verlangen wir auch, daß $f(1_R) = 1_S$ gelt.

Bemerkung: Dies folgt nicht automatisch!

$S = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \mid a \in \mathbb{Q} \right\} \xhookrightarrow{f} R = M_2(\mathbb{Q})$ Inklusion.

$f(1_S) \neq 1_R$. s.o.

Werden viele weitere Beispiele für Homomorphismen später sehen.

Übung. Seien G, H Gruppen $f: G \to H$ Homomorphismus.

Zeige Sie, daß die Umkehrabbildung ebenfalls ein Homom. ist!

Analoge Aussagen gelten auch für Ringe und Vektorräume, wobei für Vektorräume gelt: Homomorphismus = lineare Abbildung

§2 Faktorstrukturen

Sei M eine Menge und $\sim$ eine Äquivalenzrelation auf M. (reflexiv, symmetrisch, transitiv). Für $m \in M$ bezeichne

$[m] := \{ m' \in M \mid m' \sim m \}$ die zugehörige Äquivalenzklasse

und $M/\sim := \{ [m] \mid m \in M \}$ die Menge der Äquivalenzklassen.

Ist M nicht nur eine Menge, sondern eine algebraische Struktur, und erfüllt $\sim$ bestimmte Zusatzbedingungen, so kann man auch $M/\sim$ wieder zu einer algebraischen Strukturen machen. Dies ist ein sehr nützliches und schlagkräftiges Konstruktionsprinzip.

Beispiel 2.1 Konstruktion von $\mathbb{Q}$ aus $\mathbb{Z}$.

$M := \mathbb{Z} \times (\mathbb{Z} \setminus 0)$ = Menge aller Paare (a,b) mit $a,b \in \mathbb{Z}, b \neq 0$

Def. $(a,b) \sim (c,d) \overset{\text{def.}}{\Leftrightarrow} a \cdot d = b \cdot c$

reflexiv: $(a,b) \sim (a,b)$ denn $a \cdot b = b a$

symmetrisch: $(a,b) \sim (c,d) \Rightarrow (c,d) \sim (a,b)$, denn $cb = bc$
$ad = da$.

transitiv $(a,b) \sim (c,d)$ und $(c,d) \sim (e,f) \Rightarrow (a,b) \sim (e,f)$

denn: $ad = bc$ und $cf = de \Rightarrow afd = (ad)f = (bc)f = b(cf) = bde$

Nun ist $d \neq 0$ und in $\mathbb{Z}$ können wir Faktor d kürzen,

also $af = be$ ✓.

Bezeichne: $[a/b]$ als a/b also z.B. $2/3 = 4/6 = -10/-30$ etc.

jede Äquivalenzklasse stellt genau einen Bruch in üblichem Sinne dar. Setze: $\mathbb{Q} := \{ a/b \mid a,b \in \mathbb{Z}, b \neq 0 \}$.

Definiere neue Verknüpfungen:

$$a/b + c/d := \frac{ad+bc}{bd} \qquad a/b \cdot c/d := ac/bd.$$

Beachte: Wenn man neue Operationen für Äquivalenzklassen definiert, so muß man zuerst nachprüfen, daß diese "wohl-definiert" sind, also nicht von der Wahl von Repräsentanten abhängen. In diesem Fall heißt das: Sei $a/b = a'/b'$ und $c/d = c'/d'$. Dann muß man zeigen, daß

$$ad+bc/bd = a'd'+b'c'/b'd'$$

und $ac/bd = a'c'/b'd'$ gelb ⇝ selbst

Nachdem dies getan ist, zeigt man, daß $(\mathbb{Q}, +, \cdot)$ ein Körper ist. Durch die Zuordnung $\mathbb{Z} \to \mathbb{Q}$, $u \mapsto u/1$ fassen wir $\mathbb{Z}$ als Teilmenge von $\mathbb{Q}$ auf, so wie wir üblicherweise $3 = 3/1$ schreiben. Dann auch

$$\mathbb{Q} = \{ ab^{-1} \mid a,b \in \mathbb{Z}, b \neq 0 \}.$$

Beisp. 2.2 Konstruktion von $\mathbb{R}$ aus $\mathbb{Q}$ (P)

Sei $\mathcal{F}$ die Menge aller Folgen $(a_n)_{n\in\mathbb{N}}$ mit $a_n \in \mathbb{Q}$ für alle $n \in \mathbb{N}$

(Folge = Abbildung $\mathbb{N} \to \mathbb{Q}$, $n \mapsto a_n$.)

Eine Folge (a_n) heißt Nullfolge, wenn es zu jedem $\varepsilon > 0$ ($\varepsilon \in \mathbb{Q}$) ein $n_0 \in \mathbb{N}$ gibt mit $|a_n| < \varepsilon$ für alle $n \geq n_0$

Eine Folge (a_n) heißt Cauchy-Folge, wenn es zu jedem $\varepsilon > 0$ ($\varepsilon \in \mathbb{Q}$) ein $n_0 \in \mathbb{N}$ gibt mit $|a_n - a_m| < \varepsilon$ für alle $n, m \geq n_0$

$|\cdot|$ = Absolutbetrag rationaler Zahlen.

Sei $\mathcal{F}_0$ Menge aller Cauchy-Folgen.

$(a_n) \sim (b_n) \overset{\text{def}}{\Leftrightarrow} (a_n - b_n)$ Nullfolge. (Äquivalenzrelation)

Sei $\mathbb{R} :=$ Menge aller Äquivalenzklassen $[a_n]$, $(a_n) \in \mathcal{F}_0$.

Addition + Multiplikation

$$[a_n] + [b_n] := [a_n + b_n]$$
$$[a_n] \cdot [b_n] := [a_n \cdot b_n]$$

Dann zeigt, daß $\mathbb{R}$ ein Körper ist so daß jede Cauchy-Folge einen Grenzwert hat. Durch die Zuordnung

$$\mathbb{Q} \to \mathbb{R},\ a \mapsto [a] \quad (\text{konst. Folge } (a, a, a, \ldots))$$

fassen wir $\mathbb{Q}$ als Teilmenge von $\mathbb{R}$ auf.

Übung: Konstruktion von $\mathbb{Z}$ aus $\mathbb{N}$ (durch analoge Konstruktion wie $\mathbb{Z} \subseteq \mathbb{Q}$)

Beisp. 2.3 Die Zahl $\mathbb{Z}/d$.

Sei $d \in \mathbb{Z}$, $d > 0$, fest. Für $n, m \in \mathbb{Z}$ definiere

$$n \sim_d m \overset{\text{def}}{\Leftrightarrow} d \mid n - m \quad (d \text{ teilt } n - m).$$

Dann ist $\sim_d$ eine Äquivalenzrelation (selbst).

Bezeichne Äquivalenzklasse $[n]$ mit $\bar{n}$ und

$\mathbb{Z}/\sim_d$ mit $\mathbb{Z}/d = \{\bar{n} \mid n \in \mathbb{Z}\}$.

Gelt $n \sim_d m$ so heißen n, m kongruent modulo d

Schreibweise $n \equiv m \bmod d$.

Äquivalenzklassen heißen auch Kongruenzklassen.

Definiere Addition und Multiplikation:

$\bar{n} + \bar{m} := \overline{n+m}$ und $\bar{n} \cdot \bar{m} := \overline{n \cdot m}$.

Wohldefiniert: sei $n \sim_d k$ und $m \sim_d l$ Müssen zeigen:

$n+m \sim_d k+l$ und $n \cdot m \sim_d k \cdot l$.

Dazu: Nach Vor. ist $d \mid n-k$ und $d \mid m-l$, also gibt es

$r, s \in \mathbb{Z}$ mit $n-k = rd$ und $m-l = sd$.

$\Rightarrow (n+m) - (k+l) = (n-k) + (m-l) = rd + sd = (r+s)d$

also $d \mid (n+m) - (k+l) \Rightarrow n+m \sim_d k+l$.

$n \cdot m - k \cdot l = (rd+k)(sd+l) - kl = rsd^2 + rdl + ksd + kl - kl$

$= (rsd + rl + sk)d$, also $d \mid n \cdot m - k \cdot l$

also $n \cdot m \sim_d k \cdot l$.

Erinnerung Division mit Rest. Zu $n \in \mathbb{Z}$ gibt es

$q, r \in \mathbb{Z}$ mit $n = qd + r$ mit $0 \le r \le d-1$.

Hierbei sind q, r eindeutig bestimmt. Es gilt also $n \equiv r \bmod d$.

Beweis mit Algorithmus: man nehme etwas positives (oder 0)

Ist $n > 0$, so ziehe d solange ab, bis erhält

Ist $n < 0$, so addiere solange d, bis man etwas positives (oder 0) erhält.

$d = 3$ $n = 16 \to 13 \to 10 \to 7 \to 4 \to (1) \to -2$.

$= r$.

$16 = 5 \cdot 3 + 1$

$= q$.

$n = -16 \to -13 \to -10 \to -7 \to -4 \to -1 \to (2)$

$= r$.

$-16 = (-6) \cdot 3 + 2$

Satz 2.4 Sei $\mathbb{Z}/d = \{\bar{n} \mid n \in \mathbb{Z}\}$ mit Verknüpfungen $+, \cdot$ wie oben.
Dann gelt:

(a) $\mathbb{Z}/d$ hat genau d Elemente; $\mathbb{Z}/d = \{\bar{0}, \bar{1}, \dots, \overline{d-1}\}$.

(b) $\mathbb{Z}/d$ ist ein kommutativer Ring mit Einselement $\bar{1}$.

Beweis: a) Sei $n \in \mathbb{Z}$ bel. Division mit Rest $\Rightarrow$
$n \equiv r \bmod d$ mit $0 \le r \le d-1$.

$\Rightarrow \mathbb{Z}/d = \{\bar{0}, \bar{1}, \dots, \overline{d-1}\}$. Bleibt noch zu zeigen,
daß $\bar{n} \neq \bar{m}$ gilt falls $n \neq m$ und $0 \le n, m \le d-1$.
Sei also $\bar{n} = \bar{m}$, d.h. $d \mid n-m$.
Können oBdA annehmen, daß $m < n$ gilt. Dann
$0 < n-m \le d-1$ und $d \mid n-m$ ↯.

Also ist $|\mathbb{Z}/d| = d$.

b) Regeln folgen sofort aus analogen Regeln in $\mathbb{Z}$ selbst, z.B.

$$\bar{n} \cdot (\bar{m} + \bar{k}) = \bar{n} \cdot \overline{m+k} = \overline{n(m+k)} = \overline{nm+nk}$$
$$= \overline{n \cdot m} + \overline{n \cdot k} = \bar{n} \cdot \bar{m} + \bar{n} \cdot \bar{k} \quad \text{usw.} \qquad \square$$

Erinnerung Seien $n, m \in \mathbb{Z}$, $n, m \neq 0$. Dann liefert der folgende "Euklidische Algorithmus" Elemente $r, s, t \in \mathbb{R}$ mit

(*) $t \neq 0$ ist ein gemeinsamer Teiler von n, m und es gilt

$$t = rn + sm, \quad t > 0.$$

Beweis: Sei zuerst $n > 0$.
Ist $m \mid n$, so setze $t := n$, $r := 0$, $s := 1$ OK.
Sei nun $m \nmid n$ und setze $r_0 := n > 0$. Dann dividiere fortlaufend mit Rest:

$$n = r_0 q_1 + r_1 \quad \text{mit} \quad 0 \le r_1 < r_0.$$
$$r_0 = r_1 q_2 + r_2 \quad \text{mit} \quad 0 \le r_2 < r_1.$$
$$r_1 = r_2 q_3 + r_3 \quad \text{mit} \quad 0 \le r_3 < r_2$$
$$\vdots \quad \text{usw.}$$

bis das Verfahren abbricht, d.h. der Rest gleich 0 ist.

Beweis: Wegen $r_0 > r_1 > r_2 > \ldots \geq 0$ muß dieses Verfahren nach endl. vielen Schritten abbrechen, d.h. es gibt ein $N \geq 1$ mit $r_i \neq 0$ für $0 \leq i \leq N$ und $r_{N-1} = r_N q_{N+1}$, $r_{N+1} = 0$

Setze dann $t := r_N$.

Beh.: $t \mid n$ und $t \mid m$.

denn: $r_{N-1} = t q_{N+1} \Rightarrow t \mid r_{N-1} \Rightarrow t \mid r_{N-2} = r_{N-1} q_N + r_N$

usw. bis $t \mid r_0 = m$ und $t \mid n = r_0 q_1 + r_1$.

Wie findet man r_is?

$n = r_0 q_1 + r_1 \Rightarrow r_1 =$ Kombination von n und m

$\Rightarrow r_2 = \underbrace{r_0}_{=m} - r_1 q_2 =$ Kombination von n und m.

$r_3 = r_1 - r_2 q_3 =$ Kombination von n und m

usw bis $t = r_N =$ ——— " ———

Für $m < 0$ wende alles auf $n, -m$ an.

Beisp: $n = 17$ $m = 3$ $r_0 = 3$,

$17 = \underline{3} \cdot 5 + \underline{2}$ $\quad -r_1$

$\underline{3} = \underline{2} \cdot 1 + \underline{1}$ $\quad -r_2$

$\underline{2} = \underline{1} \cdot 2 + 0$ $\quad -r_3$

also $N = 2$ $\quad r_N = 1 = t$.

$\underline{2} = 17 - 3 \cdot 5$

$1 = 3 - \underline{2} \cdot 1 = 3 - (17 - 3 \cdot 5)$

$= \underbrace{(-1)}_{=r} \cdot 17 + \underbrace{6}_{=s} \cdot 3$

Satz 2.5 $\mathbb{Z}/d$ ist genau dann ein Körper, wenn $d = p$ eine Primzahl ist.

Beweis: Sei $d = p$ Pz. und $1 \leq n < p$. Müssen zeigen: $\bar{n}$ hat Inverses in $\mathbb{Z}/d$.

Wende Euklidischen Algorithmus auf n und p an, also es

$r, s, t \in \mathbb{Z}$ mit $t \neq 0$, $t \mid n$ und $t \mid p$

$t = rn + sp$.

p Pz. $\Rightarrow t = 1$ oder $t = p$. Wäre $t = p$, so $p \mid n$ $\lightning$ $(n < p)$.

Also $t = 1$, d.h. $1 = rn + sp \Rightarrow \bar{1} = \bar{r}\bar{n} + \bar{s}\bar{p} = \bar{r}\bar{n}$

$\Rightarrow \bar{n}^{-1} = \bar{r}$ ✓.

Ungekehrt sei d keine Primzahl, also $d = d_1 d_2$ mit $2 \le d_1, d_2 < d$. Dann $\bar{0} = \bar{d} = \bar{d}_1 \bar{d}_2$ und $\bar{d}_1 \neq 0$, $\bar{d}_2 \neq 0$.

Wäre $\mathbb{Z}/d$ Körper, so ex. $\bar{d}_1^{-1} \in \mathbb{Z}/d$. Aber dann:

$$\bar{0} = \bar{0} \cdot \bar{d}_1^{-1} = \bar{d}_1 \bar{d}_2 \bar{d}_1^{-1} = \bar{d}_2 \quad \lightning. \qquad \square$$

Die Konstruktion von $\mathbb{Z}/d$ lässt sich wie folgt verallgemeinern.

Def. 2.7 Sei R ein kommutativer Ring mit 1.
Eine Teilmenge $I \subseteq R$ heißt Ideal, wenn $I \neq R$, wenn $(I, +)$ eine Untergruppe von $(R, +)$ ist und $x \cdot y \in I$ für alle $x \in I$, $y \in R$ gilt.

Sei z.B. $a \in R$ fest. Dann setze $(a) := R \cdot a := \{ra \mid r \in R\}$.
Man prüft sofort nach, dass (a) ein Ideal ist. Solche von einem Element erzeugten Ideale heißen Hauptideale.

z.B. $R = \mathbb{Z}$ $\quad (d) = \{dn \mid n \in \mathbb{Z}\}$. $\quad$ Bsp $d = 2$.
$\Rightarrow (d) = \{$alle geraden Zahlen$\}$.

Sei nun $I \neq R$ wie oben. Definiere Relation $\sim_I$ auf R:

$$a \sim_I b \overset{\text{def}}{\Longleftrightarrow} a - b \in I.$$

reflexiv: $a \sim_I a$ denn $0 = a - a \in I$

symmetrisch: $a \sim_I b \Rightarrow b \sim_I a$ denn $a - b \in I \Rightarrow b - a \in I$.

transitiv: $a \sim_I b$, $b \sim_I c \Rightarrow a \sim_I c$, denn $a - b \in I$, $b - c \in I$

$\Rightarrow a - c = a - b + b - c \in I$ ✓.

Also $\sim_I$ Äquivalenzrelation. Sei $a \in R$. Dann

$$[a] = \{b \in R \mid a \sim_I b\} = \{b \in R \mid b - a \in I\}.$$
$$= \{b \in R \mid \text{ex. } x \in I \text{ mit } b = a + x\} = \{a + x \mid x \in I\}.$$
$$= a + I \quad \text{(Kurzschreibweise)}$$

Menge der Äquivalenzklassen $R/I = \{[a] \mid a \in R\} = \{a + I \mid a \in R\}$

Definiere Verknüpfungen auf R/I.

$[a]+[b] := [a+b]$ $\quad [a]\cdot[b] := [a\cdot b]$.

wohldefiniert: Sei $[a]=[c]$ und $[b]=[d]$.
Müssen zeigen $[a+b]=[c+d]$ und $[a\cdot b]=[c\cdot d]$

Dazu: Nach Vor ist $a-c \in I$ und $b-d \in I$.
also ex. $r,s \in I$ mit $a-c=r$ und $b-d=s$.

$\Rightarrow a+b-(c+d) = a-c+b-d = r+s \in I$ weil I Ugr. von $(R,+)$

und $a\cdot b - c\cdot d = (c+r)(d+s) - c\cdot d = cd+cs+rd+rs-cd$.

$= \underbrace{cs}_{\in I} + \underbrace{rd}_{\in I} + \underbrace{rs}_{\in I} \in I$

Beachte: Hier ist es wichtig, daß Produkte von Elementen aus I mit beliebigen Elementen aus R wieder in I liegen!

Dann erhält man auch wieder:
Mit diesen Verknüpfungen ist R/I ein kommutativer Ring mit Eins-Element $[1_R]$, neutrales Element bzgl $+$ ist $[0]$

Insbesondere: Bsp 2.3 ist der Spezialfall $R=\mathbb{Z}$, $I=(d)$.

Def 2.8 Mit den Bezeichnungen in Def. 2.7 heißt I ein maximales Ideal, wenn $I \neq R$ gilt und es kein weiteres Ideal zwischen I und R gibt. D.h. ist $J \trianglelefteq R$ mit $I \subseteq J \subseteq R$, so folgt $I=J$ oder $R=J$.

Satz 2.9 R/I ist ein Körper genau dann wenn I ein maximales Ideal ist

Beweis: Sei I ein max. Ideal und $a \in R$ mit $[a] \neq 0$.
Müssen zeigen, daß $[a]$ ein Inverses in R/I hat.
Sei $J := \{ar+x \mid r \in R, x \in I\} \subseteq R$. Man zeigt sofort, daß dies ein Ideal ist. Klar: $I \subseteq J$. I maximal
$\Rightarrow I=J$ oder $R=J$. Wäre $I=J$ so $a \in I$ also $[a]=[0]$ ↯ Vor. Also $R=J$ also ex. $r \in R, x \in I$ mit $1_R = ar+x$.

Hier dann: $[1_R] = [a][r] + [x] = [a][r] + [0]$

also $[r] = [a]^{-1}$ ✓.

Umgekehrt sei I nicht maximal und $J \trianglelefteq R$ mit $I \subsetneq J \subsetneq R$. Sei $a \in J \setminus I$. Dann $[a] \neq [0]$.

denn: R/I Körper $\Rightarrow$ $[a]^{-1}$ existiert in R/I, d.h. es gibt $b \in R$ mit $[a][b] = [1_R]$ also $ab - 1 \in I$.

also $ab - 1 = x \in I_R \subseteq J \Rightarrow 1_R = \underbrace{ab - x}_{\in J} \in J \Rightarrow r = r \cdot 1_R \in J$ für alle $r \in R$

also $J = R$ ↯ □

Durch Kombination von Satz 2.5 und Satz 2.9 erhalten wir also:

Sei $R = \mathbb{Z}$ und $0 \neq d \in \mathbb{Z}$, $d > 0$. Dann ist

$(d) \trianglelefteq \mathbb{Z}$ ein maximales Ideal $\Leftrightarrow$ $d = p$ Primzahl

Satz 2.9 wird ein wichtiges Hilfsmittel sein, um allgemeine neue Körper mit bestimmten Eigenschaften zu konstruieren.

~~Satz 2.10 (Homomorphiesatz) Sei R kommutativ Ring mit 1 und $I \trianglelefteq R$ ein Ideal. Dann gibt es einen Ringhomomorphismus~~

§3 Teilbarkeit in Integritätsringen

Hauptsatz der elementaren Arithmetik: Jede natürliche Zahl $\neq 1$ lässt sich schreiben als Produkt von Primzahlen, wobei die Faktoren bis auf die Reihenfolge eindeutig bestimmt sind

z.B. $12 = 2 \cdot 2 \cdot 3 = 2^2 \cdot 3$.

Wollen untersuchen, unter welchen allgemeineren Bedingungen eine solche Aussage richtig bleibt. In diesem § sei stets R ein kommutativer Ring mit 1. Sind $a, b \in R$, so schreiben wir $a \mid b$ wenn es ein $c \in R$ gibt mit $b = ac$ "a teilt b". z.B $a \mid 0$ für alle $a \in R$. (nimm $c = 0$).

Def. 3.1 R heißt Integritätsring, wenn für alle $a, b \in R$ mit $a \neq 0$, $b \neq 0$ auch $a \cdot b \neq 0$ gilt.

[Ist $a \cdot b = 0$ mit $a \neq 0$, $b \neq 0$, so heißen a, b "Nullteiler"]

Ist $0 \neq a \in R^\times$, so gilt $a \cdot b \neq 0$ für alle $b \neq 0$

denn sonst: $ab = 0 \Rightarrow a^{-1}(ab) = b = 0$ ↯.

Insbesondere: R Körper $\Rightarrow$ R Integritätsring.

oder allgemeiner: R Teilring eines Körpers $\Rightarrow$ R Integritätsring

Standardbeispiel $R = \mathbb{Z}$ Von nun an sei R stets ein Integritätsring.

Beachte: $a, b \neq 0$: $a \mid b$ und $b \mid a \Rightarrow b = ua$ mit $u \in R^\times$ [schreibe: $b = ra$, $a = sb \neq$ $b = rsb$, $b \neq 0 \Rightarrow rs = 1$]

Def. 3.2 Sei $0 \neq p \in R$ ein Element, das keine Einheit ist.

(a) p heißt unzerlegbar, wenn gilt: Ist $p = ab$ mit $a, b \in R$, so ist $a \in R^\times$ oder $b \in R^\times$.

(b) p heißt Primelement, wenn gilt: Sind $a, b \in R$ mit $p \mid ab$, so folgt $p \mid a$ oder $p \mid b$.

Beachte: Ist $u \in R^\times$ und $p \in R$ unzerl., so auch up.

" " " Primelement, " " "

unzerlegbare Elemente in $\mathbb{Z} = \{ \pm p \mid p \in \mathbb{N}$ Primzahl$\}$.

Bemerkung 3.3 (a) Ist p Primelement, so ist p unzerlegbar.

denn: Sei $p = ab$. Dann ist $p \mid ab$ also $p \mid a$ oder $p \mid b$.

Sei zuerst $p \mid a$ also $a = pc$ mit $c \in R$. Dann ist

$p = ab = pbc$ also $p(1 - bc) = 0$ wegen $p \neq 0$ und R Integritätsring folgt $1 - bc = 0$, also $bc = 1$, d.h. $b, c \in R^\times$

Ist $p \mid b$, so folgt analog $a \in R^\times$.

(b) Für $R = \mathbb{Z}$ gilt auch die Umkehrung in (a).

Denn sei p unzerlegbar und $p \mid ab$ mit $a, b \in R$.

Annahme: $p \nmid a$. Dann müssen wir zeigen $p \mid b$.

Wende Euklidischen Algorithmus auf a und p an.
$\Rightarrow \exists\, r,s,t \in \mathbb{Z}$ mit $t \neq 0$, $t \mid a$, $t \mid p$ und $t = ra + sp$.
$t \mid p$ bedeutet $p = tc$ mit $c \in \mathbb{Z}$. p unzerl. $\Rightarrow$ $t = \pm 1$ oder $c = \pm 1$
Wäre $c = \pm 1$ so $t = \pm p$, also auch $p \mid a$ ↯.
Also $t = \pm 1$, d.h. $\pm 1 = ra + sp \Rightarrow \pm b = \underbrace{rab + spb}_{\text{ist } \cdot p} \Rightarrow p \mid b$ ✓

Beisp. 3.4 Sei $R = \mathbb{Z}[\sqrt{-5}] = \{n + m\sqrt{-5} \mid n, m \in \mathbb{Z}\} \subseteq \mathbb{C}$
Teilring siehe Übungsblatt 1. Es gilt offenbar:

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Übungsblatt 1: $R^\times = \{\pm 1\}$. **Beh.:** 2, 3, $1 \pm \sqrt{5}$ sind unzerlegbar, aber keine Primelemente.

Bew: Für $z \in \mathbb{C}$ sei $\bar{z} \in \mathbb{C}$ konj. komplexe Zahl.
Setze $N(z) = z\bar{z}$. Für $z = n + m\sqrt{-5}$ folgt:
$N(z) = (n + m\sqrt{-5})(n - m\sqrt{-5}) = n^2 + 5m^2 \in \mathbb{N}$
Wegen $\overline{zz'} = \bar{z} \cdot \bar{z'}$ folgt auch $N(zz') = N(z)N(z')$ für alle $z, z' \in \mathbb{C}$.

Ann.: $2 = ab$ mit $a, b \in R$ mit $a, b \notin R^\times$.
$4 = N(2) = N(a)\,N(b)$ $\quad N(a), N(b) \in \{1, 2, 4\}$.

$N(a) = 1 \Rightarrow n^2 + 5m^2 = 1 \Rightarrow m = 0$, $n = \pm 1$, also $a = \pm 1$
$a = n + m\sqrt{-5}$ $\quad a \in R^\times$ ↯.

Also $N(a) \geq 2$, $N(b) \geq 2$, also $N(a) = N(b) = 2$.
$a = n + m\sqrt{-5}$ $\quad 2 = n^2 + 5m^2$ unmöglich ↯

Also gibt es keine solche Faktorisierung. Also 2 unzerlegbar.

Ann.: 2 Primelement $\Rightarrow 2 \mid 1 + \sqrt{-5}$ oder $2 \mid 1 - \sqrt{-5}$
$\Rightarrow 4 = N(2) \mid N(1 \pm \sqrt{-5}) = 1 + 5 = 6$ ↯.

Also 2 kein Primelement.
Der Beweis ist analog für 3 und $1 \pm \sqrt{-5}$.
Werden sehen, daß "p unzerl. $\Leftrightarrow$ p Primelement" die entscheidende Eigenschaft ist.

Satz 3.5 Seien $n, m \geq 1$, $p_1, \dots, p_n, q_1, \dots, q_m \in R$ Primelemente mit $p_1 \cdots p_n = u\, q_1 \cdots q_m$ wobei $u \in R^\times$. Dann gilt $n = m$, es gibt $u_1, \dots, u_n \in R^\times$ und $q_{\pi(i)} = u_i p_i$ für $1 \leq i \leq n$ wobei $\pi : \{1, \dots, n\} \to \{1, \dots, n\}$ Bijektion (Umordnung der Indizes).

Beweis: Induktion nach $n+m$. Anfang $n+m = 2$, also $n = m = 1$. Dann $p_1 = u q_1$ also Beh. klar ✓. Sei nun $n+m > 2$.

$p_1 \mid p_1 \cdots p_n = u q_1 \cdots q_m$ also auch $p_1 \mid q_1 \cdots q_m$ (weil $u \in R^\times$).

Beh.: ex. $i_1 \in \{1, \dots, m\}$ mit $p_1 \mid q_{i_1}$.

denn: $p_1 \mid q_1 (q_2 \cdots q_m)$ und p_1 Prim $\Rightarrow$ $p_1 \mid q_1$ oder $p_1 \mid q_2 \cdots q_m$

Ist $p_1 \mid q_1$ so $i_1 = 1$ fertig. Ist $p_1 \nmid q_1$ so $p_1 \mid q_2 (q_3 \cdots q_m)$ wiederhole Argument, entweder $p_1 \mid q_2$ dann $i_1 = 2$ fertig oder $p_1 \mid q_3 \cdots q_m$ usw. Irgendwann ex. $i_1 \in \{1, \dots, m\}$ mit $p_1 \mid q_{i_1}$.

q_{i_1} Prim $\Rightarrow$ q_{i_1} unzerl. $\Rightarrow$ $q_{i_1} = u_1 p_1$ mit $u_1 \in R^\times$

Damit
$$p_1 \cdots p_n = u\, q_1 \cdots q_{i_1 - 1}\, u_1 p_1\, q_{i_1 + 1} \cdots q_m$$
$$= (u u_1)\, q_1 \cdots q_{i_1 - 1}\, p_1\, q_{i_1 + 1} \cdots q_m$$

R Integritätsbereich $\Rightarrow$ können p_1 auf beiden Seiten kürzen

also $p_2 \cdots p_n = (u u_1)\, q_1 \cdots q_{i_1 - 1}\, q_{i_1 + 1} \cdots q_m$.

Induktion $\Rightarrow$ $n - 1 = m - 1$ also $n = m$, und es gibt $u_2, \dots, u_n \in R^\times$ mit $q_{\pi(i)} = u_i p_i$ für $2 \leq i \leq n$, wobei

$\pi : \{1, \dots, i_1 - 1, i_1 + 1, \dots, n\} \to \{1, \dots, n\}$ Bijektion.

Setze $\pi(i_1) = 1$. Dann π gewünschte Bijektion. □

Def 3.6 R heißt faktorieller Ring wenn die beiden folgenden Aussagen erfüllt sind.

(a) Sei $0 \neq a \in R$ keine Einheit. Dann gibt es unzerlegbare Elemente $p_1, \dots, p_n \in R$ mit $a = p_1 \cdots p_n$.

(b) Jedes unzerlegbare Element in R ist auch ein Primelement.

Nach Satz 3.5 ist dann jede solche Darstellung $a = p_1 \cdots p_n$ bis auf die Reihenfolge der Faktoren und Multiplikation mit Einheiten eindeutig bestimmt.

Faktorielle Ringe sind also genau die ~~xxx~~ Ringe, in denen sinngemäß so etwas wie der Hauptsatz der elementaren Arithmetik gilt. Wollen nun Kriterien finden, um zu zeigen, daß R faktoriell ist.

Def. 3.7 R heißt Hauptidealring, wenn jedes Ideal von R ein Hauptideal ist, also von der Form $(a) = Ra$ mit $a \in R$ (siehe Def. 2.7).

Lemma 3.8 Sei R ein Hauptidealring. Dann gelt:

(a) Jede aufsteigende Folge von Idealen $I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$ in R wird stationär, d.h. es gibt ein $n_0 \geq 1$ mit

$$I_{n_0} = I_{n_0+1} = I_{n_0+2} = \ldots$$

(b) Sei $0 \neq a \in R$ keine Einheit. Dann läßt sich a als Produkt von endlich vielen irred. Elementen schreiben, d.h. Bedingung (a) in Def. 3.6 gelt.

Beweis: (a) Setze $I := \bigcup_{n \geq 1} I_n \subseteq R$. Beh.: I ist ein Ideal. Seien $a, b \in I \Rightarrow$ ex. $n, m \geq 1$ mit $a \in I_n$, $b \in I_m$.

Sei $n_0 = \max\{n, m\} \Rightarrow a, b \in I_{n_0}$.

also $a \pm b \in I_{n_0} \subseteq I$ und $ca \in I_{n_0}$ für $c \in R$ $\subseteq I$. bel.

R Hauptidealring also $I = (d)$ mit $d \in R$.

ex. $n_0 \geq 1$ mit $d \in I_{n_0}$. $\Rightarrow$ $I = (d) \subseteq I_n \subseteq I$ (↑ sowieso klar.)

also $I = I_{n_0}$.

Für $n \geq n_0$ ist dann auch $I = I_{n_0} \subseteq I_n \subseteq I$, also

$$I_{n_0} = I = I_n \quad \checkmark$$

(b) Sei $X := \{ a \in R \mid a \neq 0,\ a \notin R^\times$ und a lässt sich nicht schreiben als Produkt von endl. vielen irred. Elementen $\}$.

Wollen zeigen: $X = \emptyset$. Dann: $X \neq \emptyset$ sei $a \in X$.

Dann ist a selbst nicht irreduzibel, also $a = a_1 b_1$ mit $0 \neq a_1, b_1 \in R \setminus R^\times$. Wäre $a_1 \notin X$ und $b_1 \notin X$, so kann man jeweils a_1, b_1 als Produkte von endl. vielen irred. Elementen schreiben, also auch $a = a_1 b_1$ $\lightning$. Also ist $a_1 \in X$ oder $b_1 \in X$. Wählen Bezeichnung so dass $a_1 \in X$. Beh.

$$(a) \subsetneq (a_1).$$

denn: $a = a_1 b_1$, also $(a) \subseteq (a_1)$. Wäre $(a) = (a_1)$, so auch $a_1 \in (a)$, d.h. $a_1 = ac$ mit $c \in R$. Aber dann

$$a = a_1 b_1 = acb_1 \quad \text{also} \quad cb_1 = 1 \quad \text{also} \quad b_1 \in R^\times \lightning.$$

Wiederhole Argument mit a_1. Also $a_1 = a_2 b_2$ mit $a_2, b_2 \in R \setminus R^\times$ und Bezeichnung so, dass $a_2 \in X$. Wie oben

$$(a_1) \subsetneq (a_2).$$

Falte so fort und erhalte unendl. Folge von Idealen

$$(a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \ldots \quad \lightning \text{ zu } (a). \qquad \square$$

Lemma 3.9 Sei R ein Hauptidealring. Ist $p \in R$ irreduzibel, so ist $R/(p)$ ein Körper (d.h. (p) max. Ideal, siehe Satz 2.9).

Beweis: Sei $I \subseteq R$ ein Ideal mit $(p) \subseteq I$. Müssen zeigen: $I = (p)$ oder $I = R$. Dann: $(p) \subsetneq I$ müssen also $I = R$ zeigen.

R Hauptidealring also $I = (a)$ mit $a \in R$

$(p) \subseteq I = (a)$ also $p = ac$ mit $c \in R$.

p irreduzibel $\Rightarrow$ $a \in R^\times$ oder $c \in R^\times$. Wäre $a \in R^\times$, so $I = (a) = R$ fertig. Sei also $a \notin R^\times$. Dann $c \in R^\times$.

über dann $(p) = (pc) = (a)$ ↯. □

Satz 3.10 Ist R ein Hauptidealring, so ist R faktoriell

Beweis: Bedingung (a) in Def. 3.6 gilt nach Lemma 3.8(b).

Bedingung (b). Sei also $p \in R$ unzerlegbar. Heißen zeigen:
p Primelement. Sei also $p \mid ab$ mit $a, b \in R$, d.h.

$ab = pc$ mit $c \in R$ Rechne in $R/(p) = \{\underbrace{x + (p)}_{=[x]} \mid x \in R\}$ Äquivalenzklassen
$\in (p)$

$ab = pc \Rightarrow$ ~~$ab + (p) = pc + (p) \in R/(p)$~~

$\Downarrow$ ~~$(a+(p))(b+(p)) \in (p) = 0$~~

$[a] \cdot [b] = [ab] = [pc] = [0]$ (denn $pc - 0 = pc \in (p)$).

Lemma 3.9 $\Rightarrow$ $R/(p)$ Körper also $[a] = [0]$ oder $[b] = [0]$

$\Updownarrow$ $\Updownarrow$

$a \in (p)$ $b \in (p)$

$\Downarrow$ $\Downarrow$

$p \mid a$ $p \mid b$ □.

Schließlich benötigen wir auch noch ein Kriterium, um zu zeigen, daß R ein Hauptidealring ist.

Def. 3.11 R heißt Euklidischer Ring, wenn es eine Funktion $\delta : R \setminus \{0\} \to \mathbb{N}_0$ gibt mit folgender Eigenschaft.
Sind $a, b \in R$ mit $b \neq 0$, so gibt es $q, r \in R$ mit

$a = bq + r$ und $r = 0$ oder $\delta(r) < \delta(b)$.

Standardbeispiel: $R = \mathbb{Z}$ Setze $\delta(n) = |n|$ Absolutbetrag.

Seien $a, b \in \mathbb{Z}$, $b \neq 0$. Ist $b > 0$, so teile mit Rest

$a = bq + r$, $q, r \in \mathbb{Z}$, $0 \leq r < b$.

d.h. $r = 0$ oder $\delta(r) = r < b = \delta(b)$ ✓

Ist $b < 0$ so teile $-a$ mit Rest durch $-b$:

$-a = -bq + r'$ $q, r' \in \mathbb{Z}$, $0 \leq r' < -b$. $\Rightarrow b < -r' \leq 0$.

$\Rightarrow a = bq - r'$ mit $r' = 0$ oder $\delta(-r') = r' < -b = \delta(b)$ ✓

Lemma 3.12 R Eukl. Ring $\Rightarrow$ R Hauptidealring

Beweis: Sei $I \trianglelefteq R$ Ideal. Ist $I = \{0\}$, so $I = (0)$ v.

Sei nun $I \neq \{0\}$ und $n := \min\{\delta(r) \mid 0 \neq r \in I\}$.

Sei $0 \neq d \in I$ mit $\delta(d) = n$. Dann $(d) \subseteq I$. Beh. $I = (d)$

Sei $a \in I$ bel. $\Rightarrow$ $a = qd + r$ mit $q, r \in R$, $r = 0$ oder $\delta(r) < \delta(d)$.

