Skript zur Vorlesung

Algebra

Wintersemester 2005/2006

Universität Konstanz
Prof. Dr. Claus Scheiderer

private Mitschrift

Stand: 17. Februar 2006
www.meidert.net/uni

Achtung:
Dies ist kein offizielles Skript, sondern nur eine private Mitschrift. Ich kann daher keine Gewähr für die Richtigkeit und Vollständigkeit übernehmen. Vor allem können die Nummerierungen zum Teil von den in den Vorlesungen verwendeten abweichen. Falls jemand einen Fehler entdeckt, so möge er/sie mir bitte eine eMail schicken - vielen Dank!

Frieder Meidert (uni@meidert.net)

Inhaltsverzeichnis

1. Kommutative Ringe

a. Polynome, Potenzreihen, Quotientenkörper

1.1.
Seien alle Ringe kommutativ mit 1.
Alle Ringhomomorphismen $\varphi : A \to B; \varphi(1) = 1$
Ideale $I \subset A$: $aI \subset I \; \forall \; a \in A$
$\rightsquigarrow A/I = \{a + I : a \in A\}$
$a + I = b + I \Rightarrow b - a \in I$.
$V : A \to B \rightsquigarrow \ker(\varphi)$ ist Ideal in A.
$A/\ker\varphi \cong B$, falls φ surjektiv.
A nullteilerfrei: $\forall \; a, b \in A \; (ab = 0 \Rightarrow a = 0 \vee b = 0)$
$A^* = \{u \in A : \; \exists \; v \in A \; mit \; uv = 1\}$, die Gruppe der Einheiten, $v = u^{-1}$.
Körper $\mathbb{K}$: $(\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p)$, Ringe: $\mathbb{K}[t], Z, Z[i]$.

1.2.
Sei $d \in \mathbb{Z}$, betrachte den Ring $\mathbb{Z}[\sqrt{d}] := \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}$ ($\sqrt{d} \in \mathbb{C}$ fest gewählt)
$\mathbb{Z}[\sqrt{d}] \subset \mathbb{C}$ ist ein Teilring: $(a + b\sqrt{d})(a' + b'\sqrt{d}) = (aa' + bb'd) + (ab' + a'b)\sqrt{d}$.

Setze voraus: d keine Quadratzahl in $\mathbb{Z}$. Dann sind $1, \sqrt{d}$ linear unabhängig in $\mathbb{Q}$:
$a + b\sqrt{d} = 0, a, b = 0 \Rightarrow a^2 = b^2 d \Rightarrow d$ ist Quadratzahl, Widerspruch.

Was sind die Einheiten in $\mathbb{Z}[\sqrt{d}]$?
Definiere für $x = a + b\sqrt{d}$ $(a, b \in \mathbb{Z})$ die **Norm von** x als $N(x) := a^2 - b^2 \in \mathbb{Z}$.

Satz 1.3.

(a) $N(xy) = N(x)N(y) \; \forall \; x, y \in \mathbb{Z}[\sqrt{d}]$

(b) $\mathbb{Z}[\sqrt{d}]^* = \{x \in \mathbb{Z}[\sqrt{d}] : N(x) = \pm 1\}$.

Beweis:

(a) Sei $\sigma : \mathbb{Z}[\sqrt{d}] \to \mathbb{Z}[\sqrt{d}]$ der durch $\sigma(a + b\sqrt{d}) := a - b\sqrt{d}$ definierte Ringhomomorphismus.
$\sigma((a + b\sqrt{d})(a' + b'\sqrt{d})) = (aa' + bb'd) - (ab' + a'b)\sqrt{d} = (a - b\sqrt{d})(a' - b'\sqrt{d}) = \sigma(a + b\sqrt{d}) \cdot \sigma(a' + b'\sqrt{d})$
Es ist $N(x) = x \cdot \sigma(x)$, also $N(xy) = (xy)\sigma(xy) = xy \cdot \sigma(x) \cdot \sigma(y) = N(x) \cdot N(y)$.

(b) Sei x eine Einheit: $1 = N(1) = N(xx^{-1}) = N(x) \cdot N(^{-1}) = N(x) \cdot N(x)^{-1} \Rightarrow N(x) \in \{\pm 1\}$.
Umgekehrt: ist $N(x) =: \varepsilon = \pm 1 \Rightarrow 1 = \varepsilon^2 = x\sigma(x) \cdot \varepsilon \Rightarrow x^{-1} = \varepsilon \cdot \sigma(x) \Rightarrow x$ ist eine Einheit.

□

Bemerkung 1.4.
$\mathbb{Z}[\sqrt{d}]^*$ besteht aus allen $a + b\sqrt{d}$, bei denen $(a, b) \in \mathbb{Z}^2$ die Lösungen von $a^2 - b^2 d = \pm 1$ durchläuft.
$d = -1$: $\mathbb{Z}[\sqrt{-1}]^* = \{\pm 1, \pm i\}$
$d \leq -2$: $\mathbb{Z}[\sqrt{d}]^* = \{\pm 1\}$
$d > 2$: man kann zeigen, dass es unendlich viele Einheiten gibt.

1.5.
Zu jedem Ring A habe $A[t]$.
Elemente sind die $f = \sum_{i=0}^{n} a_i \cdot t^i, a_i \in A, n \in \mathbb{N} \cup \{0\}$.

Ist $a_n \neq 0 \Rightarrow n = \deg(f)$. Es gilt:
$\deg(f + g) \leq \max\{\deg(f), \deg(g)\}$
$\deg(f\dot{g}) \leq \deg(f) + \deg(g)$, Gleichheit falls A nullteilerfrei.
$\deg(0) := -\infty$.

Insbesondere: A nullteilerfrei $\Rightarrow A[t]$ nullteilerfrei, und $A[t]^* = A^*$.
Universelle Eigenschaft:

Lemma 1.6.
Sei $\varphi : A \to B$ ein Ringhomomorphismus, sei $b \in B$. Dann existiert genau eine Fortsetzung $\psi : A[t] \to B$ von φ zu einem Ringhomomorphismus ψ mit $\psi(t) = b$.

Beweis:
Man muss definieren $\psi(\sum_i a_i t^i) := \sum_i \varphi(a_i) b^i$.

□

$a \in A$ heißt **Nullstelle** von $f \in A[t]$, wenn $f(a) = 0$.

Lemma 1.7.
Ist $f \in A[t]$ und $a \in A$ mit $f(a) = 0$, so $\exists\, g \in A[t]$ mit $f = (t - a) \cdot g$.

Beweis:
Induktion nach $n = \deg(f)$.
Ist $\deg(f) \leq 0 \Rightarrow f = 0$: OK.
Sei $f = ct^n + (\textit{kleinere Grade})$, schreibe $f := ct^{n-1}(t-a) + f_1 \Rightarrow \deg(f_1) < n$ und $f_1(a) = 0 \Rightarrow f_1 = (t-a)g_1 \Rightarrow f = (t-a)\underbrace{(ct^{n-1} + g_1)}_{=:g}$.

□

Korollar 1.8.
Ist A nullteilerfrei, $f \in A[t]$ und sind $a_1, \ldots, a_r \in A$ paarweise verschiedene Nullstellen von f, so $\exists\, g \in A[t]$: $f = (t-a_1) \cdot \ldots \cdot (t-a_r) \cdot g$.
Insbesondere ist $r \leq \deg(f)$.

Beweis:
$f = (t-a_1) \cdot f_1$ nach Lemma 1.7 Einsetzen von $a_2 \Rightarrow f_1(a_2) = 0$. Nun Induktion.

□

1.9.
Man definiert induktiv:
$A[t_1, \ldots, t_n] := A[t_1, \ldots, t_{n-1}][t_n]$ für $n \in \mathbb{N}$.
Die Elemente von $A[t_1, \ldots, t_n]$ sind die endlichen Summen $\sum\limits_{\alpha \in \mathbb{Z}_+^n} a_\alpha t^\alpha$, mit $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}_+^n$ ($\mathbb{Z}_+ := \mathbb{N}_0 := \mathbb{N} \cup \{0\}$).
$t^\alpha := t_1^{\alpha_1} \cdot \ldots \cdot t_n^{\alpha_n}$, $a_\alpha = 0$ *f.f.a. a.*
A nullteilerfrei $\Rightarrow A[t_1, \ldots, t_n]$ nullteilerfrei und $A[t_1, \ldots, t_n]^* = A^*$.

Ist $A = \mathbb{K}$ ein Körper, so hatten wir gesehen: $A[t]$ ist ein Hauptidealring.
In $n \geq 2$ Variablen ist dies falsch.

1.10.
Eine **formale Potenzreihe** über A (in t) ist

$$f = \sum_{n=0}^{\infty} a_n t^n \text{ mit } a_n \in A$$

(beliebig viele dürfen $\neq 0$ sein!).

Nebenbemerkung:
Keine Konvergenzbetrachtung: $f = \sum\limits_{n=0}^{\infty} a_n t^n = a_0 + a_1 t + a_2 t^2 + \ldots$ als symbolischer

Ausdruck!

Definiere + und · für formale Potenzreihen:

$$\left(\sum_n a_n t^n\right) + \left(\sum_n b_n t^n\right) := \left(\sum_n (a_n + b_n) t^n\right)$$
$$\left(\sum_n a_n t^n\right) \cdot \left(\sum_n b_n t^n\right) := \sum_n c_n t^n$$

wobei $c_n := \sum_{i=0}^{n} a_i b_{n-i}$ $(n \geq 0)$ sei.

Man sieht sofort, dass diese Operationen die Ringaxiome erfüllen, und definiert:

Definition 1.11.
Der Ring aller formalen Potenzreihen über A wird mit $A[\![t]\!]$ bezeichnet.

1.12.
Wie bei Polynomen gibt es eine Art „Grad“:
für $f = \sum_{n\geq 0} a_n t^n$ sei $w(f) := \inf\{n \geq 0 : a_n \neq 0\}$ $(w(0) := \infty)$, die Ordnung von f.

Es gilt: $w(f + g) \geq \min\{w(f), w(g)\}$, $w(f \cdot g) \geq w(f) + w(g)$.

Ist A nullteilerfrei, so gilt $w(fg) = w(f) + w(g)$.
Insbesondere ist dann auch $A[\![t]\!]$ nullteilerfrei.

Vorsicht:
In formalen Potenzreihen kann man im Allgemeinen keine Werte einsetzen. Ausnahme ist $t = 0$: $f(0) := a_0$ für $f = \sum_{n\geq 0} a_n t^n$. Die Abbildung $A[\![t]\!] \to A, f \mapsto f(0)$ ist ein Ringhomomorphismus.

Satz 1.13.
Für $f \in A[\![t]\!]$ gilt: $f \in A[\![t]\!]^* \Rightarrow f(0) \in A^*$.

Beweis:

„⇒“ : $f \cdot g = 1 \Rightarrow f(0) \cdot g(0) = 1 \Rightarrow f(0) \in A^*$.

„⇐“ : sei $f = \sum_{n\geq 0} a_n t^n$ mit $f(0) = a_0 \in A^*$.
Schreibe $f = a_0 \cdot \underbrace{\left(1 + \frac{a_1}{a_0}t + \frac{a_2}{a_0}t^2 + \ldots\right)}_{=:g} =: a_0(1+g)$ mit $w(g) \geq 1$.

Zeige: für solches g ist $1 + g \in A[\![t]\!]^*$.
$\left[\frac{1}{1+x} = 1 - x + x^2 - x^3 + \ldots\right]$
Setze $h := \sum_{n\geq 0} (-1)^n g^n = 1 - g + g^2 - g^3 + \ldots$
(das ist eine Definition (!!)

Behaupte $(1+g)\dot{h} = 1$. Für jedes feste $n \geq 0$ ist $h = 1 - g + g^2 + - \ldots + (-1)^n g^n + h_1$
mit $w(h_1) \geq n+1 \Rightarrow (1+g)h = \underbrace{(1+g)(1 - g + g^2 + \ldots \pm g^n)}_{1 \pm \underbrace{g^{n+1}}_{w\geq n+1}} + (1 + \underbrace{g)h_1}_{w\geq n+1}$

$\Rightarrow (1+g) \cdot h = 1$ (da für jedes $n \geq 0$ obiges gilt)

□

Satz 1.14.
Ist $A = \mathbb{K}$ ein Körper, so ist $K[\![t]\!]$ ein Hauptidealring.
Für $f, g \in \mathbb{K}[\![t]\!]$ gilt: $f \mid g \Leftrightarrow w(f) \leq w(g)$.
Die einzigen Ideale von $K[\![t]\!]$ sind (0) und (t^n) für $n \geq 0$.

Beweis:
Sei $w(f) = n \geq 0$ da A ein Körper ist, folgt $f = t^n \cdot g$ mit $g(0) \neq 0$. Nach 1.13 ist g eine Einheit $\Rightarrow f \sim t^n$.

□

Frage: Welche Ringe lassen sich in Körper einbetten?
Notwendig: nullteilerfrei, zeigen: das ist auch hinreichend!

Definition 1.15.
Eine **multiplikative Teilmenge** von A (= beliebiger Ring) ist eine Teilmenge $S \subset A$ mit $1 \in S$ und mit $(s_1, s_2 \in S \Rightarrow s_1 \cdot s_2 \in S)$

Beispiel 1.16.

(1) $S :=$ Menge aller Nichtnullteiler von A: $1 \in S$, $s_1, s_2 \cdot q = 0 \Rightarrow q = 0$.

(2) $S := \{1, s, s^2, s^3, \ldots\}$ für ein festes $s \in A$.

(3) $A = \mathbb{Z}$, p eine feste Primzahl, $S := \{n \in \mathbb{Z} : p \nmid n\}$.

Konstruktion 1.17.
Sei $S \subset A$ eine multiplikative Teilmenge aus Nichtnullteilern.
Für $(a, s), (a', s') \in A \times S$ definiere
$(a, s) \sim (a', s') :\Leftrightarrow as' = a's$.
Das ist eine Äquivalenzrelation auf $A \times S$ (symmetrisch, reflexiv OK); transitiv:
Ist $(a, s) \sim (a', s')$ und $(a', s') \sim (a'', s'')$, also $as' = a's$ (I) und $a's'' = a''s'$ (II)
zu zeigen: $as'' = a''s$.
$(as')s'' \underbrace{=}_{(I)} (a's)s'' = s(a's'') \underbrace{=}_{(II)} s(a''s')$.
Kürzen mit s' (möglich, da nicht Nullteiler) ergibt $as'' = a''s$.

Mit $\frac{a}{s}$ wird die Äquivalenzklasse von (a, s) bezeichnet. Mit $A_S := \left\{\frac{a}{s} : a \in A, s \in S\right\}$ bezeichnet man die Menge aller Äquivalenzklassen. Definiere + und $\cdot$ aus A_S:
$\frac{a}{s} + \frac{b}{t} := \frac{at+bs}{st}$, $\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}$.
Dies ist wohldefiniert, z.B. Addition:
$(a, s) \sim (a', s')$, $(b, t) \sim (b', t')$
muss zeigen: $(at + bs, st) \sim (a't' + b't', s't')$, also $(at + bs)s't' = (a't' + b's')st$.

Lemma 1.18.
Mit den so definierten Operationen + und $\cdot$ wird A_S zu einem kommutativen Ring. Die Null ist $\frac{0}{1}$, die Eins ist $\frac{1}{1}$.

Satz 1.19.

(a) Die Abbildung $\varphi : A \to A_S, \varphi(s) := \frac{a}{1}$, ist ein injektiver Ringhomomorphismus mit $\varphi(S) \subset (A_S)^*$ ($\Rightarrow$ man kann A als Unterring von A_S auffassen).

(b) Ist $\psi : A \to B$ ein beliebiger Ringhomomorphismus mit $\psi(S) \subset B^*$, so existiert eine eindeutige Fortsetzung $\widetilde{\psi} : A_S \to B$ von ψ:

$$B \underbrace{\leftarrow}_{\varphi} A_S \underbrace{\leftarrow}_{\widetilde{\psi}} A \underbrace{\rightarrow}_{\psi} B \text{ kommutiert.}$$

Beweis:

(a) $\frac{a}{1} + \frac{b}{1} = \frac{a+b}{1}, \frac{a}{1} \cdot \frac{b}{1} = \frac{ab}{1}, \varphi(1) = \frac{1}{1}$;
$\varphi(a) = \frac{0}{1} \Rightarrow \frac{a}{1} = \frac{0}{1} \Rightarrow a = 0$
$\varphi(s) = \frac{s}{1} : \frac{s}{1} \cdot \frac{1}{s} = \frac{s}{s} = \frac{1}{1}$.

(b) Für $\frac{a}{s} \in A_S$: $\frac{s}{1} \cdot \frac{a}{s} = \frac{a}{1} \Rightarrow \psi(s) = \widetilde{\psi}(\frac{s}{1}) \cdot \widetilde{\psi}(\frac{a}{s}) = \widetilde{\psi}(\frac{a}{1}) = \psi(a)$
$\Rightarrow$ es muss sein $\widetilde{\psi}(\frac{a}{s}) = \psi(s)^{-1} \cdot \psi(a)$
(das geht, da $\psi(s) \in B^*$).
Man prüft: $\widetilde{\psi}$ ist dadurch wohldefiniert und homomorph.

□

Definition und Satz 1.20.
Sei A nullteilerfrei, sei $S ::= A \setminus \{0\}$. Dann ist Quot $(A) := A_S$ ein Körper, genannt der ***Quotientenkörper von*** *A.*

Beweis:
Zu $\frac{a}{s}$ mit $0 \neq a, s \in A$, ist $\frac{s}{a}$ invers:
$\frac{a}{s} \cdot \frac{s}{a} = \frac{1}{1}$.

□

Folgerung 1.21.
Ein Ring ist genau dann nullteilerfrei, wenn er zu einem Teilring eines Körpers isomorph ist.
(„$\Rightarrow$“ sei $S := A \setminus \{0\}$; dann ist $B := \{\frac{a}{1} : a \in A\}$ ein Teilring von A_S, und $A \cong B$)

Beispiele 1.22.

1. $A = \mathbb{Z}$: Quot $(\mathbb{Z}) = \mathbb{Q}$
2. $A = \mathbb{K}[t]$, $\mathbb{K}$ ein Körper. Man schreibt $\mathbb{K}(t) =$ Quot $(\mathbb{K}[t])$
$\mathbb{K}(t) = \left\{\frac{f}{g} : f, g \in \mathbb{K}[t], g \neq 0\right\}$, mit der bekannten Gleichheitsregel.

b. Primideale und maximale Ideale

Definition 1.23.
Ein Ideal I von A heißt **prim**, oder ein **Primideal**, wenn A/I nullteilerfrei und $I \neq A$ ist.

Lemma 1.24.
Ein Ideal y von A ist genau dann prim, wenn $y \neq A$ ist und gilt: $\forall\, a, b \in A\ (a \cdot b \in y \Rightarrow a \in y \vee b \in y)$

Beispiel 1.25.

1. Die Primideale von $\mathbb{Z}$ sind genau die (0) und die (p) mit p eine Primzahl.
2. Ist A ein Hauptidealring, so sind die Primideale $\neq (0)$ von A genau die (π) mit π irreduzibel.
3. Jedes maximale Ideal m in A ist ein Primideal.
   (m maximal heißt $m \neq (1)$, und für alle Ideale n mit $m \subset n$ gilt: $m = n$ oder $n = (1)$)
   (denn: A/m ist ein Körper, siehe LA VII)
4. Ist $I \subset A$ ein Ideal, so sind die Primideale von A/I genau die J/I mit J ein Primideal von $A, I \subset J$:
   denn $\frac{(A/I)}{(J/I)} \cong A/J$ $(I \subset J \subset A)$

1.26.
Die Menge aller Primideale von A heißt das **(Zariski-)Spektrum von** A, in Zeichen Spec (A).

Satz 1.27 (Urbilder von Primidealen sind wieder Primideale)**.**
Ist $\varphi : A \to B$ ein Ringhomomorphismus, und $q \in Spec\ (B)$, so ist $\varphi^{-1}(q) \in Spec\ (A)$.

Beweis:
Der zusammengesetzte Homomorphismus $A \underbrace{\to}_{\varphi} B \underbrace{\to}_{\pi} \underbrace{B/q}_{nullteilerfrei}$ hat den Kern $\varphi^{-1}(q)$. Der Homomorphiesatz sagt:
$A/\varphi^{-1}(q) \hookrightarrow B/q$.
Da B/q nullteilerfrei ist, ist auch $A/\varphi^{-1}(q)$ nullteilerfrei. □
Der Homomorphismus $\varphi : A \to B$ induziert also eine Abbildung $\varphi^* : \text{Spec}\ (B) \to$

Spec $(A), q \to q^{-1}(q)$. (umgekehrte Richtung!)

□

Satz 1.28.
Sei S eine multiplikative Teilmenge von A, mit $0 \notin S$.
Es gibt ein bezüglich „$I \cap S = \emptyset$“ maximales Ideal I von A.
Jedes solche I ist ein Primideal von A.

Nebenbemerkung: die erste Aussage sagt: $I \cap S = \emptyset$, und für jedes Ideal $J \supset I$ mit $J \cap S = \emptyset$ ist $J = I$.

Folgerung 1.29.
Jeder Ring $A \neq \{0\}$ hat mindestens ein maximales Ideal (und insbesondere auch ein Primideal).

Beweis:
Nimm $S = \{1\}$ in 1.28.
Dann ist I aus 1.28 maximal in A, denn:
$I \neq (1)$, und für alle $J \supset I$ gilt $J = I$ oder $J = (1)$, denn: angenommen, $I \subsetneq J \neq (1)$; dann wäre I nicht maximal bezüglich „$I \cap S = \emptyset$“.

□

Definition 1.30.
Sei M eine Menge, sei $\mathfrak{X} \subset P(M)$ ($P(M)$:= Potenzmenge von M). Dann nennt man ein $A \in \mathfrak{X}$ **maximales Element von** $\mathfrak{X}$, wenn $\forall\ B \in \mathfrak{X}$ gilt: $A \subset B \Rightarrow A = B$. Die Menge $\mathfrak{X}$ heißt eine **Kette** (oder: **linear geordnet**), wenn $\forall\ A_1, A_2 \in \mathfrak{X}$ gilt: $A_1 \subset A_2$ oder $A_2 \subset A_1$.

Theorem 1.31 (Zorn'sches Lemma)**.**
Sei $\mathfrak{X} \subset P(M)$ derart, dass gilt: zu jeder Kette $y \subset \mathfrak{X}$ gibt es ein $A \in \mathfrak{X}$ mit $B \subset A$ für alle $B \in y$. Dann enthält $\mathfrak{X}$ ein maximales Element.

Beweis:
Ist trivial, falls $\mathfrak{X}$ endlich ist. Ist $\mathfrak{X}$ beliebig, so ist der Beweis nicht klar. Sein Beweis gehört in die Grundlagen der Mengenlehre:
Friedrichsdorf-Prestel: Mengenlehre für den Mathematiker, Vieweg.

□

Beweis: (von 1.28)

(i) Sei $\mathfrak{X}$:= Menge aller Ideale $I \subset A$ mit $I \cap S = \emptyset$.
$\mathfrak{X}$ erfüllt die Voraussetzungen des Zorn'schen Lemmas:
sei $(I_\nu)_{\nu \in y}$ eine Kette in $\mathfrak{X}$. Es ist $I := \bigcup_{\nu \in y} I_\nu$ wieder ein Ideal von A (!) und $I \cap S = \emptyset$, also $I \in \mathfrak{X}$. Zorn'sches Lemma $\Rightarrow$ $\mathfrak{X}$ enthält ein maximales Element.
Das ist genau die erste Aussage in 1.28.

(ii) Sei I maximal unter $I \cap S = \emptyset$. Seien $a, b \in A$ mit $ab \in I$; zu zeigen: $a \in I \vee b \in I$.
Angenommen $a \notin I, b \notin I$. Dann sind $I + (a), I + (b)$ echte Oberideale von I, treffen also S.
D.h. $\exists\, x, y \in I, c, d \in A$ mit $x + ac \in S, y + bd \in S$.
Multipliziere: $S \ni (x + ac)(y + bd) = xy + xbd + acy + abcd \in I$; Widerspruch zu $I \cap S = \emptyset \Rightarrow I$ ist ein Primideal von A.

□

Definition 1.32.
Ein $a \in A$ heißt **nilpotent**, falls $\exists\, n \in \mathbb{N}$ mit $a^n = 0$.

Korollar 1.33.
Die Menge Nil (A) aller nilpotenten Elemente von A ist genau der Durchschnitt aller Primideale von A. Insbesondere ist Nil (A) ein Ideal, genannt das ***Nilradikal*** *von A.*

Beweis:
Jedes nilpotente Element liegt in jedem Primideal (sei y ein Primideal, $a \cdot a^{n-1} = 0 \in y \Rightarrow a \in y \vee a^{n-1} \in y \Rightarrow a \in y$).
Umgekehrt sei $a \in A$ nicht nilpotent. Sei $S := \{1, a, a^2, \ldots\}$ eine multiplikative Menge mit $0 \notin S$.
1.28 $\Rightarrow$ $\exists$ Primideal y mit $y \cap S = \emptyset$. Insbesondere $a \notin y$.

□

Beispiel 1.34.
Sei $A := \mathbb{Z}/(360)$. $360 = 2^3 \cdot 3^2 \cdot 5$.
$\Rightarrow$ die Primideale von A sind $(\overline{2}), (\overline{3}), (\overline{5})$
$\Rightarrow$ Nil $(A) = (\overline{2}) \cap (\overline{3}) \cap (\overline{5}) = (\overline{30}) = \{\overline{0}, \overline{30}, \overline{60}, \ldots, \overline{330}\}$.

1.35.
Sei $S \subset A$ eine multiplikative Teilmenge von Nichtnullteilern. Was sind die Primideale von A_S?
(Nebenbemerkung: A_S wird in manchen Büchern als $S^{-1}A$ bezeichnet)
Sei $\varphi : A \to A_S, \varphi(a) = \frac{a}{1}$. Für jedes Ideal $I \subset A$ sei $I_S := IA_S := \{\frac{a}{s} : a \in I, s \in S\}$; die ist ein Ideal in A_S, genauer: $I_S = IA_S$ ist das von $\varphi(I)$ in A_S erzeugte Ideal.

Satz 1.36.

(a) *Jedes Ideal y von A_S ist von der Form $I_S = IA_S$ für ein Ideal I von A, z.B. für $I = \varphi^{-1}(y)$.*

(b) *Ist y ein Primideal von A (mit $y \cap S = \emptyset$), so ist $y_S = yA_S$ ein Primideal von A_S, und $y = \varphi^{-1}(y_S)$.*

(c) *Die Abbildung $\varphi^* : Spec\,(A_S) \to Spec\,(A), \varphi^*(q) = \varphi^{-1}(q)$ ist eine Bijektion von $Spec\,(A_S)$ auf die Menge $D(S) := \{y \in Spec\,(A) : y \cap S = \emptyset\}$. Die Umkehrabbildung ist $y \to y_S$.*

Beweis:

(a) $I := \varphi^{-1}(J)$ (I ist Ideal, da J Ideal ist). Dann $\varphi(I) \subset J$, also $I_S \subset J$.
Umgekehrt: ist $\frac{a}{s} \in J$, so $J \ni \frac{s}{1} \cdot \frac{a}{s} = \frac{a}{1} \in J$, also wegen $\frac{a}{s} = \underbrace{\frac{a}{1}}_{\in\varphi(I)} \cdot \underbrace{\frac{1}{s}}_{\in A_S} \in I_S$ gilt
$I_S = J$.

(b) (i) $\frac{1}{1} \notin y_S$ wegen $y \cap S = \emptyset$.
Seien $\frac{a}{s}, \frac{b}{t} \in A_S$ mit $\frac{ab}{st} \in y_S$, d.h. $\frac{ab}{st} = \frac{c}{u}$ mit $c \in y$.
Das heißt $ab \underbrace{u}_{\notin y} = cst \in y \underbrace{\Rightarrow}_{y\ prim} a \in y \vee b \in y$.
Also $\frac{a}{s} \in y_S \vee \frac{b}{t} \in y_S$. Also y_S prim in A_S.

(ii) $y \subset \varphi^{-1}(y_S)$. Umgekehrt: ist $\frac{a}{1} \in y_S$ prim in A_S etwa $\frac{a}{1} = \frac{b}{s}$ mit $b \in y \Rightarrow as = b \Rightarrow a \in y$.
Also $y = \varphi^{-1}(y_S)$.

(iii) $Spec\,(A_S) \underbrace{\to}_{\varphi^*} Spec\,(A), q \mapsto \varphi^{-1}(q) =: y$
$y_S \hookleftarrow y$.

□

Definition 1.37.
A heißt ein **lokaler Ring**, wenn A nur genau ein maximales Ideal hat.

Bemerkungen und Beispiele 1.38.

(1) Jeder Körper ist ein lokaler Ring (maximales Ideal (0)).

(2) $A = \mathbb{K}[\![t]\!]$ (für $\mathbb{K}$ ein Körper) ist ein lokaler Ring. (maximales Ideal: (t); denn $(0), (t^n)$ für $n \geq 1$ sind die einzigen Ideale in $\mathbb{K}[\![t]\!]$)

Definition und Satz 1.39.
*Sei A nullteilerfrei, sei y ein Primideal von A. Dann ist $S := A \setminus y$ eine multiplikative Menge in A. Man schreibt $A_y := A_S$ (Ring der Brüche mit Nennern in S) und nennt A_y die **Lokalisierung von A im Primideal** y.*
Der Ring A_y ist lokal mit dem maximalen Ideal $yA_y = \left\{\frac{a}{s} : a \in y, s \in S \setminus y\right\}$.