$r = \underbrace{a}_{\in I} - q\underbrace{d}_{\in I} \in I$ Wäre $r \neq 0$, so

$r \in I$ und $\delta(r) < \delta(d) = n$ ↯ zur Wahl von d. □

Also $r = 0$, d.h. $a = qd \in (d)$

Bemerkung 3.13 (a) In Eukl. Ringen gibt der Euklidische Algorithmus genauso wie in §2, d.h. zu $a, b \in R$, $a \neq 0, b \neq 0$ gibt es $r, s, t \in R$ mit $t \neq 0$, $t \mid a$, $t \mid b$)

und $t = ra + sb$.

(b) $R = \mathbb{Z}$ Eukl. Ring also faktoriell. Damit haben wir auch Hauptsatz der elementaren Arithmetik noch einmal bewiesen. Übrigens ist $\mathbb{Z}$ Hauptidealring: Ideale sind von der Form (d) mit $d \in \mathbb{N}_0$.

(c) Hierarchie von Ringen:

R Euklidischer Ring $\Rightarrow$ R Hauptidealring $\Rightarrow$ R faktoriell

A_{-19} (ohne Beweis). $\mathbb{Z}[X]$, siehe §4

$\Downarrow$

R Integritätsring

$\mathbb{Z}[\sqrt{-5}]$

Beisp. 3.14 Sei $R = A_{-1} = \{n + mi \mid n, m \in \mathbb{Z}\} \subseteq \mathbb{C}$ Gauß'sche Zahlen.

Setze $\delta(n + mi) := n^2 + m^2$. Dann ist R Eukl. Ring

→ Übung mit Hinweis. Also kann man auch [illegible] entscheiden. z.B. $p \in \mathbb{N}$ Primzahl

[illegible] in R $\Leftrightarrow$ $p = a^2 + b^2$ mit $a, b \in \mathbb{Z}$.

Polynomringe

Def. 3.15 Sei R faktoriell. Sei $0 \neq a \in R$.

Ist $a \in R^\times$ so setze $\ell(a) = 0$.

Ist $a \notin R^\times$ so schreibe $a = p_1 \cdots p_r$ mit $p_i \in R$ irred. und setze $\ell(a) = r$.

Dies ist wohldefiniert nach Satz 3.5 (Def. 3.6.) $\ell(a)$ heißt Länge von a.

Bemerke: Satz 3.5 zeigt auch sofort.

$$\ell(ab) = \ell(a) + \ell(b) \quad \text{für } a, b \in R,\ a \neq 0,\ b \neq 0$$

$$\ell(a) = 0 \iff a \in R^\times.$$

Dies wird nützlich in Induktionsbeweisen sein.

§4 Polynomringe

R kommutativer Ring mit 1. $\rightsquigarrow R[X]$ Polynomring in Unbestimmter X und Koeffizienten in R.

Elemente von $R[X]$: $f = a_0 + a_1 X + \ldots + a_n X^n$ mit $n \geq 0$, $a_i \in R$

Ist $a_n \neq 0$, so heißt $n = \operatorname{Grad}(f)$.

$R[X]$ ist kommutativer Ring mit 1, $R \leq R[X]$ (konstante Polynome) $a \mapsto a X^0$

Konvention: $\operatorname{Grad}(0) = -\infty$.

Addition: komponentenweise, Multiplikation: $X^i \cdot X^j = X^{i+j}$ + distributiv fortsetzen

$$g = b_0 + b_1 X + \ldots + b_m X^m$$

$$f \cdot g = c_0 + c_1 X + \ldots + c_{n+m} X^{n+m}$$

mit $c_k = a_0 b_k + a_1 b_{k-1} + \ldots + a_k b_0$. , $c_0 = a_0 b_0$, $c_{n+m} = a_n b_m$

Bem. 4.1 $\operatorname{Grad}(f \cdot g) \leq \operatorname{Grad}(f) + \operatorname{Grad}(g)$. Ist $n = \operatorname{Grad}(f) \geq 0$ und $m = \operatorname{Grad}(g) \geq 0$ wie oben und $a_n b_m \neq 0$, so

$$\operatorname{Grad}(f \cdot g) = \operatorname{Grad}(f) + \operatorname{Grad}(g).$$

Insbesondere: R Integritätsring $\Rightarrow R[X]$ Integritätsring

und $R[X]^\times = R^\times$ [$f \in R[X]^\times$, d.h. ex. $g \in R[X]$ mit $1 = f \cdot g \Rightarrow \operatorname{Grad}(f) = \operatorname{Grad}(g) = 0$ und dann $f, g \in R^\times$]

Erinnerung. Konstruktion von $R[X]$

Sei $\mathcal{F} := \{(a_n)_{n\geq 0} \mid a_n \in R \ \forall n \in \mathbb{N}_0 \text{ und } |\{i \in \mathbb{N}_0 \mid a_i \neq 0\}| < \infty\}$.

also alle Folgen $(a_0, a_1, \dots, a_n, \underbrace{0, \dots}_{\text{ab einer bestimmten Stelle}})$.

$(a_n)_{n\geq 0} + (b_n)_{n\geq 0} = (a_n + b_n)_{n\geq 0}$ ✓

$(a_n)_{n\geq 0} \cdot (b_n)_{n\geq 0} = (c_n)_{n\geq 0}$ mit $c_n = a_0 b_n + \dots + a_n b_0$.

Setze $X := (0,1,0,\dots) \in \mathcal{F}$. Dann $X^2 = (0,0,1,0,\dots)$

$X^3 = (0,0,0,1,0,\dots)$

$X^0 = (1,0,\dots,0)$.

also läßt sich jedes $f \in \mathcal{F}$ eindeutig schreiben als

$f = a_0 X^0 + a_1 X^1 + \dots + a_n X^n$.

Einbettung $R \hookrightarrow \mathcal{F}$, $a \mapsto (a,0,0,\dots)$ ✓.

Bem. 4.2 Sei $0 \neq g \in R[X]$, $g = b_0 + b_1 X + \dots + b_m X^m$

ist $b_m = 1$, so heißt g normiert. Sei nun auch $f \in R[X]$. ist g normiert, so kann man f durch g mit Rest dividieren, d.h. es gibt $q, r \in R[X]$ mit

$f = q \cdot g + r$ wobei $r = 0$ oder $r \neq 0$ und $\operatorname{grad}(r) < \operatorname{grad}(g)$

Beisp: $f = X^4 + 2X^2 - 4 \in \mathbb{Z}[X]$ $\quad g = X^3 + X^2 - 4X - 4 \in \mathbb{Z}[X]$

$$\begin{array}{r} X^4 + 2X^2 - 4 \\ \underline{X^4 + X^3 - 4X^2 - 4X} \\ -X^3 + 6X^2 + 4X - 4 \\ \underline{-X^3 - X^2 + 4X + 4} \\ 7X^2 - 8 \end{array} \quad = (X^3 + X^2 - 4X - 4)\underbrace{(X - 1)}_{=q} + \underbrace{7X^2 - 8}_{=r}.$$

Satz 4.3 Sei $R = K$ ein Körper. Dann ist $K[X]$ ein euklidischer Ring, wobei $\delta : K[X] \setminus \{0\} \to \mathbb{N}_0$ gegeben ist durch $\delta(f) = \operatorname{grad}(f)$ für $0 \neq f \in K[X]$

Beweis: Sei $f, g \in K[X]$, $g \neq 0$. Schreibe $g = c g_1$ mit $g_1 \in K[X]$ normiert und $0 \neq c \in K$ (klammere mögliche höchste Koeffizienten in g aus). Nach Bem. 4.2 gibt es $r, g_1 \in K[X]$ mit $f = g_1 \cdot g_1 + r$ wobei $r = 0$ oder $r \neq 0$ und $\operatorname{Grad}(r) < \operatorname{Grad}(g_1) = \operatorname{Grad}(g)$

$$\Rightarrow \quad f = \underbrace{(c^{-1} g_1)}_{=q} \underbrace{c \cdot g_1}_{=g} + r. \qquad \text{gewünschte Darstellung.} \quad \square$$

Insbesondere ist also $K[X]$ Hauptidealring und auch faktoriell.
$\rightsquigarrow$ Im Prinzip kann man in $K[X]$ (K Körper) genauso gute arbeiten und rechnen wie in $\mathbb{Z}$.

Frage: Was können wir über $R[X]$ sagen, wobei R kommutativer Ring mit 1, aber kein Körper?

Beisp. 4.4 $\mathbb{Z}[X]$ ist kein Hauptidealring und damit auch kein Euklidischer Ring. Dazu:

Sei $I := \{ 2 \cdot u + m X \mid u, m \in \mathbb{Z}[X] \} \subseteq \mathbb{Z}[X]$

Man sieht sofort: $I \neq \mathbb{Z}[X]$ $\quad$ denn $1 \notin I$, $I \neq 0$.

Annahme: I Hauptideal, d.h. es gibt $f \in \mathbb{Z}[X]$ mit $I = (f)$

$\Rightarrow \quad 2 \in (f)$, also $f \mid 2$, $2 = fg$ mit $g \in \mathbb{Z}[X]$

$\Rightarrow \operatorname{Grad}(f) = 0$, also $f \in \mathbb{Z}$ also $f = \pm 1$ oder $f = \pm 2$.
$\operatorname{Grad}(g) = 0$ $\quad g \in \mathbb{Z}$

Aber auch $X \in (f)$, d.h. $f \mid X$, also $X = fh$ mit $h \in \mathbb{Z}[X]$

$\Rightarrow \quad f = \pm 1$ also $1 = \underbrace{2u}_{\text{gerade}} + \underbrace{mX}_{\operatorname{Grad}() \geq 1}$ mit $u, m \in \mathbb{Z}[X]$

konstanter Term gerade. $\quad \lightning \quad \square$

Unser Ziel ist es zu zeigen:

Satz 4.5 (Gauß) Ist R ein faktorieller Ring, so auch $R[X]$.
Insbesondere: $\mathbb{Z}[X]$ faktorieller Ring.

1. Schritt:

Lemma 4.6 Sei R faktoriell und $0 \neq f \in R[X]$. Dann ist entweder $f \in R^\times$ oder f läßt sich schreiben als $f = f_1 \cdots f_r$ mit $f_i \in R[X]$ irreduzibel

Beweis: Sei $f = a_0 + a_1 X + \cdots + a_n X^n$ mit $a_n \neq 0$, also $\mathrm{Grad}(f) = n$

Dann setze $L(f) := \mathrm{Grad}(f) + \ell(a_n)$, wobei $\ell(a_n)$ in [illegible]. Def. 3.15. Ist auch $0 \neq g \in R[X]$, so gilt $\mathrm{Grad}(fg) = \mathrm{Grad}(f) + \mathrm{Grad}(g)$

Weil $\ell()$ multiplikativ ist, folgt sofort:

(1) $L(f) = 0 \Rightarrow f \in R^\times$

(2) $L(gh) = L(g) + L(h)$ für alle $g, h \in R[X]$, $g \neq 0$, $h \neq 0$

Zeige Induktion nach $L(f)$. Ist $L(f) = 0$, so $f \in R^\times$ nach (1) ✓.

Sei nun $L(f) > 0$. Ist f irred., so sind wir fertig.

Sei also f nicht irred. d.h. $f = gh$ mit $0 \neq g, h \in R[X]$. nicht in $R^\times$.

also $L(g) > 0$, $L(h) > 0$ nach (1).

Wegen (2) folgt dann $L(g) < L(f)$, $L(h) < L(f)$.

Also sind g, h Produkte von irred. Elementen, also auch f. □

2. Schritt: Beziehung zwischen Primelementen in R und in $R[X]$

Lemma 4.7 Sei R [illegible] Integritätsbereich und $p \in R$ Primelement. Dann ist p auch ein Primelement in $R[X]$

Beweis: Seien $f, g \in R[X]$ mit $p \mid fg$. Müssen zeigen: $p \mid f$ oder $p \mid g$. Können $f, g \neq 0$ annehmen. Annahme: $p \nmid f$ und $p \nmid g$

Schreibe $f = a_0 + a_1 X + \cdots + a_n X^n$ $\quad g = b_0 + b_1 X + \cdots + b_m X^m$

mit $n, m \geq 0$, $a_n \neq 0$, $b_m \neq 0$.

$p \nmid f \Rightarrow$ ex. $r \geq 0$ mit $p \mid a_0, p \mid a_1, \ldots, p \mid a_{r-1}, p \nmid a_r$.

$p \nmid g \Rightarrow$ ex. $s \geq 0$ mit $p \mid b_0, p \mid b_1, \ldots, p \mid b_{s-1}, p \nmid b_s$.

$fg = c_0 + c_1 X + \cdots + c_{n+m} X^{n+m}$ Betrachte Koeff. c_{r+s}:

$$p \mid c_{r+s} = \underbrace{a_0 b_{r+s} + \cdots + a_{r-1} b_{s+1}}_{p \mid} + a_r b_s + \underbrace{a_{r+1} b_{s-1} + \cdots + a_{r+s} b_0}_{p \mid} \Rightarrow p \mid a_r b_s.$$

p Primelement $\Rightarrow$ $p \mid ar$ oder $p \mid b$ s. ü.

Lemma 4.8 (Gauß) Sei R faktoriell, $0 \neq a \in R[X]$ irred. mit $\operatorname{Grad}(a) \geq 1$. Ist $a \mid bc$ in $R[X]$, mit $0 \neq b \in R$ und $c \in R[X]$, so folgt $a \mid c$ in $R[X]$

Beweis: Induktion nach $\ell(b)$. Ist $\ell(b) = 0$, so $b \in R^\times$ ✓.

Sei nun $\ell(b) > 0$ und $0 \neq p \in R$ irred. mit $p \mid b$; dann $b = pb'$ mit $0 \neq b' \in R$ und $\ell(b') = \ell(b) - 1$.

$bc = ad$ mit $d \in R[X]$ nach Vor.; also $p \mid ad$ in $R[X]$

R faktoriell $\Rightarrow$ p Primelement in $R \overset{4.7}{\Rightarrow}$ p Primelement in $R[X]$

also $p \mid a$ oder $p \mid d$. über a irred. und $\operatorname{Grad}(a) \geq 1$

$\Rightarrow p \mid d$, d.h. $d = pd'$ mit $0 \neq d' \in R$

$b'pc = bc = ad = apd' \Rightarrow$ kürzen p kürzen

also $b'c = ad'$, d.h. $a \mid b'c$

Mit Induktion folgt $a \mid c$ □

Bem. 4.9 Sei R Integritätsbereich. Genauso wie wir $\mathbb{Q}$ aus $\mathbb{Z}$ konstruiert haben, siehe Beisp. 2.1, können wir auch einen Körper K konstruieren mit $R \subseteq K$ und

$$K = \{ ab^{-1} \mid a, b \in R,\ b \neq 0 \}$$

"Quotientenkörper von R".

Also: def. $\sim$ auf $R \times (R \setminus \{0\})$ durch

$$(a,b) \sim (c,d) \overset{\text{def.}}{\Leftrightarrow} ad = bc. \qquad b \neq 0$$

Sei a/b Äquivalenzklasse von (a,b) und $K = \{ a/b \mid a, b \in R \}$.

Def. Addition + Mult. wie in Beisp. 2.1.

$R \hookrightarrow K$, $a \mapsto a/1$ identifiere a mit $a/1$.

also dann $a/b = ab^{-1}$ mit $a, b \in R$, $b \neq 0$.

können dies z.B. auch auf $R[X]$ anwenden.

$\rightsquigarrow R(X) = \{ f/g \mid f, g \in R[X],\ g \neq 0 \}$. und man kann wieder mit solchen Brüchen rechnen.

Lemma 4.10 Sei R faktorieller Ring mit Quotientenkörper K.
Sei $0 \neq f \in R[X]$ mit $\mathrm{Grad}(f) \geq 1$. Ist f irred. in $R[X]$, so ist f auch als Polynom in $K[X]$ irred.

Beweis: Sei $f = gh$ mit $g, h \in K[X]$ wobei $\mathrm{Grad}(g) \geq 1$ sei:
Dann müssen wir zeigen, daß $0 \neq h \in K$ konstantes Polynom.
Sei dann $0 \neq d \in R$ so, daß d ein Vielfaches aller Nenner in den Koeff. von g und h sind, also $\tilde{g} := dg \in R[X]$, $\tilde{h} := dh \in R[X]$
$\Rightarrow \mathrm{Grad}(\tilde{g}) = \mathrm{Grad}(g)$ und $\mathrm{Grad}(\tilde{h}) = \mathrm{Grad}(h)$. und

$$d^2 f = \tilde{g}\tilde{h} \quad \text{Identität in } R[X]$$

$\mathrm{Grad}(\tilde{g}) \geq 1 \rightarrow \tilde{g} \notin R^\times = R[X]^\times$ also nach Lemma 4.6:

$$\tilde{g} = g_1 \cdots g_r \quad \text{mit } g_i \in R[X] \text{ irred.}$$

Wegen $\mathrm{Grad}(\tilde{g}) \geq 1$ können wir Bezeichnungen so wählen, daß $\mathrm{Grad}(g_1) \geq 1$. $\Rightarrow$ $g_1 \mid d^2 f$ also $g_1 \mid f$ nach Lemma 4.8
f irred. und g_1 kein Einheit $\Rightarrow$ $f = g_1 u$ mit $u \in R^\times$
$\Rightarrow$ $d^2 g_1 u = g_1 \cdots g_r \tilde{h}$ $\Rightarrow$ $\underbrace{d^2 u}_{\mathrm{Grad}=0} = g_2 \cdots g_r \tilde{h}$ $\Rightarrow$ $\mathrm{Grad}(\tilde{h}) = 0$.
$h = d^{-1}\tilde{h} \in K$. □

z.B.: $\underbrace{24X^3 + 4X^2 - 6X - 1}_{\in \mathbb{Z}[X]} = \underbrace{(4X + \frac{2}{3})(6X^2 - \frac{3}{2})}_{\text{Faktorisierung in } \mathbb{Q}[X]}$

$= (2X + \frac{1}{3})(12X^2 - 3) = (6X + 1)(4X^2 - 1)$

Es muß also nach obigem Lemma auch eine Faktorisierung in $\mathbb{Z}[X]$ geben ▽

Beweis des Satzes von Gauß: Bedingung (a) in Def. 3.6 gilt nach Lemma 4.6. Nun zu Bedingung (b). Sei also $0 \neq f \in R[X]$ unzerlegbar. Müssen zeigen, daß f ein Primelement ist.
Ist $\mathrm{Grad}(f) = 0$, so gilt dies nach Lemma 4.7. [Beachte: f irred. in $R[X] \Rightarrow f$ irred. in $R \Rightarrow f$ Primelement in R] ($R^\times = R[X]^\times$)
Sei also jetzt $\mathrm{Grad}(f) \geq 1$ und $g, h \in R[X]$ mit $f \mid gh$. Dann gilt auch $f \mid gh$ in $K[X]$. Nach Lemma 4.10 ist f irred.

ist $K[X]$, K Euklid. $\Rightarrow$ $K[X]$ faktoriell $\Rightarrow$ $f \mid g$ oder $f \mid h$

Sei $f \mid g$ in $K[X]$ also $g = af$ mit $a \in K[X]$ in $'K[X]$

Wähle Vielfaches $0 \neq d \in R$ der Nenner in a $\Rightarrow$ $\tilde{a} := da \in R[X]$

also $dg = \tilde{a} f$ Gradidität in $R[X]$. Lemma 4.8 $\Rightarrow$ $f \mid g$ in $R[X]$

Argument für $f \mid h$ in $K[X]$ analog. $\square$

Beisp. 4.11 Sei R Integritätsbereich. Dann def. Polynomring in n Unbestimmten $X_1, \dots, X_n$ rekursiv durch:

$$R[X_1, X_2] := (R[X_1])[X_2], \dots, \quad R[X_1, \dots, X_n] := (R[X_1, \dots, X_{n-1}])[X_n]$$

Mit Induktion nach n folgt dann sofort: $R[X_1, \dots, X_n]$ Integritätsbereich. Außerdem: R faktoriell $\Rightarrow$ $R[X_1, \dots, X_n]$ faktoriell

z.B. sind $\mathbb{Z}[X_1, \dots, X_n]$ und $\mathbb{C}[X_1, \dots, X_n]$ faktorielle Ring.

Satz 4.12 (Eisenstein-Kriterium) Sei R faktoriell und $0 \neq f \in R[X]$ mit $\text{Grad}(f) \geq 1$, $f = a_0 + a_1 X + \dots + a_n X^n$, $a_i \in R$, $n \geq 1$, $a_n = 1$ (f normiert).

Es gebe ein Primelement $p \in R$ mit

$p \mid a_0, \dots, a_{n-1}$ aber $p \nmid a_n$ und $p^2 \nmid a_0$.

Dann ist f irred. in $K[X]$, K Quotientenkörper von R

Beweis: Dann: $f \in K[X]$ nicht irred. Lemma 4.10 $\Rightarrow$ $f \in R[X]$ nicht irred., also $f = gh$ mit $g, h \in R[X]$, $g, h \notin R^\times$.

Schreibe

$$g = b_0 + \dots + b_r X^r \qquad b_r \neq 0, \ r \geq 0 \qquad r + s = n.$$
$$h = c_0 + \dots + c_s X^s \qquad c_s \neq 0, \ s \geq 0 \qquad b_r c_s = 1$$

$a_0 = b_0 c_0$ $\quad p \mid a_0 \Rightarrow p \mid b_0$ oder $p \mid c_0$. Wähle Bezeichnungen so, daß $p \mid b_0$. Sei $k \geq 1$ so daß

$p \mid b_0, p \mid b_1, \dots, p \mid b_{k-1}$ aber $p \nmid b_k$. $\neq 1$

Beachte: wäre $p \mid b_i$ für alle $0 \leq i \leq r$, so auch $p \mid a_n = b_r c_s$ $\lightning$

$\Rightarrow \quad a_k = \underbrace{b_0 c_k + b_1 c_{k-1} + \dots + b_{k-1} c_1}_{p \mid} + b_k c_0$

Wäre $k < n$, so $p \mid a_k$ also auch $p \mid b_k c_0$. Wegen $p \nmid b_k$ folgt $p \mid c_0$, aber dann $p^2 \mid b_0 c_0 = a_0$ ↯. Also ist $k = n$ d.h. $\mathrm{Grad}(g) = n$ und $\mathrm{Grad}(h) = 0$, $0 \neq h \in R$

also $f = hg$, $h \in R$ sogar $h \in R^\times$ Also $f \in R[X]$ erf. □.
$\Rightarrow f \in K[X]$ erf.

Beisp: $f = X^{17} - 2X^3 + 6 \in \mathbb{Z}[X]$ Wähle $p = 2$

alle Vor. von Eisenstein erfüllt also $f \in \mathbb{Q}[X]$ irreduzibel.

Sehr einfaches, schlagkräftiges Kriterium!

Im Allgemeinen ist Test auf Irreduzibilität ein schwieriges Problem

Weiteres wichtiges Hilfsmittel.

Satz 4.13 (Universelle Eigenschaft von Polynomringen)

Seien R, S kommutative Ringe mit 1 und $\varphi: R \to S$ ein Ringhomomorphismus. Sei $s \in S$ fest. Dann gibt es genau einen Ringhomom. $\varphi_s: R[X] \to S$ mit $\varphi_s(X) = s$.

Für $f = a_0 + a_1 X + \dots + a_n X^n \in R[X]$ bel. gilt

$$\varphi_s(f) = \varphi(a_0) + \varphi(a_1) s + \dots + \varphi(a_n) s^n \in S.$$

φ_s heißt "Einsetzungshomomorphismus".

Beweis: Definiere φ_s durch obige Formel. Man rechnet sofort nach, dass φ_s Ringhomom. ist. Eindeutigkeit klar, weil Bild von X festgeschrieben ist und φ_s Ringhomom. ⇒ φ_s für alle $f \in R[X]$ festgelegt.

Beisp. 4.14 (a) Wichtigster Spezialfall sei K Körper und $R \subseteq K$ Teilring, z.B. $R = \mathbb{Z} \subseteq K = \mathbb{Q}$. Dann $R \subseteq K$ Ringhomom. ist also $z \in K$ fest, so erhalten wir

$\varphi_z: R[X] \to K$, $f = a_0 + a_1 X + \dots + a_n X^n \longmapsto a_0 + a_1 z + \dots + a_n z^n =: f(z)$

"z wurde für X eingesetzt"!

z heißt Nullstelle von f wenn $f(z)=0$ gilt

(b) Um Irred. von $f \in \mathbb{R}[X]$ zu testen, verwende geschickt $\varphi: R \to S$ so daß man vielleicht einfacher Irreduzibilität von $\varphi_*(f) \in S$ testen kann $\rightsquigarrow$ (1) Reduktions-Kriterium

Bem. 4.15 Sei K Körper und $0 \neq f \in K[X]$.

(a) Ist $z \in K$ Nullstelle von f, so gilt $f = (X-z)g$ mit $0 \neq g \in K[X]$ und $\mathrm{Grad}(g) = \mathrm{Grad}(f) - 1$

(b) Ist $\mathrm{Grad}(f) = n \geq 1$, so hat f höchstens n Nullstellen.

Beweis: (a) Teile mit Rest: $f = (X-z)g + r$ mit $g, r \in K[X]$ und $r = 0$ oder $\mathrm{Grad}(r) < \mathrm{Grad}(X-z) = 1$, d.h. $r \in K$

Setze z ein: Satz 4.13 $\rightarrow$ $0 = f(z) = g(z)(z-z) + r(z) = r$ ✓.

(b) Induktion nach n, $n=1$ $f = aX+b$, $a \neq 0$, $b \in K$

$\Rightarrow$ genau eine Nullstelle.

$n > 1$: Sei $z_1 \in K$ Nullstelle $\overset{a)}{\Rightarrow}$ $f = (X-z_1)g$.

Nach Induktion hat g höchstens $n-1$ Nullstellen.

Dann: f hat noch eine weitere Nullstelle $z' \in K$ mit $g(z) \neq 0$.

$\rightarrow$ $0 = f(z) = (z-z_1)\underbrace{g(z)}_{\neq 0} \Rightarrow z = z_1$.

Also hat f nur höchstens n Nullstellen. □

Bemerkung: Aussage i.A. falsch über Ringen. z.B. $R = \mathbb{Z}/8\mathbb{Z}$

$f = X^2 - \bar{1} \in R[X]$ hat Nullstellen $\bar{1}, \bar{3}, \bar{5}$ und $\bar{7}$ in R ▽

Beisp. 4.16 Sei $n \geq 1$ und $f = X^n - 1 \in \mathbb{Z}[X]$.

Wie zerfällt f in irred. Polynome ?

$n=1$ $f = X-1$ ✓

$n=2$ $f = X^2-1 = (X-1)(X+1)$

$n=3$ $f = X^3-1 = (X-1)(X^2+X+1)$

$n=4$ $f = X^4-1 = (X^2-1)(X^2+1) = (X-1)(X+1)(X^2+1)$

$X^2+X+1 \in \mathbb{Z}[X]$ irred. (keine Nullstelle in $\mathbb{Q}$). $-\frac{1}{2} \pm \sqrt{-3}/2$

$X^2+1 \in \mathbb{Z}[X]$ irred. (keine Nullstelle in $\mathbb{Q}$) $(\pm i)$

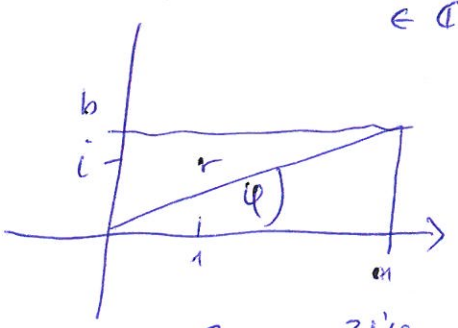
Idee: Setze $E_n := \{z \in \mathbb{C} \mid z \text{ Nullstelle von } f\}$.
$= \{z \in \mathbb{C} \mid z^n = 1\}$. Dies ist eine Untergruppe von $\mathbb{C}^\times$.

$(z, z' \in E_n \Rightarrow (zz')^n = z^n z'^n = 1,\ (z^{-1})^n = (z^n)^{-1} = 1$ /

Was können wir über diese Untergruppe sagen?

Nach Bem. 4.15: $|E_n| \le n$. Aber über $\mathbb{C}$ können wir sogar n Nullstellen finden, nämlich:

Erinnerung: $z = a + bi = re^{i\varphi} = r\cos(\varphi) + i\, r\sin(\varphi)$
$\in \mathbb{C}$



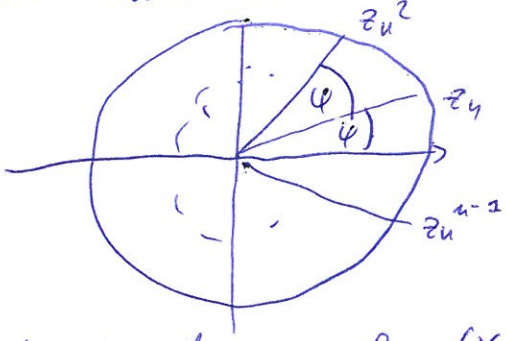
Setze $r = 1$, $\varphi = \frac{2\pi}{n}$

$z_n = e^{\frac{2\pi i}{n}} \in \mathbb{C}$.

Dann $z_n^2 = (e^{i\varphi})^2 = e^{2i\varphi} = e^{2\cdot\frac{2\pi i}{n}}$

$z_n^3 = e^{3i\varphi} = e^{3\cdot\frac{2\pi i}{n}}$ usw. $z_n^n = e^{ni\varphi} = e^{2\pi i} = 1$.

also $z_n \in E_n$ und damit auch $z_n^2, z_n^3, \dots, z_n^{n-1} \in E_n$



Teile Kreis in genau n gleiche Teile ein.

Also $E_n = \{1, z_n, z_n^2, \dots, z_n^{n-1}\}$.

$|E_n| = n$.

und damit $f = (X-1)(X-z_n)(X-z_n^2)\cdots(X-z_n^{n-1})$

Kann man Faktoren so zusammenfassen, daß man Faktoren in $\mathbb{Q}[X]$ erhält? Dazu benötigen wir etwas Gruppentheorie.

§5 Der Satz von Lagrange und Euler's φ-Funktion

Sei G eine Gruppe (Verknüpfung $g \cdot h$ mit $g, h \in G$).
$|G|$ heißt Ordnung von G. Wir werden meistens Gruppen endlicher Ordnung betrachten, aber die folgenden Konstruktionen funktionieren ganz allgemein.

Sei $U \le G$ eine Untergruppe (Def. 1.3) Analog zu Def. 2.7 definieren wir eine Relation $\sim_U$ auf G wie folgt:

$a \sim_U b \overset{\text{def}}{\Leftrightarrow} a^{-1}b \in U$ (wobei $a, b \in G$).

Dies ist eine Äquivalenzrelation, denn:

reflexiv: $a \sim_U a$ weil $1 = a^{-1}a \in U$.

symmetrisch: $a \sim_U b \Rightarrow b \sim_U a$, weil $b^{-1}a = \underbrace{(a^{-1}b)}_{\in U}{}^{-1} \in U$

transitiv: $a \sim_U b$, $b \sim_U c \Rightarrow a \sim_U c$ weil $a^{-1}c = \underbrace{a^{-1}b}_{\in U}\,\underbrace{b^{-1}c}_{\in U} \in U$. ✓

Sei $[a]$ die Äquivalenzklasse von $a \in G$ und
$G/H = \{[a] \mid a \in G\}$ die Menge der Äquivalenzklassen

Satz 5.1 (a) Für $a \in G$ ist $[a] = a \cdot U := \{au \mid u \in U\}$
"Linksnebenklasse von a nach U"

(b) Für festes $a \in G$ ist $U \to aU$, $u \mapsto au$, eine Bijektion

(c) Ist $|G| < \infty$, so gilt $|G| = |U| \cdot |G/U|$ also insbesondere
$|U| \mid |G|$ "Satz von Lagrange".

In diesem Fall heißt $|G/U|$ auch der Index von U in G

Beweis: a) $[a] = \{b \in G \mid a \sim_U b\} = \{b \in G \mid a^{-1}b \in U\} =$
$= \{b \in G \mid \text{ex. } u \in U \text{ mit } a^{-1}b = u\} = \{b \in G \mid \text{ex. } u \in G \text{ mit } b = au\}$
$= \{au \mid u \in U\} = aU$ ✓

b) $f: U \to aU$, $u \mapsto au$ bijektiv zu zeigen: Sei $au = f(u) = f(v) = av$
$\Rightarrow u = a^{-1}(au) = a^{-1}av = v$ also auch injektiv:

c) Seien $a_1, \dots, a_r \in G$ so dass $G/U = \{[a_1], \dots, [a_r]\}$ und
$r = |G/U|$. $\Rightarrow G = [a_1] \dot\cup \dots \dot\cup [a_r] = a_1U \dot\cup \dots \dot\cup a_rU$.
$\Rightarrow |G| = |a_1U| + \dots + |a_rU| \overset{b)}{=} \underbrace{|U| + \dots + |U|}_{r\text{-mal}} = r|U|$ □

Bem. 5.2 Analog kann man auch definieren:
$a \sim_U' b \overset{\text{def}}{\Leftrightarrow} ab^{-1} \in U$. Wiederum Äquivalenzrelation.
Äquivalenzklasse von $a \in G$ ist $Ua = \{ua \mid u \in U\}$ "Rechtsnebenklasse"
Sei $U\backslash G$ Menge der Äquivalenzklassen. Wie oben: $|G| < \infty$
$\Rightarrow |G| = |U| \cdot |U\backslash G|$ also $|U\backslash G| = |G/U|$.
Ist G abelsch, so gilt natürlich $aU = Ua$ für alle $a \in G$
also sind hier Rechtsnebenklassen = Linksnebenklassen.

Beisp. 5.3 Sei $g \in G$ fest. Dann ist
$\langle g \rangle := \{g^m \mid m \in \mathbb{Z}\}$ eine Untergruppe von G
mit den Konventionen $g^0 = 1$, $g^{-5} = (g^{-1})^5$ usw.
also dann $g^m \cdot g^n = g^{m+n}$ für alle $m, n \in \mathbb{Z}$.

$o(g) := |\langle g \rangle|$ heißt dann Ordnung von g.

Nach Lagrange gelt also: $|G| < \infty \Rightarrow o(g) \mid |G|$.

Beh.: Gibt es ein $n \geq 1$ mit $g^n = 1$, so ist $o(g) \mid n$
(insbes. $o(g) < \infty$) und $o(g) = \min\{m \geq 1 \mid g^m = 1\}$
Außerdem: $\langle g \rangle = \{1, g, g^2, \dots, g^{o(g)-1}\}$ und $g^{|G|} = 1$ falls $|G| < \infty$

Dann: Sei $d := \min\{m \geq 1 \mid g^m = 1\}$. Division mit Rest:
$n = dq + r$ mit $0 \leq r < d \Rightarrow 1 = g^n = g^{dq+r} = \underbrace{(g^d)^q}_{=1} g^r = g^r$
$\Rightarrow r = 0$ wegen Def. von d. also $d \mid n$.
Weiterhin: $m \in \mathbb{Z}$ bel. $m = dq + r$ mit $0 \leq r < d$.
$\Rightarrow g^m = g^{dq} g^r = g^r$ also $\langle g \rangle = \{g^r \mid 0 \leq r < d\}$.
Sind $0 \leq i < j < d$ mit $g^i = g^j$, so $1 = g^{-i} g^i = g^{-i} g^j = g^{j-i}$
$1 \leq j - i < d$ ↯ zur Def. von d.
Also $\langle g \rangle = \{g^r \mid 0 \leq r < d\}$ genau d Elemente, also $d = o(g)$ □.

G heißt zyklisch, wenn es ein $g \in G$ gibt mit $G = \langle g \rangle$.

Beisp. 5.4 (a) Sei G Gruppe endl. Ordnung mit $|G| = p$ Primzahl.
$\Rightarrow$ G zyklisch, $G = \langle g \rangle$ für jedes $1 \neq g \in G$.

denn: Sei $1 \neq g \in G$ $U := \langle g \rangle \leq G$ Lagrange $|U| \mid |G| = p$.
p Pr. also $|U| = 1$ oder $|U| = p$. $g \neq 1 \Rightarrow |U| \neq 1$.
also $U = G$.

(b) Sei $G = S_3$ symmetrische Gruppe auf $\{1,2,3\}$.
$U \leq G \overset{\text{Lagrange}}{\Rightarrow} |U| = 1, 2, 3$ oder 6 $|U| = 1 \Rightarrow U = \{id\}$.
$|U| = 6 \Rightarrow U = S_3$.
Ist $|U| = 2$, so nach a) $U = \langle \tau \rangle$ mögliche Elemente
$\tau_1 = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}, \tau_2 = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}, \tau_3 = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$ $\rightsquigarrow$ 3 Untergruppen der Ordnung 2.
Ist $|U| = 3$ so nach a) $U = \langle \pi \rangle$ mögliche Elemente

$\pi = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$ und $\pi^2 = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$ $\Rightarrow$ $U = \{id, \pi, \pi^2\}$ genau eine Möglichkeit.

also $\{id\}$, $\underbrace{\langle\sigma_1\rangle, \langle\sigma_2\rangle, \langle\sigma_3\rangle}_{\text{Ordnung 2}}$, $\underbrace{\langle\pi\rangle}_{\text{Ordnung 3}}$, S_3 komplette Liste aller Untergruppen von S_3.

Zyklische Gruppen = von einem Element "erzeugte" Gruppen $G = \langle g \rangle$.

Dies läßt sich wie folgt verallgemeinern:

Def 5.5 Sei $X \subseteq G$ beliebige Teilmenge. Dann heißt

$$\langle X \rangle := \bigcap_{\substack{U \leq G \text{ Ugr.} \\ \text{mit } X \subseteq U}} U$$

die von X erzeugte Untergruppe von G

Bemerke: 1) Ist $\{U_i\}_{i \in I}$ beliebige Familie von Untergruppen von G, so ist $\bigcap_{i \in I} U_i$ auch eine Untergruppe.

2) Ist $H \subseteq G$ Untergruppe mit $X \subseteq H$, so folgt $\langle X \rangle \subseteq H$ (denn H kommt in obigem Schnitt vor), d.h. $\langle X \rangle$ ist tatsächlich die kleinste Untergruppe von G, die X enthält.

Bem. 5.6 Ist $X = \emptyset$, so ist $\langle \emptyset \rangle = \{1\}$. Ist $X \neq \emptyset$, so

$$\langle X \rangle = \{ x_1 \cdots x_r \mid r \geq 1,\ x_i \in X \text{ oder } x_i^{-1} \in X \} \cup \{1_G\}$$

Zusatz: $X = \{g\} \Rightarrow \langle X \rangle = \{g^m \mid m \in \mathbb{Z}\} = \langle g \rangle$ wie in Beisp. 5.3

Beweis: Sei H = rechte Seite. H abgeschlossen unter Mult. und Inversen, $X \subseteq H$ also $H \leq G$ mit $X \subseteq H$ und damit $\langle X \rangle \subseteq H$. Andererseits: Ist $U \leq G$ bel. Ugr. mit $X \subseteq U$, so gilt auch $H \subseteq U$, also $H \subseteq \langle X \rangle$. Damit $\langle X \rangle = H$ □

Im Allgemeinen kann es sehr schwierig sein, genau zu bestimmen, welche Elemente von G nun zu $\langle X \rangle$ gehören.

(!): Diedergruppen und $SL_2(K) = \left\langle \begin{pmatrix}1&t\\0&1\end{pmatrix}, \begin{pmatrix}1&0\\s&1\end{pmatrix} \mid s,t \in K \right\rangle$ (K Körper)

Lemma 5.7 Sei $g \in G$ und $n := o(g) < \infty$. Sei $d \geq 1$.

(a) Ist $d \mid n$, so gilt $o(g^d) = \frac{n}{d}$.

(b) $o(g^d) = o(g) \iff \langle g^d \rangle = \langle g \rangle \iff ggT(d, n) = 1$.

Beweis: a) Sei $m := o(g^d) \Rightarrow 1 = (g^d)^m = g^{dm} \xrightarrow{\text{Beispiel 5.3}} n \mid dm$ also $dm = cn$ mit $c \in \mathbb{N}$. $\Rightarrow m = c\frac{n}{d} \geq \frac{n}{d}$. Andererseits $(g^d)^{\frac{n}{d}} = g^n = 1$ also $m = o(g^d) \leq \frac{n}{d}$ Damit $o(g^d) = \frac{n}{d}$.

(b) $g^d \in \langle g \rangle \Rightarrow \langle g^d \rangle \subseteq \langle g \rangle$ also $\langle g^d \rangle = \langle g \rangle \iff o(g^d) = o(g)$.
Müssen also noch Äquivalenz mit $ggT(n, d) = 1$ zeigen:
Sei $ggT(n, d) = 1$ und $m := o(g^d) \Rightarrow 1 = (g^d)^m = g^{dm}$
$\Rightarrow n \mid dm$ also $dm = cn$ mit $c \in \mathbb{N}$ $ggT(d, n) = 1 \Rightarrow n \mid m$
d.h. $m \geq 1$ also $m = |\langle g^d \rangle| \geq |\langle g \rangle| = n$. Wegen $\langle g^d \rangle \leq \langle g \rangle$
gilt auch $m \leq n$, also $m = n$.
Umgekehrt: $\langle g^d \rangle = \langle g \rangle$ also $g = (g^d)^r$ für ein $r \geq 1$.
$= g^{dr}$
$\Rightarrow g^{dr-1} = 1 \Rightarrow n \mid dr - 1$ und damit $dr - 1 = cn$ mit $c \in \mathbb{N}$.
$\Rightarrow 1 = dr - cn \Rightarrow ggT(d, n) = 1$. □

Lemma 5.8 Seien $g_1, g_2 \in G$ mit $o(g_1) < \infty$, $o(g_2) < \infty$.
Es gelte $g_1 g_2 = g_2 g_1$ und $ggT(o(g_1), o(g_2)) = 1$. Dann ist $o(g_1 g_2) = o(g_1)\, o(g_2)$

Beweis: $\longrightarrow$ Übung. □

Satz 5.9 Sei G eine abelsche Gruppe und $|G| < \infty$.
Sei $n := \max\{o(g) \mid g \in G\}$. Dann gilt $o(g) \mid n$ für alle $g \in G$.

Beweis: Sei $g \in G$ mit $o(g) = n$ Sei $x \neq 1$ und $m = o(x) > 1$.
Sei p Primzahl mit $p \mid m$ Schreibe: $m = p^k a$, $n = p^\ell b$ mit $k, \ell \geq 0$, $p \nmid a$, $p \nmid b$. Dann genügt es zu zeigen: $k \leq \ell$.
(denn dann kommt jede Primzahl in m höchstens so oft vor wie in,

also folglich $m \mid n$.) Nach Lemma 5.7 ist $o(x^a) = p^k$ und $o(g^{p^l}) = b$. Wegen $ggT(p, b) = 1$ und G abelsch folgt mit Lemma 5.8: $o(x^a g^{p^l}) = p^k b$ also $p^k b \leq n = p^l b$ und damit $p^k \leq p^l$ also $k \leq l$ ✓. □

Bemerke: Obiger Satz gilt nicht in nicht abelschen Gruppen, z.B. in S_3! ✓

Folgerung 5.10 Sei K ein Körper und G eine endliche Untergruppe von $K^\times$. Dann ist G zyklisch.

Beweis: Sei $n := \max\{o(g) \mid g \in G\} < \infty$. (existiert weil $|G| < \infty$) Sei $g_0 \in G$ mit $o(g_0) = n$. Dann $g^n = 1 \ \forall g \in G$ nach Satz 5.9. Also sind alle Elemente von G Nullstellen von $X^n - 1 \in K[X]$. Aber $X^n - 1$ hat höchstens n Nullstellen in K, siehe Bem. 4.15. Also $|G| \leq n$. Aber $o(g_0) = n$ also $G = \langle g_0 \rangle$. □

Insbesondere ist also $\mathbb{F}_p^\times$ zyklisch (p Primzahl).

z.B. $\mathbb{F}_2^\times = \langle \bar{1} \rangle$, $\mathbb{F}_3^\times = \langle \bar{2} \rangle$, $\mathbb{F}_5^\times = \langle \bar{2} \rangle$ etc.

Def. 5.11 Sei $n \geq 1$. Dann setze $\phi(n) := |\{1 \leq d \leq n \mid ggT(d, n) = 1\}|$

Die Funktion $n \mapsto \phi(n)$ heißt Euler's ϕ-Funktion.

Ist also $G = \langle g \rangle$ zyklische Gruppe der Ordnung n, so ist

$\phi(n)$ = Anzahl der Erzeuger von G.
= Anzahl der g^d mit $1 \leq d \leq n$ und $G = \langle g^d \rangle$

(siehe Lemma 5.7).

z.B. $\phi(1) = 1$ $\phi(2) = 2$ $\phi(3) = 2$ $\phi(4) = 2$

1, 2, ✗ 1, ✗, 3, ✗

$\phi(5) = 4$ $\phi(6) = 2$

1 2 3 4 ✗ 1 ✗ ✗ ✗ ✗ etc. allgemeine Formel?

$\phi(p) = p - 1$ falls p Primzahl, denn
$ggT(d, p) = 1$ für $1 \leq d \leq p - 1$.

Beisp 5.12 Sei p Primzahl und $r \geq 1 \Rightarrow \phi(p^r) = p^{r-1}(p-1)$

Beweis: Betrachte alle d mit $1 \leq d \leq p^r$.

$ggT(d, p^r) = 1$ falls $p \nmid d$, $p \mid ggT(d, p^r)$ falls $p \mid d$

$\Rightarrow \phi(p^r) = p^r -$ Anzahl der Vielfachen von p im Intervall $1, \dots, p^r$

$1 \cdot p,\ 2 \cdot p,\ 3 \cdot p, \dots, p^{r-1} p$

insgesamt p^{r-1}

$= p^r - p^{r-1} = p^{r-1}(p-1)$ □

Allgemeine Formel für $\phi(n)$ $\rightsquigarrow$ siehe §6

Nun zurück zu den Polynomen $f = X^n - 1 \in \mathbb{Z}[X]$

Wie in Beisp. 4.16 sei $E_n = \{z \in \mathbb{C} \mid z^n = 1\} \leq \mathbb{C}^\times$ Untergruppe

Nach Folg. 5.10 ist E_n zyklisch, wir kennen bereits einen Erzeuger aus Beisp. 4.16, nämlich $z_n = e^{2\pi i/n} \in \mathbb{C}$.

Sei $E_n^* = \{z \in E_n \mid E_n = \langle z \rangle\} = \{z_n^d \mid 1 \leq d \leq n, ggT(d,n) = 1\}$ (siehe Def. 5.11.

Also $|E_n^*| = \phi(n)$.

Def. 5.13 Mit den obigen Bezeichnungen heißt

$\Phi_n := \prod_{z \in E_n^*} (X - z) \in \mathbb{C}[X]$ das n-te Kreisteilungspolynom (oder zyklotomisches Polynom)

$\text{Grad}(\Phi_n) = \phi(n)$.

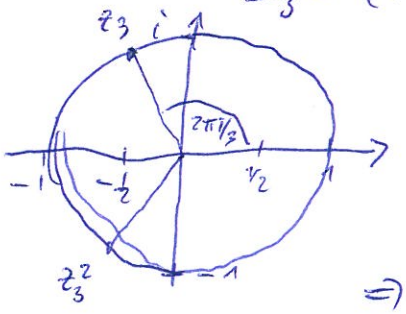
z.B. $n=1$ $z^1 = 1$ $E_1 = \{1\} = E_1^*$ also $\Phi_1 = X - 1$

$n=2$ $z^2 = 1$ $E_2 = \{\pm 1\}$ $E_2^* = \{-1\}$ also $\Phi_2 = X + 1$.

$n=3$ $z^3 = 1$ $E_3 = \{1, z_3, z_3^2\}$ $E_3^* = \{z_3, z_3^2\}$

$\Phi_3 = (X - z_3)(X - z_3^2) = X^2 - (z_3 + z_3^2) + \underbrace{z_3^3}_{=1}$

$z_3 + z_3^2 = -1$ $= X^2 + X + 1$.



$n=4$ $z^4 = 1$ $E_4 = \{1, -1, i, -i\}$. $E_4^* = \{i, -i\}$.

$\Rightarrow \Phi_4 = (x - i)(x + i) = x^2 - i^2 = x^2 + 1$

Wir erkennen also die Polynome in Beisp. 4.16 wieder!

Satz 5.14 Es gilt $n = \sum_{d \mid n} \phi(d)$ und $X^n - 1 = \prod_{d \mid n} \Phi_d$

und $\Phi_n \in \mathbb{Z}[X]$ für alle $n \geq 1$.

Beweis: Ist $d \mid n$, so $E_d \subseteq E_n$ und damit $E_d^* \subseteq E_n$.

Umgekehrt: Sei $z \in E_n$ bel. und $d = \#\langle z \rangle \geq 1 \Rightarrow z^d = 1$

$\Rightarrow z \in E_d$ und damit $z \in E_d^*$; außerdem $d \mid n$ nach Lagrange. $\#\langle z \rangle = |E_d|$.

$\Rightarrow E_n = \bigcup_{d \mid n} E_d^*$ disjunkte Vereinigung

↑ weil jedes $z \in E_n$ eine eindeutig bestimmte Ordnung hat.

$$\Rightarrow X^n - 1 = \prod_{z \in E_n} (X - z) = \prod_{d \mid n} \prod_{z \in E_d^*} (X - z)$$

$\prod_{z \in E_d^*} (X - z) = \Phi_d$.

$\Rightarrow$ „ $\mathrm{Grad}(X^n - 1) = \sum_{d \mid n} \mathrm{Grad}(\Phi_d) = \sum_{d \mid n} \phi(d)$.

Schließlich zeige $\Phi_n \in \mathbb{Z}[X]$ mit Induktion nach n.

$n = 1$ $\Phi_1 = X - 1 \in \mathbb{Z}[X]$ s.o. Sei nun $n > 1$.

$$\Rightarrow X^n - 1 = \Phi_n \cdot \Big(\prod_{\substack{d \mid n \\ d \neq n}} \Phi_d \Big)$$

$=: g \in \mathbb{Z}[X]$ nach Induktion; außerdem g normiert nach Def. der Φ_d.

Division mit Rest in $\mathbb{Z}[X]$ möglich nach Bem 4.2:

$$X^n - 1 = q \cdot g + r \quad \text{mit } q, r \in \mathbb{Z}[X],\ r = 0 \text{ oder } \mathrm{Grad}(r) < \mathrm{Grad}(g)$$

$$= \Phi_n \cdot g$$

$\Rightarrow q \cdot g + r = \Phi_n \cdot g$ Identität in $\mathbb{C}[X]$

$\Rightarrow r = \Phi_n \cdot g - q \cdot g = (\Phi_n - q) \cdot g$.

$r = 0$ oder $\mathrm{Grad} < \mathrm{Grad}(g)$ Falls $\Phi_n \neq q$, dann $\mathrm{Grad} \geq \mathrm{Grad}(g)$ ↯

Also $\Phi_n = q \in \mathbb{Z}[X]$ □

Mit obiger Formel kann man die Φ_n rekursiv berechnen.

Werden später sehen, daß die $\Phi_n \in \mathbb{Q}[X]$ sogar irreduzibel sind!

Jetzt noch eine Anwendung auf Primzahlen. Der folgende Satz ist ein berühmter Satz der Zahlentheorie (und nicht einfach zu beweisen)

Satz von Dirichlet (1837) Seien $a, b \in \mathbb{N}$ fest mit $ggT(a,b)=1$. Dann enthält die Folge $\{na+b \mid n \in \mathbb{N}\}$ unendlich viele Primzahlen.

"Kleiner Satz von Dirichlet": Sei $d \in \mathbb{N}$ fest. Dann enthält die Folge $\{nd+1 \mid n \in \mathbb{N}\}$ unendlich viele Primzahlen.

Beweis: Angenommen, die Folge enthält nur endlich viele Primzahlen, seien diese $p_1, \dots, p_r$. (oder gar keine; dann setze auch $p_0 = 1$ und $r=0$)

$\Phi_d \in \mathbb{Z}[X]$ normiert $\Rightarrow$ $\lim_{x \to +\infty} \Phi_d(x) = +\infty$. Also gibt es ein $x_0 > 0$ mit $\Phi_d(x) \geq 2$ für alle $x \geq x_0$. Wähle nun $n \in \mathbb{N}$ so daß $a := nd p_0 p_1 \cdots p_r \geq x_0$ gilt $\Rightarrow$ $\Phi_d(a) \geq 2$ und $\Phi_d(a) \in \mathbb{N}$. Sei p eine Primzahl mit $p \mid \Phi_d(a)$.

Nun ist $X^d - 1 = \Phi_d(a) f$ mit $f \in \mathbb{Z}[X]$ also $a^d - 1 = \Phi_d(a) f(a)$, $f(a) \in \mathbb{Z}$

also $\Phi_d(a) \mid a^d - 1$, $\Rightarrow$ $p \mid a^d - 1$

aber dann folgt insbesondere $p \nmid a$ und $p \nmid d$.

(denn sonst $p \mid a^d$ und $p \mid a^d - 1 \Rightarrow p \mid 1$ ↯)

Damit sehen wir insbesondere: $p \neq p_0, p_1, \dots, p_r$.

Betrachte nun den Körper $F = \mathbb{Z}/p\mathbb{Z}$. Wegen $p \nmid a$ ist $0 \neq \bar{a}$ in F also $\bar{a} \in F^\times$ $|F^\times| = p-1$

Sei $e \geq 1$ die Ordnung von $\bar{a}$ in $F^\times$ Lagrange $e \mid p-1$.

Außerdem $p \mid a^d - 1$ also $\bar{a}^d = 1 \Rightarrow e \mid d$.

1. Fall: $e = d$, d.h. $d \mid p-1$ also $p - 1 = cd$ mit $c \in \mathbb{N}$

$\Rightarrow$ p liegt in dieser Folge $\Rightarrow$ $p = p_i$ für ein i ↯.

2. Fall: $e < d$ $\Rightarrow$ $X^d - 1 = \prod_{d' \mid d} \Phi_{d'} = \Phi_d \cdot (X^e - 1) h$

mit $h \in \mathbb{Z}[X]$. Formale Ableitung:

$$d X^{d-1} = D(X^d - 1) = D(\Phi_d)\, h\,(X^e - 1) + \Phi_d\, D\,((X^e - 1)h)$$

$$= f \cdot (X^e - 1) + g \cdot \Phi_d \quad \text{mit} \quad f, g \in \mathbb{Z}[X]$$

$$\Rightarrow \quad d a^{d-1} = f(a)\underbrace{(a^e - 1)}_{p\,|} + g(a)\underbrace{\Phi_d(a)}_{p\,|} \quad \Rightarrow \quad p \mid d a^{d-1}$$

$\Rightarrow p \mid d$ oder $p \mid a$ $\lightning$. Also in beiden Fällen $\lightning$, und damit Annahme falsch. □

§6 Der Chinesische Restsatz und das RSA-System

Seien $n, m \in \mathbb{N}$ und $a, b \in \mathbb{N}$ vorgegeben. Gibt es eine Lösung $x \in \mathbb{Z}$ der beiden Kongruenzgleichungen

$$x \equiv a \bmod n \quad \text{und} \quad x \equiv b \bmod m \,?$$

Satz 6.1 (Chinesischer Restsatz) Sei $ggT(n, m) = 1$. Dann gibt es genau eine Lösung $x \in \mathbb{N}$ mit $1 \le x \le n \cdot m$.

Beweis: $ggT(n, m) = 1 \Rightarrow$ (Eukl. Algorithmus) $1 = rn + sm$ mit $r, s \in \mathbb{Z}$.

Setze $x_1 := brn + asm \in \mathbb{Z}$.

$$x_1 = brn + a(1 - rn) = a + \underbrace{brn - arn}_{n\,|} \equiv a \bmod n$$

$$x_1 = b(1 - sm) + asm = b \underbrace{- bsm + asm}_{m\,|} \equiv b \bmod m$$

Sei $c \in \mathbb{N}_0 \Rightarrow x_1 + c\,n \cdot m$ Lösung, denn

$x_1 + c\,n\,m \equiv x_1 \bmod n$ und $x_1 + c\,n\,m \equiv x_1 \bmod m$.

Also wähle x mit $1 \le x \le n \cdot m$ und $x \equiv x_1 \bmod n\,m$.

Eindeutigkeit: Sei auch $1 \le y \le n\,m$ mit $y \equiv a \bmod n$, $y \equiv b \bmod m$.

$\Rightarrow x \equiv y \bmod n$ und $x \equiv y \bmod m$

$\Rightarrow n \mid x - y$ und $m \mid x - y$ $\quad ggT(n, m) = 1 \Rightarrow n \cdot m \mid x - y$.

Also $x \bmod n\,m$ eindeutig. □

Beispiele in den (1)

Seien R, S Ringe. Dann ist auch $R \times S = \{(r,s) \mid r \in R, s \in S\}$ ein Ring mit Verknüpfungen

$(r_1, s_1) + (r_2, s_2) := (r_1 + r_2, s_1 + s_2)$

(Addition in R, Addition in S)

$(r_1, s_1) \cdot (r_2, s_2) := (r_1 r_2, s_1 s_2)$.

Neutrales Element bzgl. $+$ ist $(0,0)$, bezüglich $\cdot$ ist $(1,1)$ das 1-Element von $R \times S$. In diesem Fall: $(R \times S)^\times = \{(r,s) \mid r \in R^\times, s \in S^\times\}$.

$R \times S$ kommutativ $\Leftrightarrow$ R und S kommutativ.

$R \times S$ heißt direktes Produkt von R und S.

Satz 6.2 (Chinesischer Restsatz, 2. Fassung) Seien $n, m \in \mathbb{N}$ mit $ggT(n,m) = 1$. Dann ist die Abbildung

$$\mathbb{Z}/nm\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$
$$x + nm\mathbb{Z} \mapsto (x + n\mathbb{Z}, x + m\mathbb{Z})$$

wohldef. und ein Ring-Isomorphismus.

Beweis: Sei $x + nm\mathbb{Z} = y + nm\mathbb{Z} \Rightarrow nm \mid x - y \Rightarrow$ $n \mid x - y$ und $m \mid x - y$ also $x + n\mathbb{Z} = y + n\mathbb{Z}$, $x + m\mathbb{Z} = y + m\mathbb{Z}$ also wohldef. Dann folgt auch sofort, daß Abb. ein Homomorphismus ist. Nach Satz 6.1 ist dieser surjektiv. Wegen $|\mathbb{Z}/nm\mathbb{Z}| = nm = |\mathbb{Z}/n\mathbb{Z}| \cdot |\mathbb{Z}/m\mathbb{Z}|$ also auch injektiv. □

Bem. 6.3 Betrachte Einheiten von $\mathbb{Z}/n\mathbb{Z}$: Sei $1 \le a \le n$.

Dann $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ $\Leftrightarrow$ ex. $b \in \mathbb{Z}$ mit $\bar{a} \cdot \bar{b} = \bar{1}$

$\Leftrightarrow$ ex. $b \in \mathbb{Z}$ mit $n \mid ab - 1$.

$\Leftrightarrow$ ex. $b, c \in \mathbb{Z}$ mit $ab - 1 = cn$

$\Leftrightarrow$ ex. $b, c \in \mathbb{Z}$ mit $1 = ab - cn$

$\Leftrightarrow$ $ggT(a,n) = 1$.

(für "$\Leftarrow$" benutze Euklidischen Algorithmus). Also folgt.

$$\phi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$$

(neue Interpretation von Euler's ϕ-Funktion)

Sei nun $n \in \mathbb{N}$ mit $ggT(n,m) = 1$. Dann folgt mit Satz 6.2:

$\mathbb{Z}/nm\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, also auch

$$(\mathbb{Z}/nm\mathbb{Z})^\times \cong (\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z})^\times \cong (\mathbb{Z}/n\mathbb{Z})^\times \times (\mathbb{Z}/m\mathbb{Z})^\times$$

und damit:

$\phi(nm) = \phi(n)\,\phi(m)$ falls $ggT(n,m)=1$

Zusammen mit Bem. 5.12 folgt jetzt:

Sei $n = p_1^{n_1} \cdots p_r^{n_r}$ mit paarweise versch. Primzahlen $p_1, \dots, p_r$, $n_1 \geq 1, \dots, n_r \geq 1$.

$$\Rightarrow \quad \phi(n) = \phi(p_1^{n_1}) \cdots \phi(p_r^{n_r}) = p_1^{n_1-1}(p_1-1) \cdots p_r^{n_r-1}(p_r-1).$$

allgemeine Formel für $\phi(n)$!

Folgerung 6.4 (Satz von Euler) Sei $a \in \mathbb{Z}$ mit $ggT(a,n)=1$

Dann $a^{\phi(n)} \equiv 1 \mod n$.

Beweis: Arbeite in $\mathbb{Z}/n\mathbb{Z}$ $\quad ggT(a,n)=1 \Rightarrow \bar{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$

$\phi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$. Lagrange: $o(\bar{a}) \mid \phi(n)$

$\Rightarrow \bar{a}^{\phi(n)} = 1 \Rightarrow a^{\phi(n)} \equiv 1 \mod n$ ∎

Folgerung 6.5 (Kleiner Satz von Fermat). Sei $a \in \mathbb{Z}$ und p eine Primzahl. Dann $a^p \equiv a \mod p$.

Beweis: Ist $p \mid a$, so Aussage offensichtlich. Ist $p \nmid a$,

so $ggT(a,p)=1$ also $a^{\phi(p)} \equiv 1 \mod p$ nach Euler.

aber $\phi(p) = p-1$ also $a^{p-1} \equiv 1 \mod p \Rightarrow a^p \equiv a \mod p$ ∎

Bsp. 6.6 Man kann manchmal den kleinen Satz von Fermat benutzen um zu zeigen, daß ein gegebenes $n \in \mathbb{N}$ keine Primzahl

z.B. $n = 943$. Berechne $2^{942} \equiv 496 \mod 943$

$\not\equiv 1$

also n keine Pz.

Das funktioniert natürlich nicht immer! z.B. $2^{340} \equiv 1 \mod 341$

aber $341 = 11 \cdot 31$.

Bsp. 6.7 [illegible] $a \mod n$ [illegible]

Bem. 6.7 Sei $n \in \mathbb{N}$ gegeben. Wir haben 2 Verfahren, um $\phi(n)$ zu berechnen.

1) Gehe $a = 1, \dots, n$ durch und prüfe ob $ggT(a,n) = 1$ ist
↳ Eukl. Algorithmus.

2) Faktorisiere $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ und benutze Formel in Bem. 6.3

Für n groß ist 1) viel zu aufwändig und 2) extrem schwierig.

z.B.: Für $n \neq 1$ heißt $F_n := 2^{2^n} + 1$ Fermat-Zahl.

Fermat glaubte, daß alle diese F_n Primzahlen sind

n	F_n	
0	3	← prim
1	5	← "
2	17	← "
3	257	← "
4	65537	← $641 \cdot 6700417$ (Euler)
5	4294967297	
6	$\approx 1{,}8 \times 10^{19}$	
⋮		
9	155 Ziffern	← nicht prim Lenstra, Lenstra, Manasse, Pollard 1990

Hier haben wir hier ein Beispiel für eine Diskrepanz zwischen theoretischem Resultat und praktischer Anwendbarkeit.

Dies ist Grundlage des RSA-Verschlüsselungsverfahrens.
(Rivest, Shamir, Adleman) mathematisch ~1978, Patent 1983

siehe Wikipedia RSA Cryptosystem für historischen Hintergrund.

Beisp. 6.8 (RSA-Verschlüsselung) Alice erwartet von Bob (üblicherweise in Texten zur Verschlüsselung) eine Nachricht, aber sie möchte vermeiden, daß andere auch diese Nachricht verstehen können (selbst wenn andere die Nachricht sehen können). Eine Nachricht ist hier einfach eine Zahl $m \in \mathbb{N}$, die man

nach einem bestimmten Verfahren aus Buchstaben oder sonstigen Daten bildet. Konkretes Beispiel:
Alice erwartet von Bob einen Tipp, ob der VfB Stuttgart am nächsten Bundesliga-Spieltag gewinnt oder verliert oder unentschieden spielt. Um dies zu vereinfachen, soll Bob also einfach nur ein G, V oder U senden.
also als Zahl m: 7 23 oder 22
(7-ter Buchstabe, etc.).

Idee der Verschlüsselung von m. Alice wählt zwei Primzahlen $p \neq q$ und bildet $N := p \cdot q$ wobei muß gelten: $m < N$.
Alice wählt noch eine weitere Zahl $e \in \mathbb{N}$ mit

$$1 < e < \varphi(N) = \varphi(p)\varphi(q) = (p-1)(q-1) \quad \text{und}$$

$$ggT(e, \varphi(N)) = 1.$$

(z.B. einfach eine weitere Primzahl die weder $p-1$ noch $q-1$ teilt). Nun veröffentlicht Alice das Paar (e, N) "public key".
Jeder, der Alice eine Nachricht verschlüsselt schicken will, geht nun wie folgt vor. Ist $m \in \mathbb{N}$ die Nachricht $(0 \leq m < N)$, so berechne $0 \leq c \leq N-1$ mit

$$c \equiv m^e \bmod N \quad \text{(Division mit Rest)}$$

Versende dann c als verschlüsselte Nachricht.
Wie kann Alice aus c, e, N das m zurückberechnen?
Man könnte einfach alle $1 \leq a \leq N$ testen, ob $c \equiv a^e \bmod N$ gilt, aber für große N ist dies nicht praktikabel (zu viele Multiplikationen und Divisionen mit Rest.)

Idee der Entschlüsselung Alice hatte e so gewählt, daß $ggT(e, \varphi(N)) = 1$ mit dem Eukl. Algorithmus gilt.

$r, s \in \mathbb{Z}$ mit $1 = re + s\varphi(N)$ also $\bar{1} = \bar{r}\bar{e}$ in $\mathbb{Z}/\varphi(N)\mathbb{Z}$

Dividiert r mit Rest durch $\varphi(N)$: $r = q\varphi(N) + d$ mit $0 \le d < \varphi(N)$

$\Rightarrow \bar{r} = \bar{d}$ also $de \equiv 1 \bmod \varphi(N)$

Dieses d heißt "private key".

Lemma 6.9 Mit obigen Bezeichnungen gilt $(m^e)^d \equiv m \bmod N$.

Beweis: Wir zeigen $(m^e)^d \equiv m \bmod p$ und $(m^e)^d \equiv m \bmod q$

also $p \mid (m^e)^d - m$ und $q \mid (m^e)^d - m$. Wegen $p \neq q$ folgt

dann auch $N = pq \mid (m^e)^d - m$ also $(m^e)^d \equiv m \bmod N$.

Zuerst mod p: Ist $p \mid m$ so auch $p \mid (m^e)^d$ also

$(m^e)^d \equiv 0 \equiv m \bmod p$ ✓. Ist $p \nmid m$, so verfahren wir

folgt: Wegen $de \equiv 1 \bmod \varphi(N)$ gibt es $l \in \mathbb{Z}$ mit $ed = 1 + l\varphi(N)$

$\Rightarrow (m^e)^d = m^{ed} = m^{1+l\varphi(N)} = m\left(m^{\varphi(N)}\right)^l = m\left(m^{(p-1)(q-1)}\right)^e$

$= m\left(m^{p-1}\right)^{(q-1)e}$

$\equiv m \cdot 1 \bmod p$ ← Fermat's kleiner Satz: $m^{p-1} \equiv 1 \bmod p$.

✓.

Argument mod q völlig analog. □

Hat also Alice c erhalten, so bildet sie ~~[illegible]~~

$m' = c^d \bmod N$ (m' = Rest der Division von N durch c^d)

$0 \le m' < N$. Wegen Lemma 6.9. gilt:

$m' \equiv c^d \equiv (m^e)^d \equiv m \bmod N$.

$0 \le m, m' < N \Rightarrow m' = m$ also hat sie so die

ursprüngliche Nachricht gefunden!

Zusammenfassung Alice hält den "private key" d geheim.

Sie kann d einfach mit Eukl. Algorithmus und

$\mathrm{ggT}(e, \varphi(N)) = 1$ ausrechnen, weil sie $\varphi(N) = (p-1)(q-1)$

kennt. Aber wie oben bemerkt ist es für jemand anders

sehr schwierig, $\varphi(N)$ zu berechnen, weil man dazu Faktorisierung in Primfaktoren kennen müßte.
In praktischen Anwendungen nimmt man p, q mit etwa 200 oder mehr Ziffen.

Zurück zum konkreten Beisp. mit Tipp für V+B.

Alice wählt $p = 101$, $q = 103$ $\Rightarrow$ $N = 10403$

$\Rightarrow \varphi(N) = 100 \cdot 102 = 10200$

und berechnet $d = 2201$, also

$(e, N) = (1001, 10200)$ "public key"

$d = 2201$ "secret key"

Alice erhält die Nachricht: $c = 2532$

Welchen Tipp hat Bob über geschickt?

$$\left[c^d = 2532^{2201} \equiv 7 \bmod 10403 \right]$$

also nämlich $7 =$ Gewonnen.

Siehe Buchmann, Introduction to Cryptography, für mehr dazu.

Beachte: Wie geheim ist der "secret code" d?

Um d zu berechnen, benötigt man $\varphi(N) = (p-1)(q-1)$.

Kennt man $\varphi(N)$, so also $\varphi(N) = (p-1)(q-1) = pq - (p+q) + 1 = N - (p+q) + 1$

und damit auch $p+q$ bekannt.

$N = pq$ ebenfalls bekannt

also $q(p+q) = N + q^2$ $\Rightarrow$ q Lösung der quadratischen Gleichung $X^2 - \underbrace{(p+q)}_{\text{bekannt.}} X + N = 0$

Also p, q bekannt $\rightarrow$ aber dies ist sehr schwierig!

§7 Körpererweiterungen ⟷ Lösen von polynomialen Gleichungen.

Seien L und K Körper mit $K \subseteq L$ und so, daß die Verknüpfungen in K genau die Einschränkungen der Verknüpfungen in L auf K sind.

Dann heißt: K Teilkörper von L } je nach Standpunkt
L Erweiterungskörper von K }

$L \supseteq K$ Körpererweiterung (manchmal auch L/K geschrieben)

Beispiele: $\mathbb{Q} \subseteq \mathbb{R}$, $\mathbb{R} \subseteq \mathbb{C}$, $\mathbb{Q} \subseteq \mathbb{C}$, $\mathbb{Q}(i) = \{a+bi \mid a,b \in \mathbb{Q}\} \subseteq \mathbb{C}$.

Bem. 7.1 Sei $L \supseteq K$ Körpererweiterung. Dann können wir L als K-Vektorraum auffassen. Skalare Multiplikation

$s \cdot v$ = Mult. in L ($\rightsquigarrow$ alle Vektorraumaxiome automatisch erfüllt)

$s \in K$, $v \in L$

Dann heißt $[L:K] = \dim_K L$ Körpergrad von L über K.

$L \supseteq K$ heißt endliche Erweiterung, wenn $[L:K] < \infty$ gilt.

Zu obigen Beispielen:

$[\mathbb{R}:\mathbb{Q}] = \infty$ siehe ☞ genauso $[\mathbb{C}:\mathbb{Q}] = \infty$.

$[\mathbb{C}:\mathbb{R}] = 2$ denn $\{1, i\}$ $\mathbb{R}$-Basis von $\mathbb{C}$. Jedes $z \in \mathbb{C}$ läßt sich eindeutig schreiben als $z = a+bi$ mit $a,b \in \mathbb{R}$.

Genauso $[\mathbb{Q}(i):\mathbb{Q}] = 2$.

Beachte ebenfalls: $[L:K] = 1 \iff L = K$.

$\rightsquigarrow$ Werden ausführlicher endliche Erweiterungen studieren.

Bem. 7.2 Sei K Körper und $\{K_i\}_{i \in I}$ Familie von Teilkörpern von K. Dann sieht man sofort, daß auch $\bigcap_{i \in I} K_i$ ein Teilkörper von K. Insbesondere ist

$K_0 := \bigcap_{K' \subseteq K \text{ bel. Teilkörper}} K'$ ein Teilkörper. Dieser heißt Primkörper von K.

Def. 7.3 Sei K ein Körper. Die kleinste natürliche Zahl $n \geq 1$ mit $\underbrace{1+\dots+1}_{n\text{-mal}} = 0$ heißt Charakteristik von K.

Schreibe $\operatorname{char}(K) = n$. Gibt es kein solches n, so schreibe $\operatorname{char}(K) = 0$.

Klar: In $\mathbb{Q}$ gilt $n \cdot 1 = \underbrace{1+\dots+1}_{n\text{-mal}} \neq 0$ für alle $n \in \mathbb{N}$.
also $\operatorname{char}(\mathbb{Q}) = 0$

In $K = \mathbb{Z}/p$ (p Primzahl) gilt $\underbrace{\bar{1}+\dots+\bar{1}}_{p\text{-mal}} = 0$
also $0 < \operatorname{char}(K) \leq p$.

Satz 7.4 Sei K Körper und $\operatorname{char}(K) = n \geq 0$. Dann ist entweder $n = 0$ oder $n = p$ eine Primzahl. Im ersten Fall ist $K_0 \cong \mathbb{Q}$, im zweiten Fall ist $K_0 \cong \mathbb{Z}/p$.

Beweis: Sei $n > 0$ und angenommen, n ist keine Primzahl.
Dann $n = n_1 n_2$ mit $1 \leq n_i < n$ und

$$0 = \underbrace{1+\dots+1}_{n} = \underbrace{(1+\dots+1)}_{n_1}\underbrace{(1+\dots+1)}_{n_2} \quad K \text{ Körper}$$

$\Rightarrow 1+\dots+1 = 0$ mit n_1 oder n_2 Summanden, $n_i < n$ $\lightning$ zur Def. von n.
also n Primzahl. Nun zu Primkörpern:

1. Fall: $\operatorname{char}(K) = 0$. Für $r \in \mathbb{Z}$ setze $r \cdot 1 = \underbrace{1+\dots+1}_{r\text{-mal}}$ falls $r > 0$

$r \cdot 0 = 0$ $\quad r \cdot 1 = \underbrace{(-1)+\dots+(-1)}_{(-r)\text{-mal}}$ falls $r < 0$.

Dann $r \cdot 1 \neq 0$ für alle $0 \neq r \in \mathbb{Z}$. $\Rightarrow$

$$M := \{(r \cdot 1)(s \cdot 1)^{-1} \mid r, s \in \mathbb{Z},\ s \neq 0\}$$ Teilkörper von K

Klarerweise enthält jeder Teilkörper von K die Menge M, also $K_0 = M$.

Schließlich:
$$\begin{array}{ccc} \mathbb{Q} & \longrightarrow & M \\ r/s & \longmapsto & (r \cdot 1)(s \cdot 1)^{-1} \\ (r, s \in \mathbb{Z},\ s \neq 0) & & \end{array}$$
ist ein Isomorphismus, also $K_0 \cong \mathbb{Q}$.

2. Fall: $\operatorname{char}(K) = p > 0$, p Primzahl. Für $m \in \mathbb{Z}$ definiere wieder $m \cdot 1$ wie oben und setze

$M := \{m \cdot 1 \mid m \in \mathbb{Z}\}$. Dann ist M ein Teilring von K.

Sei $m \in \mathbb{Z}$. Division mit Rest $m = q \cdot p + r$ mit $q, r \in \mathbb{Z}$, $0 \leq r < p$.

$\Rightarrow \quad m \cdot 1 = q \cdot \underbrace{(p \cdot 1)}_{=0} + r \cdot 1 = r \cdot 1.$

Also $M = \{0 \cdot 1, 1 \cdot 1, \dots, (p-1) \cdot 1\}$.

Wie im Beweis von Satz 2.4 sieht man, daß diese p Elemente paarweise verschieden sind, also $|M| = p$.