Beweis:
Nach 1.36 sind die Primideale von Ay genau die qAy, wo q die Primideale von A mit $q \cap S = \emptyset$ ist, also $q \subset y$. Also ist yAy das eindeutige maximale Ideal von Ay. (jedes maximale Ideal ist ein Primideal)

□

Beispiel 1.40.

1. $A = \mathbb{Z}, y = (p)$, p eine Primzahl.
   $\Rightarrow \mathbb{Z}_{(p)} = \left\{\frac{a}{b} : a, b \in \mathbb{Z}, p \nmid b\right\}$ ist ein lokaler Ring mit Ideal $p\mathbb{Z}_{(p)} = \left\{\frac{a}{b} : a, b \in \mathbb{Z}, p \mid a, p \nmid b\right\}$.
2. $A = \mathbb{C}[t]$, sei $m = (t)$ (das maximale Ideal aller in σ verschwindenden Polynome)
   $\Rightarrow \mathbb{C}[t]_{(t)} = \left\{\frac{p(t)}{q(t)} : p, q \in \mathbb{C}[t], q(0) \neq 0\right\}$.
   Dies ist der Teilring Quot $(\mathbb{C}[t])$ von $\mathbb{C}[t]$ aus denjenigen rationalen Funktionen $f(t)$, die in einer Umgebung von $t = 0$ definiert sind.
   Das macht die Sprechweise „Lokalisierung“ plausibel.

c. Eindeutige Primfaktorzerlegung

Stets: A ist ein nullteilerfreier Ring.

Definition 1.41.
Sei $0 \neq a \in A, a \notin A^*$.

(a) a heißt **unzerlegbar** (oder **irreduzibel**), wenn a keinen echten Teiler in A hat.

(b) Das Element a heißt **prim** (oder ein **Primelement**), wenn $(a) = Aa$ ein Primideal ist.

Bemerkung 1.42.
Sei $0 \neq q \in A, a \notin A^*$. Genau dann ist a unzerlegbar, wenn für alle $b, c \in A$ gilt: $a = bc \Rightarrow b \in A^* \vee c \in A^*$.
Genau dann ist a ein Primelement, wenn $\forall\, b, c \in A$ gilt:
$a \mid b \cdot c \Rightarrow a \mid b \vee a \mid c$
(a Primelement $\Rightarrow (a)$ *Primideal* $\Leftrightarrow \forall\, b, c \in A\ (bc \in (a) \Rightarrow b \in (a) \vee c \in (a)))$

Lemma 1.43.
Jedes Primelement ist unzerlegbar.

Beweis:
Sei $a \in A$ prim, sei $a = b \cdot c$, mit $b, c \in A$.
$a \mid a = b \cdot c \Rightarrow a \mid b$ oder $a \mid c$, wegen a prim.
Andererseits $ba, c \mid a$. Ohne Beschränkung der Allgemeinheit sei $a \mid b$, dann also $a \sim b$ (a und b sind assoziiert).
$b\dot{c} = a = b \cdot u, u \in A^* \Rightarrow c = u \in A^*$.

□

Bemerkung 1.44.
Wir hatten gesehen (LA VII): ist A ein Hauptidealring, so sind unzerlegbar und prim äquivalent.
Wir zeigen nun: im Allgemeinen ist das *nicht* so:

(i) $A := \mathbb{Z}[\sqrt{-5}] = \left\{a + b\sqrt{-5} : a, b \in \mathbb{Z}\right\}$.
In A : $6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$ (*)
$2 \nmid 1 \pm \sqrt{-5}, 3 \nmid 1 \pm \sqrt{-5}$. Also sind $2, 3$ in $\mathbb{Z}[\sqrt{-5}]$ *nicht prim*.
Sie sind aber *zerlegbar*: brauche $N(a + b\sqrt{-5}) = a^2 + 5b^2$: $N(x_1x_2 = N(x_1)N(x_2)$.
$N(2) = 4$. Wäre $2 = x \cdot y \Rightarrow 4 = N(x) \cdot N(y)$. Wäre 2 zerlegbar in $\mathbb{Z}[\sqrt{-5}]$, so müsste $N(x) = N(y) = 2$ sein. (denn: $N(x) = 1 \Rightarrow x \in \mathbb{Z}[\sqrt{-5}]$). Aber 2 ist

keine Norm (d.h. nicht von der Form $a^2 + 5b^2$ mit $a, b \in \mathbb{Z}$)!
Also ist 2 unzerlegbar. Analog sind auch 3 und $1 \pm \sqrt{-5}$ unzerlegbar.
In (*) habe also zwei wesentlich verschiedene Zerlegungen von 6 in unzerlegbare Faktoren.

(ii) In A existieren im Allgemeinen auch keine ggT's:
sei $x := 2 + 2\sqrt{-5}$, $y := 6$. Dann sind $u := 2, v := 1 + \sqrt{-5}$ gemeinsame Teiler von x und y. Würde $w = \mathrm{ggT}(x, y)$ existieren, so müsste $u \mid w, v \mid w$ sein.
$\Rightarrow (4 = N(u)) \mid N(w), (6 = N(v)) \mid N(w)$.
$\Rightarrow 12 \mid N(w)$
$w \mid x, w \mid y \Rightarrow N(w) \mid N(x) = 24, N(w) \mid N(y) = 36$
$\Rightarrow N(w) \mid 12$.

$\Rightarrow N(w) = 12$. Aber 12 ist keine Norm; Widerspruch.

Wir haben verschiedene Defizite erkannt:

- Zerlegung in unzerlegbare Faktoren ist nicht eindeutig bis auf dei Reihenfolge und Assoziiertheit,
- unzerlegbare Elemente sind im Allgemeinen nicht prim,
- ggT und kgV existieren im Allgemeinen nicht.

Diese drei Defizite sind im Wesentlichen zueinander äquivalent:

Satz 1.45.
Sei A nullteilerfrei. Es sind äquivalent:

(i) Jede Nichteinheit $\neq 0$ in A ist Produkt von Primelementen,

(ii) jede Nichteinheit $\neq 0$ ist Produkt von unzerlegbaren Elementen, und die Darstellung ist eindeutig bis auf Reihenfolge und $\sim$,

(iii) es gibt keine unendlichen Teilerketten in A, und je zwei Elemente $\neq 0$ haben einen ggT,

(iv) es gibt keine unendlichen Teilerketten, und jedes unzerlegbare Element ist prim.

Beweis:
(i) $\Rightarrow$ (ii) (vgl. LA VII):
Sei $a = b_1 \cdot \ldots \cdot b_r = c_1 \cdot \ldots \cdot c_s$ mit b_i prim, c_j unzerlegbar.
b_1 prim, $b_1 \mid a = c_1 \cdot \ldots \cdot c_s$
$\Rightarrow \exists\, j\ b_1 \mid c_j$, o.E. $j = 1$: $b_1 \mid c_1$.
c_1 unzerlegbar $\Rightarrow b_1 \sim c_1$, d.h. $c_1 = ub_1$ mit $u \in A^*$
$\Rightarrow$ (Kürzen durch b_1): $b_2 \cdot \ldots \cdot b_r = (uc_2) \cdot c_3 \cdot \ldots \cdot c_s$.
Fertig mit Induktion.

(ii) $\Rightarrow$ (iii):
Sei $0 \neq a \in A$ eine Nichteinheit, etwa $a = a_1 \cdot \ldots \cdot a_r$ mit a_i unzerlegbar. Jeder Teiler von a ist assoziiert zu einem Teilprodukt $a_{i1} \cdot \ldots \cdot a_{is}$ mit $1 \leq i_1 < \ldots < i_s \leq r$.
$\Rightarrow$ keine unendliche Teilerkette, die mit a endet.
Seien $a = a_1 \cdot \ldots \cdot a_r, b = b_1 \cdot \ldots \cdot b_s$ Nichteinheiten mit a_i, b_j unzerlegbar. Nach Umnummerieren kann erreicht werden: $a_1 \sim b_1, \ldots, a_t \sim b_t$ mit $1 \leq t \leq \min\{r, s\}$ und $a_i \not\sim b_j$ für $t < j \leq r$, $t < i \leq s$. Behaupte, $d : a_1 \cdot \ldots \cdot a_t$ ($\sim b_1 \cdot \ldots \cdot b_t$) ist ein ggT von a und b (...)

(iii) $\Rightarrow$ (iv):
Sei a unzerlegbar, sei $a \mid bc$. Zu zeigen: $a \mid b$ oder $a \mid c$. Nach Voraussetzung existiert $d : \mathrm{ggT}(ac, bc)$. Also $a \mid d$, ebenso $c \mid d$. Schreibe $d = c \cdot d'$ mit $d' \in A$.
Aus $cd' = d \mid ac$ folgt $d' \mid a$.
1. Fall: $d' \sim 1 \Rightarrow d \sim c, a \mid d \sim c \Rightarrow a \mid c$;
2. Fall: $d' \sim a \Rightarrow ac \sim d \mid bc \Rightarrow ac \mid bc \Rightarrow a \mid b$.

(Iv) $\Rightarrow$ (i):
klar aus LA VII.:
keine unendliche Teilerkette $\Rightarrow$ jedes Element ist Produkt von unzerlegbaren Elementen. □

Bemerkung 1.46.
$\mathbb{Z}[\sqrt{-5}]$ hat keine unendliche Teilerkette $\ldots a_3 \mid a_2 \mid a_1 \Rightarrow \ldots N(a_3) \mid N(a_2) \mid N(a_1)$
$\Rightarrow a_{i+1} \sim a_i$ für i genügend groß.
(i) - (iv) sind alle verletzt in A.

Definition 1.47.
Ein (nullteilerfreier) Ring A heißt **faktoriell**, wenn (i) - (iv) aus Satz 1.45 gelten.

Insbesondere sind alle Hauptidealringe faktoriell.
Analog zu LA VII: ein Vertretersystem für Primelemente in A ist eine Teilmenge

$P \subset A$ so, dass jedes Primelement π in A zu genau einem Element in P assoziiert ist.

Korollar 1.48 (Primfaktorzerlegung)**.**
Sei A faktoriell, P ein Vertretersystem der Primelemente. Sei $\mathbb{K} := Quot(A)$. Jedes $x \in \mathbb{K}^*$ hat eine eindeutige Darstellung $x = u \cdot \prod_{\pi \in P} \pi^{v_\pi(x)}$ mit $u \in A^*, v_\pi(x) \in \mathbb{Z}, v_\pi(x) = 0$ f.f.a. $\pi \in P$.

Beweis:
klar aus der entsprechenden Aussage für Elemente in A.

□

Die Zahl $v_\pi(x) \in \mathbb{Z}$ heißt die **π-adische Bewertung** von $x \in \mathbb{K}^*$. Formal setzt man $v_\pi(0) := -\infty$ für alle $\pi \in P$. Es gelten:

Satz 1.49.
Sei A faktoriell, $\pi \in P, x, y \in \mathbb{K}$.

(a) $v_\pi(xy) = v_\pi(x) + v_\pi(y)$,

(b) $v_\pi(x + y) \geq \min\{v_\pi(x), v_\pi(y)\}$ *und Gleichheit gilt, falls* $v_\pi(x) \neq v_\pi(y)$.

Beweis:

(i) $x \cdot y = u_x \cdot u_y \cdot \prod_{\pi \in P} \underbrace{\pi^{v_\pi(x)} \cdot \pi^{v_\pi(y)}}_{\pi^{v_\pi(x)+v_\pi(y)}}$.

(ii) Seien $x, y \neq 0$, sei o.E. $v_\pi(x) \leq v_\pi(y)$. Man kann x und y durch xz und yz ersetzen mit beliebigem $z \in \mathbb{K}^*$. Nimm etwa $z := x^{-1}$: somit o.E. $v_\pi(x) = 0 \leq v_\pi(y)$. Sind $x, y \in A$, so ist die Ungleichung klar; ist dabei $v_\pi(x) = 0, v_\pi(y) \geq 1$, so gilt $\pi \nmid x, \pi \mid y \Rightarrow \pi \nmid x + y$.
Im allgemeinen Fall schreibe $x = \frac{x'}{s}, y = \frac{y'}{s}$ mit $x' \mid y' \in A, 0 \neq s, t \in A, \pi \nmid st$.
$\Rightarrow x + y = \frac{tx' + sy'}{st} \Rightarrow v_\pi(x + y) = v_\pi(tx' + sy')$.
Behauptung aus vorigem Fall.

□

Definition 1.50.
Sei A faktoriell, $\mathbb{K} = \text{Quot}(A)$.
Für $x, y \in \mathbb{K}^*$ sage x **teilt** y **(bezüglich** A**)**, in Zeichen: $x \mid y$, falls $\exists\, a \in A$ mit $y = ax$.
Ist $x \mid y$ und $y \mid x$, so sage: x **und** y **sind assoziiert (bezüglich** A**)**, in Zeichen $x \sim y$.

Bemerkung 1.51.

1. $x \mid y \Leftrightarrow \frac{x}{y} \in A$, $x \sim y \Leftrightarrow \frac{x}{y} \in A^*$.
2. Bezüglich dieser Teilbarkeit auf $\mathbb{K}$ können wir ggT und kgV für Elemente aus $\mathbb{K}^*$ definieren (zugleich für mehrere Elemente):
   sind $x_1, \ldots, x_n \in \mathbb{K}^*$ und $d \in \mathbb{K}^*$, so gilt nach Definition $d \sim \text{ggT}(x_1, \ldots, x_n) \Leftrightarrow d \mid x_i$ $(i = 1, \ldots, n)$, und aus $e \mid x_i$ $(i = 1, \ldots, n)$ folgt $e \mid d$. Analog für kgV.

   Klar: ggT und kgV existieren und sind eindeutig bis auf $\sim$. Es gilt:

Lemma 1.52.
Seien $x_1, \ldots, x_n \in \mathbb{K}^*$, P ein Vertretersystem der Primelemente.

(a) $ggT(x_1, \ldots, x_n) \sim \prod_{\pi \in P} \pi^{\min\{v_\pi(x_1), \ldots, v_\pi(x_n)\}}$

(b) $ggT(cx_1, \ldots, cx_n) \sim c \cdot ggT(x_1, \ldots, x_n)$.