Schließlich:

$$\begin{aligned} \mathbb{Z}/p\mathbb{Z} &\longrightarrow M. \\ r + p\mathbb{Z} &\longmapsto r \cdot 1 \end{aligned}$$

wohl-def. und Ring-Homomorphismus.

surjektiv, also auch injektiv damit Isomorphismus.

$\mathbb{Z}/p\mathbb{Z}$ Körper $\Rightarrow$ M Teilkörper von K. Jeder Teilkörper von K enthält M also $K_0 = M \cong \mathbb{Z}/p\mathbb{Z}$ □.

(") Sei K Körper mit $\operatorname{char}(K) = p > 0$. Dann gilt

$$(a+b)^p = a^p + b^p \quad \text{für alle } a, b \in K.$$

Die Abbildung $F: K \to K$, $a \mapsto a^p$ ist ein injektiver Homomorphismus.

Def 7.5 Sei $L \supseteq K$ eine Körpererweiterung. Sei $z \in L$.

Dann haben wir den Einsetzungs-Homomorphismus

$$\varphi_z: K[X] \longrightarrow L, \quad f \longmapsto f(z)$$

[wobei $\varphi: K \hookrightarrow L$ Inklusion]

"Setze z in f ein"

(a) z heißt algebraisch über K, wenn es ein $0 \neq f \in K[X]$ gibt mit $f(z) = 0$. Andernfalls heißt z transzendent über K.

Ist jedes $z \in L$ algebraisch über K, so heißt $L \supseteq K$ eine algebraische Körpererweiterung. Bevor wir Beispiele betrachten, eine sehr nützliche Aussage.

Lemma 7.6 Sei $L \supseteq K$ Körpererweiterung. Dann gilt:

$$[L : K] < \infty \quad \Longrightarrow \quad L \supseteq K \text{ algebraisch.}$$

Beweis: Sei $n := [L:K] < \infty$. Sei $z \in L \Rightarrow$

$1, z, z^2, \dots, z^n$ ist eine linear abhängige Teilmenge von L.

Also gibt es $a_0, \dots, a_n \in K$ (nicht alle gleich 0) mit

$a_0 1 + a_1 z + a_2 z^2 + \dots + a_n z^n = 0$ Sei $f := a_0 + a_1 X + \dots + a_n X^n \in K[X]$

Dann $= f(z)$, also z algebraisch über K. $f \neq 0$ □

Beisp. 7.7 (a) $\mathbb{C} \supseteq \mathbb{R}$ ist algebraisch, weil $[\mathbb{C}:\mathbb{R}] = 2 < \infty$.
Genauso $[\mathbb{Q}(i):\mathbb{Q}]$.

(b) Betrachte $\mathbb{R} \supseteq \mathbb{Q}$. $\sqrt{2} \in \mathbb{R}$ ist algebraisch über $\mathbb{Q}$, weil $\sqrt{2}$ Nullstelle von $X^2 - 2 \in \mathbb{Q}[X]$.

Betrachte $\mathbb{C} \supseteq \mathbb{Q}$, $n \geq 1$ Die Einheitswurzeln.

$z_n = e^{2\pi i/n}$, $z_n^2, \dots, z_n^{n-1} \in \mathbb{C}$ sind algebraisch über $\mathbb{Q}$ weil Nullstellen von $X^n - 1 \in \mathbb{Q}[X]$ siehe Beisp. 4.16.

Für eine gegebene komplexe Zahl $z \in \mathbb{C}$ kann es im konkreten Einzelfall extrem schwierig sein, zu entscheiden, ob z algebraisch ist. Hermite (1873): e transzendent über $\mathbb{Q}$.

Lindemann (1882): π —— " ——

Bem.: Es gibt unendlich viele $z \in \mathbb{R}$, die transzendent über $\mathbb{Q}$ sind.

Denn: Benutze Cantor's Zählargument. Sei

$\mathbb{Q}[X]'$ = Menge der nicht-konstanten, normierten Polynome in $\mathbb{Q}[X]$

$= \bigcup_{n \geq 1} P_n$, wobei P_n = normierte Polynome vom Grad n.

Haben Bijektion $\mathbb{Q}^n \hookrightarrow P_n$

$(a_0, \dots, a_{n-1}) \hookrightarrow f = a_0 + a_1 X + \dots + a_{n-1} X^{n-1} + X^n$

$\Rightarrow P_n$ abzählbar $\Rightarrow$ $\mathbb{Q}[X]'$ (abzählbare Vereinigung von abzählbaren Mengen) auch abzählbar.

Jedes $f \in P_n$ hat höchstens n Nullstellen.

$\Rightarrow$ $\{z \in \mathbb{R} \mid f(z)=0$ für ein $f \in \mathbb{Q}[X]\}$ = abzählbare Vereinigung

$= \bigcup_{n \geq 1} \{z \in \mathbb{R} \mid f(z)=0$ für $f \in P_n\}$ von endlichen Mengen

$= \bigcup_{n \geq 1} \bigcup_{f \in P_n} \{z \in \mathbb{R} \mid f(z)=0\}$ also insgesamt wieder abzählbar.

$\Rightarrow$ Menge der alg. Zahlen in $\mathbb{R}$ ist abzählbar $\mathbb{R}$ überabzählbar

$\Rightarrow$ "Die meisten" reellen Zahlen sind transzendent über $\mathbb{Q}$!

Liouville (1844): sehr schnell konvergierende Reihen definieren transzendente Zahlen. z.B:

$$\sum_{n=1}^{\infty} 10^{-n!} = 0,\ 1\ 1\ 0\ 0\ 0\ 1\ \ 0 \ldots\ 0\ 1\ 0 \ldots\ 0\ 1\ 0\ldots$$

Position: $\uparrow 1$ $\uparrow 2$ $\quad 6$ $\quad 24$ $\quad 120$ usw

Suche im Internet nach: "Approximationssatz von Liouville".

(c) Sei wieder $\mathbb{C} \supseteq \mathbb{Q}$. In einfachen Fällen kann man durch direkte Manipulationen ein Polynom f mit $f(z)=0$ finden, z.B

$z = i+\sqrt{2}$. Bilde: $z^2 = (i+\sqrt{2}) = -1+2i\sqrt{2}+2 = 1+2i\sqrt{2}$

$z^3 = (i+\sqrt{2})(1+2i\sqrt{2}) = i - 2\sqrt{2} + \sqrt{2} + 4i = 5i - \sqrt{2}$

$z^4 = (1+2i\sqrt{2})^2 = 1 + 4i\sqrt{2} - 8 = 4i\sqrt{2} - 7 = 2(z^2-1) - 7 = 2z^2 - 9$

Also $f(z)=0$ für $f = X^4 - 2X^2 + 9 \Rightarrow z$ algebraisch

Satz 78 Sei $L \supseteq K$ Körpererweiterung und $z \in L$ algebraisch. Dann gibt es ein eindeutiges normiertes Polynom kleinsten Grades $\mu_z \in K[X]$ mit $\mu_z(z)=0$. Es gilt:

(a) μ_z ist irreduzibel

(b) $\mu_z \mid f$ für alle $f \in K[X]$ mit $f(z)=0$

Das Polynom μ_z heißt Minimalpolynom von z.

[Vgl. Lineare Algebra: Zu einer Matrix $A \in M_n(K)$ gibt es ein eindeutiges normiertes Polynom kleinsten Grades $\mu_A \in K[X]$ mit $\mu_A(A)=0$. "Minimalpolynom von A". Buch!

μ_A muß nicht irreduzibel sein, z. B. hat $A = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ Minimalpolynom $\mu_A = (X-1)(X+1)$. !

Beweis: z algebraisch $\Rightarrow$ es gibt $0 \neq f \in K[X]$ mit $f(z) = 0$

$f = a_0 + a_1 X + \ldots + a_n X^n$ mit $n \geq 1$, $a_n \neq 0$

$\Rightarrow \quad a_0 + a_1 z + \ldots + a_n z^n = 0 \quad \Rightarrow \quad a_0 a_n^{-1} + a_1 a_n^{-1} z + \ldots + a_{n-1} a_n^{-1} z^{n-1} + z^n = 0$

also können auch normiertes Polynom finden, daß z als Nullstelle hat. Sei $0 \neq f_0 \in K[X]$ normiert mit minimalem Grad, so daß $f_0(z) = 0$ gilt.

Sei $0 \neq f \in K[X]$ beliebig mit $f(z) = 0$. Teile mit Rest:

$f = q \cdot f_0 + r$ mit $q, r \in K[X]$, $r = 0$ oder $\mathrm{Grad}(r) < \mathrm{Grad}(f_0)$

$\Rightarrow$ (Einsetzen ist Homom.) $\quad 0 = f(z) = q(z) \underbrace{f_0(z)}_{=0} + r(z)$

$\Rightarrow \quad r(z) = 0$. [illegible] Annahme: $r \neq 0$

[illegible] Schreibe $r = c r'$ mit $0 \neq c \in K$ und $r' \in K[X]$ normiert

$\Rightarrow \quad r'(z) = 0$ und $\mathrm{Grad}(r') = \mathrm{Grad}(r) < \mathrm{Grad}(f_0)$ $\lightning$ zur Wahl von f_0

Also $r = 0$ und damit $f_0 \mid f$.

Sei f' weiteres normiertes Polynom mit $f'(z) = 0$ und $\mathrm{Grad}(f') = \mathrm{Grad}(f_0)$.
Wende obiges Argument auf f' an

$\Rightarrow \quad f_0 \mid f' \quad \mathrm{Grad}(f') = \mathrm{Grad}(f_0)$ und beide normiert

$\Rightarrow \quad f_0 = f'$!

Also $\mu_z = f_0$ eindeutiges Polynom minimalen Grades.
Wäre μ_z nicht irreduzibel, so schreibe $\mu_z = f_1 f_2$ mit $f_i \in K[X]$, $1 \leq \mathrm{Grad}(f_i) < \mathrm{Grad}(\mu_z)$

$\Rightarrow \quad 0 = \mu_z(z) = f_1(z) f_2(z) \quad$ L Integritätsring

$\Rightarrow \quad f_1(z) = 0$ oder $f_2(z) = 0$ $\lightning$ zu $\mathrm{Grad}(\mu_z)$ minimal $\square$.

Bemerkung Sei $z \in L$ und $f \in K[X]$ normiert irreduzibel mit $f(z)=0$
$\Rightarrow \quad f = \mu_z$.

denn: Satz 7.8 (b) $\Rightarrow \mu_z \mid f$ aber f irred. also $f = c\mu_z$ mit $c \in K$
f, μ_z beide normiert $\Rightarrow \quad f = \mu_z \quad (c=1)$

z.B. $z = \sqrt{2}$ $\quad f = X^2 - 2 \in \mathbb{Q}[X]$ irred. nach Eisenstein $(p=2)$
also $f = \mu_z$ $\rightsquigarrow$ weitere Beisp. siehe Ü.

Satz 7.9 Sei $L \supseteq K$ Körpererweiterung und $z \in L$ algebraisch.
Sei $K(z) := \{ f(z) \mid f \in K[X] \} \subseteq L$. Dann gilt:
$K(z)$ ist ein Teilkörper und $[K(z) : K] = \text{Grad}(\mu_z)$
"Adjunktion von z an K".

Beweis: Man sieht sofort: $K(z) \subseteq L$ Teilring
$(f, g \in K[X] \Rightarrow (f+g)(z) = f(z) + g(z) \in K(z)$
$(f-g)(z) = f(z) \cdot g(z) \in K(z)$ ✓)

Betrachte: $\varphi : K[X]/(\mu_z) \longrightarrow K(z)$
$f + (\mu_z) \longmapsto f(z)$

wohldef. surjektiver Ring-Homomorphismus
$f + (\mu_z) = g + (\mu_z) \Rightarrow \mu_z \mid f-g \Rightarrow 0 = \mu_z(z) = f(z) - g(z)$
also $f(z) = g(z)$
Hom.-Eigenschaft und surjektiv dann klar.
Beh.: Injektiv denn sei $f(z) = g(z) \Rightarrow (f-g)(z) = 0$
$\Rightarrow \mu_z \mid f-g \Rightarrow f + (\mu_z) = g + (\mu_z)$ ✓.

Also φ Isomorphismus von Ringen. Lemma 3.9:
$K[X]/(\mu_z)$ Körper denn $K[X]$ Hauptidealring und μ_z irred.
φ Isom. $\Rightarrow$ $K(z)$ Körper also Teilkörper von L.

Sei $d = \text{Grad}(\mu_z)$ Beh.: $\{1, z, z^2, \dots, z^{d-1}\}$ K-Basis von $K(z)$
denn: Sei $f \in K[X]$ bel. Division mit Rest
$f = q\mu_z + r$ mit $q, r \in K[X]$, $r = 0$ oder $\text{Grad}(r) < d$

$\Rightarrow f(z) = q(z)\mu_z(z) + r(z) = r(z)$ also

$K(z) = \{ r(z) \mid r \in K[X],\ r = 0 \text{ oder } r < d \}$.

$= \{ a_0 + a_1 z + \dots + a_{d-1} z^{d-1} \mid a_i \in K \}$ also $\{1, z, \dots, z^{d-1}\}$ Erzeugendensystem.

Sei $a_0 + a_1 z + \dots + a_{d-1} z^{d-1} = 0$ mit $a_i \in K$

Setze $f := a_0 + a_1 X + \dots + a_{d-1} X^{d-1}$ also $f(z) = 0$

Aber dann $\mu_z \mid f$ $\operatorname{Grad}(f) \le d-1$ $\Rightarrow$ $f = 0$

also $\{1, z, \dots, z^{d-1}\}$ linear unabhängig. □

z.B.: $\mathbb{Q}(i) \subseteq \mathbb{C}$ $\mu_i := X^2 + 1 \in \mathbb{Q}[X]$ Minimalpolynom.

$= \{ a + bi \mid a, b \in \mathbb{Q} \}$ $[\mathbb{Q}(i) : \mathbb{Q}] = 2$.

(Gradsatz)

Satz 7.10 Seien L, M, K Körper so daß wir Körpererweiterungen $L \supseteq M \supseteq K$ haben. Ist $[M:K] < \infty$ und $[L:M] < \infty$, so auch $[L:K] = [L:M] \cdot [M:K] < \infty$.

Beweis: Sei $n = [M:K]$ und $\{x_1, \dots, x_n\}$ eine K-Basis von M.

sei $m := [L:M]$ und $\{y_1, \dots, y_m\}$ eine M-Basis von L.

Beh.: $B := \{ x_i y_j \mid 1 \le i \le n,\ 1 \le j \le m \}$ K-Basis von L

$(\Rightarrow [L:K] = n \cdot m < \infty)$.

dann: 1) Erzeugendensystem: Sei $z \in L$ bel. $\Rightarrow$

$z = \sum_{j=1}^{m} a_j y_j$ mit $a_j \in M$. und $a_j = \sum_{i=1}^{n} b_{ij} x_i$ mit $b_{ij} \in K$

$\Rightarrow z = \sum_j \sum_i b_{ij} x_i y_j$ K-Linearkombination von B.

2) Linear unabhängig. Seien $a_{ij} \in K$ mit $\sum_{i=1}^{n} \sum_{j=1}^{m} a_{ij} x_i y_j = 0$

$\Rightarrow \sum_{j=1}^{m} \underbrace{\left(\sum_{i=1}^{n} a_{ij} x_i \right)}_{=: b_j \in M} y_j = 0$ $\{y_1, \dots, y_m\}$ l.u. über M.

$\Rightarrow 0 = b_j = \sum_{i=1}^{n} a_{ij} x_i$ für alle j.

$\{x_1, \dots, x_n\}$ l.u. über K $\Rightarrow$ $a_{ij} = 0$ für alle i, j. □

Bemerkung 7.11 $L \supseteq K$ Körpererweiterung und $S \subseteq L$ Teilmenge

Analog zu Def. 5.5 für Gruppen:

$$K(S) := \bigcap_{\substack{K' \subseteq L \text{ Teilkörper} \\ \text{mit } K \subseteq K',\ S \subseteq K'}} K'$$

ist ein Teilkörper von L, "Adjunktion von S zu K"

und dies ist der kleinste Teilkörper von L, der S (und K) enthält

(a) Ist $S = \{z\}$ und z algebraisch ∞ $K(S) = K(z)$, Satz 7.9

denn: Jedes K' wie oben enthält z und alle Elemente von K, also auch $f(z)$ für alle $f \in K[X] \Rightarrow K(z) \subseteq K'$. Aber $K(z)$ Körper $\Rightarrow K(z)$ kommt im Schnitt vor $\Rightarrow K(S) = K(z)$.

(b) Sei $|S| < \infty$ und alle Elemente von S über K algebraisch.

Schreibe $S = \{z_1, \dots, z_r\}$ und bilde

$$K_1 = K(z_1), \quad K_2 = K_1(z_2), \dots, \quad K_r = K_{r-1}(z_r)$$

Dann gilt $K(S) = K_r$ und $[K(S) : K] < \infty$.

Insbesondere ist also auch $K(S) \supseteq K$ eine algebraische Erweiterung

Denn: $[K_1 : K] = \text{Grad}(\mu_{z_1}) < \infty$ also $K_1 \supseteq K$ algebraisch.

z_2 algebraisch über K mit Minimalpolynom $\mu_{z_2} \in K[X]$

μ_{z_2} auch Polynom in $K_1[X]$ also z_2 algebraisch über K_1

Sei f_2 = Minimalpolynom von z_2 über $K_1 \Rightarrow f_2 \mid \mu_{z_2}$ in $K_1[X]$.

$[K_2 : K_1] = \text{grad}(f_2) < \infty$.

Gradsatz $[K_2 : K] = [K_2 : K_1] \cdot [K_1 : K] < \infty$.

fahre so fort $\Rightarrow \dots \Rightarrow [K_r : K] < \infty$.

Jedes K' wie oben enthält $z_1, \dots, z_r$ und alle Elemente von K.

also $K' \supseteq K(z_1) = K_1$, dann auch $K' \supseteq K_1(z_2) = K_2$ etc.

also $K' \supseteq K_r$. Aber K_r selbst Körper, kommt also im Schnitt über alle K' vor $\Rightarrow K_r = K(S)$.

Leicht zu sehen: $K(S) = \{ f(z_1, \dots, z_r) \mid f \in K[X_1, \dots, X_r] \}$ ☒

Polynome in r Unbestimmten

siehe Beisp. 4.11.

Folgerung 7.12 Seien K, L, M Körper so daß wir Körpererweiterungen $L \supseteq M$ und $M \supseteq K$ haben. Dann gelt:

$L \supseteq M$ algebraisch und $M \supseteq K$ algebraisch $\Rightarrow$ $L \supseteq K$ algebraisch

Beweis: Sei $z \in L$. $L \supseteq M$ algebraisch $\Rightarrow$ ex. $0 \neq f \in M[X]$ mit $f(z) = 0$. Sei $f = a_0 + a_1 X + \dots + a_n X^n \in M[X]$ mit $n \geq 1$, $a_i \in M$.

Jedes $a_i \in M$ nach Vor. algebraisch über K.

Bem. 7.11. $M' := K(a_0, \dots, a_n) \supseteq K$ endliche Erweiterung. und $f \in M'[X]$ also z algebraisch über M' mit $[M'(z) : M'] \leq \mathrm{Grad}(f) < \infty$.

Gradsatz:

$$\Rightarrow [M'(z) : K] = \underbrace{[M'(z) : M']}_{<\infty} \cdot \underbrace{[M' : K]}_{<\infty} < \infty.$$

also alle Elemente von $M'(z)$ algebraisch über K. □

Folgerung 7.13 Sei $L \supseteq K$ Körpererweiterung. Dann ist $\{z \in L \mid z \text{ algebraisch über } K\}$ ein Teilkörper von L.

Beweis: Seien $u, v \in L$ $(u \neq 0)$ algebraisch über K. Heissen zeigen: $u \pm v$, $u \cdot v$, u^{-1} wieder algebraisch über K. Sei w eines dieser Elemente. Dann $w \in K(u, v)$

Nach Bem. 7.11 ist $K(u,v)$ algebraisch über K, also auch w □

Beisp. 7.14 Betrachte $\mathbb{Q} \subseteq \mathbb{C}$ (a) Beh.: $\mathbb{Q}(i + \sqrt{2}) = \mathbb{Q}(i, \sqrt{2})$.

Dazu: Haben in Beisp. 7.7(c) gesehen, daß $i + \sqrt{2}$ algebraisch ist, Minimalpolynom hat kleinstes Grad 4. Klar: $\mathbb{Q}(i+\sqrt{2}) \subseteq \mathbb{Q}(i, \sqrt{2})$.

$\mathbb{Q}(i, \sqrt{2}) \supseteq (\mathbb{Q}(\sqrt{2}))(i) \supseteq \underbrace{\mathbb{Q}(\sqrt{2}) \supseteq \mathbb{Q}}_{\text{Grad 2}}$.

Gradsatz: $[\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}] = 4$.

i Nullstelle von $X^2 + 1 \in \mathbb{Q}(\sqrt{2})[X]$

$i \notin \mathbb{Q}(\sqrt{2}) \Rightarrow$ $X^2 + 1$ Minimalpolynom von i über $\mathbb{Q}(\sqrt{2})$

$\mathbb{Q} \subseteq \mathbb{Q}(i+\sqrt{2}) \subseteq \mathbb{Q}(i,\sqrt{2})$ Grad = 4

Gradsatz: Entweder $\mathbb{Q}(i+\sqrt{2}) = \mathbb{Q}(i,\sqrt{2})$ oder $[\mathbb{Q}(i+\sqrt{2}) : \mathbb{Q}] = 2$

Annahme: $[\mathbb{Q}(i+\sqrt{2}) : \mathbb{Q}] = 2$

Satz 7.9 Sei $z = i+\sqrt{2}$. Dann Grad$(\mu_z) = 2$.

z Nullstelle $\Rightarrow$ $\bar{z} = -i+\sqrt{2}$ auch Nullstelle.

Sei $\mu_z = X^2 + aX + b \in \mathbb{Q}[X]$

also $\mu_z = (X-i-\sqrt{2})(X+i-\sqrt{2}) = ((X-\sqrt{2})-i)((X-\sqrt{2})+i) = (X-\sqrt{2})^2 - i^2$

$= X^2 - 2\sqrt{2}X + 2 + 1 \notin \mathbb{Q}[X]$ ↯.

Also $\mathbb{Q}(i+\sqrt{2}) = \mathbb{Q}(i,\sqrt{2})$ und damit auch $\mu_z = f = X^4 - 2X^2 + 9$

siehe Beisp. 7.7(c)

(b) $\bar{\mathbb{Q}} = \{ z \in \mathbb{C} \mid z$ algebraisch über $\mathbb{Q} \}$ ist ein Teilkörper von $\mathbb{C}$.

Zählargument wie in Beisp. 7.7 (b): $\bar{\mathbb{Q}}$ abzählbar $\Rightarrow [\mathbb{C} : \bar{\mathbb{Q}}] = \infty$.

aber auch $[\bar{\mathbb{Q}} : \mathbb{Q}] = \infty$ denn z.B. $\sqrt[n]{2} \in \bar{\mathbb{Q}}$ für alle $n \in \mathbb{N}$

$[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] =$ Grad (Minimalpolynom von $\sqrt[4]{2}$) $= n$.

$= X^4 - 2$ (Eisenstein $p=2$).

§8 Eine Anwendung: Konstruktionen mit Zirkel und Lineal

Klassische Probleme der antiken Mathematik:

- Quadratur des Kreises (konstruiere aus einem gegebenen Kreis ein Quadrat mit gleichem Flächeninhalt)
- Dreiteilung des Winkels (unterteile einen gegebenen Winkel in genau 3 gleich große Teile)
- Würfelverdoppelung (konstruiere aus einem gegebenen Würfel einen Würfel mit doppeltem Volumen)

Konstruktion: "Euklidische Werkzeuge": in endlich vielen Schritten nur mit Zirkel und Lineal.

Lösung erst im 19. Jahrhundert: Gauß, Galois, Wantzel (1837)

+ Lindemann's Beweis der Transzendenz von π.

Siehe wikipedia: "Würfelverdoppelung" und folge den Links auf dieser Seite

(Zugé Folien bzw. mit laptop)

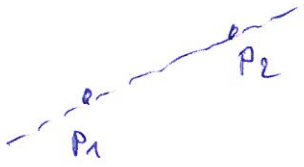
Idee der Lösung Übersetze geometrische Fragestellung in eine algebraisches Problem (über Körper, Zahlé etc.)

Müssen dazu präzisieren, was genau "Konstruktion mit Zirkel und Lineal" sind. Sei $P_0 \subseteq \mathbb{R}^2$.

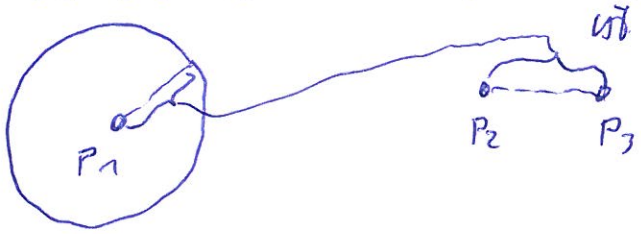
Zwei elementare Konstruktionsschritte:

(L) Durch 2 verschiedene Punkte von P_0 zieht eine Gerade

(Z) Schlage einen Kreis um einen Punkt aus P_0, wobei der Radius der Abstand zweier verschiedener Punkte aus P_0 ist



bzw.



Def. 8.1 Sei $P_0 \subseteq \mathbb{R}^2$ gegeben. Werden stets annehmen, daß die "Startpunkte" $(1,0), (0,1)$ zu P_0 gehören.

(a) Sei $(x,y) \in \mathbb{R}^2$. Wir sagen, daß (x,y) aus P_0 elementar konstruierbar ist, wenn (x,y) Schnittpunkt von 2 verschiedenen Geraden wie in (L) ist, oder Schnittpunkt einer Geraden wie in (L) und eines Kreises wie in (Z), oder Schnittpunkt von 2 verschiedenen Kreisen wie in (Z).

(b) $(x,y) \in \mathbb{R}^2$ heißt (mit Zirkel und Lineal) aus P_0 konstruierbar, wenn es $(x_1,y_1), \dots, (x_n,y_n) = (x,y)$ gibt, so daß jedes (x_i,y_i) für $1 \le i \le n$ aus $P_0 \cup \{(x_1,y_1), \dots, (x_{i-1},y_{i-1})\}$ elementar konstruierbar ist.

(c) $\mathrm{Kon}(P_0) \subseteq \mathbb{R}^2$ bezeichnet die Menge aller aus P_0 konstruierbaren Punkte in $\mathbb{R}^2$.

Lemma 8.2 Sei $P_0 \subseteq \mathbb{R}^2$ und $(x,y) \in \mathbb{R}^2$ elementar aus P_0 konstruierbar. Sei $K_0 = \mathbb{Q}(u,v \mid (u,v) \in P_0) \subseteq \mathbb{R}$.
Dann sind x, y Nullstellen von quadratischen Polynomen mit Koeffizienten in K_0, also $[K_0(x):K_0], [K_0(y):K_0] = 1$ oder 2.

Beweis: Müssen 3 Fälle betrachten.

(1) (x,y) Schnittpunkt von 2 Geraden.
(2) (x,y) Schnittpunkt eines Kreises und einer Geraden.
(3) (x,y) Schnittpunkt von 2 Kreisen.

Vorbetrachtung: Gerade G durch $(x_1,y_1), (x_2,y_2) \in P_0$.

$\Rightarrow G = \{(u,v) \in \mathbb{R}^2 \mid au + bv = c\}$ wobei $a = y_1 - y_2$, $b = x_2 - x_1$, $c = x_2 y_1 - x_1 y_2$. ✓

"Koordinatenform" Beachte: $a, b, c \in K_0$.

Kreis K mit Mittelpunkt $(x_0,y_0) \in P_0$ und Radius r = Abstand zwischen $(x_1,y_1), (x_2,y_2) \in P_0$.

$\Rightarrow K = \{(u,v) \in \mathbb{R}^2 \mid (u-x_0)^2 + (v-y_0)^2 = r^2\}$.

$r^2 = (x_2-x_1)^2 + (y_2-y_1)^2 \in K_0$.

zu 1) $G_1 = \{(u,v) \mid a_1 u + b_1 v = c_1\}$
$G_2 = \{(u,v) \mid a_2 u + b_2 v = c_2\}$

Schnittpunkt $\rightsquigarrow$ lineares Gleichungssystem $a_1 u + b_1 v = c_1$, $a_2 u + b_2 v = c_2$
mit eindeutiger Lösung Cramersche Regel $u, v \in K_0$ ✓.

zu 2) Schnittpunkte erfüllen $au + bv = c$, $(u-x_0)^2 + (v-y_0)^2 = r^2$?

1. Fall: $b \neq 0 \Rightarrow v = b^{-1}c - b^{-1}u$ setze ein

$$\underbrace{(u-x_0)^2 + (b^{-1}c - b^{-1}u - y_0)^2}_{\alpha u^2 + \beta u + \gamma = 0 \text{ mit } \alpha,\beta,\gamma \in K_0} = r^2 \in K_0$$

✓.

2. Fall: $a \neq 0$ analog.

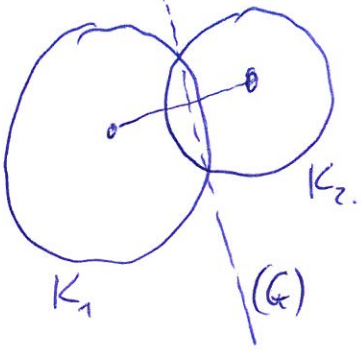
zu 3). Schreibe die beiden Gleichungen für Kreise K, K' an:

$u^2 + v^2 + du + ev + f = 0$
$u^2 + v^2 + d'u + e'v + f' = 0$

mit $d, d', e, e', f, f' \in K_0$
$d \neq d'$ oder $e \neq e'$.

Schnittpunkte $\Rightarrow$ $(d-d')u + (e-e')v + f - f' = 0$ (G)

Geradengleichung in Koordinatenform.



Schnittpunkte von K_1, K_2
= Schnittpunkte von K_1, G.
also OK nach Fall 2).

Satz 8.3 Sei $P_0 \subseteq \mathbb{R}^2$ und $(x,y) \in \mathbb{R}^2$ aus P_0 konstruierbar.
Sei $K_0 = \mathbb{Q}(u,v \mid (u,v) \in P_0) \subseteq \mathbb{R}$ Teilkörper wie oben.
Dann sind $[K_0(x) : K_0]$ und $[K_0(y) : K_0]$ 2-Potenzen

Beweis: Def. 8.1 $\Rightarrow$ ex. $(x_1,y_1), \dots, (x_n, y_n) = (x,y)$ so dass
jedes (x_i, y_i) aus $P_{i-1} := P_0 \cup \{(x_1,y_1), \dots, (x_{i-1}, y_{i-1})\}$
elementar konstruierbar ist.

Setze $K_1 = K_0(x_1,y_1)$, $K_2 = K_1(x_2,y_2), \dots, K_n = K_{n-1}(x_n,y_n)$.

$[K_n : K_0] = [K_0(x_1,y_1) : K_0] =$ (Gradsatz)
$= [(K_0(x_1))(y_1) : K_0(x_1)] \cdot [K_0(x_1) : K_0]$
jeweils 1 oder 2 nach Lemma 8.2

$= 1, 2$ oder 4

$[K_2 : K_1]$ = genauso $= 1, 2$ oder 4.
(((x_2,y_2) elementar aus P_1 konstruierbar))

$[K_n : K_{n-1}]$ = genauso $= 1, 2$ oder 4.
((x_n, y_n) elementar aus P_{n-1} konstruierbar)

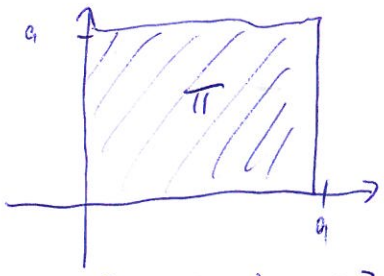
Also wiederum mit Gradsatz:
$[K_n : K_0] = [K_n : K_{n-1}] \cdots [K_1 : K_0] =$ 2-Potenz

Schließlich: $[K_n : K_0] = [K_n : K_0(x)] \cdot [K_0(x) : K_0]$
2-Potenz $\Rightarrow$ $[K_0(x) : K_0]$ 2-Potenz, genauso für $[K_0(y) : K_0]$ ∎

Beisp. 8.4 Quadratur des Kreises ist unmöglich.

Genauer formuliert: Gegeben sei Kreis mit Mittelpunkt $(0,0)$ und Radius 1.

Konstruiere mit Zirkel und Lineal die Ecken eines Quadrats, dessen Flächeninhalt gleich π ist.



$\Rightarrow$ $a = \sqrt{\pi}$ also muss $(\sqrt{\pi}, 0)$ mit Zirkel und Lineal konstruierbar sein (aus $P_0 = \{(0,0), (1,0)\}$.)

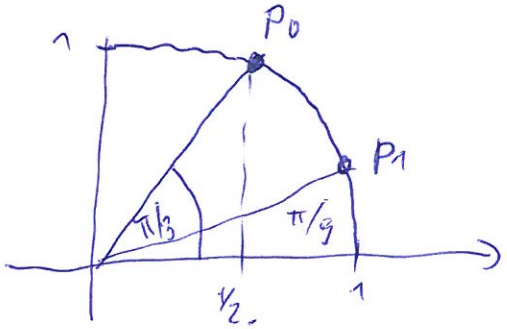
$\Rightarrow$ $[\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}] = 2$- Potenz nach Satz 8.3

$\Rightarrow$ $\sqrt{\pi}$ algebraisch über $\mathbb{Q}$ $\Rightarrow$ π algebraisch über $\mathbb{Q}$

$\lightning$ zum Satz von Lindemann (1882). dass π transzendent über $\mathbb{Q}$ ist.

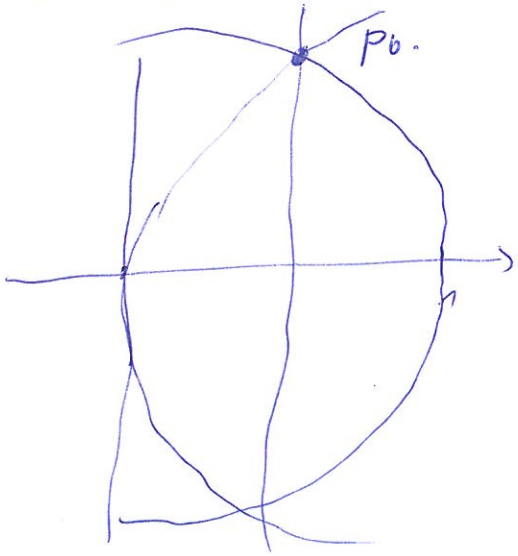
Beisp. 8.5 Winkeldreiteilung ist i.A. unmöglich

Betrachte den Winkel $\pi/3$ ($60°$ grad).



P_0 mit Zirkel und Lineal aus $\{(0,0), (0,1)\}$ konstruierbar.

Gerade durch $x = 1/2$ Schnittpunkt von 2 Kreisen



Annahme: P_1 konstruierbar

Satz 8.3 $\Rightarrow$ $[\mathbb{Q}(\cos \pi/9) : \mathbb{Q}] =$ 2-Potenz.

$\cos \pi/9$: x-Koordinate von P_1.

Müssten also Minimalpolynom von $\cos(\pi/9)$ bestimmen:

Dazu sei $\alpha = \pi/9$ $\quad e^{i\alpha} = \cos\alpha + i \sin\alpha$.

$(\cos\alpha + i\sin\alpha)^3 = (e^{i\alpha})^3 = e^{3i\alpha} = \underbrace{\cos(3\alpha)}_{=1/2} + i \sin(3\alpha)$

Linke Seite: $(\cos\alpha + i\sin\alpha)^3 = (\cos\alpha)^3 + 3(\cos\alpha)^2 i\sin\alpha$
$- 3(\cos\alpha)(\sin\alpha)^2 - i(\sin\alpha)^3$.

$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$

Realteil ist $(\cos\alpha)^3 - 3(\cos\alpha)(\sin\alpha)^2$

$= (\cos\alpha)^3 - 3(\cos\alpha)(1-(\cos\alpha)^2) =$

$= 4(\cos\alpha)^3 - 3\cos\alpha.$

Realteil rechte Seite $= \frac{1}{2}$.

$8X^3 - 6X - 1$

Also gilt $f(\cos\alpha) = 0$ für $f =$

Betrachte: $z = 2\cos\alpha \Rightarrow g(z) = 0$ für $g = X^3 - 3X - 1$.

$g(X+1) = (X+1)^3 - 3(X+1) - 1 = X^3 + 3X^2 + 3X + 1 - 3X - 3 - 1 = X^3 + 3X^2 - 3$

wend. Eisenstein $p = 3$

$\Rightarrow$ g irreduzibel (siehe Ü6A2).

$\Rightarrow$ $[\mathbb{Q}(z):\mathbb{Q}] = 3 \Rightarrow [\mathbb{Q}(\cos\alpha):\mathbb{Q}] = 3$ ↯

$\neq$ 2-Potenz.

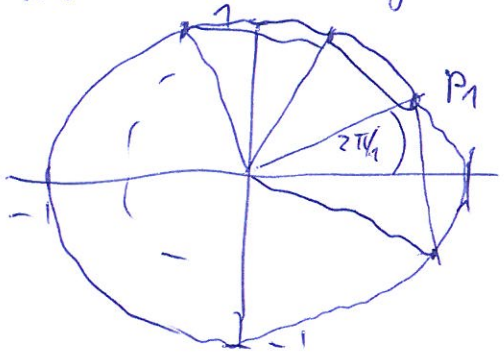
Beisp. 8.6 Würfelverdoppelung ist unmöglich.

Damit ist gemeint: Gegeben Würfel mit Kantenlänge 1
konstruiere mit Zirkel und Lineal Kantenlänge eines
Würfels mit Volumen $= 2$

Müssten also $(\sqrt[3]{2}, 0)$ mit Zirkel und Lineal
konstruieren. Satz 8.3 $\Rightarrow$ $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]$ = 2-Potenz.