Analog für kgV, mit max *statt* min *in (a).*

Beispiel:
$A = \mathbb{Z}, \mathbb{K} = \mathbb{Q}, \text{ggT}\left(\frac{4}{5}, \frac{6}{5}, \frac{8}{7}\right) = \frac{2}{5 \cdot 7} = \frac{2}{35}$ oder $\frac{1}{5 \cdot 7} \cdot \text{ggT}(4 \cdot 7, 6 \cdot 7, 8 \cdot 5) = \frac{2}{5 \cdot 7}$.

d. Das Gauß'sche Lemma

Sei A stets faktoriell, $\mathbb{K} = \text{Quot}(A), 0 \neq f \in \mathbb{K}[t]$. Versuche, die multiplikative Struktur von A für die Faktorisierung von f auszunutzen.

Definition 1.53.
Sei $f = a_n t^n + \ldots + a_1 t + a_0 \in \mathbb{K}[t], (f \neq 0)$. Man nennt $I(f) := \text{ggT}(a_n, \ldots, a_1, a_0) \in \mathbb{K}^*$ den **Inhalt von** f. Das Polynom f heißt **primitiv**, falls $I(f) \sim 1$.
Der Inhalt ist wohldefiniert bis auf $\sim$. Es gilt: $f \in A[t] \Leftrightarrow I(f) \in A$.
Insbesondere liegt jedes primitive Polynom in $A[t]$.
Für $0 \neq c \in \mathbb{K}$ und $0 \neq f \in \mathbb{K}[t]$ ist $I(c \cdot f) \sim c \cdot I(f)$. Insbesondere ist $I(f)^{-1} \cdot f$ stets primitiv.

Satz 1.54 (Gauß'sches Lemma)**.**
Seien $0 \neq f, g \in \mathbb{K}[t]$. *Dann ist* $I(f \cdot g) = I(f) \cdot I(g)$.
Insbesondere: f, g *primitiv* $\Rightarrow f \cdot g$ *primitiv.*

Beweis:
Schreibe $f = c \cdot f_1, g = d \cdot g_1$ mit f_1, g_1 primitiv und $c, d \in \mathbb{K}^*$. $I(fg) = I(cd \cdot f_1 g_1) = cd \cdot I(f_1 g_1) = I(f) \cdot I(g) \cdot I(f_1 g_1)$. Es genügt also zu zeigen:
$I(f_1 g_1) \sim 1$. Wir können also annehmen: f, g sind primitiv; zu zeigen: $f \cdot g$ ist primitiv.

Sei $f = \sum_i a_i t^i, g = \sum_j b_j t^j$ und $f \cdot g =: \sum_k c_k t^k$.
Sei π ein festes Primelement; zu zeigen: $\pi \nmid c_k$ für ein k.
Seien i, j minimal mit $\pi \nmid a_i, \pi \nmid b_j$ gewählt.
Behaupte: $\pi \nmid c_{i+j} : c_{i+j} = \underbrace{a_i b_j}_{\not\equiv 0(\pi)} + \underbrace{\sum_{i'+j'=i+j, i \neq j} a_{i'} b_{j'}}_{\equiv 0(\pi)}$.

□

Korollar 1.55.
Seien $f, g \in A[t]$ *mit* f *primitiv.*
Ist $g = f \cdot h$ *mit* $h \in \mathbb{K}[t]$, *so ist* $h \in A[t]$.

Beweis:
$A \supset I(g) \sim I(f) \cdot I(h) \sim I(h) \Rightarrow h \in A[t]$.

□

Korollar 1.56 (Variation von 1.55)**.**
Sei $f \in A[t]$. Gibt es nicht konstante Polynome $g, h \in \mathbb{K}[t]$ mit $f = g \cdot h$, so gibt es solche g, h sogar in $A[t]$.

Beweis:
$I(f) = I(g) \cdot I(h)$; $g_1 := I(g)^{-1} \cdot g$ ist primitiv; $h_1 := I(g) \cdot h$: $f = g_1 h_1 : I(h_1) = I(f) \in A$ $\Rightarrow h_1 \in A[t]$.

□

Korollar 1.57.
Sei $f = a_n t^n + \ldots + a_1 t + a_0 \in A[t]$ mit $n \geq 1, a_n \neq 0$. Jede Nullstelle x von f in $\mathbb{K}$ hat die Form $x = \frac{a}{b}$ mit $a, b \in A, b \neq 0$, wobei $a \mid a_0$ und $b \mid a_n$.

Insbesondere: ist f normiert, so liegt jede Nullstelle von f in $\mathbb{K}$ schon in A.

Beweis:
$x = \frac{a}{b}$ mit $a, b \in A, b \neq 0, f(x) = 0$.
Dabei sei ggT$(a, b) = 1$. $f(x) = 0 \Rightarrow t - \frac{a}{b} \mid f(t)$ in $\mathbb{K}[t]$, oder $\underbrace{(bt - a)}_{\text{primitiv}} \mid f(t)$ in $\mathbb{K}[t]$.

Mit 1.55 folgt $f(t) = (bt - a) \cdot h(t)$ mit $h(t) \in A[t]$.
Koeffizientenvergleich ergibt $a \mid a_0, b \mid a_n$.

□

Theorem 1.58.
Ist A faktoriell, so ist auch $A[t]$ faktoriell.

Die Primelemente von $A[t]$ sind (bis auf $\sim$):

(a) Die Primelemente aus A,

(b) alle nichtkonstanten primitiven $f \in A[t]$, die irreduzibel in $\mathbb{K}[t]$ sind ($\mathbb{K} = Quot\,(A)$).

Beweis:
Typ (1): jedes Primelement $\pi \in A$ ist prim in $A[t]$.
Homomorphismus $A[t] \to (A/\pi A)[t], \sum a_i t^i \mapsto \sum \overline{a}_i t^i$ hat Kern $\pi A[t]$. Aus dem Homomorphiesatz folgt: $A[t]/\pi A[t] \cong (\underbrace{A/\pi A}_{\text{nullteilerfrei}})[t]$.
Nach Voraussetzung ist $A/\pi A$ nullteilerfrei $\Rightarrow A[t]/\pi A[t]$ ist nullteilerfrei $\Rightarrow \pi$ ist

prim in $A[t]$.

Typ (2): sei $f(t)$ primitiv, nicht konstant und irreduzibel in $\mathbb{K}[T]$. Da Homomorphismus $A[t] \hookrightarrow \mathbb{K}[t] \to \underbrace{\mathbb{K}[t]/f\mathbb{K}[t]}_{\text{Koerper, siehe LA II, VII.b}}$
Der Kern des zusammengesetzten Homomorphismus $A[t] \to \mathbb{K}[t]/f\mathbb{K}[t]$ ist gerade $fA[t]$: das ist Aussage von 1.55.
Also $A[t]/f\mathbb{K}[t] \hookrightarrow \underbrace{\mathbb{K}[t]/f\mathbb{K}[t]}_{\text{Koerper}}$
$\Rightarrow f$ ist prim in $A[t]$ (wie oben)

Es genügt nun, zu zeigen, dass jede Nichteinheit $0 \neq f \in A[t]$ bis auf Assoziiertheit Produkt von Elementen (1) und (2) ist.
Ist f konstant, so ist f Produkt von Elementen vom Typ (1).
Sei f nichtkonstant, sei $f = f_1 \cdot \ldots \cdot f_r (r \geq 1)$ mit $f_i \in \mathbb{K}[t]$, f_i irreduzibel in $\mathbb{K}[t]$.
Setze $g_i := \frac{1}{I(f_i)} \cdot f_i$ (primitiv) ist vom Typ (2) und $f = \underbrace{g_1 \cdot \ldots \cdot g_r}_{\text{Typ (2)}} \cdot \underbrace{I(f)}_{\in A, \text{ zerlegbar in Produkt vom Typ (1)}}$. □

Beispiel 1.59.
A faktoriell $\Rightarrow A[t_1, \ldots, t_n]$ faktoriell.
Für $n \geq 1$ sind diese Ringe (nach Aufgabe 6) keine Hauptidealringe. Also gibt es viele Beispiele von faktoriellen Ringen, die keine Hauptidealringe sind:
$\mathbb{K}[t_1, \ldots, t_n] (n \geq 2), A[t_1, \ldots, t_n] (n \geq 1)$.

1.60. Hierarchie von kommutativen Ringen:
kommutative Ringe $\supset$ nullteilerfreie Ringe $\supset$ faktorielle Ringe $\supset$ Hauptidealringe $\supset$ euklidische Ringe $\supset$ Körper

Fragestellung 1.61.
Sei A faktoriell, $f \in A[t]$ primitiv. Wie finde ich eine Faktorzerlegung von f in irreduzible Faktoren über $\mathbb{K}$ (in $\mathbb{K}[t]$)?
Insbesondere $A = \mathbb{Z}, \mathbb{K} = \mathbb{Q}$.

Sei $f \in \mathbb{Z}[t]$ primitiv. $f = a_n t^n + \ldots + a_0, a_n \neq 0$, Nullstellen von f in $\mathbb{Q}$? Leicht mit 1.57:
jede hat Form $x = \frac{a}{b}, a \mid a_0, b \mid a_n$.
Beispiel: $f = 2t^5 + 4t^3 - 3t^2 - 6$
$f(x) = 0 \Rightarrow x = \frac{a}{b}$ mit $a \mid 6, b \mid 2$.
Einsetzen $\Rightarrow f$ hat keine Nullstelle in $\mathbb{Q}$.

Trotzdem ist f reduzibel: $f(2t^3 - 3)(t^2 + 2)$.

Wie finde nichtlineare Faktoren von f?

1.62. Methode von Kronecker:
Sei $n = \deg(f)$. Ist f nicht irreduzibel, so hat f einen Faktor mit $\deg \leq \lfloor \frac{n}{2} \rfloor =: s$. Wähle $s + 1$ Stützstellen $k_0, \ldots, k_s \in \mathbb{Z}$. Ist $g(t) \mid f(t)$, so auch $g(k) \mid f(k)$ in $\mathbb{Z}$. Berechne $f(k_0), \ldots, f(k_s)$, berechne alle $a_0, \ldots, a_s$ mit $a_i \mid f(k_i)$ und für jedes solche berechne das eindeutige Polynom mit $g(t)$ mit $\deg(g) \leq s$, $g(k_i) = a_i$ $(i = 0, \ldots, s)$. Prüfe dann, ob $g \mid f$. Ist f reduzibel, so finde auf diese Weise einen Teiler. Ist f irreduzibel, so wird das durch dieses Verfahren ebenfalls gezeigt.

Nebenbemerkung: Lagrange-Interpolation
$\deg(g) \leq s$ $g(k_i) = a_i (i = 0, \ldots, s)$;
$g(t) = \sum_{i=0}^{k} a_i \prod_{j \neq i} \frac{t-k}{k_i - k_j}$.

2. Methode: (Reduktion modulo)
$f \in \mathbb{Z}[t]$ primitiv. Sei p eine Primzahl, sei $\overline{f}(t) := f \mod p \in (\mathbb{Z}/p)[t] = \mathbb{F}_p[t]$ ($f = suma_i t^{i\ 2}$ $\overline{f} = sum\overline{a_i} t^i$)
Jede Faktorisierung $f = g \cdot h$ in $\mathbb{Z}[t]$ gibt auch eine Faktorisierung $\overline{f} = \overline{g} \cdot \overline{h}$ in $\mathbb{F}_p[t]$ (denn $\mathbb{Z}[t] \to \mathbb{F}_p[t]$ ist homomorph).
So erhalte eventuell aus Faktorisierung in $\mathbb{F}_p[t]$ Rückschlüsse auf Faktorisierung in $\mathbb{Z}[t]$.
Beispiel: ist $\overline{f}$ irreduzibel in $\mathbb{F}_p[t]$, so auch f irreduzibel in $\mathbb{Z}[t]$.
Vorsicht: $\exists$ Polynome $f \in \mathbb{Z}[t]$, irreduzibel, aber $f \mod p$ reduzibel in $\mathbb{F}_p[t]$ $\forall$ Primzahlen p, z.B. $f = t^4 + 1$.

Beispiele 1.63.

1. $f = t^5 + 3t^4 - 6t^2 + 1 \in \mathbb{Z}[t]$. Kronecker's Methode?

n	-3	-2	-1	0	1	2	...
$f(n)$	-53	-7	-3	1	-1	57	...

Nullstellen von f in $\mathbb{Q}$? Die einzigen Möglichkeiten sind $x = \pm 1$: Einsetzen zeigt: f hat keine Nullstellen in $\mathbb{Q}$.
Quadratische Teiler von f? Stützstellen $s_0 = -1$, $s_1 = 0$, $s_2 = 1$. Jeder Teiler g von f muss erfüllen $g(-1) \in \{\pm 1, \pm 3\}$, $g(0), g(1) \in \{\pm 1\}$. $g = at^2 + btc \rightsquigarrow$ es gibt nur 3 solche Polynome g:
$g_1 = t^2 - t + 1$, $g_2 = t^2 + t - 1$, $g_3 = t^2 - t - 1$.

Teste, ob die g_i Teiler von f sind. Finde heraus: nein. Also folgt f ist irreduzibel in $\mathbb{Q}[t]$.

2. Reduktion mod p?
   mod 2: $\overline{f}(t) = t^5 + t^4 + 1 \in \mathbb{F}_2[t]$, $\overline{f}(t) = (t^2 + t + 1)(t^3 + t + 1)$ (beide Faktoren irreduzibel in $\mathbb{F}_2[t]$).

   mod 3: $\overline{f}(t) = t^5 + 1 \in \mathbb{F}_3[t]$, $\overline{f} = (t + 1)(t^4 - t^3 + t^2 - t + 1)$ (beide Faktoren irreduzibel in $\mathbb{F}_3[t]$).

   Wäre f in $\mathbb{Z}[t]$ zerlegbar, so erhalte einen Widerspruch:
   $f = g \cdot h$: $\deg(g) = 2 \Rightarrow$ Widerspruch mod 3; $\deg(g) = 1$: Widerspruch mod 2. $\Rightarrow f(t)$ ist in $\mathbb{Q}[t]$ irreduzibel.

Satz 1.64. *(Eisenstein)*
Sei A ein faktorieller Ring, sei $f = a_n t^n + \ldots + a_1 t + a_0 \in A[t]$ mit $a_n \neq 0$. Es gebe ein Primelement π in A mit $\pi \nmid a_n, \pi \mid a_i$ für $i = 0, \ldots, n-1$, $\pi^2 \nmid a_0$.
Dann ist f irreduzibel in $\mathbb{K}[t]$.

Beweis:
Sei $f = g \cdot h$ mit $g, h \in A[t]$, zu zeigen:
g oder h ist konstant.
Wegen $f(0) = a_0 = g(0) \cdot h(0)$ teilt π genau einen der beiden $g(0), h(0)$. O.E. $\pi \mid g(0), \pi \nmid h(0)$. Sei $g = \sum b_i t^i, h = \sum c_i t^i$ also $\pi \mid b_0, \pi \nmid c_0$.
Sei $k \geq 1$ minimal mit $\pi \nmid b_k$ (wäre $\pi \mid b_k$ für alle k, so wäre auch $\pi \mid a_n$, Widerspruch zu Voraussetzung). Es ist $f = g \cdot h \Rightarrow a_k = \underbrace{b_k c_0}_{\not\equiv 0(\pi)} + \underbrace{b_{k-1} c_1 + \ldots + b_0 c_k}_{\text{durch } \pi \text{ teilbar}}$
$\Rightarrow \pi \nmid a_k \Rightarrow k = n \Rightarrow \deg(g) = n \Rightarrow \deg(h) = 0$.

□

Definition 1.65.
Ein Polynom f wie in 1.64 heißt ein **Eisenstein-Polynom (zum Primelement π)**.

Beispiele 1.66.

1. $(A = \mathbb{Z}, \mathbb{K} = \mathbb{Q})$
   Das Polynom $f = t^n - p$ ist irreduzibel für jede Primzahl p, alle $n \geq 1$. Denn f ist ein Eisenstein-Polynom zur Primzahl p. Allgemein ist $t^n - q$ irreduzibel $\forall\, q \in \mathbb{Z}$, für die eine Primzahl p existiert mit $v_p(q) = 1$.

2. Wir sehen auch: ist A faktoriell, kein Körper, so gibt es in $\mathbb{K}[t]$ irreduzible Polynome von jedem Grad $n \geq 1$ (z.B. Eisenstein-Polynome zu einem Primelement aus A).
   Insbesondere ist $\mathbb{K}$ nicht algebraisch abgeschlossen.

1.67. Weitere Anwendungen:
Sei p eine Primzahl, sei $\zeta \in \mathbb{C}$ mit $\zeta^p = 1$, $\zeta \neq 1$ (eine p-te Einheitswurzel), also $\zeta = e^{2\pi ik/p}, k \in \{1, \ldots, p-1\}$.
$0 = \zeta^p - 1 = \underbrace{(\zeta - 1)}_{\neq 0} \underbrace{(\zeta^{p-1} + \zeta^{p-2} + \ldots + \zeta + 1)}_{=0}$.
$\Rightarrow \zeta$ ist Nullstelle von $\Phi_p(t) := t^{p-1} + t^{p-2} + \ldots + t + 1$.

Definition 1.68.
$\Phi_p(t)$ heißt das **p-te Kreisteilungspolynom**, $\zeta, \zeta^2, \ldots, \zeta^{p-1}$ sin Nullstellen von $\Phi_p(t)$
$\Rightarrow \Phi_p(t) = \prod_{j=1}^{p-1} (t - \zeta^j)$.

Satz 1.69.
$Phi_p(t)$ ist irreduzibel in $\mathbb{Q}[t]$.

Beweis:
Mach Substitution $u := t - 1$.
$\Rightarrow \Phi_p(t) = \frac{t^p - 1}{t-1} = \frac{(u+1)^p - 1}{u} = \frac{1}{u}(u^p + \binom{p}{1}u^{p-1} + \ldots + \binom{p}{p-1}u + 1 - 1)$
$= u^{p-1} + \binom{p}{1}u^{p-2} + \ldots + \binom{p}{p-1}$.

Dies ist ein Eisenstein-Polynom zur Primzahl p:
p teilt $\binom{p}{i} = \frac{p(p-1)\cdot\ldots\cdot(p-i+1)}{i!}, i = 1, \ldots, p-1$.
$p^2 \nmid \binom{p}{p-1} = p \Rightarrow \Phi_p$ ist ein irreduzibles Polynom.

□

e. Zahlgitter (in $\mathbb{C}$)

Wiederholung:
Ein nullteilerfreier Ring A ist euklidisch, wenn es eine euklidische Wertefunktion auf A gibt, d.h. eine Abbildung
$\Phi : A \setminus \{0\} \to \mathbb{N} \cup \{0\}$ mit der Eigenschaft, dass zu $a, b \in A \setminus \{0\}$ stets $1, r \in A$ existieren mit
$a = qb + r$ und $\Phi(r) < \Phi(b)$ sofern $r \neq 0$.

Standardbeispiele:

(1) $A = \mathbb{Z}$ mit $\Phi : \mathbb{Z} \to \mathbb{N}$, $z \to |z|$ als euklidische Wertefunktion;

(2) $A = \mathbb{K}[t]$, der Polynomring in t über dem Körper $\mathbb{K}$, mit $\deg : \mathbb{K}[t] \setminus \{0\} \to \mathbb{N}$ als euklidische Wertefunktion.

Bemerkung:
Ein euklidischer Ring ist immer ein Hauptidealring, insbesondere faktoriell.

Ende Wiederholung .....

Definition 1.70. (Zahlgitter (in $\mathbb{C}$))
Sei $\omega \in \mathbb{C}$ Nullstelle $X^2 + rX + s$ mit $r, s \in \mathbb{Z}$.
Dann ist $A = \mathbb{Z}[\omega] = \{a + b \cdot \omega | a, b \in \mathbb{Z}\} \subset \mathbb{C}$ ein Teilring von $\mathbb{C}$ (und damit insbesondere nullteilerfrei).
(denn: $(a + b\omega)(a' + b'\omega) = aa' + (ab' + a'b)\omega + bb'\omega^2 = (aa' - sbb') + (ab' + a'b - bb'r)\omega$ wegen $\omega^2 = -rw - s$)

Im Folgenden sei zusätzlich stets $\omega \in \mathbb{C} \setminus \mathbb{R}$.
Wir bezeichnen dann $A = \mathbb{Z}[\omega]$ als **Zahlgitter in** $\mathbb{C}$.

Beispiel 1.71.
$d \in \mathbb{N}$. Dann ist $\omega = \sqrt{-d} = \sqrt{d}i$ eine Nullstelle von $X^2 + d \in \mathbb{Z}[X]$.

Spezialfall: $d = 1 \Rightarrow A = \mathbb{Z}[i]$ heißt der **Ring der ganzen Gauß'schen Zahlen**.

Beobachtung:
Für $x \in \mathbb{Z}[\omega]$ ist $|x|^2 = x \cdot \overline{x} \in \mathbb{N}$ für $\omega \in \mathbb{C} \setminus \mathbb{R}$.

Beweis: ω und $\overline{\omega}$ Nullstellen von $X^2 + rX + s$. Dabei $\omega \neq \overline{\omega}$, weil $\omega \notin \mathbb{R}$.
$X^2 + rX + s = (X - \omega)(X - \overline{\omega}) = X^2 - (\omega + \overline{\omega})X + \underbrace{\omega \cdot \overline{\omega}}_{=|\omega|^2}$,

d.h. $\omega \cdot \overline{\omega} = s$; $\omega + \overline{\omega} = -r \in \mathbb{Z}$.
Zu $x = a + b\omega$ ist $|x|^2 = x \cdot \overline{x} = (a + b\omega)(a + b\overline{\omega}) = a^2 + ab\underbrace{(\omega + \overline{\omega})}_{\in\mathbb{Z}} + b^2\underbrace{\omega \cdot \overline{\omega}}_{\in\mathbb{Z}} \in \mathbb{Z}$.

Wegen $|x|^2 \geq 0$ folgt $|x|^2 \in \mathbb{N}$.

Wir definieren: $N_A : \mathbb{Z}[\omega] \to \mathbb{N}, x \mapsto |x|^2$.
$\mu = \mu_A = \sup\{dist(z, A) | z \in \mathbb{C}\}$ $(\in \mathbb{R}_+)$

Bemerkung 1.72.
Ist $\mu_A < 1$, so ist N_A eine euklidische Wertefunktion, also A euklidisch.

Beweis: Seien $\alpha, \beta \in A \setminus \{0\}$. Gegeben: $z := \frac{\alpha}{\beta} \in \mathbb{C}$. Wegen $\mu_A < 1$ gibt es ein $q \in A$ mit $\left|\frac{\alpha}{\beta} - q\right| < 1$. Dann $|\alpha - q\beta| < |\beta$. Setze $r = \alpha - q\beta$. Dann $\alpha = q\beta + r$ und $N_A(r) = |\alpha - \beta|^2 < |\beta|^2 = N_A(\beta)$.

□

$\mu_A = \sqrt{\left(\frac{1}{2}\right)^2 + \left(\frac{\sqrt{d}}{2}\right)^2} = \frac{\sqrt{1+d}}{2}$.

Korollar 1.73.
Für $d = 1$ oder 2 ist $\mathbb{Z}[\sqrt{-d}]$ ein euklidischer Ring bezüglich $N_{\mathbb{Z}[\sqrt{-d}]} : \mathbb{Z}[\sqrt{-d}] \to \mathbb{N} \cup \{0\}$.

Für $d \geq 3$ ist $\mathbb{Z}[\sqrt{-d}]$ kein Hauptidealring.

Beispiel 1.74.
Division mit Rest in $\mathbb{Z}[i]$
$a = 3 + 4i$, $b = 2 - i$
$\frac{a}{b} = \frac{a \cdot \bar{b}}{b \cdot \bar{b}} = \frac{1}{2^2+1} \cdot (3 + 4i)(2 + i) = \frac{1}{5}(6 - 4 + 8i + 3i) = \frac{3}{5} + \frac{11}{5}i$
Wähle $q = 2i$. Dann
$\left|\frac{a}{b} - q\right|^2 = \left|\frac{2}{5} + \frac{1}{5}i\right|^2 = \frac{1}{25}|2 + i|^2 = \frac{1}{5}$.
$\Rightarrow r = a - qb$. Dann $a = qb + r$ und $N(r) = |a - qb|^2 = \frac{1}{5}|b|^2 < |b|^2 = N(b)$.

Definition 1.75 (Dreiecksgitter)**.**
Sei $d \in \mathbb{N}, d \equiv -1 \mod 4$, dann ist $\omega = \frac{1}{2}(1+\sqrt{-d})$ eine Nullstelle von $X^2 - X - \frac{d-3}{4}$.

$A = \mathbb{Z}[\frac{1}{2}(1+\sqrt{-d})] \supset \mathbb{Z}[\sqrt{-d}]$.
$\mu_A = \sup\{dist(z, A) | z \in \mathbb{C}\} = \mu_A = \frac{d+1}{4\sqrt{d}}$ (Umkreisradius).

Für $d = 3, 7, 11$ ergibt sich $\mu_A < 1$ und damit wieder: $A = \mathbb{Z}[\frac{1}{2}(1+\sqrt{d})]$ ist ein euklidischer Ring bezüglich N_A.
Jedoch ist $\mathbb{Z}[\frac{1}{2}(1+\sqrt{d})]$ zumindest noch ein Hauptidealring für $d = 19, 43, 67, 163$.

Definition 1.76.
$d = 1 \Rightarrow A = \mathbb{Z}[i]$ heißt der **Ring der ganzen Gauß'schen Zahlen**.
(wie in 1.71)

Wie sehen die Primelemente in diesem faktoriellen Ring aus?

Lemma 1.77.
Sei p eine Primzahl mit $p \equiv 1 \mod 4$. Dann gibt es $z \in \mathbb{Z}$ mit $z^2 \equiv -1 \mod p$.

Beweis:
$\mathbb{F}_p = \mathbb{Z}/(p)$ ist ein endlicher Körper. Zu zeigen: -1 ist Quadrat in $\mathbb{F}_p$.
$\prod_{x \in \mathbb{F}_p^*} x = 1 \cdot (-1) \cdot \underbrace{x_1 \cdot x_1^{-1}}_{=1} \cdot \ldots \cdot \underbrace{x_k \cdot x_k^{-1}}_{=1} = -1$ (da 1 und -1 die einzigen Elemente sind, die zu sich selbst invers sind)
Außerdem, mit $p = 4 \cdot k + 1$, $\mathbb{F}_p^* = \{-\overline{2k}, \ldots, -\overline{1}, \overline{0}, \overline{1}, \ldots, \overline{2k}\}$
$\prod_{x \in \mathbb{F}_p^*} x = \prod_{j=1}^{2k} \bar{j} \cdot (-\bar{j}) = (-1)^{2k} \cdot \prod_{j=1}^{2k} \bar{j}^2 = (\overline{2k!})^2$.
Also insgesamt $-1 = \prod_{x \in \mathbb{F}_p^*} x = (\overline{2k!})^2$.

□

Lemma 1.78.
Sei $p \in \mathbb{N}$ eine Primzahl. In $\mathbb{Z}[i]$ haben wir:

(1) $2 \sim (1+i)^2$ *und* $1+i$ *ist prim in* $\mathbb{Z}[i]$ *(Fall $p = 2$)*

(2) Falls $p \equiv -1 \mod 4$, *so ist p auch in* $\mathbb{Z}[i]$ *prim.*

(3) *Falls* $p \equiv 1 \mod 4$, *so ist* $p = \pi \cdot \overline{\pi}$ *für ein Primelement* $\pi \in \mathbb{Z}[i]$, *wobei* $\pi \not\sim \overline{\pi}$.

Beweis:
$N : \mathbb{Z}[i] \to \mathbb{N} \cup \{0\}$,k $a + bi \mapsto a^2 + b^2$ für $a, b \in \mathbb{Z}$.
$\mathbb{Z}[i]^* = \{x \in \mathbb{Z}[i] | N(x) = 1\} = \{1, -1, i, -i\}$.

(1) $(1+i)^2 = 1 - 1 + 2i = 2i = i \cdot 2 \sim 2$; $N(1+i) = 2$. Bei $1 + i = \alpha\beta$ ($\alpha, \beta \in \mathbb{Z}[i]$) folgt $2 = N(1+i) = N(\alpha) \cdot N(\beta) \Rightarrow N(\alpha) = 1 \vee N(\beta) = 1 \Rightarrow \alpha \in \mathbb{Z}[i]^* \vee \beta \in \mathbb{Z}[i]^*$.

(2) $p \equiv -1 \mod 4$. Sei $p = \alpha\beta \in \mathbb{Z}[i]$, mit α, β Nichteinheiten.
Dann gilt $p^2 = N(p) = \underbrace{N(\alpha)}_{\neq 1} \cdot \underbrace{N(\beta)}_{\neq 1}$, also $N(\alpha) = N(\beta) = p$, insbesondere $\equiv 3 \mod 4$.
Es ist aber stets $N(x) \equiv 0, 1, 2 \mod 4$ für $x \in \mathbb{Z}[i]$, denn $x = a + bi$ ($a, b \in \mathbb{Z}$) $\Rightarrow N(x) = a^2 + b^2 \Rightarrow a, b \equiv 0, 1 \mod 4$.
Also liegt ein Widerspruch vor. $\Rightarrow p$ war prim.