↑ Minimalpolynom ist $X^3 - 2$
(Eisenstein $p = 2$)

Beisp. 8.7 Sei $n \geq 3$ und betrachte Teilung des Einheitskreises in n gleiche Teile: Erhalte regelmäßiges n-Eck.



Frage: Kann man Eckpunkte des regelmäßigen n-Ecks mit Zirkel und Lineal aus $\{(0,0),(0,1)\}$ konstruieren?

Annahme: Dies ist der Fall Satz 8.3

$\Rightarrow$ $[\mathbb{Q}(\cos\frac{2\pi}{n}) : \mathbb{Q}] =$ 2-Potenz $\quad P_1 = (\cos\frac{2\pi}{n}, \sin\frac{2\pi}{n})$.

$[\mathbb{Q}(\sin\frac{2\pi}{n}) : \mathbb{Q}] =$ 2-Potenz

Sei $z_n = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n} = e^{2\pi i/n} \in \mathbb{C}$.

Nun beachte: $z_n \in \mathbb{Q}(\cos\frac{2\pi}{n}, \sin\frac{2\pi}{n}, i)$.

$[\mathbb{Q}(\cos\frac{2\pi}{n}, \sin\frac{2\pi}{n}) : \mathbb{Q}(\cos\frac{2\pi}{n})] = 1$ oder 2

$(\sin\alpha)^2 + (\cos\alpha)^2 = 1$

$\Rightarrow$ $[\mathbb{Q}(\cos\frac{2\pi}{n}, \sin\frac{2\pi}{n}, i) : \mathbb{Q}] = \underbrace{[\mathbb{Q}(\cos\frac{2\pi}{n}, \sin\frac{2\pi}{n}, i) : \mathbb{Q}(\cos\frac{2\pi}{n}, \sin\frac{2\pi}{n})]}_{= 1 \text{ oder } 2 \text{ wegen } i^2 = -1}$

$\cdot \underbrace{[\mathbb{Q}(\cos\frac{2\pi}{n}, \sin\frac{2\pi}{n}) : \mathbb{Q}]}_{= [\mathbb{Q}(\cos\frac{2\pi}{n}, \sin\frac{2\pi}{n}) : \mathbb{Q}(\cos\frac{2\pi}{n})] \cdot [\mathbb{Q}(\cos\frac{2\pi}{n}) : \mathbb{Q}]}$

$= 1$ oder 2 (2-Potenz)

Also $\underbrace{\mathbb{Q}(\cos\frac{2\pi}{n}, \sin\frac{2\pi}{n}, i) \supseteq \mathbb{Q}(z_n) \supseteq \mathbb{Q}}$.

Grad = 2-Potenz.

$\Rightarrow$ $[\mathbb{Q}(z_n) : \mathbb{Q}] =$ 2-Potenz.

z_n Nullstelle von Φ_n = n-tes Kreisteilungspolynom. (Def. 5.13)

Angenommen, wir wüßten, daß Φ_n zerfällt.

Dann $\underbrace{[\mathbb{Q}(z_n) : \mathbb{Q}]}_{\text{2-Potenz}} = \text{Grad}(\Phi_n) = \varphi(n)$ Euler-Funktion

also $\varphi(n) =$ 2-Potenz.

$n = p_1^{n_1} \cdots p_r^{n_r} \Rightarrow \varphi(n) = (p_1 - 1) p_1^{n_1 - 1} \cdots (p_r - 1) p_r^{n_r - 1}$

$1 < p_1 \leq \ldots \leq p_r$. (Formel in Bem. 6.3).

$\Rightarrow$ $n = 2^{n_1} p_2 \cdots p_r$ wobei $n_1 \geq 1$ und. $p_i \geq 3$ Primzahl

so daß $p_i - 1 =$ 2-Potenz

Solche Primzahlen heißen auch Fermatsche Primzahlen.

z.B. $3 = 2+1$, $5 = 2^2+1$, $17 = 2^4+1$, $257 = 2^6+1$,
$65537 = 2^{16}+1$ Es ist nicht bekannt, ob es noch weitere gibt!

Gauß 1796: z_n mit Zirkel und Lineal konstruierbar
(19 Jahre alt) $\Leftrightarrow$ $\varphi(n)$ ist eine 2-Potenz

Erster Fortschritt zu klassischen Problemen der Antike seit 2000 Jahren!

Insbesondere: Regelmäßiges 17-Eck konstruierbar.

88 (Kronecker 1854)
Satz (Gauß) Für alle $n \geq 1$ ist das n-te Kreisteilungspolynom $\Phi_n \in \mathbb{Q}[X]$ irreduzibel. (Def. 5.13).

Beweis: Da $\mathbb{Z}[X]$ faktoriell und $\mathbb{Q}$ Quotientenkörper ist, genügt es zu zeigen, daß $\Phi_n \in \mathbb{Z}[X]$ irreduzibel ist.

Sei $\Phi_n = f \cdot g$ mit $f, g \in \mathbb{Z}[X]$ normiert. Können annehmen, daß f irreduzibel ist und $f(z_n) = 0$ gilt. ($\operatorname{grad}(f) \geq 1$.)

Sei weiterhin $E_n = \{z \in \mathbb{C} \mid z^n = 1\} = \langle z_n \rangle$.

Beh.: (*) Sei $z \in E_n$ und p Primzahl mit $p \nmid n$.
Dann gilt: $f(z) = 0 \Rightarrow f(z^p) = 0$

Daraus folgt der Satz, denn sei $d \in \{1, \dots, n\}$ beliebig mit $\operatorname{ggT}(d, n) = 1$
schreibe $d = p_1 \cdots p_k$ mit Primzahlen p_i (es kann $p_i = p_j$ für $i \neq j$ gelten) $\Rightarrow$ $p_i \nmid n$ für alle i:

Nun: $f(z_n) = 0 \overset{(*)}{\Longrightarrow} f(z_n^{p_1}) = 0$ Wende (*) auf $z = z_n^{p_1}$ an $\Rightarrow$ $f(z^{p_2}) = 0$ also $z^{p_2} = z_n^{p_1 p_2}$ ebenfalls Nullstelle von f.
usw. $\Rightarrow$ $z_n^{p_1 p_2 p_3}, \dots, z_n^{p_1 p_2 \cdots p_k}$ sind Nullstellen von f.
Also ist z_n^d Nullstelle von f $\Rightarrow$ f hat mindestens $\varphi(n)$ Nullstellen. $\operatorname{Grad}(\Phi_n) = \varphi(n) \Rightarrow f = \Phi_n$ V.

Müssen also noch (*) zeigen. Sei also $z \in E_n$ mit $f(z)=0$ und p Primzahl mit $p \nmid n$. Wegen $f(z)=0$ ist auch $\Phi_n(z)=0$ also $E_n = \langle z \rangle$ Wegen $p \nmid n$ dann auch $E_n = \langle z^p \rangle$ siehe Lemma 5.7. also $\Phi_n(z^p)=0$. Wegen $\Phi_n = f \cdot g$ also $f(z^p)=0$ oder $g(z^p)=0$.

Annahme: $f(z^p) \neq 0$. Dann also $g(z^p)=0$

Also z Nullstelle von $\tilde{g} := g(X^p) \in \mathbb{Z}[X]$.

Beh.: $f \mid \tilde{g}$ in $\mathbb{Z}[X]$.

Dann: f normiert ird. und $f(z)=0 \Rightarrow f$ = Minimalpolynom von z

Wegen $\tilde{g}(z)=0$ also $f \mid \tilde{g}$ in $\mathbb{Q}[X]$. Schreibe $\tilde{g} = fh$ mit $h \in \mathbb{Q}[X]$

Sei $0 \neq c \in \mathbb{Z}$ mit $\hat{h} := ch \in \mathbb{Z}[X] \Rightarrow c\tilde{g} = (ch)f = \hat{h}f$ Gleichung in $\mathbb{Z}[X] \Rightarrow f \mid c\tilde{g}$ in $\mathbb{Z}[X]$ Lemma 4.8 $\Rightarrow f \mid \tilde{g}$ in $\mathbb{Z}[X]$ ✓.

Nun reduzieren mod p. Sei $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ $h \in \mathbb{Z}[X] \rightsquigarrow \bar{h} \in \mathbb{F}_p[X]$

$\bar{\Phi}_n = \bar{f} \cdot \bar{g}$ und $\bar{f} \mid \bar{\tilde{g}} = \overline{g(X^p)}$ Sei $g = \sum_j b_j X^j$ mit $b_j \in \mathbb{Z}$

$$\Rightarrow \overline{g(X^p)} = \sum_j b_j X^{jp} = \sum_j \bar{b}_j X^{jp} = \sum_j \bar{b}_j^{\,p} X^{jp} = \sum_j (b_j X^j)^p$$

$$= \Big(\sum_j \bar{b}_j X^j\Big)^p = \bar{g}^p$$ kleiner Satz von Fermat

Ü8

Also gilt $\bar{f} \mid \bar{g}^p$ in $\mathbb{F}_p[X]$. Sei $f_1 \in \mathbb{F}_p[X]$ ird. Faktor von $\bar{f}$

$\Rightarrow f_1 \mid \bar{g}^p \Rightarrow f_1 \mid \bar{g}$ Weil auch $f_1 \mid \bar{f}$ folgt damit

$f_1^2 \mid \bar{\Phi}_n$ in $\mathbb{F}_p[X]$. $\Rightarrow f_1^2 \mid X^n - \bar{1}$ in $\mathbb{F}_p[X]$, d.h.

$X^n - \bar{1} \in \mathbb{F}_p[X]$ hat mehrfachen Faktor $\Leftrightarrow f_1 \mid D(X^n - \bar{1}) = \bar{n} X^{n-1} \neq 0$

$\neq 0$ weil $p \nmid n$.

Ü7 A1

$f_1 \mid X^n - 1$ und $f_1 \mid X^{n-1} \Rightarrow f_1 = \text{const.}$ ↯

Damit Satz vollständig bewiesen. □

Beisp. 8.9 Sei $p \geq 2$ Primzahl. $\Rightarrow X^p - 1 = (X-1)\Phi_p$

$\Rightarrow \Phi_p = X^{p-1} + \dots + X + 1 \in \mathbb{Z}[X]$ irreduzibel.

Dieser Spezialfall wurde schon von Gauß 1801 bewiesen.

§9 Zerfällungskörper

Sei K Körper und $0 \neq f \in K[X]$ nicht konstant. Sei $L \supseteq K$ Erweiterungskörper. Wir sagen, daß f in L in Linearfaktoren zerfällt, wenn gilt

$$(*) \qquad f = c\,(X-\alpha_1)^{n_1}(X-\alpha_2)^{n_2}\cdots(X-\alpha_r)^{n_r}$$

mit $0 \neq c \in K$, $n_i \geq 1$, $\alpha_i \in L$ paarweise verschieden.

Ist $n_i = 1$, so heißt α_i eine einfache Nullstelle von f.

Ist $n_i > 1$, so heißt α_i eine mehrfache Nullstelle von f.

Gilt $(*)$ und außerdem $L = K(\alpha_1, \dots, \alpha_r)$ so heißt L Zerfällungskörper von f.

Beisp. 9.1 (a) $L = \mathbb{C}$ ist Zerfällungskörper von $f = X^2+1 \in \mathbb{R}[X]$ denn $X^2+1 = (X+i)(X-i)$ und $\mathbb{C} = \mathbb{R}(i, -i) = \mathbb{R}(i)$

(b) Sei $n \geq 2$ und $z_n = e^{2\pi i/n} \in \mathbb{C}$. $\Phi_n \in \mathbb{Q}[X]$ n-tes Kreisteilungspolynom $\Phi_n = \prod_{ggT(d,n)=1} (X - z_n^d)$ also $L = \mathbb{Q}(z_n)$ $[L:\mathbb{Q}] = \varphi(n)$. Zerfällungskörper von Φ_n.

(c) Sei $f = X^2 + pX + q \in \mathbb{Q}[X]$ Quadratische Ergänzung $f = (X + p/2)^2 - D/4$ mit Diskriminante $D = p^2 - 4q$.

Sei $L = \mathbb{Q}(\sqrt{D}) \subseteq \mathbb{C} \Rightarrow$ L Zerfällungskörper von f.

$$[L:\mathbb{Q}] = \begin{cases} 1 & \text{falls } D \text{ ein Quadrat in } \mathbb{Q} \text{ ist} \\ 2 & \text{sonst.} \end{cases}$$

(d) Sei $L = \mathbb{Q}(\sqrt[4]{2}) \supseteq \mathbb{Q}$ $z = \sqrt[4]{2}$ hat Minimalpolynom $f = X^4 - 2$ (Eisenstein mit $p=2$). aber L ist nicht Zerfällungskörper von f, denn $f = X^4 - 2 = (X^2 - \sqrt{2})(X^2 + \sqrt{2})$

$$= (X - \sqrt[4]{2})(X + \sqrt[4]{2})(X - i\sqrt[4]{2})(X + i\sqrt[4]{2})$$

Nullstellen $\pm i\sqrt[4]{2}$ liegen nicht in L!

Zerfällungskörper ist $L' = \mathbb{Q}(\sqrt[4]{2}, i\sqrt[4]{2}) = \mathbb{Q}(\sqrt[4]{2}, i)$.

$L' = \mathbb{Q}(\sqrt[4]{2}, i) \supseteq \mathbb{Q}(\sqrt[4]{2}) \supseteq \mathbb{Q}$.

i Nullstelle von X^2+1 — Grad $= 4$.

aber $i \notin \mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{R}$ $\Rightarrow$ $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})] = 2$

Gradsatz $[L' : \mathbb{Q}] = 8$.

Beisp. 9.2 Die Formeln von Gerolamo Cardano (1545)

siehe wikipedia "Cardanische Formeln"

Sei $f = X^3 + aX^2 + bX + c \in \mathbb{R}[X]$ Zwischenwertsatz der reellen Analysis:

$\lim_{x \to +\infty} f(x) = +\infty$ $\lim_{x \to -\infty} f(x) = -\infty$ $\Rightarrow$ ex. $x \in \mathbb{R}$ mit $f(x) = 0$.

Formeln für Nullstellen?

1. Schritt: Ersetze $X \to x+d$. Dann

$f(X+d) = (X+d)^3 + a(X+d)^2 + b(X+d) + c = X^3 + 3dX^2 + 3dX^2 + d^3 + aX^2 + 2adX + ad^2 + bX + bd + c$

$= X^3 + (3d+a)X^2 + \ldots$ setze $d = -a/3$. Dann wird Koeff von X^2 gleich 0.

Also genügt es:

2Schritt. Betrachte $f = X^3 + pX + q$.

Sei z Nullstelle von f Ansatz $z = u+v$.

$z^3 = (u+v)^3 = u^3 + 3u^2v + 3uv^2 + v^3 = 3uv\underbrace{(u+v)}_{=z} + u^3 + v^3$

$\Rightarrow$ $z^3 \underbrace{- 3uv}_{=p} z \underbrace{- (u^3+v^3)}_{=q} = 0$. $uv = -p/3$

$u^3 + v^3 + q = 0$ $\Rightarrow$ $u^6 + \underbrace{u^3v^3}_{= -(p/3)^3} + qu^3 = 0$

Setze $t = u^3$ Dann erhält man quadratische Gleichung

$t^2 - (p/3)^3 + qt = 0$.

Lösung $t_{1,2} = -q/2 \pm \sqrt{(\frac{q}{2})^2 + (\frac{p}{3})^3}$

$u = \sqrt[3]{-q/2 \pm \sqrt{(\frac{q}{2})^2 + (\frac{p}{3})^3}}$

$v^3 = q - u^3 = q - t_{1,2} = -\frac{q}{2} \mp \sqrt{(\frac{q}{2})^2 + (\frac{p}{3})^3}$

$v = \sqrt[3]{-\frac{q}{2} \mp \sqrt{(\frac{q}{2})^2 + (\frac{p}{3})^3}}$

Müssen dabei u, v so wählen, dass $uv = -p/3$ gilt.

Beachte: $u^3 v^3 = (-p/3)^3$ also gibt dies immer $(uv)^3$

Also:

$$z = \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}$$

Produkt $= -p/3$

$\rightsquigarrow$ 3 Möglichkeiten

$\Rightarrow uv = -p/3\, \varepsilon$ wobei ε = 3-te Einheitswurzel.

$\Rightarrow (\varepsilon^{-1} u)\, v = -p/3$.

↑ modifiziere so das u!

Setze $\Delta := \left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3$

(Selbststudium):

$\Delta > 0$: 1 reelle Lösungen sowie 2 komplex konjugierte.

$\Delta = 0$: 3 reelle Lösungen (von denen 2 gleich sind oder sogar alle 3).

$\Delta < 0$: 3 verschiedene reelle Lösungen

siehe auch wikipedia-Artikel.

Bsp:

$X^3 + 6X - 20 \rightarrow \Delta > 0$

$X^3 - 3X - 2 \rightarrow \Delta = 0$

$X^3 - 3X - 1 \rightarrow \Delta < 0$

} schreiben Sie alle Lösungen jeweils explizit hin!

Zusammenfassung: Für $f = X^3 + pX + q \in \mathbb{Q}[X]$ gibt es stets einen Zerfällungskörper $L \subseteq \mathbb{C}$, $L = \mathbb{Q}(z_1, z_2, z_3)$

μ_{z_1} = Min. Pol. von z_1 $\Rightarrow$ $[\mathbb{Q}(z_1) : \mathbb{Q}] \leq 3$.

$\Rightarrow \mu_{z_1} \mid f \Rightarrow \operatorname{Grad}(\mu_{z_1}) \leq 3$

$f = (X - z_1)\, g$ mit $\operatorname{grad}(g) = 2$, $g \in \mathbb{Q}(z_1)[X]$

Lösungen von g durch quadratische Gleichung siehe Bsp. 9.1.(c)

also $[\mathbb{Q}(z_1, z_2, z_3) : \mathbb{Q}(z_1)] \leq 2$.

Gradsatz: $[L : \mathbb{Q}] \leq 2 \cdot 3 = 6$.

Analoge Formeln gibt es auch für Polynome vom Grad 4 (Ludovico Ferrari)

Für beliebige Polynome brauchen wir ein abstraktes Argument!

Satz 9.3 Sei K Körper und $0 \neq f \in K[X]$ mit $n = \mathrm{Grad}(f) \geq 1$.
Dann gibt es einen Zerfällungskörper $L \supseteq K$ von f mit $[L:K] \leq n!$

Beweis: Induktion nach n. Ist $n=1$, so $f = aX+b$ mit $a \neq 0$
$\Rightarrow -a^{-1}b \in K$ einzige Nullstelle von $f \Rightarrow L = K$ Zerfällungskörper.
Sei nun $n \geq 2$ und $f_1 \in K[X]$ normiert irred. mit $f_1 \mid f$
Setze $K_1 = K[X]/(f_1) = \{ \bar{g} = g + (f_1) \mid g \in K[X] \}$
$K[X]$ Hauptidealring + f_1 irred. $\Rightarrow K_1$ Körper siehe Lemma 3.9
Abbildung $K \to K_1$, $a \mapsto \bar{a}$, injektiv denn
$\bar{a} = \bar{b} \Rightarrow a + (f_1) = b + (f_1) \Rightarrow a - b \in (f_1) \Rightarrow f_1 \mid \underbrace{a-b}_{\in K}$ $\Rightarrow a = b$
($\uparrow$ Grad ≥ 1)
außerdem $\overline{a \pm b} = \bar{a} \pm \bar{b}$
Können also K als Teilkörper von K_1 auffassen (schreibe einfach a anstelle von $\bar{a}$) Sei $z_1 := \bar{X} \in K_1$.
Sei $g \in K[X]$ bel., $g = b_0 + b_1 X + \dots + b_m X^m$ mit $b_i \in K$.
$\Rightarrow \bar{g} = \bar{b}_0 + \bar{b}_1 X + \dots + \bar{b}_m \bar{X}^m = b_0 + b_1 z_1 + \dots + b_m z_1^m = g(z_1)$.
Für $g = f_1$ erhalte $f_1(z_1) = \bar{f}_1 = \bar{0}$ also f_1 Minimalpolynom von z_1 über K
Satz 7.9: $K_1 = K(z_1)$ und
$[K_1 : K] = \mathrm{Grad}(f_1) \leq n$.
Wegen $f_1 \mid f$ gilt auch $f(z_1) = 0$ Schreibe $f = (X - z_1)h$
mit $h \in K_1[X]$, $\mathrm{Grad}(h) = n-1$. Nach Induktion gibt es
Zerfällungskörper $L \supseteq K_1$ von h mit $[L : K_1] \leq (n-1)!$
Nun $L = K_1(\underbrace{z_2, \dots, z_n}_{\text{Nullstellen von } h}) = K(z_1)(z_2, \dots, z_n) = K(z_1, \dots, z_n)$
Also $L \supseteq K$ Zerfällungskörper von f und
$[L:K] = \underbrace{[L:K_1]}_{\leq (n-1)!} \cdot \underbrace{[K_1:K]}_{\leq n} \leq n!$ nach Gradsatz $\square$

Bem. 9.4(a) Sei $K = \mathbb{Q} \subseteq \mathbb{C}$. "Fundamentalsatz der Algebra":
Jedes $0 \neq f \in \mathbb{C}[X]$ zerfällt in Linearfaktoren über $\mathbb{C}$
(siehe z.B. Analysis-Vorlesung). Ist also $0 \neq f \in \mathbb{Q}[X]$ nichtkonstant, so können wir stets Zerfällungskörper $L \subseteq \mathbb{C}$

finden. Siehe oben Beisp. Polynome vom Grad 3.
Werden später Fundamentalsatz hier beweisen, aber dazu brauchen wir zuerst abstrakte Existenzaussage in Satz 9.3

(b) Im obigen Beweis wurde Satz 7.9 verwendet. Wir halten das noch einmal fest:

Sei $L \supseteq K$ Zerfällungskörper von $0 \neq f \in K[X]$
Sei $f_1 \in K[X]$ normiert irreduzibel und $f_1 | f$.
Sei $z_1 \in L$ Nullstelle von f_1. Dann
$K \subseteq K(z_1) \subseteq L$.

Außerdem: $[K(z_1) : K] = \mathrm{Grad}(f_1) = d$ siehe Satz 7.9

und $K[X]/(f_1) \cong K(z_1)$ siehe Beweis von 7.9

$\bar{g} = g + (f_1) \longmapsto g(z_1)$

$\{1, z_1, z_1^2, \dots, z_1^{d-1}\}$ K-Basis von $K(z_1)$

Außerdem: Betrachtet man dann weitere Nullstellen von f_1, so kann man L Schritt für Schritt aufbauen: $K \subseteq K(z_1) \subseteq K(z_1, z_2) \subseteq \dots \subseteq L$.

Bem. 9.5 Sei K Körper, $0 \neq f \in K[X]$ nicht-konstant und $L \supseteq K$ Zerfällungskörper von f. Wir sagen, daß f vielfachheitsfrei ist, wenn f in L nur einfache Nullstellen hat, also

$f = c(X - z_1) \cdots (X - z_n)$ mit $0 \neq c \in K$, $z_i \in L$
$z_i \neq z_j$ für $i \neq j$
$n = \mathrm{Grad}(f)$.

Dies kann man mit der formalen Ableitung $D(f)$ testen, ohne zuerst L und die z_i zu berechnen!

Nämlich; es gilt: f vielfachheitsfrei $\Longleftrightarrow$

$D(f) \neq 0$ und f, $D(f)$ teilerfremd in $K[X]$

Beweis "$\Leftarrow$": f, $D(f)$ teilerfremd $\Rightarrow$ 1 ist ggT von f, $D(f)$.
also Eukl. Algorithmus $\Rightarrow$ es gibt $g, h \in K[X]$ mit

$1 = gf + hD(f)$

Annahme: f hat mehrfache Nullstelle in L

d.h. es gibt $z \in L$ mit $f = (X-z)^2 \tilde{f}$ mit $\tilde{f} \in L[X]$

Berechne $D(f)$ in $L[X]$: $D(f) = 2(X-z)\tilde{f} + (X-z)^2 D(\tilde{f})$

also $D(f)(z) = 0 \Rightarrow 1 = g(z) f(z) + h(z) D(f)(z) = 0$ ↯

"$\Rightarrow$": Sei $f = (X-z_1)g$ mit $g \in L[X]$ f vielfachheitsfrei $\Rightarrow g(z_1) \neq 0$

Nun $D(f) = g + (X-z_1) D(g)$ also $D(f)(z_1) = g(z_1) \neq 0$

Insbesondere $D(f) \neq 0$. Sei $0 \neq d \in K[X]$ ggT von $f, D(f)$

Dann: d nicht konstant. Wegen $d \mid f$ gibt es also $z_1 \in L$ mit $d(z_1) = 0$

Wegen $d \mid D(f)$ dann auch $D(f)(z_1) = 0$ ↯ s.o. (Nullstelle von f) □

Beisp 9.6 Sei K ein endlicher Körper, $K_0 \subseteq K$ Primkörper

Satz 7.4 $\Rightarrow$ $K_0 \cong \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ für eine Primzahl p.

Wegen $|K| < \infty$ gilt außerdem $n = [K : K_0] < \infty$.

(7.8A2) $\Rightarrow$ $|K| = p^n$.

Jetzt betrachte multiplikative Gruppe $K^\times$: $|K^\times| = |K| - 1 = p^n - 1$.

Lagrange: $\beta^{p^n - 1} = 1$ für alle $0 \neq \beta \in K$.

also $\beta^{p^n} = \beta$ für alle $\beta \in K$.

Sei $f = X^{p^n} - X \in K_0[X]$. Dann ist jedes $\beta \in K$ Nullstelle von f, Grad $(f) = p^n = |K|$ also $f = \prod_{\beta \in K} (X - \beta)$.

Also: K Zerfällungskörper von f.

Bemerke: f vielfachheitsfrei. Dies kann man auch mit formaler Ableitung sehen: $D(f) = \underbrace{p^n}_{=0 \text{ in } K} \cdot X^{p^n - 1} - 1 = -1$

also $D(f) \neq 0$ und $f, D(f)$ teilerfremd.

Folgerung 9.7 Sei K beliebiger Körper, $A \in K^{m \times n}$ und $b \in K^m$

Dann hat das lineare Gleichungssystem $Ax = b$ entweder keine Lösung, oder genau eine Lösung, oder unendlich viele Lösungen oder die Anzahl der Lösungen ist eine Primzahlpotenz. Insbesondere: Es gibt kein lineares

Gleichungssystem mit genau 6 Lösungen.
(beliebte Frage in mündlichen Prüfungen, ...)

Beweis: Selbst. □

Satz 9.8 (Hauptsatz über endliche Körper)
Sei p eine Primzahl und $n \geq 1$. Dann gibt es einen Körper K mit $|K| = p^n$, und alle diese Körper sind zueinander isomorph. Außerdem gilt: $K^\times$ ist zyklisch, es gibt also ein $\alpha \in K^\times$ mit $K^\times = \langle \alpha \rangle$. Ist $\mu_\alpha \in K_0[X]$ Minimalpolynom von α (wobei $K_0 \cong \mathbb{F}_p$ Primkörper von K), so gilt

$$K \cong K_0[X]/(\mu_\alpha) \quad \text{und} \quad \operatorname{Grad}(\mu_\alpha) = n.$$

Insbesondere: Es gibt ein irred. Polynom vom Grad n in $\mathbb{F}_p[X]$.

Beweis: Betrachte $f = X^{p^n} - X \in \mathbb{F}_p[X]$. Sei $L \supseteq \mathbb{F}_p$ Zerfällungskörper von f (siehe Satz 9.3). Setze

$$K := \{z \in L \mid z^{p^n} = z\} = \{z \in L \mid f(z) = 0\}.$$

$\operatorname{Grad}(f) = p^n \Rightarrow |K| \leq p^n$. Wegen $D(f) = p^n X^{p^n-1} - 1 = -1$ sind $f, D(f)$ teilerfremd, also hat f genau p^n verschiedene Nullstellen in L also gilt $|K| = p^n$.

Klar: $z, z' \in K \Rightarrow zz' \in K$. $0 \neq z \in K \Rightarrow z^{-1} \in K$.

ÜA 2: $(z \pm z')^{p^n} = z^{p^n} \pm z'^{p^n} = z \pm z'$ für alle $z, z' \in K$.

$\Rightarrow$ K Teilkörper von L, aber K enthält bereits alle Nullstellen von f, also $K = L$. Körper mit p^n Elementen.

Jetzt betrachte $K^\times$. Nach Folg. 5.10: $K^\times$ zyklisch, also existiert $0 \neq \alpha \in K$ mit $K^\times = \langle \alpha \rangle = \{1, \alpha, \alpha^2, \dots, \alpha^{p^n-2}\}$.

$\Rightarrow$ $K = \mathbb{F}_p(\alpha)$. Sei $\mu_\alpha \in \mathbb{F}_p[X]$ Minimalpolynom von α.

Bem. 9.4: $K \cong \mathbb{F}_p[X]/(\mu_\alpha)$ und $\operatorname{Grad}(\mu_\alpha) = [K : \mathbb{F}_p] = n$.

Beachte auch:

$\mu_\alpha(\alpha) = 0$ und $f(\alpha) = 0 \Rightarrow \mu_\alpha \mid f$ in $\mathbb{F}_p[X]$

Sei nun K' weiterer Körper mit $|K'| = p^n$. Ebenfalls Primkörper $K_0' \cong \mathbb{F}_p$ (identifiziere $K_0' = \mathbb{F}_p = \{\bar{0}, \bar{1}, \dots, \overline{p-1}\}$.

Beisp. 9.6 $X^{p^n} - X = \prod_{\beta' \in K'} (X - \beta') \in K'[X]$.

Haben oben gesehen: $\mu_\alpha \mid X^{p^n} - X$ also ex. $\alpha' \in K'$ mit $\mu_\alpha(\alpha') = 0$

$\Rightarrow$ $\mu_\alpha \in \mathbb{F}_p[X]$ Minimalpolynom von α' über $\mathbb{F}_p$.

$\mathbb{F}_p(\alpha') \subseteq K'$ Teilkörper

Nach Satz 7.9. $[\mathbb{F}_p(\alpha') : \mathbb{F}_p] = \operatorname{Grad}(\mu_\alpha) = n$ also

$\mathbb{F}_p(\alpha') = K'$ weil auch $[K' : \mathbb{F}_p] = n$.

Damit erhalten wir einen Isomorphismus: (siehe Bem. 9.4):

$$K = \mathbb{F}_p(\alpha) \cong \mathbb{F}_p[X]/(\mu_\alpha) \cong \mathbb{F}_p(\alpha') = K'$$

$$g(\alpha) \longrightarrow g(\alpha').$$

$(g \in \mathbb{F}_p[X])$

□.

Beisp. 9.9 (a) Sei $p = 2$ und $n = 2$. $f = X^2 + X + 1 \in \mathbb{F}_2[X]$ irreduzibel

also $K = \mathbb{F}_2[X]/(f)$ Körper mit 4 Elementen.

Sei $\alpha := \bar{X} \in K$ Dann $K = \{\bar{0}, \bar{1}, \alpha, \alpha^2\}$.

$(|K^\times| = 3 \Rightarrow \alpha^3 = \bar{1})$

+	$\bar{0}$	$\bar{1}$	α	α^2
$\bar{0}$	$\bar{0}$	$\bar{1}$	α	α^2
$\bar{1}$	$\bar{1}$	$\bar{0}$	α^2	α
α	α	α^2	0	$\bar{1}$
α^2	α^2	α	$\bar{1}$	0

·	$\bar{0}$	$\bar{1}$	α	α^2
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	α	α^2
α	$\bar{0}$	α	α^2	$\bar{1}$
α^2	$\bar{0}$	α^2	$\bar{1}$	α

✓

Es gilt $f(\alpha) = 0$ also $\alpha^2 + \alpha + 1 = 0$ also $\alpha^2 = \alpha + 1$.

siehe auch Ü5 A5 $\alpha = \alpha^2 + 1$.

$1 = \alpha + \alpha^2$

(b) Sei $p = 3$ und $n = 2$ $f = X^2 + 1 \in \mathbb{F}_3[X]$

irreduzibel (hat keine Nullstelle in $\mathbb{F}_3$).

also $K = \mathbb{F}_3[X]/(f)$ Körper mit 9 Elementen.

Sei $\alpha = \bar{X} \in K$ Dann $K = \{a + b\alpha \mid a, b \in \mathbb{F}_3\}$.

beachte: $|K^\times| = 8$ und $\alpha^2 = -1$ also $K^\times \neq \langle \alpha \rangle$!

	$\bar{0}$	$\bar{1}$	$\bar{2}$	α	$\bar{1}+\alpha$	$\bar{2}+\alpha$	$\bar{2}\alpha$	$\bar{1}+2\alpha$	$\bar{2}+2\alpha$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	α	$1+\alpha$	$2+\alpha$	2α	$1+2\alpha$	$2+2\alpha$
$\bar{1}$		2	0	$1+\alpha$	$2+\alpha$	α	$1+2\alpha$	$2+2\alpha$	2α
$\bar{2}$			1	$2+\alpha$	α	$1+\alpha$	$2+2\alpha$	2α	$1+2\alpha$
α				2α	$1+2\alpha$	$2+2\alpha$	0	1	2
$\bar{1}+\alpha$					$1+2\alpha$	2α	1	2	0
$\bar{2}+\alpha$						$1+\alpha$	2	0	1
$\bar{2}\alpha$							α	$1+\alpha$	$2+\alpha$
$\bar{1}+2\alpha$								$2+\alpha$	α
$\bar{2}+2\alpha$									$1+\alpha$

	$\bar{0}$	$\bar{1}$	$\bar{2}$	α	$1+\alpha$	$2+\alpha$	2α	$1+2\alpha$	$2+2\alpha$
0	0	0	0	0	0	0	0	0	0
1		1	2	α	$1+\alpha$	$2+\alpha$	2α	$1+2\alpha$	$2+2\alpha$
2			1	2α	$2+2\alpha$	$1+2\alpha$	α	$2+\alpha$	$1+\alpha$
α				2	$\alpha+2$	$2\alpha+2$	1	$\alpha+1$	$2\alpha+1$
$1+\alpha$									
$2+\alpha$									
2α									
$1+2\alpha$									
$2+2\alpha$									

$\alpha^2 = -\bar{1} = \bar{2}$

usw.

Also hier: Addition einfach mod. "schieben"

Bemerkung: Wenn man ein anderes Polynom vom Grad 2 wählt, so kann man nicht erreichen, daß $K^\times = \langle \alpha \rangle$ gilt

z.B. $f = X^2 + X - 1 \in \mathbb{F}_3[X]$ (keine Nullstelle in $\mathbb{F}_3$) irreduzibel.

$\alpha = \bar{X} \in K = \mathbb{F}_3[X]/(f)$.

$f(\alpha) = 0$ also $\alpha^2 + \alpha - 1 = 0$.

$\alpha^2 = 1 - \alpha$.

$|K^\times| = 8$

$\alpha^4 = (1-\alpha)^2 = 1 - 2\alpha + \alpha^2 = 1 - 2\alpha + 1 - \alpha$

$= 2 - 3\alpha = -1$.

$\alpha^8 = (-1)^2 = 1$ ✓

also $K^\times = \langle \alpha \rangle$

und damit:

$K = \{\bar{0}, \bar{1}, \bar{2}, \alpha, \alpha^2, \alpha^3, \alpha^5, \alpha^6, \alpha^7\}$.
α^4

und man kann Verknüpfungstabelle mini (es) aufstellen.

d.h. Multiplikation einfach, Addition "schwierig".

Fortsetzung der Körpertheorie:
Ordne Erweiterung $L \supseteq K$ eine Gruppe G zu.

Bem. 9.10 Seien L_1, L_2 Körper. Dann sind L_1, L_2 kommutative Ringe und wir haben den Begriff des Ring-Homomorphismus $\varphi: L_1 \to L_2$, d.h. $\varphi(x \pm y) = \varphi(x) \pm \varphi(y)$ für alle $x, y \in L_1$ und $\varphi(1_{L_1}) = 1_{L_2}$.

Bsp.: φ ist automatisch injektiv:
denn sei $x \neq x'$ in L_1 mit $\varphi(x) = \varphi(x')$. $\Rightarrow \varphi(x - x') = \varphi(x) - \varphi(x') = 0$.
Setze $0 \neq z := x - x' \in L_1$ Körper $\Rightarrow$ es $z^{-1} \in L_1$. Dann

$$1_{L_2} = \varphi(1_{L_1}) = \varphi(z \cdot z^{-1}) = \varphi(z) \cdot \varphi(z^{-1}) = \underbrace{\varphi(x - x')}_{=0} \cdot \varphi(z^{-1}) = 0 \quad \lightning$$

Ist φ auch surjektiv, so heißt φ ein Körper-Isomorphismus.
Ist φ Isom. und $L_1 = L_2$, so heißt φ auch ein Automorphismus.
Sei schließlich K Körper mit $K \subseteq L_1, L_2$ so daß wir Körpererweiterungen $K \subseteq L_1$ und $K \subseteq L_2$ haben.
Dann heißt φ ein K-Isomorphismus, wenn $\varphi: L_1 \to L_2$ Isomorphismus wie oben und $\varphi(x) = x$ für alle $x \in K$ gelt.
In diesem Fall ist φ K-linear, denn für $x \in K$, $z \in L_1$ gelt:

$$\varphi(x \cdot z) = \varphi(x) \cdot \varphi(z) = x \cdot \varphi(z) \quad \checkmark$$

Def. 9.11 Sei $L \supseteq K$ Körpererweiterung. Dann setze

$$\mathrm{Aut}(L, K) := \{\varphi: L \to L \mid \varphi \text{ } K\text{-Isomorphismus}\}.$$

Bsp.: $\varphi \in \mathrm{Aut}(L, K) \Rightarrow \varphi^{-1} \in \mathrm{Aut}(L, K)$.
$\varphi, \psi \in \mathrm{Aut}(L, K) \Rightarrow \varphi \circ \psi \in \mathrm{Aut}(L, K)$

Also ist $\mathrm{Aut}(L, K)$ eine Gruppe mit Hintereinanderausführung $\circ$ als Verknüpfung, neutrales Element ist $\mathrm{id}: L \to L$.
$\mathrm{Aut}(L, K)$ heißt Automorphismengruppe von $L \supseteq K$.
Ist L Zerfällungskörper eines nicht konstanten Polynoms $f \in K[X]$, so heißt $\mathrm{Aut}(L, K)$ auch Galois-Gruppe von f.
Zu Ehren von E. Galois (1811–1832) → wikipedia

Beisp. 9.12 Sei $L = \mathbb{C} \supseteq K = \mathbb{R}$.