(3) $p \equiv 1 \mod 4$. Dann $\exists\, z \in \mathbb{Z}$ mit $p \mid z^2 + 1 = (z+i)(z-i)$ (nach Lemma 1.76).
Jedoch $p \nmid z + i, p \nmid z - i$ in $\mathbb{Z}[i]$. Damit ist p nicht prim, also $p = \pi \cdot \sigma$ mit $\pi \in \mathbb{Z}[i]$ prim und $\sigma \in \mathbb{Z}[i]$ Nichteinheit. Somit $p^2 = N(p) = \underbrace{N(\pi)}_{\neq 1} \cdot \underbrace{N(\sigma)}_{\neq 1}$.
Also $N(\pi) = N(\sigma) = p$, d.h. $p = N(\pi) = \pi \cdot \overline{p}$. Also $\sigma = \overline{\pi}$.

Noch zu zeigen: $\pi \not\sim \overline{\pi}$:
Angenommen, $\overline{\pi} \sim \pi$, also $\overline{\pi} = \varepsilon \cdot \pi$ mit $\varepsilon \in \mathbb{Z}[i]^* = \{\pm 1, \pm i\}$.
Schreibe $\pi = a + i$ für $a, b \in \mathbb{Z}$. $p = \pi \cdot \overline{\pi} = \varepsilon(a + bi)^2 = \varepsilon \cdot (a^2 - b^2 + 2abi)$

- falls $\varepsilon = \pm 1$, so folgt $ab = 0$, also $a = 0 \vee b = 0$. $\Rightarrow p = N(\pi) = a^2 + b^2$ ist Quadrat in $\mathbb{N}$. $\Rightarrow$ Widerspruch.
- Falls $\varepsilon = \pm i$, so folgt $a^2 = b^2$, somit $p = N(\pi) = a^2 + b^2 = 2a^2$ gerade in $\mathbb{Z}$ $\Rightarrow$ Widerspruch.

□

Satz 1.79.
Doe Primelemente in $\mathbb{Z}[i]$ *sind bis auf Assoziiertheit genau folgende:*

(1) $1 + i$;

(2) *Primzahl* $p \in \mathbb{N}$ *mit* $p \equiv -1 \mod 4$;

(3) $a \pm bi$, wobei $a, b \in \mathbb{N}$ mit $a < b$ und $p = a^2 + b^2$ eine Primzahl ($\equiv 1 \mod 4$) in $\mathbb{N}$ ist.

Beweis:
Alle angegebenen Elemente sind prim.
Umgekehrt $0 \neq x \in \mathbb{Z}[i]$.
Zerlege $n := |x|^2 = x\overline{x}$ in $\mathbb{Z}$ in Primfaktoren.
$n = p_1 \cdot p_2 \cdot \ldots \cdot p_r$, p_i Primzahlen. Jedes p_i, und damit auch $n = x\overline{x}$, ist Produkt von Elementen aus der Liste (bis auf $\sim$).
Daher kommt auch jeder Primteiler von x in der Liste vor (bis auf $\sim$), also ist die Liste vollständig.

□

Korollar 1.80.
Eine Primzahl p ($\in \mathbb{Z}$) ist genau dann Summe von zwei Quadraten, $p = a^2 + b^2$ mit $a, b \in \mathbb{N}$, wenn $p \equiv 1 \mod 4$ ist.
Bis auf Vertauschen sind dabei a und b eindeutig bestimmt.

Beweis:
$p \equiv 1 \mod 4 \Rightarrow p = a^2 + b^2$ für geeignete a, b: 1.78.
$p \equiv -1 \mod 4$: p kann keine solche Darstellung haben, denn die einzigen Quadrate $\mod (4)$ sind $0, 1$.

Eindeutigkeit: Sei $p \equiv 1 \mod 4$, p prim, sei $p \sim \pi\overline{\pi}$ mit $\pi \in \mathbb{Z}[i]$, $|\pi|^2 = p^2$.
Sei $p = \underbrace{a^2 + b^2}_{=(a+bi)(a-bi)} = \pi\overline{\pi} \Rightarrow \pi$ teile einen von $a \pm bi \Rightarrow \pi \sim a \pm bi$ (für eine Wahl von $\pm$).
$\Rightarrow a + bi \in \{\pm\pi, \pm i\pi, \pm\overline{\pi}, \pm i\overline{\pi}\}$
$\pi = c + di \rightsquigarrow \pm c \pm di, \pm d \pm ci$.

□

Korollar 1.81 (Fermat)**.**
Eine natürliche Zahl n ist genau dann Summe von zwei Quadraten, wenn für jede Primzahl $p \equiv -1 \mod 4$ gilt $v_p(n)$ ist gerade.

Beweis:
n ist genau dann Summe von zwei Quadraten, wenn $\exists\, x \in \mathbb{Z}[i]$ mit $n = x \cdot \overline{x} = N(x)$.
Schreibe x als Produkt von Primelementen in $\mathbb{Z}[i]$, siehe 1.79:
dort ist (1) $N(1 + i) = 2$, (2) $N(p) = p^2$ für $p \equiv -1(4)$, (3) $N(a \pm bi) = p$, für $p \equiv 1(4)$.
Die Produkte dieser Normen sind genau die angegebenen n.

□

Bemerkung 1.82 (vgl. Aufgabe 11)**.**
Zerlegung von $x \in \mathbb{Z}[i]$ in Primfaktoren in $\mathbb{Z}[i]$? $x = a + bi \to N(x) = a^2 + b^2$. Zerlege $N(x)$ in Primfaktoren (in $\mathbb{Z}$). Jeder Faktor 2 gibt einen Faktor $1 + i$ von x, jeder Faktor p^2 (mit $p \equiv -1(4)$ prim) gibt einen Faktor p von x, jeder Faktor $p \equiv 1(4)$ prim ergibt einen Faktor $a \pm bi$ mit $a < b$ in $\mathbb{N}$, $a^2 + b^2 = p$ von x (welchen, muss man durch Probieren herausfinden).

Beispiel 1.83.
$x = 21 - 3i$. $N(x) = 21^2 + 3^2 = 450 = 2 \cdot 3^2 \cdot 5^2$.
$\Rightarrow x \sim (1 + i) \cdot 3 \cdot \pi_1\pi_2$ mit $\pi_1, \pi_2 \in \{1 \pm 2i\}$.
Hier: $\pi_1 = \pi_2 = 1 + 2i$.

f. Abelsche Gruppen und die Gruppe der primen Restklassen modulo n

Definition 1.84.
Sei G eine Gruppe (nicht notwendig abelsch)

(a) $|G|$ (die Mächtigkeit von G) heißt die **Ordnung** von G.

(b) Die Ordnung eines Elements $g \in G$ ist $\operatorname{ord}(g) := |\langle g \rangle|$.

Bemerkung 1.85.
Satz von Lagrange (LA III): G endlich $\Rightarrow \operatorname{ord}(g) \mid |G|$ für jedes $g \in G$.

1.86.
Zyklische Gruppen: eine Gruppe G heißt **zyklisch**, wenn $G = \langle g \rangle$ für ein $g \in G$ ist, $\langle g \rangle = \{g^n : n \in \mathbb{Z}\}$.
$\Rightarrow \varphi : \mathbb{Z} \to G, \varphi(n) = g^n$ ist ein surjektiver Homomorphismus.
$\Rightarrow G \cong \mathbb{Z}/\ker(\varphi)$. Zwei Fälle:
Ist $\ker(\varphi) = \{0\}$, so also $G iso(\mathbb{Z}, +)$.
Ist $\ker(\varphi) = \mathbb{Z}n$ mit $n \in \mathbb{N}$, so also $G \cong (\mathbb{Z}/n\mathbb{Z}, +)$.

Ab jetzt schreibe alle (abelschen) Gruppen additiv. Schreibe $\mathbb{Z}/n := \mathbb{Z}/n\mathbb{Z}$.

1.87.
Sei $G = \langle g \rangle$ zyklisch, additiv geschrieben. Untergruppen von G?
1. Fall: $|G| = \infty$, dann sind die Untergruppen genau die $\langle ng \rangle$, $n \in \mathbb{N}$, sowie $\{0\}$.
2. Fall $|G| < \infty$, so:

Satz 1.88.
Sei $G = \langle g \rangle$ zyklisch, $|G| = n < \infty$.

(a) Jede Untergruppe U von G ist zyklisch: $U \langle dg \rangle$ mit $d \mid n$, $d \geq 1$. Damit ist d eindeutig.
Dabei $|U| = \frac{n}{d}$, $[G : U] = d$.

(b) Für d, e Teiler von n:
$\langle dg \rangle \subset \langle eg \rangle \Leftrightarrow e \mid d$.

(c) Für $k_1, \ldots, k_r \in \mathbb{Z}$, $U := \langle k_1 g, \ldots, k_r g \rangle$ ist $U = \langle dg \rangle$ mit $d = ggT(k_1, \ldots, k_r)$.

(d) Insbesondere $\forall\, k \in \mathbb{Z}$: $ord(kg) = \frac{n}{ggT(k,n)}$.

Beweis:
$\varphi : \mathbb{Z} \to G, \varphi(m) = mg$.
Die Untergruppen von G sind also die $\varphi(A)$, wobei $A \subset \mathbb{Z}$ eine Obergruppe von $\ker(\varphi) = n\mathbb{Z}$.
Also $A = d\mathbb{Z}$ mit $d \mid n$.

□

Beispiel 1.89.
siehe Handschrift

Abelsche Gruppen = $\mathbb{Z}$-Moduln:

Theorem 1.90 (LA VII d)**.**
Jede endlich erzeugte abelsche Gruppe G erfüllt
$G \cong \mathbb{Z}^r \oplus \mathbb{Z}/d_1 \oplus \ldots \oplus Z/d_s$ *mit* $r, s \geq 0, 1 \neq d_1 \mid d_2 \mid \ldots \mid d_s > 0$ *die Elementarteiler von G. Dabei sind r, s und alls d_i eindeutig bestimmt.*

Theorem 1.91. *(LA VII d)*
Jede endlich erzeugte abelsche Gruppe G erfüllt
$G \cong \mathbb{Z}^r \oplus \bigoplus_{i=1}^{k} \bigoplus_{j=1}^{s_i} \mathbb{Z}/\left(p_i e^{ij}\right)$ *mit* $r \geq 0, k \geq 0$, $p_1 < \ldots < p_k$ *Primzahlen und* $s_i \geq 1$, $e_{i1} \leq e_{i2} \leq \ldots \leq e_{is_i}$.
Wieder alle Daten eindeutig bestimmt.
r heißt der ***(torsionsfreie) Rang*** *von G.*

Bemerkung 1.92.
Wieviele abelsche Gruppen der Ordnung $n < \infty$ gibt es bis auf $\cong$?

Beispiel: $n = 16 = 2^4$: Elementarteilerform: $G \cong \mathbb{Z}/(2^{a_1}) \oplus \mathbb{Z}/(2^{a_2}) \oplus \ldots \oplus \mathbb{Z}/(2^{a_s})$ mit $1 \leq a_1 \leq \ldots \leq a_s$ und $16 = 2^{a_1} \cdot 2^{a_2} \cdot \ldots \cdot 2^{a_s}$, also $a_1 + \ldots + a_s = 4$. Also korrespondieren diese Gruppen genau zu den Partitionen von 4. Eine Partition von $k \in \mathbb{N}$ ist $(a_1, \ldots, a_s), a_i \in \mathbb{N}, \sum a_i = k, 1 \leq a_1 \leq \ldots \leq a_k$.
$4 = k$:

$1 + 1 + 1 + 1$	$(\mathbb{Z}/2)^4$
$1 + 1 + 2$	$(\mathbb{Z}/2)^2 \oplus \mathbb{Z}/4$
$1 + 3$	$\mathbb{Z}/2 \oplus \mathbb{Z}/8$
$2 + 2$	$(\mathbb{Z}/4)^2$
4	$\mathbb{Z}/16$

Mit $p(k)$ bezeichnet man die Anzahl der Permutationen von k.

k	1	2	3	4	5	6
$p(k)$	1	2	3	5	7	...

Korollar 1.93.
Sei $n = p_1^{m_1} \cdots p_r^{m_r}$ mit p_i prim, paarweise verschieden, $m_i \geq 1$. Dann gibt es bis auf Isomorphie genau $p(m_1) \cdots p(m_r)$ viele abelsche Gruppen der Ordnung n.

Bemerkung 1.94.
Sei G eine gegebene endliche abelsche Gruppe, sei $n \in \mathbb{N}$. Wie viele Elemente der Ordnung n gibt es in G?
Wir fragen also nach der Funktion $f_G(n) := |\{x \in G : \operatorname{ord}(x) = n\}|$. Es ist leichter,

$$g_G(n) := |\{x \in G : \operatorname{ord}(x) \mid n\}| = \Big|\underbrace{\{x \in G : nx = 0\}}_{=:G_n}\Big|.$$

G_n ist eine Untergruppe von G.
Ist $G = G_1 \oplus \ldots \oplus G_r$, so ist $G_n = (G_1)_n \oplus \ldots \oplus (G_r)_n$.
Also $g_{G_1 \oplus \ldots \oplus G_r}(n) = \prod_{i=1}^{r} g_{G_i}(n)$.
Ist G zyklisch, $|G| = m$, so ist $g_G(n) = \operatorname{ggT}(m, n)$.
Also: ist $G \cong \bigoplus_{i=1} r\mathbb{Z}/m_i$, so

$$g_G(n) = \prod_{i=1}^{r} \operatorname{ggT}(n, m_i).$$

Wie bekommt man nun $f_G(n)$ aus $g_G(n)$?

Definition 1.95.
Die **Möbiusfunktion** $\mu : \mathbb{N} \to \{-1, 0, +1\}$ ist definiert als

$$\mu(n) = \begin{cases} (-1)^r & \text{, falls } n = p_1, \ldots, p_r \text{ mit } p_i \text{ prim, paarweise verschieden;} \\ 0 & \text{, falls } \exists\, k > 1, k^2 \mid n. \end{cases}$$

Satz 1.96 (Möbiussche Umkehrformel)**.**
Sei $f : \mathbb{N} \to \mathbb{Z}$ eine Abbildung, sei $g : \mathbb{N} \to \mathbb{Z}$ definiert durch $g(n) := \sum_{d \mid n} f(d)$.

Dann ist $f(n) = \sum_{d \mid n} \mu(d) \cdot g(\frac{n}{d})$ für alle $n \in \mathbb{N}$.

Beweis:
Behaupte zuerst: für $m \in \mathbb{N}$ ist $\sum_{d \mid m} \mu(d) = \begin{cases} 1 & , m = 1; \\ 0 & , m > 1. \end{cases}$
Denn: ist $1 < m = p_1^{e_1} \cdots p_r^{e_r}$ mit p_i prim, paarweise verschieden, $e_i \geq 1$, so ist:

Linke Seite $= \mu(1) + \sum_i \mu(p_i) + \sum_{i<j} \mu(p_i p_j) + \sum_{i<j<k} \mu(p_i p_j p_k) + \ldots = 1 + r \cdot (-1) + \binom{r}{2} \cdot (+1) +$
$\binom{r}{3} \cdot (-1) + \ldots = \sum_{i=0}^{r} \binom{r}{i} (-1)^i = (1-1)^r = 0$. Damit folgt:

$$\sum_{d|n} \mu(d) \cdot g\left(\tfrac{n}{d}\right) = \sum_{d|n} \sum_{e|\frac{n}{d}} \mu(d) f(e) = \sum_{e|n} \left(\sum_{d|\frac{n}{e}} \mu(d) \right) \cdot f(e) = 1.$$

$$(\ldots) = \begin{cases} 0 & \text{für } \frac{n}{e} \neq 1 \\ 1 & \text{für } \frac{n}{e} = 1. \end{cases}$$

□

Beispiel 1.97.
$G := \mathbb{Z}/2 \times \mathbb{Z}/4 \times \mathbb{Z}/3$, $|G| = 24$.

n	1	2	3	4	6	8	12	24
$f_G(n)$	1	3	2	4	6	0	8	0
$g_G(n)$	1	4	3	8	12	8	24	24

Satz 1.98.
Sei $\mathbb{K}$ *ein Körper. Jede endliche Untergruppe von* $\mathbb{K}^*$ *ist zyklisch.*

Beweis:
Sei $G \leq \mathbb{K}^*$ eine endliche Untergruppe.
Seien $1 \neq d_1 \mid d_2 \mid \ldots \mid d_r$ die Elementarteiler von G, also $G \cong (\mathbb{Z}/d_1) \times \ldots \times (\mathbb{Z}/d_r)$.
Es gibt in G genau d_1^r Elemente $x \in G$ mit $x^{d_1} = 1$. Das Polynom $x^{d_1} - 1$ hat höchstens d_1 Nullstellen in $\mathbb{K} \Rightarrow r = 1$, also G ist zyklisch.

□

Korollar 1.99.
Ist $\mathbb{K}$ *ein endlicher Körper mit* $|\mathbb{K}| = q < \infty$*, so ist* $\mathbb{K}^*$ *zyklisch von Ordnung* $q - 1$.

1.100.
Allgemeiner wollen wir die Struktur von $(\mathbb{Z}/n)^* = (\mathbb{Z}/n\mathbb{Z})^*$ studieren. Die Elemente von $(\mathbb{Z}/n)^*$ heißen die **primen Restklassen** modulo n (für $n \in \mathbb{N}, n > 1$). Es ist $(\mathbb{Z}/n)^* = \{\overline{a} = a + (n) : a \in \mathbb{Z}, \mathrm{ggT}(a,n) = 1\}$. Denn $\overline{a} \in (\mathbb{Z}/n)^*$
$\Leftrightarrow \exists\, b \in \mathbb{Z}$ mit $ab \equiv 1 (\mod n)$
$\Leftrightarrow \exists\, b, c \in \mathbb{Z}$ mit $ab + cn = 1$
$\Leftrightarrow \mathrm{ggT}(a,n) = 1$.

Chinesischer Restsatz: ist $n = n_1 \cdot \ldots \cdot n_r$ mit $\mathrm{ggT}(n_i, n_j) = 1$ für $i \neq j$, so $\mathbb{Z}/n \cong (\mathbb{Z}/n_1) \times \ldots \times (\mathbb{Z}/n_r)$ (Ringisomorphismus, Chinesischer Restsatz).
$\Rightarrow (\mathbb{Z}/n)^* \cong (\mathbb{Z}/n_1)^* \times \ldots \times (\mathbb{Z}/n_r)^*$.

Daher genügt es, $(\mathbb{Z}/n)^*$ für $n = p^e$, p prim, $e \geq 1$, zu studieren.

Definition 1.101.
Für $n \in \mathbb{N}$ setze $\varphi(n) := |(\mathbb{Z}/n)^*|$.
φ heißt die **Eulersche φ-Funktion**.

Es ist also $\varphi(n) = |\{a \in \{0, 1, \ldots, n-1\} : \mathrm{ggT}(a, n) = 1\}$.

1.102. Eigenschaften der φ-Funktion:
Seien $m, n \in \mathbb{N}$.

(a) $\mathrm{ggT}(m, n) = 1 \Rightarrow \varphi(mn) = \varphi(m) \cdot \varphi(n)$.

(b) p prim $\Rightarrow \varphi(p^e) = p^e - p^{e-1} = p^{e-1}(p-1)$ für alle $e \geq 1$.

(c) Ist $n = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$ mit p_i prim und paarweise verschieden, $e_i \geq 1$, dann folgt $\varphi(n) = p_1^{e_1-1} \cdot \ldots \cdot p_r^{e_r-1} \prod_{i=1}^{r}(p_i - 1) = n \cdot \prod_{i=1}^{r}\left(1 - \frac{1}{p_i}\right)$.

(d) (Verallgemeinerter) kleiner Satz von Fermat:
Ist $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a, n) = 1$, so ist $a^{\varphi(n)} \equiv 1 (\mod n)$ (für $n \in \mathbb{N}$ beliebig).

Beweis: (a) Chinesischer Restsatz: $(\mathbb{Z}/mn)^* \cong (\mathbb{Z}/m)^* \times (\mathbb{Z}/n)^*$.

(b) Die zu p^e nicht teilerfremden Zahlen in $\{1, 2, \ldots, p^e\}$ sind $\{p, 2p, 3p, \ldots, p^{e-1} \cdot p\}$, also p^{e-1} Stück.

(c) klar aus (a) und (b).

(d) sagt: in der Gruppe $(\mathbb{Z}/n)^*$ (von Ordnung $\varphi(n)$) gilt $x^{\varphi(n)} = 1 \quad \forall\ x \in (\mathbb{Z}/n)^*$ (vgl. Satz von Lagrange)

□

Bemerkung 1.103.

1 Unter dem kleinen Satz von Fermat versteht man den Spezialfall von 1.102 (d), wo $n = p$ eine Primzahl ist:
für alle $a \in \mathbb{Z}, p \nmid a$ ist $a^{p-1} \equiv 1 (\mod p)$.

2 Für $n \in \mathbb{N}$ ist $\varphi(n)$ auch die Anzahl der zyklischen Erzeuger einer zyklischen Gruppe G von Ordnung n. Somit sagt 1.102 (c):
$\frac{\varphi(n)}{n} = \prod_{i=1}^{r}(1 - \frac{1}{p_i})$ ist die Wahrscheinlichkeit dafür, dass ein zufällig gewähltes Element in G die Gruppe G erzeugt.

Hilfssatz 1.1.
Sei p prim, seien $x, y \in \mathbb{Z}$, $x \equiv y \not\equiv 0 (\mod p)$.
Dann ist $v_p(x^{p^i} - y^{p^i}) = v_p(x - y) + i$ für alle $i \geq 1$, ausgenommen (eventuell) für $p = 2$ und $v_2(x - y) = 1$.

Beweis:
Induktion nach i, es genügt, den Fall $i = 1$ zu beweisen.
Sei $y = x + ap^e$ mit $e = v_p(x - y) \geq 1$, $a \in \mathbb{Z}, p \nmid a$.

$$y^p - x^p = \underbrace{\binom{p}{1}x^{p-1} \cdot ap^e}_{v_p = e+1} + \underbrace{\binom{p}{2}x^{p-2}a^2p^{2e}}_{v_p = 2e+1} + \ldots + \underbrace{\binom{p}{p-1}x(ap^e)^{p-1}}_{v_p=(p-1)e+1} + \underbrace{(ap^e)^p}_{v_p = ep}.$$

Es ist $e + 1 < 2e + 1 < \ldots < (p - 1)e + 1$ und $e + 1 < ep$, ausgenommen $p = 2$ und $e = 1$.
Nach 1.49 ist also $v_p(y^p - y^p) = e + 1 = v_p(x - y) + 1$.

□

Sei zunächst $p > 2$, p eine Primzahl.

Satz 1.104.
Für $p > 2$ prim und $e \geq 1$ ist $(\mathbb{Z}/p^e)^*$ zyklisch von Ordnung $p^{e-1}(p - 1)$. Die Restklasse $\overline{1 + p}$ hat darin die Ordnung p^{e-1} erzeugt also den p-primären Teil dieser Gruppe.

Beweis:
Sei $G := (\mathbb{Z}/p^e)^*$. Betrachte den Homomorphismus
$G = (\mathbb{Z}/p^e)^* \twoheadrightarrow (\mathbb{Z}/p)^*$ (surjektiv)
Sei $K := \ker(g)$. Es ist $G/K \cong (\mathbb{Z}/p)^* \cong \mathbb{Z}/p - 1$ (Kleiner Fermat). Es ist $|K| = p^{e-1}$.
Es ist also K die p-primäre Komponente von G, und daher $G \cong K \times (G/K)$.
Wegen ggT$(|K|, |G/K|) = 1$ und G/K zyklisch, genügt es zu zeigen: K ist zyklisch.

Behaupte: $\overline{1 + p} \in K$ erzeugt die Gruppe K. Das folgt aus dem Hilfssatz 1.1:
$v_p((1 + p)^{p^i}) = i + v_p(p + 1 - 1) = i + 1$ für $i = 1, 2, \ldots$. Das kleinste i, wo dieser Wert $\geq e$ ist, ist $i = e - 1$. Also hat $\overline{1 + p}$ in K die Ordnung p^{e-1}, und erzeugt damit K.

□

Sei nun $p = 2$: $(\mathbb{Z}/2)^* = \{1\}, (\mathbb{Z}/4)^* \cong \mathbb{Z}/2, (\mathbb{Z}/8)^* = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\} \cong (\mathbb{Z}/2) \times (\mathbb{Z}/2)$, also nicht zyklisch.

Satz 1.105.
Für $e \leq 2$ ist $(\mathbb{Z}/2^e)^*$ zyklisch.
Für $e \geq 3$ ist $(\mathbb{Z}/2^e)^* \cong \mathbb{Z}/2 \times (\mathbb{Z}/2)^{2e-2}$.

Beweis:
Aus dem Hilfssatz 1.1 folgt $v_2(5^{2^i} - 1) = v_2(5 - 1) + i = i + 2$.
Das kleinste i, wo dies $\geq e$ wird, ist also $i = e - 2$.
$\Rightarrow \overline{5}$ hat die Ordnung 2^{e-w} in $(\mathbb{Z}/2^e)^*$.
Außerdem ist $\overline{-1}$ keine Potenz von $\overline{5}$, denn das ist schon modulo 8 nicht der Fall.
Also ist $(\mathbb{Z}/2^e)^* = \left\langle \overline{-1} \right\rangle \times \left\langle \overline{5} \right\rangle \cong (\mathbb{Z}/2) \times (\mathbb{Z}/2^{e-2})$.

□

Beispiel 1.106.
Mit Hilfe von 1.104 und 1.105 kann man leicht die Struktur von $(\mathbb{Z}/n)^*$ für beliebiges $n \in \mathbb{N}$ berechnen:
Z.B. $n = 168 = 2^3 \cdot 3 \cdot 7$: $(\mathbb{Z}/168)^* \cong (\mathbb{Z}/8)^* \times (\mathbb{Z}/3)^* \times (\mathbb{Z}/7)^*$
$\cong (\mathbb{Z}/2 \times \mathbb{Z}/2) \times \mathbb{Z}/2 \times \mathbb{Z}/6$
$\cong (\mathbb{Z}/2)^4 \times (\mathbb{Z}/3)$.

g. Das RSA Public Key Kryptosystem

Ein Kryptosystem ist ein Verfahren zur Verschlüsselung von Nachrichten.
RSA: R. Rivest, A. Shamir, L. Adleman (1978)

Jeder Teilnehmer, etwa A, wählt zwei sehr große Primzahlen $p \neq q$ und berechnet $N := pq =: N_A$. Dieses N gibt sie öffentlich bekannt. Sie weiß $\varphi(N) = (p-1)(q-1)$ und wählt ein $e \in \mathbb{N}$ mit $\text{ggT}(e, \varphi(N)) = 1$. Aus $e = e_A$ gibt sie öffentlich bekannt.
Der öffentliche Schlüssel von A ist also das Paar (N_A, e_A).
Angenommen, B will eine Nachricht an A schicken. Eine Nachricht kann man sich vorstellen als Folge $(m_1, m_2, \ldots, m_r)$ mit $m_i \in \{0, 1, \ldots, N_A - 1\}$. Also Blöcke zu $\lfloor \frac{N}{128} \rfloor$ Zeichen, bei einem Alphabet aus 128 Zeichen.

Sei der Klartext ein $m \in \{0, 1, \ldots, N_A - 1\}$.
B verschlüsselt dieses m so:
$x := m^{e_A} \mod N_A \in \{0, 1, \ldots, N_A - 1\}$
Dieses x sendet er an A.
A empfängt x: Mit dem euklidischen Algorithmus berechnet sie ein Inverses $d = d_A$ von e_A modulo $\varphi(N)$, also $de \equiv 1 \mod \varphi(N)$.
$\Rightarrow x^d = (m^e)^d = m^{de} \equiv m \mod N$.

Lemma 1.107.
Sei $N \in \mathbb{N}$ quadratfrei, sei $r \in \mathbb{N}$ mit $r \equiv 1 \mod \varphi(N)$.
Dann gilt $a^r \equiv a \mod N$ für alle $a \in \mathbb{Z}$.

Beweis: $N = p_1 \cdot \ldots \cdot p_k$, p_i prim und paarweise verschieden.
$\varphi(N) = (p_1 - 1) \cdot \ldots \cdot (p_k - 1)$. Also $p_i - 1 \mid \varphi(N) \mid r - 1$.
$\mathbb{Z}/(N) \cong \mathbb{Z}/(p_1) \times \ldots \times \mathbb{Z}/(p_k) \Rightarrow$ genügt zu zeigen $a^r \equiv a \mod p_i$ für alle $i = 1, \ldots, k$.
Fall 1: ist $(a, p_i) = 1$, so folgt (mit Kleinem Fermat) $a^{p_i - 1} \equiv 1 \mod p_i \Rightarrow a^{r-1} \equiv 1 \mod p_i$.
Fall 2: ist $p_i \mid a$, also $a \equiv 0 \mod p_i$. $\Rightarrow a^r \equiv 0 \mod p_i$.