$\mathbb{C} = \{x + iy \mid x, y \in \mathbb{R}\}$. $-: \mathbb{C} \to \mathbb{C}$ komplexe Konjugation ist ein $\mathbb{R}$-Automorphismus

Also $\mathrm{Aut}(\mathbb{C}, \mathbb{R}) \supseteq \{id, -\}$. Gibt es noch weitere?

Sei $\varphi: \mathbb{C} \to \mathbb{C}$ bel. $\mathbb{R}$-Autom. Dann $-1 = \varphi(-1) = \varphi(i^2) = \varphi(i)^2$

also $\varphi(i) = \pm i$ Ist $\varphi(i) = i$ so $\varphi = id$

Ist $\varphi(i) = -i$ so $\varphi = -$

also $\mathrm{Aut}(\mathbb{C}, \mathbb{R}) = \{id, -\}$ Gruppe mit 2 Elementen.

Bem. 9.13 Sei $L \supseteq K$ Körpererweiterung, $0 \neq f \in K[X]$ und $\varphi \in \mathrm{Aut}(L, K)$. Sei $z \in L$. Dann gilt:

$$f(z) = 0 \Rightarrow f(\varphi(z)) = 0$$

denn: $f = a_0 + a_1 X + \dots + a_n X^n \in K[X]$ Dann

$f(z) = a_0 + a_1 z + \dots + a_n z^n$ also $\varphi(f(z)) = \varphi(a_0) + \varphi(a_1)\varphi(z) + \dots + \varphi(a_n)\varphi(z)^n$

$\varphi|_K = id|_K \Rightarrow \varphi(f(z)) = a_0 + a_1 \varphi(z) + \dots + a_n \varphi(z)^n = f(\varphi(z))$.

Also gilt ganz allgemein: $\boxed{\varphi(f(z)) = f(\varphi(z))}$.

Ist $f(z) = 0$, so also auch $f(\varphi(z)) = \varphi(f(z)) = \varphi(0) = 0$ ✓

Folgerung 9.14 Sei $L \supseteq K$ Körpererweiterung mit $[L:K] < \infty$.

Dann ist $\mathrm{Aut}(L, K)$ eine endliche Gruppe.

Beweis: Sei $n = [L:K] < \infty$ und $\{z_1, \dots, z_n\}$ eine K-Basis von L.

Sei $f_i \in K[X]$ Minimalpolynom von z_i für $1 \leq i \leq n$. Setze

$f := f_1 \cdots f_n \in K[X]$ Sei $d := \mathrm{Grad}(f) \geq 1$.

Sei $\varphi \in \mathrm{Aut}(L, K)$. Bem. 9.10: φ K-linear, also eindeutig bestimmt durch Werte auf Basis $\{z_1, \dots, z_n\}$.

Bem. 9.13 $\Rightarrow$ $f(\varphi(z_i)) = \varphi(\underbrace{f(z_i)}_{=0}) = 0$

d.h. $\varphi(z_i)$ muß weitere Nullstelle von f sein; davon gibt es höchstens d in L, also: es gibt höchstens d Möglichkeiten für $\varphi(z_i)$. Dies gilt für $1 \leq i \leq n \Rightarrow$

$$|\mathrm{Aut}(L, K)| \leq d^n$$

(werden später bessere Abschätzung finden!) □

Def. 9.15 Sei K Körper und $0 \neq f \in K[X]$ nicht-konstant.
Wir sagen, daß f durch Radikale auflösbar ist, wenn sich die Nullstellen von f (in einem Zerfällungskörper L von f) sich durch wiederholtes Wurzelziehen und die üblichen Körperoperationen $+, -, \cdot, /$ ausdrücken lassen, genauer: es gibt eine Folge von Körpererweiterungen

$$K \subseteq K_1 = K(a_1) \subseteq K_2 = K_1(a_2) \subseteq \dots \subseteq K_r = K_{r-1}(a_{r-1})$$

so daß $a_i^{n_i} \in K_{i-1}$ mit $n_i \geq 1$ für alle i gilt

und $L \subseteq K_r$.

Beisp: (a) $f = X^2 + pX + q$ $\quad \Delta = p^2 - 4q$.

Zerfällungskörper enthalten in $K_1 = K(\sqrt{\Delta})$. (a_1)

(b) $f = X^3 + pX + q$ $\quad \Delta = \left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3$

Zerfällungskörper enthalten in $K \subseteq K_1 = K(a_1) \subseteq K_2 = K_1(a_2) \subseteq K_3 = K_2(a_3)$

wobei $a_1^2 = \Delta \in K_1$ und $a_2^3 = -\frac{q}{2} + a_1 \in K_1$

$a_3^3 = -\frac{q}{2} - a_1 \in K_2$.

siehe Cardano's Formeln.

Abel-Ruffini (1799/1824): Für $n \geq 5$ gibt es Polynome $f \in \mathbb{Q}[X]$ mit $\operatorname{Grad}(f) = n$, die sich nicht durch Radikale auflösen lassen.

[unvollständiger Beweis.

Heutiger Beweis: Galois (1830):

$f \in K[X]$ ist durch Radikale auflösbar, wenn die Galoisgruppe $\operatorname{Aut}(L, K)$ (L = Zerfällungskörper von f) eine "lösbare" Eigenschaft besitzt → § 10.

Insbesondere: Ist f so daß $n = \operatorname{Grad}(f) \geq 5$ und $\operatorname{Aut}(L, K) \cong S_n$, so ist f nicht durch Radikale auflösbar.

Konkrete Polynome, die nicht durch Radikale auflösbar sind.

(1) Sei p Primzahl und $0 \neq f \in \mathbb{Q}[X]$ irreduzibel mit $\text{Grad}(f) = p$. Hat f genau $p-2$ reelle und 2 komplex konjugierte Nullstellen, so ist $\text{Gal}(L, \mathbb{Q}) \cong S_p$.

z. B. $p = 5$ und $f = X^5 - 16X - 2$
(und mit Eisenstein $p = 2$ + Kenntnis komplexe)

(2) Sei $n \geq 2$ und $f_n = X^n - X - 1 \in \mathbb{Q}[X]$
Dann ist f_n irreduzibel (Selmer 1956)
und $\text{Gal}(f, \mathbb{Q}) \cong S_n$ (Ohada 1987).

Schließlich: "Umkehrproblem der Galoistheorie":
Gegeben eine endliche Gruppe G. Gibt es ein Polynom $0 \neq f \in \mathbb{Q}[X]$ so daß $\text{Gal}(L, \mathbb{Q}) \cong G$?

z.B. $G = S_n$ Antwort JA (s.o.).
Problem offen in Allgemeinen !?

$\rightsquigarrow$ Vorlesung "Galois-Theorie"

Plan: Seminar dazu im WiSe 18/19 aufbauend auf dieser Vorlesung.

Rest dieser Vorlesung: Grundlagen aus der Gruppentheorie
Insbesondere: Was ist die "berühmte" Eigenschaft im Satz von Galois?

§10 Normalteiler und Gruppen-Homomorphismen

11. Woche

Erinnerung: Faktorstrukturen §2 $\mathbb{Z}/d\mathbb{Z}$, R/I — R kommutativer Ring, $I \trianglelefteq R$ Ideal

Wollen dies nun allgemein für Gruppen einführen.

Sei G Gruppe, $U \leq G$ Untergruppe.

§5 $a \sim_U b \overset{\text{def}}{\Leftrightarrow} a^{-1}b \in U$ Äquivalenzrelation

$(a, b \in G)$ Äquivalenzklassen $[a] = aU = \{au \mid u \in U\}$.

Linksnebenklasse von a nach U.

$G/U = \{aU \mid a \in G\}$

Menge der Linksnebenklassen. analog zu §2 definiere

Verknüpfung auf G/U durch $G/U \times G/U \to G/U$

$(aU, bU) \mapsto abU$.

wie üblich müssen wir zeigen, daß dies "wohldefiniert" ist

Def 10.1 $U \leq G$ heißt Normalteiler von G, in Zeichen $N \trianglelefteq G$, wenn $g^{-1}ug \in U$ für alle $g \in G$ und $u \in U$ gilt

Klar: $\{1\}$ und G sind Normalteiler

Ist G abelsch, so ist jedes $U \leq G$ ein Normalteiler.

Satz 10.2 Sei G Gruppe, $U \trianglelefteq G$ Normalteiler. Dann ist auch G/U eine Gruppe mit Verknüpfung wie oben.

Neutrales Element: $1 \cdot U$ Inverses: $(aU)^{-1} = a^{-1}U$.

G/U heißt Faktorgruppe von G nach U.

Beweis: Verknüpfung wohldef., denn seien $a, a', b, b' \in G$ und

$aU = a'U$, $bU = b'U$. zu zeigen: $abU = a'b'U$.

$u := a^{-1}a' \in U$ $v := b^{-1}b' \in U$. also $a' = au$, $b' = bv$.

$\Rightarrow (ab)^{-1}a'b' = b^{-1}a^{-1}a'b' = b^{-1}a^{-1}aubv = \underbrace{b^{-1}ubv}_{\in U \trianglelefteq G} \in U$ ✓

also $abU = a'b'U$ ✓.

Dann folgt auch sofort Assoziativität:

$(aU)(bUcU) = (aU)(bcU) = a(bc)U = (ab)cU = (abU)(cU) = (aUbU)cU$ ✓

$1U$ neutrales Element ✓ $(aU)(a^{-1}U) = 1 \cdot U$, also $a^{-1}U = (aU)^{-1}$ □

Bem. 10.3 Sei $U \leq G$. Dann gelt: $U \trianglelefteq G \Leftrightarrow gU = Ug$ für alle $g \in G$.
(also: jede Linksnebenklasse ist auch Rechtsnebenklasse und umgekehrt).

Beweis: "$\Rightarrow$" Sei $g \in G$ und $u \in U$. Dann ist
$gu = \underbrace{gug^{-1}}_{\in U} g \in Ug$ also $gU \subseteq Ug$.
genauso $Ug \subseteq gU$ also insgesamt $Ug = gU$.
"$\Leftarrow$" Sei $g \in G$ und $u \in U$. Dann $gu = vg$ für ein $v \in U$.
also $gug^{-1} = vgg^{-1} = v \in U$ ✓ ∎

Beisp. 10.4 (a) Sei $G = S_3$ Beisp. 5.4. alle Untergruppen von G.
$\{id\}$ und G sind Normalteiler. Sei nun $U \leq G$, $\{id\} \neq U \neq G$
$\Rightarrow |U| = 2$ oder $|U| = 3$.
$|U| = 2 \rightsquigarrow$ 3 Möglichkeiten $U = \langle \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} \rangle$ oder $\langle \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} \rangle$ oder $\langle \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} \rangle$.
Sei $U = \langle \underbrace{\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}}_{=u} \rangle$ $g = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} \Rightarrow g^{-1} = g$ und

$$g^{-1}ug = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} \notin U \text{ also}$$

U kein Normalteiler, genauso für die beiden anderen.
Damit kann man auch sehen, daß G/U keine Gruppe mit obiger Verknüpfung ist!
$|U| = 3 \rightsquigarrow$ genau 1 Möglichkeit $U = \{id, \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}, \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\}$.
Dann $U \trianglelefteq G$ denn $[G:U] = 2$ siehe (b)
(b) Sei $U \leq G$ mit $[G:U] = 2$. Beh. $U \trianglelefteq G$.
Dann sei $g \in G$ bel. Ist $g \in U$, so $gU = U = Ug$ ✓.
Sei nun $g \notin U$ Dann $gU \neq U$, $Ug \neq U$ und damit
$G = U \dot\cup gU$ Zerlegung in Linksnebenklassen nach U
$= U \dot\cup Ug$ ——— Rechts———
also auch hier $gU = Ug$. Bem. 10.3 $\Rightarrow U \trianglelefteq G$.
(c) $G = Q_8$ Quaternionengruppe $\leq GL_2(\mathbb{C})$ siehe Ü1 A3.
$|G| = 8$ und G nicht abelsch.
$G = \{\pm I, \pm J, \pm K, \pm E\}$ $I^2 = J^2 = K^2 = IJK = -E$

E Einheitsmatrix. Sei $U \subseteq G$, $\{E\} \neq U \neq G$. Lagrange
$|U| = 2$ oder 4 $\quad [G:U] = 2 \Rightarrow U \trianglelefteq G$ nach b)
$|U| = 2 \Rightarrow U = \{\pm E\}$. E = Einheitsmatrix $\Rightarrow g(\pm E)g^{-1} = \pm E$
also $U \trianglelefteq G$. für alle $g \in GL_2(\mathbb{C})$

Damit $G = Q_8$ nicht abelsch, aber trotzdem sind alle Untergruppen Normalteiler.

Def. 10.5 Seien G, H Gruppen und $\varphi: G \to H$ ein Gruppen-Homomorphismus also $\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)$ für alle $g_1, g_2 \in G$.
Dann heißt (automatisch $\varphi(1_G) = 1_H$)

$\operatorname{Kern}(\varphi) := \{g \in G \mid \varphi(g) = 1_H\}$ der Kern von φ.
$\operatorname{Bild}(\varphi) := \{\varphi(g) \mid g \in G\}$ das Bild von φ.

Man sieht sofort: $\operatorname{Kern}(\varphi)$ Untergruppe von G
$\operatorname{Bild}(\varphi)$ Untergruppe von H.

Außerdem: $x \in \operatorname{Kern}(\varphi)$ und $g \in G$ bel.
$\Rightarrow \varphi(gxg^{-1}) = \varphi(g)\varphi(x)\varphi(g^{-1}) = \varphi(g)\,1_H\,\varphi(g)^{-1} = \varphi(g)\varphi(g)^{-1} = 1_H$.
also auch $gxg^{-1} \in \operatorname{Kern}(\varphi)$ und damit
$\operatorname{Kern}(\varphi) \trianglelefteq G$.

Beisp. 10.6 Sei G Gruppe und $U \trianglelefteq G$ Normalteiler.
Sei $H := G/U$ Faktorgruppe. Dann ist
$\pi_U: G \to H,\ g \mapsto gU$
ein surjektiver Homomorphismus mit $\operatorname{Kern}(\pi_U) = U$.
π_U heißt "kanonischer Homomorphismus"

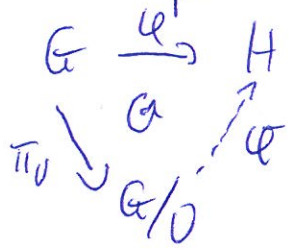
denn: π_U Homom.: $\pi_U(g_1 g_2) = g_1 g_2 U = (g_1 U)(g_2 U) = \pi_U(g_1)\pi_U(g_2)$
π_U surjektiv klar.
$\operatorname{Kern}(\pi_U) = \{g \in G \mid gU = \pi_U(g) = 1 \cdot U\} = \{g \in G \mid g \in U\} = U$. ✓

Satz 10.7 (Homomorphiesatz) Seien G, H Gruppen und $\varphi: G \to H$ ein Homomorphismus. Dann gibt es genau einen
Sei $U := \operatorname{Kern}(\varphi) \trianglelefteq G$.

Homomorphismus $\bar{\varphi}: G/U \to H$ mit $\varphi = \bar{\varphi} \circ \pi_U$

φ ist injektiv und $\text{Bild}(\varphi) = \text{Bild}(\bar{\varphi})$

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



Beweis: Wir definieren $\bar{\varphi}: G/U \to H,\ gU \mapsto \varphi(g)$

zeige zuerst: wohldefiniert Seien also $g, g' \in G$ mit $gU = g'U$.

Dann $g^{-1}g' \in U = \text{Kern}(\varphi)$, also $1 = \varphi(g^{-1}g') = \varphi(g)^{-1}\varphi(g')$

also $\varphi(g) = \varphi(g')$ ✓.

$\bar{\varphi}$ Homom, denn $\bar{\varphi}(gU \cdot g'U) = \bar{\varphi}(gg'U) = \varphi(gg') = \varphi(g)\varphi(g')$

$= \bar{\varphi}(gU) \cdot \bar{\varphi}(g'U)$. ✓

$(\bar{\varphi} \circ \pi_U)(g) = \bar{\varphi}(\pi_U(g)) \overset{\text{Def. } \pi_U}{=} \varphi(gU) = \varphi(g)$ für alle $g \in G$

also $\varphi = \bar{\varphi} \circ \pi_U$.

Sei auch $\psi: G/U \to H$ Homom. mit $\varphi = \psi \circ \pi_U$.

Dann $\psi(gU) = \psi(\pi_U(g)) = (\psi \circ \pi_U)(g) = \varphi(g)$ für alle $g \in G$

also $\psi(gU)$ eindeutig festgelegt

$\text{Bild}(\varphi) = \text{Bild}(\bar{\varphi})$ klar $\quad \text{Kern}(\bar{\varphi}) = \{gU \in G/U \mid \underbrace{\bar{\varphi}(gU)}_{=\varphi(g)} = 1\}$

$= \{gU \mid g \in \text{Kern}(\varphi) = U\} = \{1 \cdot U\}$ also $\bar{\varphi}$ injektiv ☐

Bem. 10.8 Analoge Aussagen gelten auch für Ringe und Ideale

Seien also R, S (kommutative) Ringe und $\varphi: R \to S$ ein Ring-Homomorphismus. Dann ist

$\text{Kern}(\varphi) := \{r \in R \mid \varphi(r) = 0\}$ ein Ideal von R

und $\text{Bild}(\varphi) := \{\varphi(r) \mid r \in R\}$ ein Teilring von S

Sei $I := \text{Kern}(\varphi)$. Dann gibt es einen eindeutigen Ring-Homom. $\bar{\varphi}: R/I \to S$ mit $\varphi = \bar{\varphi} \circ \pi_I$

wobei $\pi_I: R \to R/I,\ r \mapsto r + I$, kanonischer Hom. ist

(Beweis völlig analog zum Beweis von Satz 10.7.)

Bem. 10.9 G, H Gruppen und $\varphi: G \to H$ Homomorphismus.
Dann gilt: φ injektiv $\iff$ $\mathrm{Kern}(\varphi) = \{1_G\}$

denn: "$\Rightarrow$" klar weil $\mathrm{Kern}(\varphi) = \{g \in G \mid \varphi(g) = 1_H = \varphi(1_G)\}$
"$\Leftarrow$" Seien $g, g' \in G$ mit $\varphi(g) = \varphi(g')$. $\Rightarrow$ $\varphi(g^{-1}g') = \varphi(1_G) = 1_H$.
$\Rightarrow g^{-1}g' \in \mathrm{Kern}(\varphi) = \{1_G\} \Rightarrow g = g'$. ✓

Beisp. 10.10 (a) Sei K Körper und $G := GL_n(K)$. Dann ist $\det: G \to K^\times$ ein Homomorphismus. (LAA G: $\det(AB) = \det(A)\det(B)$ und $\det(A) \neq 0 \iff A$ invertierbar)

$\mathrm{Kern}(\det) = \{A \in GL_n(K) \mid \det(A) = 1\} =: SL_n(K)$
"spezielle lineare Gruppe"

Für $0 \neq a \in K$ ist $\det\begin{pmatrix} a & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix} = a$, also $\det$ surjektiv;
Homomorphiesatz $GL_n(K)/SL_n(K) \cong K^\times$.

(b) Sei G zyklische Gruppe, also existiert $g \in G$ mit
$G = \langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$ siehe Beisp. 5.3.

Betrachte Gruppe $(\mathbb{Z}, +)$ und definiere $\varphi: \mathbb{Z} \to G, n \mapsto g^n$.
Dann φ surjektiver Homom. mit $\mathrm{Kern}(\varphi) = \{n \in \mathbb{Z} \mid g^n = 1\}$.
Sei $d := o(g)$ Ordnung von g. Ist $d = \infty$, so $g^m \neq 1$ für alle $m \in \mathbb{N}$, also auch $g^{-m} \neq 1$ für alle $m \in \mathbb{N}$.
Also $\mathrm{Kern}(\varphi) = \{0\}$ also φ Isomorphismus in diesem Fall:

$$G \cong (\mathbb{Z}, +)$$

Sei nun $d < \infty$. Beisp. 5.3: Ist $m \in \mathbb{Z}$ mit $g^m = 1$, so $d \mid m$.
also $\mathrm{Kern}(\varphi) = \{$alle Vielfachen von $d\} = d\mathbb{Z}$.
Homomorphiesatz: $G \cong \mathbb{Z}/d\mathbb{Z}$.

Alle zyklischen Gruppen sind also entweder isomorph zu $(\mathbb{Z}, +)$ oder zu $\mathbb{Z}/d\mathbb{Z}$ für ein $d \in \mathbb{N}$.

c) $\exp: (\mathbb{R}, +) \to (\mathbb{R}^\times, \cdot)$, $x \mapsto \exp(x)$, ist ein Homomorphismus:

Lemma 10.11 Sei G endliche Gruppe, $g \in G$ und $N \trianglelefteq G$. Ist $ggT(o(g), [G:N]) = 1$, so gilt $g \in N$.

Beweis: Betrachte kanonischen Homom. $\pi: G \to G/N$, $x \mapsto \bar{x} := xN$.

Sei $d = o(g) \Rightarrow g^d = 1 \Rightarrow \bar{g}^d = 1$, also $o(\bar{g}) \mid d$.
Außerdem $o(\bar{g}) \mid [G:U]$ (Lagrange)
$\Rightarrow ggT(d, [G:N]) = 1 \Rightarrow o(\bar{g}) = 1$.

d.h. $\bar{g} = 1$ also $g \in \ker(\pi) = N$ □

Def. 10.12 Sei G Gruppe. Dann heißt G auflösbar, wenn es eine Folge von Untergruppen gibt $\{1\} = U_0 \subseteq U_1 \subseteq \dots \subseteq U_r = G$ mit $U_{i-1} \trianglelefteq U_i$ und U_i / U_{i-1} abelsch für alle $i \geq 1$.

z.B.: G abelsch $\Rightarrow$ G auflösbar mit Folge $\{1\} = U_0 \subseteq U_1 = G$

Ursprung der Bezeichnung:
K Körper $f \in K[X]$ nicht-konstant, $L \supseteq K$ Zerf. körper

Satz von Galois: f durch Radikale auflösbar
(siehe §9) (d.h. Nullstellen kann man durch mehrfaches Wurzelziehen ausdrücken, wie z.B. in Cardano-Formeln)

$\Leftrightarrow$ $\mathrm{Gal}(L|K)$ ist auflösbar.

Haben dort erwähnt, daß es f gibt mit $\mathrm{Gal}(L|K) \cong S_n$ symmetrische Gruppe.

z.B. $K = \mathbb{Q}$, $f = X^n - X - 1$.

Also Frage: Wann ist S_n auflösbar.

Lemma 10.13 Sei G Gruppe und $U \subseteq G$ Untergruppe. Ist G auflösbar, so ist auch U auflösbar.

Beweis: Sei $\{0\} = U_0 \subseteq U_1 \subseteq \dots \subseteq U_r = G$ Folge für G.
Setze $U_i' := U \cap U_i \leq U$. Dann $\{0\} = U_0' \subseteq U_1' \subseteq \dots \subseteq U_r' = U$
Sei $1 \leq i \leq r$ fest. Betrachte kanonischen Homomorphismus
$\pi: U_i' \to U_i / U_{i-1}$, $x \mapsto xU_{i-1}$ (beachte: $U_i' = U \cap U_i \subseteq U_i$).

$\ker(\pi) = \{x \in U_i' \mid xU_{i-1} = 1 \cdot U_{i-1}\} = \{x \in U_i' \mid x \in U_{i-1}\} = U_i' \cap U_{i-1}$
$= U_i \cap U \cap U_{i-1} = U_{i-1}'$ also $U_{i-1}' \trianglelefteq U_i'$ und
Homomorphiesatz: U_i'/U_{i-1}' isom. zu Untergruppe von U_i/U_{i-1} ← abelsch! □

§11 Die symmetrische Gruppe

Sei $n \geq 1$ und S_n = symmetrische Gruppe vom Grad n
= alle Permutationen von $\{1, \dots, n\}$ mit $\circ$ als Verknüpfung.

$\pi \in S_n$ $\quad \pi = \begin{pmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ \pi(1) & \pi(2) & \pi(3) & \cdots & \pi(n-1) & \pi(n) \end{pmatrix}$

n Möglichkeiten für $\pi(1)$, dann noch $n-1$ für $\pi(2)$, dann $n-2$ für $\pi(3)$, schließlich noch 2 für $\pi(n-1)$ und 1 für $\pi(n)$.
also insgesamt $n \cdot (n-1) \cdots 2 \cdot 1$ Möglichkeiten, d.h.

$$|S_n| = n!$$

Erinnerung LAAG: $\operatorname{sgn}(\pi) = \pm 1$ Signum von π.

$N(\pi) := \{1 \leq i < j \leq n \mid \pi(i) > \pi(j)\}$ "Fehlstände" von π.

Dann $\operatorname{sgn}(\pi) = (-1)^{|N(\pi)|}$. Es gilt: $\operatorname{sgn}(\pi\pi') = \operatorname{sgn}(\pi)\operatorname{sgn}(\pi')$.

Also $\operatorname{sgn}: S_n \longrightarrow \{\pm 1\}$ Gruppen-Homomorphismus.

$A_n := \operatorname{Kern}(\operatorname{sgn}) \trianglelefteq S_n$ alternierende Gruppe.

Beachte: Für $n \geq 2$ betrachte $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 2 & 1 & 3 & 4 & \cdots & n \end{pmatrix} \in S_n$.

$\pi(1) = 2 > 1 = \pi(2)$

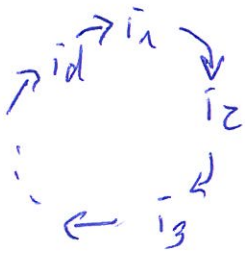
also $N(\pi) = \{1 < 2\}$ $\Rightarrow$ $\operatorname{sgn}(\pi) = -1$ also sgn surjektiv.

$S_n / A_n \cong \{\pm 1\}$ $\Rightarrow$ $2 = \dfrac{|S_n|}{|A_n|}$ $\Rightarrow$ $|A_n| = \frac{1}{2} n!$

(Für $n = 1$ ist $S_n = A_n = \{\mathrm{id}\}$)

Vereinfachte Schreibweise für Elemente von S_n.

Gegeben seien paarweise verschiedene Ziffern $i_1, \dots, i_d \in \{1, \dots, n\}$
Dann erhalten wir Permutation σ in S_n durch:



und $\sigma(i) = i$ für alle $i \notin \{i_1, \dots, i_d\}$

σ heißt d-Zyklus (oder einfach Zyklus)

Schreibe einfach $\sigma = (i_1 i_2 \cdots i_d)$

Beachte: Man kann an beliebiger Stelle im Kreis anfangen und erhält immer gleiche Permutation, also auch $\sigma = (i_2 i_3 \cdots i_d i_1)$ etc.

Potenzen von σ: Durch Kreis um 1, 2, etc. Kanten weiter.

$\Rightarrow$ **$\mathrm{ord}(\sigma) = d$** — d-Zyklus hat Ordnung d

z.B. $\sigma = (354) \in S_5$ 3-Zyklus.

$\sigma = \begin{pmatrix} 1 & 2 & 3 & 5 & 4 \\ 1 & 2 & 5 & 4 & 3 \end{pmatrix}$ $\quad \sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 5 & 3 \end{pmatrix} = (345)$

$\sigma^3 = id.$

Ein 2-Zyklus heißt auch Transposition $\sigma = (ij)$
vertauscht genau 2 Ziffern und lässt alle anderen fest.

1-Zyklus: Identität (alle Ziffern bleiben fest)

Jeder $\pi \in S_n$ lässt sich als Produkt von disjunkten Zyklen schreiben

z.B. $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 6 & 4 & 5 & 1 & 8 & 7 & 2 \end{pmatrix} \in S_8$.

$= (1\,3\,4\,5) \circ (2\,6\,8) \circ (7)$ — weglassen

↑ kleinste Ziffer

↑ kleinste Ziffer, die nicht in vorherigen Zyklen ist

Beachte: σ, τ disjunkte Zyklen $\Rightarrow \sigma \circ \tau = \tau \circ \sigma$ also Reihenfolge in Zyklendarstellung beliebig!

$\pi' = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 5 & 2 & 6 & 3 & 4 & 1 & 8 \end{pmatrix} \in S_8$

$= (1\,7) \circ (2\,5\,3)(4\,6) \circ (8)$ weglassen.

σ d-Zyklus $\Rightarrow$ σ Produkt von d-1 Transpositionen

denn sei $\sigma = (i_1 i_2 \ldots i_d) \Rightarrow \sigma = (i_1 i_2)(i_2 i_3) \cdots (i_{d-1} i_d)$
(wende beide Seiten auf Ziffer i an, erhalte gleiches Ergebnis).

$\sigma = (1\,3\,4\,5) = (13)(34)(45)$ ✓

Satz 11.1 Es gilt $S_n = \langle (ij) \mid 1 \le i < j \le n \rangle$, d.h.
S_n wird von Transpositionen erzeugt

Beweis: Sei $\pi \in S_n$ beliebig. Zerlege $\pi = \sigma_1 \circ \dots \circ \sigma_r$ mit disjunkten Zyklen σ_i. Dann schreibe jeden σ_i als Produkt von Transpositionen. □

Nun kann man auch $\operatorname{sgn}(\pi)$ für $\pi \in S_n$ leicht ausrechnen:

$\sigma = (i\,j)$ Transposition $i<j$. Dann $\sigma(i) = j > i = \pi(j)$ ~~beliebig~~ ⇝ Fehlständen ungerade Anzahl von ⇝ also $\operatorname{sgn}((i\,j)) = -1$. $(13) = \begin{pmatrix} 1&2&3 \\ 3&2&1 \end{pmatrix}$ ///

σ d-Zyklus $\Rightarrow$ σ Produkt von $d-1$ Transpositionen $\Rightarrow \operatorname{sgn}(\sigma) = (-1)^{d-1}$

Folgerung 11.2 Sei $\pi \in S_n$. Dann gilt:
$\pi \in A_n \iff$ π lässt sich als Produkt einer geraden Anzahl von Transpositionen schreiben.

Beweis: Sei $\pi \in S_n$. Nach Satz 11.1 ist $\pi = \sigma_1 \circ \dots \circ \sigma_m$ mit Transpositionen σ_i $\Rightarrow$ $\operatorname{sgn}(\pi) = (-1)^m$. Also
$\pi \in A_n \iff \operatorname{sgn}(\pi) = 1 \iff m$ gerade □

Beisp. 11.3 Betrachte S_n für $n = 1, 2, 3, 4$

a) $n=1$ $\Rightarrow$ $S_n = \{id\}$ (b) $n=2$ $S_2 = \{id, (12)\}$ zyklisch der Ordnung 2 also abelsch.

c) $n=3$ kennen alle Untergruppen siehe Beisp. 10.4.
$\{1\} \subseteq A_3 \subseteq S_3$ $A_3 \trianglelefteq S_3$ mit $S_3/A_3 \cong \{\pm 1\}$
$|A_3| = \frac{1}{2} 6 = 3$ also zyklisch der Ordnung 3 $\Rightarrow$ S_3 auflösbar.

d) $n=4$. $A_4 \trianglelefteq S_4$ mit $S_4/A_4 \cong \{\pm 1\}$. $|A_4| = \frac{1}{2} \cdot 24 = 12$

$A_4 = \{id, (123), (132), (124), (142), (134), (143), (234), (243),$
3-Zyklen, Ordnung 3 jeweils
$(12)(34), (13)(24), (14)(23)\}$.
Elemente der Ordnung 2

Es gibt also nur Elemente der Ordnung 2, 3 (plus Identität)

Setze $V_4 := \{id, (12)(34), (13)(24), (14)(23)\}$.
$= \{\pi \in A_4 \mid \pi^2 = id\}$.

Sei $s = (12)(34)$, $t = (13)(24)$ $\Rightarrow$ so $t = (12)(34)(13)(24) = (14)(23)$ Ordnung 2
$\Rightarrow \langle s, t \rangle$ Untergruppe der Ordnung 4 ÜA 6.

$s, t, st \in V_4$ also $V_4 = \langle s, t \rangle$ Untergruppe.

Außerdem: Ist $\tau \in A_4$ bel. so $(\tau \pi \tau^{-1})^2 = \tau\pi\tau^{-1}\tau\pi\tau = \tau\pi^2\tau^{-1} = \tau\tau^{-1} = id$ für $\pi \in V_4$.

Also $V_4 \trianglelefteq A_4$.

(Man kann sogar zeigen $V_4 \trianglelefteq S_4$ $\rightsquigarrow$ Ü) Also

$\{1\} \subseteq V_4 \subseteq A_4 \subseteq S_4$ V_4 abelsch (nachrechnen)

$\Rightarrow$ [redacted] und S_4 auflösbar.

Damit gezeigt: S_n für $n \leq 4$ auflösbar Lemma 10.12 $\Rightarrow$ A_n für $n \leq 4$ auflösbar.

Beisp. 11.5 A_5 hat keine echten Normalteiler.

Dazu: Zuerst verschaffen wir uns einen Überblick über die Elemente in A_5

Alle 5-Zykel gehören zu A_5 $(i_1 i_2 i_3 i_4 i_5) = (1\ i_2\ i_3\ i_4\ i_5)$

$\uparrow\ \uparrow\ \uparrow\ \uparrow$

$4\ \ 3\ \ 2\ \ 1$ Möglichkeiten.

Also gibt es $24 = 4!$ 5-Zykel in A_5.

Alle 3-Zykel gehören zu A_5: $\underbrace{i<j<k}$ $\rightsquigarrow$ $(i\,j\,k)$ und $(i\,k\,j)$

zehe 3 Ziffern also $\binom{5}{3} = \binom{5}{2} = 10$ Möglichkeiten

dazu jeweils 2 3-Zykel, also insgesamt $2 \cdot 10 = 20$ 3-Zykel.

Außerdem gehören alle Doppeltranspositionen $(ij)(kl)$ mit i, j, k, l paarweise verschieden zu A_5. Davon gibt es 15.

Damit bereits $24 + 20 + 15 = 59$ Elemente gefunden. Zusammen mit id ergibt dies [redacted] also komplette Liste der Elemente von A_5.

Sei nun [redacted] $N \trianglelefteq A_5$, $\{id\} \neq N \neq A_5$.

Ü10.41 $\Rightarrow$ $N \cap A_4 \trianglelefteq A_4$.

Ü11 Normalteiler von A_4 sind $\{id\}$, V_4, A_4 also 3 Fälle.

(1) $N \cap A_4 = \{id\}$ Ü10 A1 $N A_4 \leq A_5$ und Ü7 A2 $\Rightarrow$

$|N \cdot A_4| = \frac{|N| \cdot |A_4|}{\uparrow} = |N| \cdot 12 \Rightarrow |N| \cdot 12 \mid 60 \Rightarrow |N| \mid 5 \Rightarrow |N| = 5$

$\Rightarrow 5 \nmid [G : N]$ [redacted] Lemma 10.10 $\Rightarrow$ alle Elemente der Ordnung 5 gehören zu N $\Rightarrow |N| \geq 24$ ↯

(2)+(3) $N \cap A_4 = V_4$ oder A_4 $\Rightarrow 4 \mid |N| \Rightarrow 2 \nmid [G : N]$

[redacted] Lemma 10.10 $\Rightarrow$ alle Elemente der Ordnung 2 gehören zu N

$\Rightarrow |N| \geq 15 + 1 = 16$, $|N| \mid 60 \Rightarrow |N| = 20$ oder 30

$\Rightarrow 5 \mid |N| \Rightarrow 5 \nmid [G:N]$ Lemma 10.11 $\Rightarrow$ alle Elemente der Ordnung 5 gehören zu N. $\Rightarrow |N| \geq 16 + 24 = 40$ ↯.

Folgerung 11.6 Für $n \geq 5$ sind S_n, A_n nicht auflösbar.

Beweis: Wegen $n \geq 5$ ist $S_5 \leq S_n$ und damit $A_5 \leq S_n$

Wäre S_n auflösbar, so auch A_5 nach Lemma 10.13.

$\Rightarrow A_5$ hätte echten Normalteiler $N \trianglelefteq A_5$ mit A_5/N abelsch haben

Beisp 11.6 $\Rightarrow N = \{1\}$ A_5 abelsch ↯.

Genauso $A_5 \leq A_n$ und damit A_n nicht auflösbar. □

Def. 11.7 Sei G Gruppe, $G \neq \{1\}$. Dann heißt G einfach, wenn $\{1\}, G$ die einzigen Normalteiler von G sind.

Haben gerade gesehen: A_5 einfach. außerdem: $\mathbb{Z}/p\mathbb{Z}$ (p Primzahl) einfach.

$\cup$ G einfach und auflösbar $\Rightarrow$ $G \cong \mathbb{Z}/p\mathbb{Z}$ für eine Primzahl p.

Satz von Burnside (1904) Sei G endl. Gruppe mit $|G| = p^a q^b$, p, q Primzahlen $a, b \geq 0$ $\Rightarrow$ G auflösbar (Beweis siehe mein Skript!)

Satz von Feit–Thompson (1963) Sei G endl. Gruppe mit $|G|$ ungerade $\Rightarrow$ G auflösbar (Beweis 255 Seiten lang!)

kann man mit den Mitteln dieser Vorlesung zeigen:

Satz. Ist G endl. Gruppe mit $|G| < 60$, so G auflösbar.
Ist G einfache Gruppe mit $|G| = 60$, so $G \cong A_5$

Also A_5 kleinste, nicht-abelsche einfache Gruppe.

komplette Liste aller endlichen einfachen Gruppen bekannt (1981)
siehe "classification of finite simple groups" wikipedia

Berühmtestes Beispiel: Fischer–Griess "Monster" M mit

$|M| = 8,080,174,247,945,128,758,864,599,049,617,107,$
$570,057,543,680,000,000 \approx 8 \cdot 10^{53}$

Die symmetrischen Gruppen haben auch noch aus einem anderen Grund eine besondere Bedeutung.

Satz 11.8 (Cayley 1854) Sei G endliche Gruppe. Dann gibt es ein $n \geq 1$ und einen injektiven Homomorphismus $\varphi: G \to S_n$, d.h. G ist isomorph zu einer Untergruppe von S_n.

Beweis: Für $g \in G$ def. $\pi_g: G \to G$, $x \mapsto gx$ (Linksmultiplikation mit g).
$gx = gy \Rightarrow x = y$ also π_g injektiv und damit bijektiv.
Also $\pi_g \in S_G$ (siehe Ü10). Betrachte $\pi: G \to S_G$, $g \mapsto \pi_g$.
Dies ist Homom., denn $\pi(gg')(x) = \pi_{gg'}(x) = (gg')x = g(g'x)$
$= \pi_g(\pi_{g'}(x)) = (\pi_g \circ \pi_{g'})(x)$ für alle $x \in G$ also $\pi(gg') = \pi(g) \circ \pi(g')$
$\ker(\pi)$: Sei $g \in G$ mit $\pi_g = id_G \Rightarrow gx = \pi_g(x) = id(x) = x$ für alle $x \in G$
Für $x = 1_G$ erhalte $g = g \cdot 1_G = 1_G$ also $\ker(\pi) = \{1_G\}$
also π injektiv. Wegen $|G| = n$ ist $S_G \cong S_n$ (Ü10)
also erhalten wir injektiven Homom. $\varphi: G \to S_G \cong S_n$ □

Folgerung 11.9 (Matrixversion des Satzes von Cayley) Sei G endl. Gruppe und K Körper. Dann gibt es ein $n \geq 1$ so dass G isomorph zu einer Untergruppe von $GL_n(K)$ ist.

Beweis: Sei $n = |G|$. Für $\sigma \in S_n$ def. $A^\sigma \in M_n(K)$ durch
$A^\sigma = (a_{ij}^\sigma)_{1 \leq i,j \leq n}$ mit $a_{ij}^\sigma = \begin{cases} 1 & \text{falls } i = \sigma(j) \\ 0 & \text{sonst.} \end{cases}$ Einheitsmatrix
A^σ liefert die zu σ gehörige Permutationsmatrix. $\sigma = id \Rightarrow A^{id} = I_n$
$\sigma \neq id \Rightarrow A^\sigma \neq I_n$.
Es gelt $A^\sigma \cdot A^\tau = A^{\sigma\circ\tau}$ für alle $\sigma, \tau \in S_n$. denn:

$$(A^\sigma \cdot A^\tau)_{ij} = \sum_{k=1}^{n} a_{ik}^\sigma \cdot a_{kj}^\tau = a_{i\tau(j)}^\sigma = \begin{cases} 1 & \text{falls } i = \sigma(\tau(j)) \\ 0 & \text{sonst} \end{cases}$$

$a_{kj}^\tau = 1$ falls $k = \tau(j)$ und 0 sonst.

also $= (A^{\sigma\circ\tau})_{ij}$:
Damit auch $A^\sigma \cdot A^{\sigma^{-1}} = A^{\sigma\circ\sigma^{-1}} = A^{id} = I_n$, also $A^\sigma \in GL_n(K)$
und Abbildung $S_n \to GL_n(K)$, $\sigma \mapsto A^\sigma$, ist injektiver Homom.
Mit Satz 11.8 erhalten wir also injektiven Homom.

$$G \xrightarrow{\varphi} S_n \longrightarrow GL_n(K)$$

□

§12 Operationen von Gruppen auf Mengen: Symmetrien

Sei G Gruppe und $X \neq \emptyset$ Menge. Wir sagen, daß G auf X operiert (oder daß X eine G-Menge ist), wenn es eine Abbildung

$\mu: G \times X \to X$, $(g, x) \mapsto g \cdot x$ gibt mit

(a) $1_G \cdot x = x$ für alle $x \in X$

(b) $(gh) \cdot x = g \cdot (h \cdot x)$ für alle $g, h \in G$ und $x \in X$.

(gh: Produkt in G.)

Standardbeispiel:

$G = S_n$ operiert auf $X = \{1, \dots, n\}$ mit $G \times X \to X$, $(\pi, i) \mapsto \pi \cdot i = \pi(i)$.

$(\sigma \circ \pi) \cdot i = (\sigma \circ \pi)(i) = \sigma(\pi(i)) = \sigma \cdot (\pi \cdot i)$. ✓ $\mathrm{id} \cdot i = i$ ✓

Bem. 12.1 Sei X eine G-Menge. Für festes $g \in G$ definiere

$\pi_g: X \to X$, $x \mapsto g \cdot x$

Sei auch $h \in G$. Dann sind

$\pi_h: G \to G$, $x \mapsto h \cdot x$ und $\pi_{gh}: G \to G$, $x \mapsto gh \cdot x$ def.

Es gelt:

$\pi_{gh}(x) = (gh) \cdot x = g \cdot (h \cdot x) = \pi_g(\pi_h(x)) = (\pi_g \circ \pi_h)(x)$ für alle $x \in X$

also $\pi_{gh} = \pi_g \circ \pi_h$.

Ist $h = g^{-1}$, so folgt $\pi_g \circ \pi_{g^{-1}} = \pi_{gg^{-1}} = \pi_{1_G} = \mathrm{id}_X$ (↑ wegen $1_G \cdot x = x$ für alle $x \in X$.)

Also π_g bijektiv mit $\pi_g^{-1} = \pi_{g^{-1}}$.

Damit $\pi_g \in S_X$. Dann zeigt obige Formel

$\pi: G \to S_X$, $g \mapsto \pi_g$, ist Homomorphismus

$\ker(\pi) = \{g \in G \mid \pi_g = \mathrm{id}_X\} = \{g \in G \mid g \cdot x = x \text{ für alle } x \in X\}$.

D.h. zu jeder Operation von G auf X gehört ein Homomorphismus $\pi: G \to S_X$. Umgekehrt: Ist $\varphi: G \to S_X$ ein Homomorphismus, so operiert G auf X durch

$G \times X \to X$, $(g, x) \mapsto g \cdot x = \varphi(g)(x)$

(Haben dies bereits im Beweis des Satzes von Cayley benutzt.)

Bsp.: G operiert auf $X = G$ durch Linksmultiplikation.)

Satz 12.2 (Verallgemeinerung des Satzes von Cayley) Sei G eine Gruppe und $U \leq G$ eine Untergruppe mit $n = [G:U] < \infty$. Dann gibt es einen Normalteiler $N \trianglelefteq G$ mit $N \subseteq U$ und $G/N \cong$ Untergruppe von S_n.

(Satz von Cayley: Spezialfall $|G| < \infty$ und $U = \{1\}$.)

Beweis: Sei $X = G/U = \{xU \mid x \in G\}$. Dann operiert G auf X durch

$G \times X \to X$
$(g, xU) \mapsto gxU$

Dies ist wohldef., denn sei $xU = yU \Rightarrow x^{-1}y \in U \Rightarrow (gx)^{-1}gy = x^{-1}g^{-1}gy = x^{-1}y \in U$
also $gxU = gyU$. ✓

Axiome für Operation folgen dann sofort. Nach Bem 12.1 erhalten wir Homom. $\pi: G \to S_X$ mit

$N := \mathrm{Kern}(\pi) = \{g \in G \mid gxU = xU \text{ für alle } x \in G\}$
$\subseteq \{g \in G \mid gU = U\} = \{g \in G \mid g \in U\} = U$

Homomorphiesatz: $G/N = G/\mathrm{Kern}(\pi) \cong \mathrm{Bild}(\pi) \leq S_X$
Also G/N isomorph zu Untergruppe von S_X. Ü 10 $\Rightarrow S_X \cong S_n$
wegen $|X| = [G:U] = n$, also G/N auch isomorph zu Untergruppe von S_n. □

Bem. Sei X eine G-Menge. Definiere Relation $\sim$ auf X durch:

$x \sim y \overset{\text{def}}{\Leftrightarrow}$ es existiert ein $g \in G$ mit $y = g \cdot x$.

Dies ist eine Äquivalenzrelation, denn:

- reflexiv: $x \sim x$ weil $x = 1_G \cdot x$
- symmetrisch: $x \sim y \Rightarrow y = g \cdot x$ für ein $g \in G \Rightarrow$
  $g^{-1} \cdot y = g^{-1} \cdot (g \cdot x) = (g^{-1}g) \cdot x = 1_G \cdot x = x$ also auch $y \sim x$
- transitiv: $x \sim y$ und $y \sim z \Rightarrow y = g \cdot x$ und $z = h \cdot y$
  mit $g, h \in G \Rightarrow z = h \cdot y = h(g \cdot x) = hg \cdot x$ also $x \sim z$. ✓

Für $x \in X$ sei $\mathcal{O}_x$ Äquivalenzklasse von x. Es gilt:

$\mathcal{O}_x = \{y \in X \mid y = g \cdot x \text{ für ein } g \in G\} = \{g \cdot x \mid g \in G\}$

"Bahn von x unter G"

$\Rightarrow$ X = disjunkte Vereinigung von Äquivalenzklassen
= ——— Bahnen.

Satz 123 (Bahnensatz) Sei $x \in X$ fest. Dann ist $G_x := \mathrm{Stab}_G(x)$ eine Untergruppe von G "Stabilisator von x". $:= \{g \in G \mid g.x = x\}$.
Die folgende Abbildung ist wohldef. und bijektiv:

$$\mu_x : O_x \to G/G_x \,,\ g.x \mapsto gG_x$$

Ist also $|G| < \infty$, so auch $|O_x| < \infty$ und $|O_x| = [G : G_x]$
"Länge der Bahn ist Index des Stabilisators"

Beweis: $G_x \leq G$ denn $1_G.x = x$ also $1_G \in G_x$. Seien $g, h \in G_x$.
$\Rightarrow (gh).x = g.(h.x) = g.x = x$ also $gh \in G_x$ abgeschlossen.
$x = 1_G.x = (g^{-1}g).x = g^{-1}.(g.x) = g^{-1}.x$ also $g^{-1} \in G_x$ ✓.
Jetzt zu μ_x: wohldef denn seien $g, h \in G$ mit $g.x = h.x$
$\Rightarrow (g^{-1}h).x = g^{-1}.(h.x) = g^{-1}.(g.x) = (g^{-1}g).x = 1_G.x = x$ also $g^{-1}h \in G_x$
und damit $gG_x = hG_x$. μ_x klarerweise surjektiv. Sei
schließlich $gG_x = hG_x \Rightarrow g^{-1}h \in G_x \Rightarrow g.x = g(g^{-1}h.x)$
$= (gg^{-1}h).x = h.x$ also μ_x auch injektiv. □

Beisp. 124. (a) S_n operiert auf $X = \{1, \dots, n\}$. Zu jedem i gibt es $\pi \in S_n$ mit $\pi(1) = i$ (z.B. Transposition $\pi = (1\,i)$ für $i > 1$)
Also $X = O_1$ eine Bahn. Eine solche Operation heißt "transitiv".
(b) Sei K Körper, $n \geq 1$. Dann operiert $G = GL_n(K)$ auf $V = K^n$ durch $G \times V \to V$
$(A, v) \mapsto A.v$ (Matr. Matrix mal Spaltenvektor)
$A.0 = 0$ für alle $A \in G$ $\Rightarrow$ $O_0 = \{0\}$ eine Bahn, also Operation nicht transitiv.
Sei $e_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \in V$ zu jedem $0 \neq v \in V$ gibt es ein $A \in G$, dessen 1. Spalte gleich v ist $\Rightarrow$ $Ae_1 = v$ also $O_{e_1} = V \setminus \{0\}$.
Damit $V = \{0\} \cup V \setminus \{0\}$ 2 Bahnen mit Repräsentanten 0 und e_1. Es gilt $G_0 = \mathrm{Stab}_G(0) = G$ und

$$G_{e_1} = \mathrm{Stab}_G(e_1) = \{A \in G \mid Ae_1 = e_1\} = \left\{ \left[\begin{array}{c|ccc} 1 & q_2 & \cdots & q_n \\ \hline 0 & & & \\ \vdots & & A' & \\ 0 & & & \end{array}\right] \;\middle|\; \begin{array}{l} q_i \in K \\ A' \in GL_{n-1}(K) \end{array} \right\}$$

Anwendung: Sei K endlicher Körper mit $|K| = q$ Primzahlpotenz

$\Rightarrow |V| = |K^n| = q^n$ und $|G_{e_1}| = q^{n-1} \cdot |GL_{n-1}(K)|$.

Lemma 12.3 $\Rightarrow$ $|GL_n(K)| = |G| = |O_{e_1}| \cdot |G_{e_1}| = (q^n - 1)\, q^{n-1} \cdot |GL_{n-1}(K)|$

Mit Induktion nach n folgt dann sofort:

$$|GL_n(K)| = q^{n(n-1)/2} (q^n - 1)(q^{n-1} - 1) \cdots (q^2 - 1)(q - 1) \quad \text{für } |K| = q.$$

Anfang $n = 1$: $GL_1(K) \cong K^\times$ also $|GL_1(K)| = q - 1$.

Beisp. 12.5 Sei K Körper und $G = GL_n(K)$. Dann operiert G auf $X = M_n(K)$ durch

$$\begin{array}{ccc} G \times X & \to & X \\ (T, A) & \mapsto & TAT^{-1} \end{array}$$

zwei Matrizen $A, A' \in M_n(K)$ liegen also in der gleichen Bahn genau dann, wenn A, A' ähnlich sind.

Vertreter der Bahnen $\longleftrightarrow$ Normalformen von Matrizen

Das Konzept der Operation von Gruppen ist sehr flexibel und hat Anwendungen in diversen Gebieten.

Beisp. 12.6 Sei $V = \mathbb{R}^n$ mit der üblichen Euklidischen Norm

$$\|v\| = \sqrt{v_1^2 + \ldots + v_n^2} \quad \text{für} \quad v = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \in V.$$

LAAG: Eine Abbildung $f: V \to V$ heißt Bewegung, wenn

$\|f(v) - f(w)\| = \|v - w\|$ für alle $v, w \in V$ gilt

(Abstände zwischen Punkten des $\mathbb{R}^n$ bleiben erhalten.)

z.B. Drehungen, Spiegelungen, Verschiebungen, ...

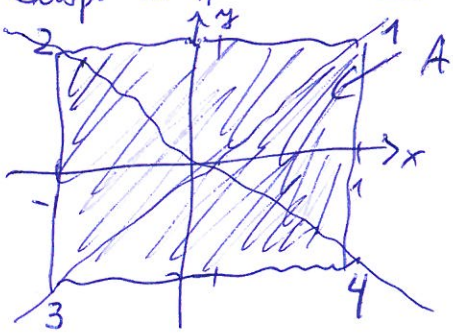
$B :=$ Menge aller Bewegungen; Gruppe mit $\circ$ als Verknüpfung.

Sei $P(V)$ Menge aller Teilmengen von V. Dann operiert B auf $P(V)$ durch

$$\begin{array}{ccc} B \times P(V) & \to & P(V) \\ (f, A) & \mapsto & f[A] = \{f(v) \mid v \in A\} \end{array}$$

Ist $A \in \mathcal{P}(V)$, so heißt $B_A = \mathrm{Stab}_B(A) = \{ f \in B \mid f(A) = A \}$
die Symmetriegruppe von A. Dies sind also alle Bewegungen,
die A wieder in sich überführen. Dann operiert auch B_A auf A
durch $B_A \times A \to A$, $(f, v) \mapsto f(v)$.
Wir erhalten also wieder einen Homomorphismus $\pi : B_A \to S_A$

Beisp. in $\mathbb{R}^2$: Sei $A = [-1,1] \times [-1,1] \subseteq \mathbb{R}^2$



$B_A = \{$ id, Drehungen um $90°, 180°, 270°$
Spiegelung an x-Achse, y-Achse sowie
den beiden Diagonalen $\}$.
$|B_A| = 8$.

Nummeriere die 4 Ecken von A mit $\{1,2,3,4\}$. Dann operiert
B_A auf $\{1,2,3,4\}$. Erhalten also Homom. $\varphi : B_A \to S_4$.

Ist $f \in \mathrm{Kern}(\varphi)$, dann bleiben alle 4 Ecken fest, also insgesamt $f = \mathrm{id}$.
Also φ injektiv d.h. B_A isomorph zu Untergruppe U von S_4.
Zu dieser Untergruppe gehören Permutationen:

(1234) (Drehung um 90°).
(14)(23) (Spiegelung an x-Achse)
(12)(34) — y-Achse)
(13) Spiegelung an Diagonale
(24) —

Man sieht dann leicht
$U = \langle (14)(23), (13) \rangle$.
Diedergruppe der Ordnung 8.
$(14)(23) \circ (13) = (1234)$ Ordnung 4.
(Ü7A6)

weitere Beispiele siehe Ü.

Def. 12-7 Sei G eine Gruppe und X eine G-Menge.
Ein Element $x \in X$ heißt Fixpunkt wenn $g \cdot x = x$ für alle $g \in G$
gilt, also $G_x = G$. Sei $X_0 := \{ x \in X \mid x \text{ Fixpunkt} \}$

Lemma 12-8 Sei G endliche Gruppe mit $|G| = p^n$, p Primzahl, $n \geq 0$.
Ist X endliche G-Menge, so gilt $|X| \equiv |X_0| \bmod p$.

Beweis: Sei $X = \mathcal{O}_1 \dot\cup \dots \dot\cup \mathcal{O}_r$ Zerlegung in Bahnen, $\mathcal{O}_i = \mathcal{O}_{x_i}$
mit $x_i \in X$ und $|\mathcal{O}_{x_i}| = [G : G_{x_i}]$. $|G| = p^n$ Lagrange $\Rightarrow$
$|G_{x_i}| = p^{n_i}$ mit $n_i \leq n$

$|\mathcal{O}_{x_i}| = 1 \iff |G : G_{x_i}| = 1 \iff G_{x_i} = G \iff x_i \in X_0$

Ist $x_i \notin X_0$, so $|\mathcal{O}_{x_i}| = |G : G_{x_i}| = p^{n-n_i}$ mit $n_i < n$, also $p \mid |\mathcal{O}_{x_i}|$. (Fixpunkt)

$\Rightarrow |X| = |\mathcal{O}_{x_1}| + \dots + |\mathcal{O}_{x_r}| = |X_0| + \sum_i |\mathcal{O}_{x_i}| \equiv |X_0| \bmod p.$
mit $p \mid |\mathcal{O}_{x_i}|$

□

Beisp. 12.9 Sei $X \neq \emptyset$ Menge. Dann operiert S_n auf $X^n = \{(x_1, \dots, x_n) \mid x_i \in X\}$ durch

$$S_n \times X^n \longrightarrow X^n$$
$$(\pi, (x_1, \dots, x_n)) \mapsto (x_{\pi^{-1}(1)}, \dots, x_{\pi^{-1}(n)})$$

denn: $\mathrm{id} \cdot (x_1, \dots, x_n) = (x_1, \dots, x_n)$ ✓

Seien $\pi, \sigma \in S_n$. $\pi \cdot (\sigma \cdot (x_1, \dots, x_n)) = \pi(x_{\sigma^{-1}(1)}, \dots, x_{\sigma^{-1}(n)})$

$= (y_{\pi^{-1}(1)}, \dots, y_{\pi^{-1}(n)}) \underset{y_i = x_{\sigma^{-1}(i)}}{=} (x_{\sigma^{-1}(\pi^{-1}(1))}, \dots, x_{\sigma^{-1}(\pi^{-1}(n))})$

$= (x_{(\pi\sigma)^{-1}(1)}, \dots, x_{(\pi\sigma)^{-1}(n)})$ ✓

Sei $\pi = (1\,2 \dots n) \in S_n$ n-Zykel und $U := \langle \pi \rangle \subseteq S_n$ Untergruppe der Ordnung n.

Dann operiert auch U auf X^n (Einschränkung obiger Operation)

Sei $(x_1, \dots, x_n) \in X^n$. Dann ist $(x_1, \dots, x_n)$ Fixpunkt unter U $\iff$ $x_1 = \dots = x_n$ alle Komponenten gleich.

Ist also $|X| < \infty$, so gibt es genau $|X|$ Fixpunkte.

Einfache Anwendung: Sei X = Menge mit m Elementen ($m \in \mathbb{N}$ beliebig) und $n = p$ Primzahl

U Gruppe der Ordnung p, operiert auf X^p

Lemma 12.8: $m^p = |X^p| \equiv |\text{Fixpunkte}| \equiv \underbrace{|X|}_{= m} \bmod p.$

also $p \mid m^p - m$ "Kleiner Satz von Fermat".

Satz 12.10 (Cauchy 1845) Sei G endl. Gruppe und p Primzahl mit $p \mid |G|$. Sei $U_p(G) :=$ Menge der Untergruppen $U \leq G$ mit $|U| = p$. Dann ist $U_p(G) \neq \emptyset$ und $|U_p(G)| \equiv 1 \mod p$.
Insbesondere gibt es also ein Element $g \in G$ mit $o(g) = p$ (Beisp. 5.4)

Beweis: Sei $\pi = (123 \cdots p) \in S_p$. Wie in Beisp. 12.9 operiert $\langle \pi \rangle \leq S_p$ auf $G^p = \{(g_1, \dots, g_p) \mid g_i \in G\}$. Fixpunkte sind alle Typen $(g, \dots, g)$ mit $g \in G$
Brauchen noch Verfeinerung. Sei $(g_1, \dots, g_p) \in G^p$ mit $g_1 \cdots g_p = 1$.
Dann $\pi \cdot (g_1, \dots, g_p) = (g_p, g_1, \dots, g_{p-1})$

$\pi = \begin{pmatrix} 1 & 2 & 3 & \cdots & p-1 & p \\ 2 & 3 & 4 & & p & 1 \end{pmatrix}$ Aus $g_1 \cdots g_p = 1$ folgt $g_p g_1 \cdots g_{p-2} = g_p (g_1 \cdots g_p) g_p^{-1} = 1$ ($g_1 \cdots g_p = 1$)

Also operiert $\langle \pi \rangle$ auch auf $Y = \{(g_1, \dots, g_p) \in G^p \mid g_1 \cdots g_p = 1\}$.

Lemma 12.8 $|Y| \equiv |Y_0| \mod p$.

$Y_0 = \{(g_1, \dots, g_p) \in G^p \mid g \in G \text{ und } g^p = 1\}$, also $|Y_0| =$ Anzahl $g \in G$ mit $g^p = 1$ (Fixpunkte)

$|Y| =$ wähle $g_1, \dots, g_{p-1} \in G$ bel., dann $g_p = (g_1 \cdots g_{p-1})^{-1}$ festgelegt, also $|Y| = |G|^{p-1}$ $p \mid |G|$ also folgt:

$$p \mid \underbrace{\text{Anzahl } g \in G \text{ mit } g^p = 1}_{\geq 1 \text{ da } 1_G^p = 1_G \quad \text{also Anzahl} \geq p}$$

Es gibt also ein $g \in G$, $g \neq 1_G$ und $g^p = 1 \Rightarrow |\langle g \rangle| = p$.
Seien $U_1, \dots, U_r$ Untergruppen der Ordnung p. $\Rightarrow U_i \cap U_j = \{1\}$ für $i \neq j$ und jedes U_i enthält $p-1$ Elemente der Ordnung p. Umgekehrt ist jedes $g \in G$ mit $o(g) = p$ in einem der U_i enthalten, also

$$\underbrace{\{g \in G \mid g^p = 1\}}_{\text{Anzahl } p \mid} = \underbrace{(U_1 \setminus \{1\} \dot\cup \cdots \dot\cup U_r \setminus \{1\})}_{p-1 \qquad\qquad p-1} \cup \{1\}$$

$$r(p-1) + 1 = rp - r + 1.$$

$\Rightarrow p \mid r - 1$ also $r \equiv 1 \mod p$. □

Obiger Satz plus Verallgemeinerungen sind fundamental für die endliche Gruppentheorie. Verallgemeinerung:

Satz von Sylow (1872) Ist G endl., p Primzahl mit $p^a \mid |G|$, $a \geq 1$.

so gibt es Untergruppen $U \leq G$ mit $|U| = p^q$ und deren Anzahl ist wieder $\equiv 1 \mod p$.

Mit Satz von Cauchy und Satz 12.2 (Verallgemeinerung Cayley) kann man bereits einige Strukturaussagen für endliche Gruppen zeigen.

Beisp 12.11 Sei $|G| = 6 = 2 \cdot 3$. Nach Cauchy gibt es Untergrupp $U \leq G$ mit $|U| = 3$, dann $[G:U] = 2$ also $U \trianglelefteq G$.
Außerdem $U = \langle x \rangle$ mit $o(x) = 3$.
Nach Cauchy gibt es auch Untergruppe $V \leq G$ mit $|V| = 2$.
Dann $V = \langle y \rangle$ mit $o(y) = 2$. Dann 2 Fälle:

① Ist auch $V \trianglelefteq G$ so $|U \cdot V| = \frac{|U| \cdot |V|}{|U \cap V|} = 6$ (Ü7A2)
also $G = U \cdot V$ und $U \cap V = \{1\}$.
$\Rightarrow$ G abelsch (Ü11A1) Lemma 5.8 $o(xy) = o(x) \cdot o(y) = 6$
also $G = \langle xy \rangle$ und damit $G \cong \mathbb{Z}/6\mathbb{Z}$ (Beisp. 10.10).

② Ist $V \not\trianglelefteq G$, so liefert Satz 12.2 einen Normalteiler $N \trianglelefteq G$ mit $N \subseteq V$ und $G/N \cong$ Untergruppe von S_3 ($3 = [G:V]$)
$V \not\trianglelefteq G \Rightarrow N \subsetneq V$. $|V| = 3 \Rightarrow N = \{1\}$ also $G \cong$ Untergruppe von S_3
aber $|G| = 6 = |S_3| \Rightarrow G \cong S_3$.
Haben also gezeigt: $|G| = 6 \Rightarrow G \cong \mathbb{Z}/6\mathbb{Z}$ oder $G \cong S_3$.

Beisp. 12.12 Sei $|G| = p^2$ mit Primzahl p. Beh.: G abelsch.
Dazu: Alle Elemente von G haben Ordnung $1, p$ oder p^2 (Lagrange)
Gibt es $g \in G$ mit $o(g) = p^2$, so $G = \langle g \rangle$, also G abelsch.
Ist gelte nun $g^p = 1$ für alle $g \in G$. Dann gibt es genau $p+1$ Untergruppen der p in G (siehe letzter Teil obiger Beweis)
Sei $U \leq G$ mit $|U| = p$. Nach Satz 12.2 gibt es $N \trianglelefteq G$ mit $N \subseteq U$ und $G/N \cong$ Untergruppe von S_p ($p = [G:U]$)
Wäre $N = \{1\}$, so $G \cong$ Untergruppe von S_p, also $p^2 \mid p! = 1 \cdot 2 \cdots p$ ↯
$|U| = p \Rightarrow N = U \trianglelefteq G$. Dies gilt für alle U mit $|U| = p$.
Sei auch $V \leq G$ mit $|V| = p$, $U \neq V$. Dann $U \cap V = \{1\}$, $V \trianglelefteq G$,
und $G = U \cdot V$ (s.o.), U, V abelsch $\overset{\text{Ü11A1}}{\Longrightarrow}$ G abelsch. ν.

Anhang zu §12: auflösbare Gruppen G mit $|G| \leq 60$

(I)

Haben bereits am Ende von §11 erwähnt: (werde nicht in Vorlesung behandelt!)

Satz: Sei G endliche Gruppe. Ist $|G| < 60$, so ist G auflösbar.
Ist $|G| = 60$, so ist G auflösbar oder $G \cong A_5$.
Also ist A_5 bis auf Isomorphie die kleinste nicht-abelsche einfache Gruppe.
Wollen zeigen, wie man dies mit obigen Methoden beweisen kann.

Lemma 1 Sei G endliche Gruppe, $N \trianglelefteq G$. Ist N auflösbar und G/N auflösbar, so ist auch G auflösbar.

Beweis: Induktion nach $|G|$. Ist $|G| = 1$, so ist G auflösbar.
Sei nun $|G| > 1$. Ist $N = \{1\}$ oder $N = G$, so ist G auflösbar nach Vor. Sei also $N \neq \{1\}$ und $N \neq G$. Sei $H := G/N$ und $\pi: G \to H$ kanonischer Homomorphismus. H auflösbar, also gibt es $\{1\} = H_0 \subsetneq H_1 \subsetneq \dots \subsetneq H_r = H$ mit $H_i \leq H_1$, $H_{i-1} \trianglelefteq H_i$ und H_i/H_{i-1} abelsch für alle i.

Sei $\pi': H \to \underbrace{H/H_{r-1}}_{\neq \{1\} \text{ und abelsch.}}$ kanonischer Homom.

$\Rightarrow$ $\varphi: G \xrightarrow{\pi} H \xrightarrow{\pi'} H/H_{r-1}$ $(\varphi = \pi' \circ \pi)$ ebenfalls Homomorphismus und auch φ surjektiv (weil π, π' surjektiv).

Sei $\tilde{G} := \operatorname{Kern}(\varphi) \trianglelefteq G$.

Homomorphiesatz:
$G/\tilde{G} = G/\operatorname{Kern}(\varphi) \cong \operatorname{Bild}(\varphi) = H/H_{r-1}$ abelsch und $\tilde{G} \subsetneq G$.

Wegen $N = \operatorname{Kern}(\pi)$ ist auch $N \subseteq \operatorname{Kern}(\varphi) = \tilde{G}$.
Nun folgende Situation: $\tilde{G}/N \leq G/N$ $(\S 10)$ Also $\tilde{G}/N$ auflösbar nach Lemma 10.12

Induktion: $\tilde{G}$ auflösbar, also gibt es Folge $\{1\} = \tilde{G}_0 \subsetneq \tilde{G}_1 \subsetneq \dots \subseteq \tilde{G}_s = \tilde{G}$ mit $\tilde{G}_i \leq \tilde{G}$, $\tilde{G}_{i-1} \trianglelefteq \tilde{G}_i$ und $\tilde{G}_i/\tilde{G}_{i-1}$ abelsch

$\Rightarrow$ $\{1\} = \tilde{G}_0 \subsetneq \tilde{G}_1 \subsetneq \dots \subsetneq \tilde{G}_s = \tilde{G} \subsetneq G$

gewünschte Folge von Untergruppen in G, also G auflösbar. □

Bem. 2(a) Um zu zeigen, daß alle G mit $|G| < 60$ auflösbar sind, gehen wir induktiv vor. Ist G gegeben und bereits gezeigt, daß

alle H mit $|H| < |G|$ auflösbar sind, so genügt es zu zeigen, daß G einen Normalteiler $N \trianglelefteq G$ besitzt mit $1 \neq N \neq G$. Denn dann ist bereits bekannt, daß N und G/N auflösbar sind, also ist auch G auflösbar nach Lemma 1 ✓

(b) Sei $|G| \leq 60$. Dann kommen höchstens 3 verschiedene Primzahlen in der Primfaktorzerlegung von $|G|$ vor. Wir haben also 3 Fälle:

(i) $|G| = p^n$ mit p Primzahl. Nach Ü13 ist $Z(G) \neq \{1\}$. Also entweder $G = Z(G)$, also G abelsch, oder $Z(G) \neq \{1\}$ und dann $G/Z(G)$ einfach also können wir a) anwenden.

(ii) $|G| = p^a q^b$ mit $p \neq q$ Primzahlen und $a, b \geq 1$.
Nach dem in §11 erwähnten Satz von Burnside ist allgemein bekannt, daß diese Gruppen auflösbar. Wir werden die Fälle mit $|G| \leq 60$ hier explizit behandeln.

(iii) $|G| = \begin{cases} 42 = 2 \cdot 3 \cdot 7 \\ 30 = 2 \cdot 3 \cdot 5 \end{cases}$ und $|G| = 60 = 2^2 \cdot 3 \cdot 5$.

Wir benötigen nun einige Aussagen im Stil von Beisp. 12.11, 12.12

Beisp. 3 Sei $|G| = 2 \cdot m$ mit $m \geq 3$ ungerade. Dann hat G einen Normalteiler $N \trianglelefteq G$ mit $|N| = m$.

Beweis: Einmaliger Beweis des Satzes von Cayley:

$\exists$ injektiver Homom. $\pi: G \to S_G$ wobei $\pi_g: G \to G$, $x \mapsto gx$.
$g \mapsto \pi_g$

Nach Cauchy ex. Element $g \in G$ mit $o(g) = 2$, $g \neq 1$ also $\pi_g(x) = gx \neq x$ für alle $x \in G$.
$(\pi_g^2(x) = g^2 x = x.)$

Schreibe $G = \{x_1, \dots, x_n\}$ mit $n = 2m$.

Dann $S_G \cong S_n$ (siehe Ü10)
$\pi \longleftrightarrow \pi'$ wobei $\pi(x_i) = x_{\pi'(i)}$ für alle i.

Dann $\pi' \longleftrightarrow \pi_g$ $\pi' \in S_n$ $o(\pi') = 2$ und ebenfalls $\pi'(i) \neq i$ für alle i:

§11: π' = Produkt von disjunkten 2-Zyklen (keine Eins-Zyklen) ← also genau m 2-Zyklen.

$\Rightarrow \quad \operatorname{sgn}(\pi') = (-1)^m = -1.$

Erhalten Homom. $\alpha: G \xrightarrow{\pi} S_G \cong S_n \xrightarrow{\text{sgn}} \{\pm 1\}$

$g \mapsto \pi_g \mapsto \pi' \mapsto -1$

Also $\text{Ker}(\alpha) \neq G$ Homomorphiesatz $G/\text{Ker}(\alpha) \cong \text{Bild}(\alpha) = \{\pm 1\}$

$\Rightarrow [G : \text{Ker}(\alpha)] = 2$ also $U = \text{Ker}(\alpha)$ gewünschter Normalteiler α

Beisp. 4 Sei $|G| = pm$ mit p Primzahl $p \nmid m$ und $p > m$

Dann gibt es genau eine Untergruppe $U \leq G$ mit $|U| = p$, also $U \trianglelefteq G$

denn: Cauchy $|U_p(G)| \equiv 1 \bmod p$, also $1, p+1, 2p+1, \ldots$

Annahme $|U_p(G)| \geq p+1$ Dann gibt es mind. $p+1$ Untergruppen

$U_1, \ldots, U_{p+1}$ mit $|U_i| = p$. $U_i \cap U_j = \{1\}$ für $i \neq j$

also $|U_1 \cup \ldots \cup U_{p+1}| = (p-1)(p+1) + 1 = p^2 > pm = |G|$ $\lightning$

also $U_p(G) = \{U\}$ und damit $U \trianglelefteq G$ (Ü 12) $\checkmark$

Bem. 5 Wenden wir obige Methoden auf $|G| < 60$ an, so bleiben noch folgende Fälle übrig, die noch nicht von diesen Methoden erfasst werden:

$|G| \in \{ 12, 24, 36, 40, 45, 48, 56 \}$

$4 \cdot 3$ $\quad$ $8 \cdot 3$ $\quad$ $4 \cdot 9$ $\quad$ $5 \cdot 8$ $\quad$ $5 \cdot 9$ $\quad$ $16 \cdot 3$ $\quad$ $7 \cdot 8$.

Lemma 6 (Schwache Form des Satzes von Sylow) Sei G endliche Gruppe, p Primzahl und $|G| = p^a \cdot m$ mit $a \geq 1$, $p \nmid m$. Ist $Z(G) = \{1\}$, so gibt es eine echte Untergruppe $U \leq G$ mit $p^a \mid |U|$ (also $[G:U] \mid m$)

Beweis: Betrachte Klassengleichung in Ü 13:

$$p \mid |G| = \underbrace{|Z(G)|}_{=1} + \underbrace{\sum_{i=s+1}^{r} [G : C_G(x_i)]}_{\Rightarrow p \nmid} \quad \text{wobei } C_G(x_i) \subsetneq G \text{ für } i > s$$

also muss es ein i geben mit $p \nmid [G : C_G(x_i)]$. Sei

$U := C_G(x_i) \subsetneq G$ Dann $p \nmid [G:U]$, also $p^a \mid |U|$

und damit $[G:U] \mid m$ $\square$

Beisp. 7 Sei $|G| = p^a m$ mit $a \geq 1$, $p \nmid m$ und $m = 2, 3, 4$.

Dann ist G nicht einfach

denn: Annahme G ist einfach. Nach Lemma 6 gibt es Untergruppe

$U \subsetneq G$ mit $[G:U] = n \mid m$ Nach Satz 12.2 gibt es
$N \trianglelefteq G$ mit $N \subseteq U$ und $G/N \cong$ Unt. von S_n.
G einfach also $N = \{1\} \Rightarrow G \cong$ Unt. von S_n.
Über $n \leq m \leq 4 \Rightarrow S_2, S_3, S_4$ auflösbar $\Rightarrow G$ auflösbar
G außerdem einfach also $|G| = p$ ($\not\in$ zu $|G| = p^q m$ $q \geq 1, m \geq 2$ ☐)

Jetzt bleiben nur noch die Fälle übrig: $|G| \in \{40, 45, 56\}$.
$= 5 \cdot 8$ $5 \cdot 9$ $7 \cdot 8$

Sei $|G| = 40$ oder 45. Wende Lema 6 an mit $p = 2$ bzw. 3
$\Rightarrow$ ex. $U \subsetneq G$ mit $p^a \mid |U|$. also $8 \mid |U|$ im 1. Fall
bzw. $9 \mid |U|$ im 2. Fall $[G:U] \mid 5$, $U \subsetneq G$ also $[G:U] = 5$
Nach Satz 12.2 gibt es $N \trianglelefteq G$ mit $N \subseteq U$ und
$G/N \cong$ Unt. von S_5. Anm: G einfach $\Rightarrow N = \{1\}$ und
$G \cong$ Unt. von $S_5 \Rightarrow |G| \mid 120 = 5!$ $\not\in$ falls $|G| = 45$.
Sei nun $|G| = 40$. Sei $G \cong \tilde{G} \leq S_5$, $|\tilde{G}| = 40$.
Wegen $|A_5| = 60$ kann $\tilde{G}$ nicht in A_5 enthalten sein,
also gibt es $\pi \in \tilde{G}$ mit $\operatorname{sgn}(\pi) = -1$. Dann
$\operatorname{sgn}: \tilde{G} \to \{\pm 1\}$ surjektiv also $\operatorname{Kern}(\operatorname{sgn}) \subsetneq \tilde{G}$
$\tilde{G}$ nicht einfach, also G nicht einfach $\not\in$

Schließlich sei $|G| = 56 = 7 \cdot 8$. Anm: G einfach
Cauchy: $|U_7(G)| \equiv 1 \bmod 7$, also $= 1, 8, 15, \ldots$
G einfach $\Rightarrow |U_7(G)| > 1 \Rightarrow$ es gibt mind. 8 Untergruppen
der Ordnung 7, also mind. $8 \cdot (7-1) = 48$ Elemente der Ordnung
7 und damit höchstens $56 - 48 = 8$ Elemente anderer Ordnung
Nach Lema 6 gibt es $U \subsetneq G$ mit $8 \mid |U|$, $[G:U] \mid 7$
$U \subsetneq G \Rightarrow |U| = 8$ Dann enthält U also genau die
übrigen, restlichen 8 Elemente und es gibt keine weiteren Untergruppen
der Ordnung 8 $\Rightarrow U \trianglelefteq G$. $\not\in$
Damit vollständig bewiesen: $|G| < 60 \Rightarrow G$ auflösbar ☐

Lemma 8 Sei G einfache Gruppe mit $|G|=60$. Dann ist $G \cong A_5$.

Beweis: Sei $U \leq G$ mit $[G:U]=n$. Satz 12-2 $\Rightarrow$ es gibt $N \trianglelefteq G$ mit $N \subseteq U$ und $G/N \cong$ Ugr. von S_n. G einfach $\Rightarrow N=\{1\}$ und $G \cong$ Ugr. von S_n. $|G|=60 \Rightarrow n \geq 5$.

Angenommen, es gilt $n=5$. Dann sind wir fertig, denn dann $G \cong \tilde{G} \leq S_5$. Wäre $\tilde{G} \not\subseteq A_5$, so ex. $\pi \in \tilde{G}$ mit $\operatorname{sgn}(\pi)=-1$ $\Rightarrow$ $\operatorname{sgn}: \tilde{G} \to \{\pm 1\}$ surjektiv $\Rightarrow$ $\operatorname{Kern}(\operatorname{sgn}) \not\subseteq \tilde{G}$ $\Rightarrow$ $\tilde{G}$ nicht einfach $\Rightarrow$ G nicht einfach $\lightning$. Also $\tilde{G} \subseteq A_5$, $|\tilde{G}|=|G|=60=|A_5|$ $\Rightarrow$ $\tilde{G}=A_5$. Also genügt:

(*) Gibt es $U \leq G$ mit $[G:U]=5$, so $G \cong A_5$.

Caudy: $|U_5(G)| \equiv 1 \bmod 5$, also $= 1, 6, 11, 16, \ldots$

$|U_5(G)| \neq 1$ weil G einfach (Ü12) also $|U_5(G)| \geq 6$, d.h. es gibt mind. 6 Untergruppen der Ordnung 5, also mind. $6 \cdot (5-1) = 24$ Elemente der Ordnung 5.

$|U_3(G)| \equiv 1 \bmod 3$, also $= 1, 4, 7, 10, 13, \ldots$

$|U_3(G)| \neq 1$ also $|U_3(G)| \geq 4$, d.h. es gibt mind. $4 \cdot (3-1) = 8$ Elemente der Ordnung 3.

Also genügt:

(**) Es gibt höchstens $60-24-8=28$ Elemente anderer Ordnung als 3 oder 5.

Lemma 6 $\Rightarrow$ es gibt $U \leq G$ mit $4 \mid |U| \Rightarrow [G:U] \mid 15$ also $= 1, 3, 5$ oder 15. (nicht möglich)

Ist $[G:U]=5$, so sind wir fertig nach (*).

Nehmen wir also jetzt an: $[G:U]=15$.

$\Rightarrow |U|=4$ Sei $X=\{U_1, \ldots, U_r\}$ Menge der Untergruppen der Ordnung 4. $r \geq 2$ denn sonst U_1 einzige Ugr. der Ordnung 4, also $U_1 \trianglelefteq G \lightning$.

G operiert auf X durch $G \times X \to X$, $(g, U_i) \mapsto g U_i g^{-1}$ (siehe Ü12)

$U_i \not\subseteq G$ $\Rightarrow$ ex. $g \in G$ mit $g \cdot U_i \neq U_i$ $\Rightarrow$ zug. Homom. $\pi: G \to S_X$ hat $\operatorname{Kern}(\pi) \not\subseteq G$. G einfach $\Rightarrow$ $\operatorname{Kern}(\pi)=\{1\}$. also $G \cong$ Ugr. von $S_X \cong S_r$

also wieder $r \geq 5$. Ist $r = 5$, so $G \cong$ Norm. von S_5 Gleiches Argument wie oben $\Rightarrow G \cong A_5$ also fertig. Nehmen wir nun an $r > 5$.

Sei $U_i \in X \Rightarrow U_i \neq G$ also $\mathcal{O}_{U_i} \neq \{U_i\}$, $U_i \leq \mathrm{Stab}_G(U_i)$

$1 < |\mathcal{O}_{U_i}| = [G : \mathrm{Stab}_G(U_i)]$ | $[G : U_i] = 15$, also wieder

1, 3, 5, 15.

geht nicht.

also $5 \mid |\mathcal{O}_{U_i}| \Rightarrow 5 \mid r$.

Sind wir im Fall $r > 5$, also $r \geq 10$. D.h. es gibt mindestens 10 Untergruppen der Ordnung 4.

Sei $U_i \cap U_j \neq \{1\}$ für $i \neq j$: $1 \neq x \in U_i \cap U_j$

$\Rightarrow U_i, U_j \leq C_G(x)$. $\Rightarrow 4 \mid |C_G(x)|$ und $4 < |C_G(x)|$

(U_i, U_j abelsch nach Beisp. 12.12.) $\Rightarrow |G : C_G(x)| \mid 15$

$= 3, 5, 15$.

also $|G : C_G(x)| = 5$ wieder fertig nach (*)

Also können wir schließlich annehmen: $U_i \cap U_j = \{1\}$ für $i \neq j$:

Dann enthält aber $U_1 \cup \dots \cup U_{10}$ $10 \cdot (4-1) = 30$ Elemente der Ordnung 2 oder 4 $\lightning$ zu (**) $\square$

Die Argumente in diesem Anhang geben vielleicht einen Eindruck davon, wie kompliziert es sein wird, alle endlichen einfachen Gruppen zu bestimmen.

(Wir haben hier gezeigt, daß A_5 die kleinste endliche einfache (nicht abelsche) Gruppe ist.) Siehe dazu etwa:

R. Solomon, A brief history of the classification of the finite simple groups, Bull. of Amer. Math. Soc., vol. 38 (2001), 315–352.

§13 Symmetrische Polynome und der Fundamentalsatz der Algebra

Zurück zu §9 $L \supseteq K$ Körpererweiterung, $G := \mathrm{Aut}(L,K)$
(also Gruppe aller Automorphismen $\varphi: L \to L$ mit $\varphi(x) = x$ für alle $x \in K$)
Dann operiert G auf L durch $G \times L \to L$, $(\varphi, z) \mapsto \varphi.z = \varphi(z)$

Bem. 13.1 Sei $0 \neq f \in K[X]$ nicht-konstant und $X := \{z \in L \mid f(z) = 0\}$ Menge der Nullstellen von f; nehmen wir an $X \neq \emptyset$. Ist $n = \mathrm{Grad}(f)$, so $|X| \leq n$. Dann operiert G auch auf X $G \times X \to X$, $(\varphi, z) \mapsto \varphi(z)$
denn Bem. 9.13: $f(z) = 0 \Rightarrow f(\varphi(z)) = 0$ für $z \in L$, $\varphi \in G$.

Erhalten Homom. $\pi: G \to S_X$. Sei nun L Zerf.-körper, also $L = K(z_1, \dots, z_n)$ wobei $X = \{z_1, \dots, z_n\}$.
jedes $z \in L$ läßt sich schreiben als Polynom in $z_1, \dots, z_n$ mit Koeff. in K. Ist also $\varphi \in G$ mit $\varphi(z_i) = z_i$ für alle i, so
$\varphi = id \Rightarrow \pi: G \to S_X$ injektiv
$\Rightarrow G \cong$ Ugr. von S_n.
Dies ist der Ausgangspunkt der Galoistheorie ☺.

Bem. 13.2 Sei $\varphi \in G$ und $M_\varphi := \{z \in L \mid \varphi(z) = z\} \subseteq L$

Beh: M_φ Teilkörper von L mit $K \subseteq M_\varphi$.

Dazu: $\varphi(x) = x$ für alle $x \in K \Rightarrow K \subseteq M_\varphi$. Seien $z, z' \in M_\varphi$
$\Rightarrow \varphi(z) = z$, $\varphi(z') = \varphi(z') \Rightarrow \varphi(z \pm z') = \varphi(z) \pm \varphi(z') = z \pm z'$
also $z \pm z' \in M_\varphi$. $z \neq 0 \Rightarrow 1 = z \cdot z^{-1} \Rightarrow$
$1 = \varphi(1) = \varphi(z)\varphi(z^{-1}) = z \cdot \varphi(z^{-1}) \Rightarrow \varphi(z^{-1}) = z^{-1} \Rightarrow z^{-1} \in M_\varphi$.
also M_φ Körper. Damit Körpererweiterung $K \subseteq M_\varphi \subseteq L$.

Satz 13.3 Ist $[L:K] < \infty$, so $|G| < \infty$ und $|G| \leq [L:K]$
Weiterhin gibt es ein $z_0 \in L$ mit $\mathrm{Stab}_G(z_0) = \{id\}$

Zum Beweis benötigen wir einen Hilfssatz der Linearen Algebra.

Lemma 13.4 Sei K unendlicher Körper und V K-Vektorraum mit $\dim V < \infty$. Gegeben seien endl. viele Teilräume $U_1, \dots, U_r \subseteq V$.
Dann gilt: $U_i \subsetneq V$ für $1 \le i \le r \Rightarrow V \neq \bigcup_{i=1}^{r} U_i$.

Beweis von 13.4 Annahme $V = \bigcup_{i=1}^{r} U_i$. Zu zeigen: ex. i mit $V = U_i$.
Sei $n = \dim V$ und $\{v_1, \dots, v_n\}$ Basis von V. Für $x \in K$ def.

$$v(x) := v_1 + x v_2 + x^2 v_3 + \dots x^{n-1} v_n \in V.$$

(Beachte: können $n \ge 2$ annehmen, denn für $n = 1$ ist $U_i = \{0\}$ falls $U_i \subsetneq V$, also Behauptung klar.). Wegen $V = \bigcup U_i$ gibt es zu jedem $x \in K$ ein s mit $v(x) \in U_s$. Wegen $|K| = \infty$ gibt es also ein s mit $v(x) \in U_s$ für unendlich viele $x \in K$.
Insbesondere gibt es paarweise verschiedene $x_1, \dots, x_n \in K$ mit

$$v(x_i) = \sum_{j=1}^{n} x_i^{j-1} v_j =: u_i \in U_s.$$

$$M := (x_i^{j-1})_{1 \le i,j \le n} = \begin{bmatrix} 1 & x_1 & x_1^2 & \dots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \dots & x_2^{n-1} \\ \vdots & & & & \\ 1 & x_n & x_n^2 & \dots & x_n^{n-1} \end{bmatrix} \in M_n(K)$$

Vandermonde Matrix:

Es gilt $\det(M) = \prod_{1 \le i < j \le n} (x_j - x_i) \neq 0$. (siehe Wikipedia oder selbst)

Also M invertierbar. Also: $\{v_1, \dots, v_n\}$ Basis $\Rightarrow$ $\{u_1, \dots, u_n\}$ Basis
$u_i \in U_s$ für alle $i \Rightarrow \dim U_s \ge n \Rightarrow U_s = V$ ☐

Zweiter Beweis von 13.3: Ist $G = \{id\}$, so sind die Aussagen klar.
Sei nun $G \neq \{id\}$. Wir zeigen zuerst: es gibt $z_0 \in L$ mit $\mathrm{Stab}_G(z_0) = \{id\}$
Für $\varphi \in G$ sei $M_\varphi \subseteq L$ Teilmenge wie in Bem. 13.2.
L K-Vektorraum und jedes $M_\varphi \subseteq L$ Teilraum.
Ist $\varphi \neq id$, so $M_\varphi \subsetneq L$. $|G| < \infty$ nach Folg. 9.13.
Ist also $|K| = \infty$, so $\bigcup_{id \neq \varphi \in G} M_\varphi \subsetneq G$ nach Lemma 13.4.
$\Rightarrow$ es gibt $z_0 \in L$ mit $z_0 \notin M_\varphi$ für alle $id \neq \varphi \in G$
also $\varphi(z_0) \neq z_0$ für alle $id \neq \varphi \in G \Rightarrow \mathrm{Stab}_G(z_0) = \{id\}$ ✓
Sei nun $|K| < \infty$ wegen $[L:K] < \infty$ dann auch $|L| < \infty$.
Nach Satz 9.8 gibt es $z_0 \in L$ mit $L^\times = \langle z_0 \rangle$,
Ist $\varphi \in G$ mit $\varphi(z_0) = z_0 \Rightarrow \varphi = id$ also $\mathrm{Stab}_G(z_0) = \{id\}$ ✓

Sei nun $f = \mu_{z_0} \in K[X]$ Minimalpolynom von z_0. Es gilt $f(z_0) = 0$ und $f(\varphi(z_0)) = 0$ für alle $\varphi \in G$ (Bem. 13.1) $\Rightarrow \{\varphi(z_0) \mid \varphi \in G\}$ Bahn von z_0, hat Länge $[G : \mathrm{Stab}_G(z_0)] = |G|$ also hat f mindestens $|G|$ Nullstellen $\Rightarrow \mathrm{Grad}(f) \geq |G|$. Aber $K \subseteq K(z_0) \subseteq L$ Teilkörper mit $[K(z_0) : K] = \mathrm{Grad}(f)$ (Satz 7.9) Gradsatz

$\Rightarrow$ (*) $[L : K] = [L : K(z_0)] \cdot [K(z_0) : K] = \underbrace{[L : K(z_0)]}_{\geq 1} \cdot \underbrace{\mathrm{Grad}(f)}_{= |G|} \geq |G|$ ✓.

Def. Ist $|G| = [L : K] < \infty$, so heißt $L \supseteq K$ Galois-Erweiterung.

Bem. 13.5 (a) Sei $L \supseteq K$ Galoiserweiterung. Dann gibt es $z_0 \in L$ mit $L = K(z_0)$. Denn sei $z_0 \in L$ wie oben. Ist $|G| = [L : K]$, dann überall "$=$" in (*) in obigem Beweis, also $[L : K(z_0)] = 1$, $L = K(z_0)$ ✓.

(b) Sei L Zerf. körper von $0 \neq f \in K[X]$, $n = \mathrm{Grad}(f) \geq 1$.

Bem. 13.1 $G \cong$ Unt. von $S_n \Rightarrow |G| \leq n!$

A5 Wiederholungsübungen (oder gehe noch einmal Beweis von Satz 9.3 durch)

$\Rightarrow [L : K] \leq n!$ Satz 13.3 $|G| \leq [L : K]$

Also gelte: Ist $|G| \geq n!$, so folgt $G \cong S_n$ und $|G| = [L : K]$, d.h. $L \supseteq K$ Galoiserweiterung.

Solche Galoiserweiterungen könnte man als "extremal" bezeichnen.

Werden nun eine solche "extremale" Erweiterung beschreiben.

Erinnerung Beisp. 4.11: Sei R kommutativer Ring mit 1 und $n \geq 1$.

Dann $R[X_1, \dots, X_n]$ Polynomring mit n Variablen $X_1, \dots, X_n$.

Jedes $f \in R[X_1, \dots, X_n]$ läßt sich schreiben als endliche Summe

$$f = \sum_{i_1, i_2, \dots, i_n \geq 0} \underbrace{a_{(i_1, \dots, i_n)}}_{\in R,\ \text{nur endl. viele} \neq 0} X_1^{i_1} X_2^{i_2} \cdots X_n^{i_n} \qquad (*)$$

(Def. von $R[X_1, \dots, X_n]$ rekursiv $R[X_1, \dots, X_n] = (R[X_1, \dots, X_{n-1}])[X_n]$ etc.)

Haben bereits gesehen: R Integritätsring $\Rightarrow R[X_1, \dots, X_n]$ Integritätsring

faktoriell $\Rightarrow$ faktoriell

Analog zu Satz 4.13 haben wir universelle Eigenschaft:
Ist S kommutativer Ring mit 1, $\varphi: R \to S$ Ring-Homom. und $s_1, \dots, s_n \in S$ fest, so gibt es genau einen Ring-Homom. $\Phi_\varphi: R[X_1, \dots, X_n] \to S$ mit $\Phi_\varphi|_R = \varphi$ und $\varphi(X_i) = s_i$ für alle i.

Für f wie in (*) gilt:

$$\Phi_\varphi(f) = \sum \varphi(a_{i_1 \dots i_n}) \cdot s_1^{i_1} s_2^{i_2} \cdots s_n^{i_n}$$

d.h. Für $X_1, \dots, X_n$ werden $s_1, \dots, s_n$ eingesetzt und φ auf Koeff. angewandt "Einsetzungs-Homomorphismus".

Beweis folgt mit Satz 4.13 und Induktion nach n ✓ (selbst).

Def. 13.6 Sei $f \in R[X_1, \dots, X_n]$ und $\pi \in S_n$.
Sei $S = R[X_1, \dots, X_n]$, $\varphi: R \hookrightarrow S$, $r \mapsto r$ (Identität) und $s_i := X_{\pi(i)}$ für $1 \le i \le n$.
Dann gibt es also einen Ring-Homom.

$$\Phi_\pi: R[X_1, \dots, X_n] \to R[X_1, \dots, X_n] \text{ mit } \Phi_\pi(X_i) = X_{\pi(i)}$$
$$\text{und } \Phi_\pi(r) = r \text{ für alle } r \in R$$

Für $f \in R[X_1, \dots, X_n]$ also

$$\Phi_\pi(f) = f(X_{\pi(1)}, \dots, X_{\pi(n)})$$

In f ersetze überall Variable X_i durch $X_{\pi(i)}$.

z.B. $f = X_2 + X_3^2$ und $\pi = (123) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (12) \circ (23)$.

$\Rightarrow \Phi_\pi(f) = X_3 + X_1^2$

$\Phi_{(12)}(f) = X_1 + X_3^2$

$\Phi_{(23)}(f) = X_3 + X_2^2$

$$(\Phi_{(12)} \circ \Phi_{(23)})(f) = \Phi_{(12)}(X_3 + X_2^2) = X_3 + X_1^2 = \Phi_{(123)}(f).$$

Man sieht damit auch leicht: S_n operiert auf $R[X_1, \dots, X_n]$ durch

$$S_n \times R[X_1, \dots, X_n] \to R[X_1, \dots, X_n]$$
$$(\pi, f) \mapsto \pi \cdot f = \Phi_\pi(f).$$

Bem. 13.7 Sei nun R Integritätsring und $F \supseteq R$ Quotientenkörper von R (Bem 4.9), z.B. $R = \mathbb{Z}$, $F = \mathbb{Q}$.

$\Rightarrow R[X_{i-1}, X_n]$ Integritätsring. Also können wir auch davon Quotientenkörper bilden:

$$F_n := F(X_{i-1}, X_n) = \left\{ \frac{f}{g} \mid f, g \in R[X_{i-1}, X_n],\ g \neq 0 \right\}.$$

(rechne wie üblich mit Brüchen.) "Körper der rationalen Funktionen in n Variablen".

Für $\pi \in S_n$ erhalten wir dann $\sigma_\pi \in \mathrm{Aut}(F_n)$ durch

$$\sigma_\pi\left(\frac{f}{g}\right) = \frac{\Phi_\pi(f)}{\Phi_\pi(g)} \quad \text{für} \quad \frac{f}{g} \in F_n.$$

wohldef., denn sei $\frac{f}{g} = \frac{f'}{g'}$ dann $fg' = f'g$ also $\Phi_\pi(f)\Phi_\pi(g') = \Phi_\pi(fg') = \Phi_\pi(f'g) = \Phi_\pi(f')\Phi_\pi(g) \Rightarrow \frac{\Phi_\pi(f)}{\Phi_\pi(g)} = \frac{\Phi_\pi(f')}{\Phi_\pi(g')}$

Homomorphieeigenschaft folgt dann auch sofort. F_n Körper $\Rightarrow$ σ_π injektiv

σ_π surjektiv weil $X_{\pi(i)} = \sigma_\pi(X_i) \in \mathrm{Bild}(\sigma_\pi)$ für $1 \le i \le n$ also alle X_{i-1}, X_n im Bild.

$\Rightarrow$ $F_n = \sigma_\pi(F_n)$ ✓.

Sei $D_n := \{ z \in F_n \mid \sigma_\pi(z) = z \text{ für alle } \pi \in S_n \}$.

Bem. 13.2 $\Rightarrow$ D_n Teilkörper von F_n; klar $F \subseteq D_n \subseteq F_n$.

$\sigma_\pi(x) = x$ für alle $x \in D_n$ also $\sigma_\pi \in \mathrm{Aut}(F_n, D_n)$ im $\S 9$.

Satz 13.8 Bezeichnungen wie in Bem. 13.7. Dann gilt:

(a) $F_n \supseteq D_n$ Galoiserweiterung mit $\mathrm{Aut}(F_n, D_n) = \{ \sigma_\pi \mid \pi \in S_n \} \cong S_n$.

(b) Das Polynom $f = (X - X_1) \cdots (X - X_n) \in F_n[X]$ hat Koeffizienten in D_n und $F_n \supseteq D_n$ ist Zerfällungskörper von $f \in D_n[X]$.

Beweis: (b) Betrachte f und multipliziere aus:

$$f = (X - X_1) \cdots (X - X_n) = \sum_{i=0}^{n} a_i X^i \text{ mit } a_i \in R[X_{i-1}, X_n].$$

Sei $\pi \in S_n$ bel. $f' = (X - X_{\pi(1)}) \cdots (X - X_{\pi(n)}) = \sum_{i=0}^{n} a_i' X^i$ mit

Man erhält a_i' aus a_i, wenn man überall X_i durch $X_{\pi(i)}$ ersetzt, also $a_i' = a_i(X_{\pi(1)}, \ldots, X_{\pi(n)})$ $a_i' \in R[X_{i-1}, X_n]$.

$= \Phi_\pi(a_i) = \sigma_\pi(a_i)$ aber $f = f'$ und damit auch $a_i = a_i' = \sigma_\pi(a_i)$ für $0 \le i \le n$ also $a_i \in D_n$.

Damit $f \in D_n[X]$. Jedes X_i Nullstelle von f, also X_i algebraisch über $D_n \Rightarrow F_n \supseteq D_n$ algebraisch. Wegen $F_n = F(X_1, \dots, X_n) = D_n(X_1, \dots, X_n)$ folgt also: F_n Zerfällungskörper von f.

(a) Wiederholungsübung (oder gehe noch einmal Beweis von Satz 9.3 durch):

$F_n \supseteq D_n$ Zerf.körper von f wie in b), $\mathrm{Grad}(f) = n \Rightarrow [F_n : D_n] \leq n!$

Satz 13.3 $\Rightarrow$ $|\mathrm{Aut}(F_n, D_n)| \leq [F_n : D_n] \leq n!$

Andererseits: Abbildung $S_n \longrightarrow \mathrm{Aut}(F_n, D_n)$ ist

$\pi \longmapsto \sigma_\pi$

ein Homomorphismus (siehe Def. 13.6 und Bemerkungen dazu). S_n operiert auf $R[X_1, \dots, X_n]$ und dann auch auf F_n.

$\pi \neq \pi'$ in $S_n \Rightarrow$ ex. i mit $\pi(i) \neq \pi'(i) \Rightarrow$

$\sigma_\pi(X_i) = X_{\pi(i)} \neq X_{\pi'(i)} = \sigma_{\pi'}(X_i) \Rightarrow \sigma_\pi \neq \sigma_{\pi'}$, also

obiger Homom. injektiv $\Rightarrow$ $|S_n| \leq |\mathrm{Aut}(F_n, D_n)|$

aber dann überall "$=$" und damit $\mathrm{Aut}(F_n, D_n) \cong S_n$ $\square$.

Beisp. 13.9 Schauen uns jetzt noch einmal genauer Koeffizienten von $f = (X - X_1) \cdots (X - X_n)$ an.

$n = 2$ $\quad f = (X - X_1)(X - X_2) = X^2 - (X_1 + X_2)X + X_1 X_2$.

$n = 3$ $\quad f = (X - X_1)(X - X_2)(X - X_3) = \dots = X^3 - (X_1 + X_2 + X_3)X^2 +$

$$(X_1X_2 + X_1X_3 + X_2X_3)X - X_1X_2X_3$$

usw. Allgemein:

$$f = (X - X_1) \cdots (X - X_n) = X^n - s_1 X^{n-1} + s_2 X^{n-2} + \dots + (-1)^{n-1} s_{n-1} X + (-1)^n s_n$$

mit

$$s_1 = X_1 + X_2 + \dots + X_n$$

$$s_2 = \sum_{1 \leq i < j \leq n} X_i X_j$$

$$\vdots$$

$$s_r = \sum_{1 \leq i_1 < \dots < i_r \leq n} X_{i_1} X_{i_2} \cdots X_{i_r}$$

$$\vdots$$

$$s_n = X_1 X_2 \cdots X_n$$

Die s_i heißen "elementar-symmetrische Polynome". Nach Satz 13.8 gilt also $s_i \in D_n$, d.h. $\pi s_i = s_i$ für alle $\pi \in S_n$.

Def. 13.10 Ein Polynom $f \in R[X_1, \dots, X_n]$ heißt symmetrisch, wenn $\pi \cdot f = f(X_{\pi(1)}, \dots, X_{\pi(n)})$ für alle $\pi \in S_n$ gilt.

Aus Bem. in Def. 13.6 folgt: Summen und Produkte von symmetrischen Polynomen sind wieder symmetrisch, also ist

$$R[X_1, \dots, X_n]^{S_n} := \{ f \in R[X_1, \dots, X_n] \mid f \text{ symmetrisch} \}$$ ein Teilring von $R[X_1, \dots, X_n]$. "Ring der symmetrischen Polynome".

Beisp: Haben oben gesehen $s_i \in R[X_1, \dots, X_n]^{S_n}$ für $1 \le i \le n$

also etwa $s_1 = X_1 + \dots + X_n$ symmetrisch. Analog:

$X_1^k + X_2^k + \dots + X_n^k$ symmetrisch für jedes $k \ge 1$.

"Newton Potenzsumme"

Beachte auch: $X_1 + X_2$ symmetrisch in $R[X_1, X_2]$, aber nicht symmetrisch in $R[X_1, X_2, X_3]$ (wende z.B. Permutation $(23) \in S_3$ an)

Satz 13.11 (Hauptsatz über symmetrische Polynome, Newton, Gauß 1816)

Ist $f \in R[X_1, \dots, X_n]$ symmetrisch, so gibt es ein Polynom $g \in R[X_1, \dots, X_n]$ mit $f = g(s_1, \dots, s_n)$. D.h. "Jedes symmetrische Polynom läßt sich als Polynom in den elementar-symmetrischen Polynomen ausdrücken".

Beweis: Sei $f \in R[X_1, \dots, X_n]$ beliebig, $f \neq 0$. $\Rightarrow f$ = endliche Summe von Termen $a_{(i_1, \dots, i_n)} X_1^{i_1} X_2^{i_2} \dots X_n^{i_n}$ wobei $i_1, \dots, i_n \ge 0$

Ordne Typen $(i_1, \dots, i_n)$ "lexikographisch" an:

$(i_1, \dots, i_n) < (j_1, \dots, j_n)$ $\overset{\text{def.}}{\Leftrightarrow}$ es gibt ein $r < n$ mit

$i_1 = j_1, \dots, i_r = j_r$ und $i_{r+1} < j_{r+1}$.

Dann def. für f den Leitterm $LT(f)$ als

$LT(f) = a_{(i_1, \dots, i_n)} X_1^{i_1} \dots X_n^{i_n}$ wobei $a_{(i_1, \dots, i_n)} \neq 0$ und

$(j_1, \dots, j_n) < (i_1, \dots, i_n)$ für alle $a_{(j_1, \dots, j_n)} \neq 0$.

z.B. $f = 2X_1^3 X_2 + 3X_1^2 X_3^2 + X_2^4$ hat $LT(f) = 2X_1^3 X_2$.

Typen $(3,1,0) > (2,0,2) > (0,4,0)$

↑ max.

Übung (selbst): Ist auch $0 \neq g \in R[X_1, \dots, X_n]$, so gilt $LT(f \cdot g) = LT(f) \cdot LT(g)$

Nun sei $0 \neq f \in R[X_1, \dots, X_n]$ symmetrisch und $LT(f) = a X_1^{i_1} \cdots X_n^{i_n}$.

Beh: $i_1 \geq i_2 \geq \dots \geq i_n$

Dann: es gibt r mit $i_r < i_{r+1}$. Wende Transposition $(r\ r+1) \in S_n$ an

$\Rightarrow f = (r\ r+1) \cdot f \Rightarrow (r, r+1) \cdot LT(f) = a X_1^{i_1} \cdots \underbrace{X_{r+1}^{i_r} X_r^{i_{r+1}}}_{\text{Position } r, r+1} \cdots X_n^{i_n}$

kommt auch in f vor

$\Rightarrow (i_1, \dots, i_{r+1}, i_r, \dots, i_n) < (i_1, \dots, i_n) \Rightarrow i_{r+1} \leq i_r$ ↯.

Nun setze $h := a\, S_1^{i_1 - i_2} S_2^{i_2 - i_3} \cdots S_{n-1}^{i_{n-1} - i_n} \cdot S_n^{i_n} \in R[X_1, \dots, X_n]$ symmetrisch.

$LT(S_1) = X_1, \quad LT(S_2) = X_1 X_2, \dots, \quad LT(S_n) = X_1 X_2 \cdots X_n$

$\Rightarrow LT(h) = a X_1^{i_1 - i_2} (X_1 X_2)^{i_2 - i_3} \cdots (X_1 \cdots X_{n-1})^{i_{n-1} - i_n} (X_1 \cdots X_n)^{i_n}$

$= \cdots = a X_1^{i_1} \cdots X_n^{i_n} = LT(f)$.

$\Rightarrow f - h \in R[X_1, \dots, X_n]$ symmetrisch. Ist $f - h = 0$, so $f = h$ ✓.

Ist $f - h \neq 0$, so $LT(f - h) = b X_1^{j_1} \cdots X_n^{j_n}$ mit $(j_1, \dots, j_n) < (i_1, \dots, i_n)$

also fahre fort mit $f - h$. Nach endlich vielen Schritten bricht Verfahren ab. □

Beisp. $f = X_1^2 + X_2^2 + X_3^2 - \underbrace{S_1^2}_{= (X_1 + X_2 + X_3)^2} = -2X_1X_2 - 2X_1X_3 - 2X_2X_3$.

$(2,0,0) \quad (0,2,0) \quad (0,0,2)$

$= -2S_2$.

also $f = g(S_1, S_2, S_3)$ mit $g = X_1^2 + 2X_2$.

Obiger Beweis liefert Algorithmus zum Finden von g!

Folgerung 13.12 Sei K Körper, $0 \neq f \in K[X]$ nicht-konstant, normiert und $L \supseteq K$ Körper, über dem f in Linearfaktoren zerfällt. Sei $f = (X - z_1) \cdots (X - z_n)$ mit $z_i \in L$.

$\Rightarrow g(z_1, \dots, z_n) \in K$ für alle symmetrischen Polynome $g \in K[X_1, \dots, X_n]$ $n = \text{Grad}(f)$

Beweis: Nach Hauptsatz ist $g = h(S_1, \dots, S_n)$ mit $h \in K[X_1, \dots, X_n]$

$f = (X - z_1) \cdots (X - z_n) = \sum_{i=0}^{n} (-1)^{n-i} S_{n-i}(z_1, \dots, z_n) X^i$, also

$S_i(z_1, \dots, z_n) \in K$ für $1 \leq i \leq n \Rightarrow$

$g(z_1, \dots, z_n) = h(S_1(z_1, \dots, z_n), \dots, S_n(z_1, \dots, z_n)) \in K$ ✓.

Damit können wir nun zum Abschluss zeigen:

Fundamentalsatz der Algebra Sei $f \in \mathbb{C}[X]$ nicht-konstant. Dann zerfällt f über $\mathbb{C}$ in Linearfaktoren.

Beweis: Genügt zu zeigen: f hat Nullstelle $z_1 \in \mathbb{C}$. Denn dann $f = (X - z_1)\, g$ mit $g \in \mathbb{C}[X]$ und $\mathrm{Grad}(g) = \mathrm{Grad}(f) - 1$ also folgt Beh. mit Induktion nach $\mathrm{Grad}(f)$.

Genügt sogar zu zeigen: (*) Sei $f \in \mathbb{R}[X]$ nicht-konstant. Dann hat f Nullstelle in $\mathbb{C}$:

denn sei $0 \neq g \in \mathbb{C}[X]$ bel. $g = \sum_{j=0}^{n} a_j X^j$ mit $a_j \in \mathbb{C}$.

Setze $\bar{g} = \sum_{j=0}^{n} \bar{a}_j X^j$ Dann $f := g \cdot \bar{g} \in \mathbb{R}[X]$

Gelt (*), so hat f eine Nullstelle $z \in \mathbb{C}$. Nun ist $0 = f(z) = g(z)\overline{g(z)}$

Ist also $g(z) = 0$ o.k.✓. Ist $g(z) \neq 0$ dann $\bar{g}(z) = 0$, aber dann auch $0 = \overline{\bar{g}(z)} = g(\bar{z})$ also $\bar{z}$ Nullstelle von g in $\mathbb{C}$ ✓.

Also zeige nun (*). Sei $n = \mathrm{Grad}(f)$, schreibe $n = 2^l \cdot m$ mit $l \geq 0$ und $m \geq 1$ ungerade. Benutzen Induktion nach l.

Anfang $l = 0 \Rightarrow \mathrm{Grad}(f)$ ungerade $\Rightarrow$ $\lim_{x \to +\infty} f(x) = +\infty$

Zwischenwertsatz aus Analysis I $\lim_{x \to -\infty} f(x) = -\infty$.

(Bzw. die Funktion $x \mapsto f(x)$ ~~selbst~~ ist eine Funktion)

$\Rightarrow f$ hat sogar Nullstelle in $\mathbb{R}$.

Sei nun $l > 0$. Sei $L \supseteq \mathbb{C}$ Zerfällungskörper von f.

Können auch annehmen, dass f normiert ist, also (~1795).

$f = (X - z_1) \cdots (X - z_n)$ mit $z_i \in L$. Laplace-Trick:

Sei $t \in \mathbb{R}$ fest und bilde $g_t := \prod_{1 \leq r < s \leq n} (X - z_r - z_s - t z_r z_s) \in L[X]$

$\mathrm{Grad}(g_t) =$ Anzahl Paare (r,s) mit $1 \leq r < s \leq n = \binom{n}{2} = \frac{1}{2} n (n-1)$

$= \frac{1}{2} 2^l m (2^l m - 1) = 2^{l-1} m \underbrace{(2^l m - 1)}_{\text{ungerade weil } l \geq 0}$

ungerade.

Also können wir Induktion anwenden, aber dazu müssen wir noch wissen, daß $g_t \in \mathbb{R}[X]$ gelt. – Warum dies?

Betrachte dazu $G_t := \prod_{1 \le r < s \le n} (X - X_r - X_s - t X_r X_s) \in (\mathbb{R}[X_1, \dots, X_n])[X]$

Wende irgendeine Permutation $\pi \in S_n$ auf $X_1, \dots, X_n$ an.
$\rightsquigarrow$ Umordnung der Terme im obigen Produkt, also

$G_t = \sum_j g_j X^j$ mit $g_j \in \mathbb{R}[X_1, \dots, X_n]$ symmetrisch.

Nun folgt: $g_t = G_t(z_1, \dots, z_n) = \sum_j \underbrace{g_j(z_1, \dots, z_n)}_{\in \mathbb{R} \text{ nach Folg. 13.12}} X^j$

Also $g_t \in \mathbb{R}[X]$ ✓.

Nach Induktion hat g_t Nullstelle in $\mathbb{C}$, also gibt es $1 \le r < s \le n$ mit $z_r + z_s + t z_r z_s \in \mathbb{C}$.

Es gibt unendl. viele $t \in \mathbb{R}$ aber nur endlich viele Paare (r,s) mit $1 \le r < s \le n$, also gibt es $t \neq t'$ in $\mathbb{R}$ und $1 \le r < s \le n$ mit

$$z_r + z_s + t z_r z_s \in \mathbb{C}$$
$$z_r + z_s + t' z_r z_s \in \mathbb{C}.$$

$\Rightarrow a := z_r + z_s \in \mathbb{C}$ (bilde Differenz)
$b := z_r \cdot z_s \in \mathbb{C}$.
also $X^2 - aX + b = (X - z_r)(X - z_s) \in \mathbb{C}[X]$

Über quadratische Polynome haben immer Nullstellen in $\mathbb{C}$ ($\mathbb{C}$!) $\Rightarrow$ $z_r, z_s \in \mathbb{C}$.

Damit Fundamentalsatz vollständig bewiesen. Haben benutzt:

* Abstrakte Existenz von Zerfällungskörpern (Satz 9.3)
* Hauptsatz über symmetrische Polynome
* aus Analysis: – Zwischenwertsatz über stetige Funktionen
  – quadratische Polynome haben Nullstellen in $\mathbb{C}$.

□