□

Angenommen, C will die Nachricht entziffern. C kennt (N, e). Er müsste d mit $de \equiv 1 \mod \varphi(N)$ finden.
Würde er $\varphi(N)$ kennen, so wäre er fertig. Aus der Faktorisierung $N = p \cdot q$ erhalte $\varphi(N) = (p-1)(q-1)$. Umgekehrt gibt $\varphi(N)$ auch die Faktorisierung von N:
$\varphi(N) = \underbrace{pq}_{=N} - (p+q) + 1$. $\Rightarrow$ kenne $p + q$.

$$(p-q)^2 = (p+q)^2 - 4\underbrace{pq}_{=N} \Rightarrow \text{kenne } p-q.$$

Man glaubt, dass das Finden eines d mit $de \equiv 1 \mod \varphi(N)$ genauso schwierig ist wie die Bestimmung von $\varphi(N)$.
Nimmt man das an, so sieht man: Entschlüsseln ist genauso schwierig wie Faktorisierung von N.
Faktorisieren sehr großer Zahlen ist vom Rechenaufwand her de facto unmöglich.

Dagegen lässt sich effektiv für sehr große Zahlen testen, ob sie prim sind. Das beruht auf dem Kleinen Satz von Fermat. Sei $m \in \mathbb{N}$; wir wollen testen, ob n prim ist.
Kleiner Satz von Fermat: ist n prim, so gilt $a^{n-1} \equiv 1 \mod n$ für alle a mit $(a,n) = 1$.
Beginne mit $a = 2, 3, 5, \ldots$
Findet man ein a mit $(a,n) = 1$ und $a^{n-1} \not\equiv 1 \mod n$, so ist bewiesen: n ist zusammengesetzt.
Ist dagegen $a^{n-1} \equiv \mod n$ für „viele“ a, so ist n „wahrscheinlich„ prim.
Verfeinere dieses Verfahren, etwa Miller-Rabin Test.

Literatur:
J. Buchmann: Einführung in die Kryptographie, Springer, 1999
S. Singh: Geheime Botschaften, dtv, 2001

2. Körpertheorie I

Wir wollen Lösungen von Gleichungen $a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 = 0$ mit Koeffizienten a_i in einem Körper $\mathbb{K}$ studieren. Dazu müssen wir Körpererweiterungen von $\mathbb{K}$ studieren.

a. Algebraische und transzendente Körpererweiterungen

Definition 2.1.
Ist $\mathbb{L}$ ein Körper und $\mathbb{K} \subset \mathbb{L}$ ein Teilkörper von $\mathbb{L}$, so heißt $\mathbb{L}$ eine **(Körper-) Erweiterung** von $\mathbb{K}$.
Man schreibt oft auch $\mathbb{L}/\mathbb{K}$ („$\mathbb{L}$ über $\mathbb{K}$“) für $\mathbb{L}$ ist Körpererweiterung von $\mathbb{K}$.
Ist $\mathbb{K} \subset \mathbb{F} \subset \mathbb{L}$ ein Körper, so heißt $\mathbb{F}$ ein **Zwischenkörper** von $\mathbb{L}/\mathbb{K}$.
Ist $\mathbb{L}/\mathbb{K}$ eine Körpererweiterung, so heißt $[\mathbb{L} : \mathbb{K}] := \dim_{\mathbb{K}}(\mathbb{L})$ (Vektorraum-Dimension) der **Körpergrad** von $\mathbb{L}/\mathbb{K}$. Die Erweiterung $\mathbb{L}/\mathbb{K}$ heißt **endlich**, falls $[\mathbb{L} : \mathbb{K}] < \infty$, andernfalls **unendlich**.

Satz 2.2.
Seien $\mathbb{K} \subset \mathbb{F} \subset \mathbb{L}$ Körper, so gilt:
$[\mathbb{L} : \mathbb{K}] = [\mathbb{L} : \mathbb{F}] \cdot [\mathbb{F} : \mathbb{K}]$.

Beweis:
Ist $[\mathbb{L} : \mathbb{F}]$ oder $[\mathbb{F} : \mathbb{K}]$ unendlich, so auch $[\mathbb{L} : \mathbb{K}]$.
Seien $[\mathbb{L} : \mathbb{F}] = m < \infty$, $[\mathbb{F} : \mathbb{K}] = n < \infty$.
Sei $(x_1, \ldots, x_m)$ eine $\mathbb{F}$-Basis von $\mathbb{L}$, $(y_1, \ldots, y_n)$ eine $\mathbb{K}$-Basis von $\mathbb{F}$.

Behaupte: $(x_i, y_j)_{i=1,\ldots,m;j=1,\ldots,n}$ ist eine $\mathbb{K}$-Basis von $\mathbb{L}$.
Jedes $z \in \mathbb{L}$ schreibt sich $z = \sum_{i=1}^{m} b_i x_i$ mit $b_i \in \mathbb{F}$. Jedes $b_i = \sum_{j=1}^{n} a_{ij} y_j$ mit $a_{ij} \in \mathbb{K} \Rightarrow$
$z = \sum_{i=1}^{m} \sum_{j=1}^{n} a_{ij} x_i y_j$.
Lineare Unabhängigkeit:
Sei $\sum_{i=1}^{m} \sum_{j=1}^{n} a_{ij} x_i y_j = 0$ mit $a_{ij} \in \mathbb{K}$.

$$\sum_{i=1}^{m} \sum_{j=1}^{n} a_{ij} x_i y_j = \sum_{i=1}^{m} \underbrace{\left(\sum_{j=1}^{n} a_{ij} y_j \right)}_{\in \mathbb{F}} x_i$$

$\Rightarrow \forall\, i \sum_{j=1}^{n} a_{ij} y_j = 0$
$\Rightarrow \forall\, i, j\ a_{ij} = 0.$

□

Notation 2.3.
Sei $\mathbb{L}/\mathbb{K}$ eine feste Körpererweiterung. Sei $(a_i)_{i\in I}$ eine Familie in $\mathbb{L}$. Man schreibt
$\mathbb{K}[a_i : i \in I]$:= der von $(a_i)_{i\in I}$ und $\mathbb{K}$ erzeugte Teilring von $\mathbb{L}$,
$K(a_i : i \in I)$:= der von $(a_i)_{i\in I}$ und $\mathbb{K}$ erzeugte Teilkörper von $\mathbb{L}$.
$\mathbb{L}/\mathbb{K}$ heißt endlich erzeugte Körpererweiterung, falls $\exists\, a_1, \ldots, a_n \in L$, $n \in \mathbb{N}$ mit $\mathbb{L} = \mathbb{K}(a_1, \ldots, a_n)$.

Bemerkung 2.4.
Die Elemente von $\mathbb{K}[a_1, \ldots, a_n]$ sind die

$$\sum_{\alpha\in\mathbb{Z}_+^n} c_\alpha \cdot a_1^{\alpha_1} \cdot \ldots \cdot a_n^{\alpha_n}$$

mit $c_\alpha \in \mathbb{K}$, fast alle $c_\alpha = 0$. Anders gesagt: $\mathbb{K}[a_1, \ldots, a_n]$ ist das Bild des Einsetz-Homomorphismus $\varphi : \mathbb{K}[t_1, \ldots, t_n] \to \mathbb{L}$, $\varphi(f(t_1, \ldots, t_n)) := f(a_1, \ldots, a_n)$.

Dagegen: $\mathbb{K}(a_1, \ldots, a_n) = \left\{ \frac{f(a_1,\ldots,a_n)}{g(a_1,\ldots,a_n)} : f(a_1, \ldots, a_n), g(a_1, \ldots, a_n) \in \mathbb{K}[a_1, \ldots, a_n], g(a_1, \ldots, a_n) \neq 0 \right\}$.

Vorsicht:
Endlich erzeugte Körpererweiterungen $\mathbb{L}/\mathbb{K}$ sind im Allgemeinen nicht endlich erzeugt als Ringerweiterung!
(Beispiel: $\mathbb{K}(t)/\mathbb{K}$)

Definition 2.5.
Seien $\mathbb{K} \hookrightarrow \mathbb{L}_1, \mathbb{K} \hookrightarrow \mathbb{L}_2$ zwei Körpererweiterungen.
Ein **$\mathbb{K}$-Homomorphismus** von $\mathbb{L}_1$ nach $\mathbb{L}_2$ ist ein (Ring-) Homomorphismus $\varphi : \mathbb{L}_1 \to \mathbb{L}_2$ mit $\varphi(a) = a\ \forall\, a \in \mathbb{K}$.
Schreibweise: $\varphi : \mathbb{L}_1 \to_{\mathbb{K}} \mathbb{L}_2$.
Es bezeichnet $\mathrm{Hom}_{\mathbb{K}}(\mathbb{L}_1, \mathbb{L}_2)$ die Menge aller $\mathbb{K}$-Homomorphismen.

Beispiel:
$\mathbb{L} = \mathbb{C}, \varphi : \mathbb{C} \to \mathbb{C}, \varphi(z) = \overline{z}$.
φ ist ein $\mathbb{Q}$-Homomorphismus, aber φ ist kein $\mathbb{Q}(\sqrt{-1})$-Homomorphismus.

Die Erweiterung $\mathbb{L}_1/\mathbb{K}$ und $\mathbb{L}_2/\mathbb{K}$ heißen $\mathbb{K}$-isomorph, wenn es einen bijektiven $\mathbb{K}$-Homomorphismus $\mathbb{L}_1 \to_{\mathbb{K}} \mathbb{L}_2$ gibt. Man schreibt: $\mathbb{L}_1 \cong_{\mathbb{K}} \mathbb{L}_2$.

2.6.
Sei $\mathbb{L}/\mathbb{K}$ eine Körpererweiterung, sei $\alpha \in \mathbb{L}$. Sei $\varphi : \mathbb{K}[t] \to_{\mathbb{K}} \mathbb{L}$, $\varphi\left(\sum_i c_i t^i\right) := \sum_i c_i \alpha^i$ der Einsetz-Homomorphismus. Es ist $\mathrm{im}(\varphi) = \mathbb{K}[\alpha]$, und $\ker(\varphi) =: \mathfrak{p}$ ist ein Primideal in $\mathbb{K}[t]$. Aus dem Homomorphiesatz folgt:

$$\mathbb{K}[t]/\mathfrak{p} \cong \mathbb{K}[\alpha].$$

Es gibt zwei Möglichkeiten:
1. Fall: $\mathfrak{p} = (0)$: dann ist φ injektiv.
2. Fall: $\mathfrak{p} \neq (0)$: dann ist $\mathfrak{p} = (f)$ für ein eindeutig bestimmtes, normiertes, irreduzibles Polynom $f \in \mathbb{K}[t]$.

Definition 2.7.
Im 1. Fall heißt α **transzendent** über $\mathbb{K}$.
Im 2. Fall heißt α **algebraisch** über $\mathbb{K}$, und f heißt das **Minimalpolynom** von α über $\mathbb{K}$, in Zeichen $f = \mathrm{MinPol}(\alpha/\mathbb{K})$.
Man nennt $\deg(\alpha/\mathbb{K}) := \deg(f) = \dim_{\mathbb{K}} \mathbb{K}[\alpha]$ den **Grad** von α über $\mathbb{K}$.

Scholium 2.8.
Sei $\mathbb{L}/\mathbb{K}$ eine Körpererweiterung. Ist $\alpha \in \mathbb{L}$ transzendent über $\mathbb{K}$, so erfüllt α keine nichttriviale Polynomidentität über $\mathbb{K}$. Es ist dann $\mathbb{K}[\alpha] \cong_{\mathbb{K}} \mathbb{K}[t]$ und $\mathbb{K}(\alpha) \cong_{\mathbb{K}} \mathbb{K}(t)$. Insbesondere ist dann $[\mathbb{K}(\alpha) : \mathbb{K}] = \infty$.

Ist dagegen α algebraisch über $\mathbb{K}$, so erfüllt α echte Polynomidentitäten über $\mathbb{K}$, $f(\alpha) = 0$ mit $f \in \mathbb{K}[t]$, und das eindeutige normierte solche f von kleinstem Grad ist $f = \mathrm{MinPol}(\alpha/\mathbb{K})$.
Dieses f ist irreduzibel, und $\mathbb{K}[t]/(f) \to \mathbb{K}[\alpha]$ ist ein $\mathbb{K}$-Isomorphismus. Da $\mathbb{K}[t]/(f)$ ein Körper ist, ist auch $\mathbb{K}[\alpha]$ ein **Körper**, und somit $\mathbb{K}[\alpha] = \mathbb{K}(\alpha)$.
Weiter ist $[\mathbb{K}(\alpha) : \mathbb{K}] = \dim_{\mathbb{K}} \mathbb{K}[\alpha] = \deg(f)$.

Sei $n := \deg(f) = [\mathbb{K}(\alpha) : \mathbb{K}]$. Es ist $\left(\overline{1}, \overline{t}, \ldots, \overline{t-1}\right)$ eine $\mathbb{K}$-Vektorraum-Basis von $\mathbb{K}[t]/(f)$, also ist auch $(1, \alpha, \alpha^2, \ldots, \alpha^{n-1})$ eine $\mathbb{K}$-Vektorraum-Basis von $\mathbb{K}(\alpha)$.

Korollar 2.9.
Sei $\mathbb{L}/\mathbb{K}$ eine Körpererweiterung, sei $\alpha \in \mathbb{L}$. Dann sind äquivalent:

(i) *α ist algebraisch über $\mathbb{K}$;*

(ii) *$\mathbb{K}[\alpha]$ ist ein Körper, d.h. $\mathbb{K}[\alpha] = \mathbb{K}(\alpha)$;*

(iii) $\dim_{\mathbb{K}} \mathbb{K}[\alpha] < \infty$;

(iv) $[\mathbb{K}(\alpha) : \mathbb{K}] < \infty$.

Beispiel 2.10.
Sei p eine Primzahl, $\zeta := e^{2\pi i/p}$.
Wir haben gesehen (in 1.68): $\Phi_p(\zeta) = 0$, mit $\Phi_p(t) := t^{p-1} + t^{p-2} + \ldots + t + 1$.
$\Phi_p(t)$ ist irreduzibel über $\mathbb{Q}$. Also $\Phi_p(t) = \mathrm{MinPol}(\zeta/\mathbb{Q})$.
$\Rightarrow \mathbb{Q}(\zeta) = \mathbb{Q}[\zeta]$ hat als $\mathbb{Q}$-Vektorraum die Dimension $p-1$. Eine $\mathbb{Q}$-Basis von $\mathbb{Q}(\zeta)$ ist $(1, \zeta, \zeta^2, \ldots, \zeta^{p-2})$. Die höheren Potenzen von ζ erhalte als Linearkombinationen von $1, \ldots, \zeta^{p-2}$ mit Hilfe der Relation $\Phi_p(\zeta) = 0$.

Korollar 2.11.
Sei $\mathbb{L}/\mathbb{K}$ eine Körpererweiterung, sei A ein Zwischenring $\mathbb{K} \subset A \subset \mathbb{L}$ mit $\dim_{\mathbb{K}}(A) < \infty$. Dann ist A selbst ein Körper.

Beweis:
Sei $0 \neq \alpha \in A \Rightarrow \mathbb{K}[\alpha] \subset A \Rightarrow \dim_{\mathbb{K}} \mathbb{K}[\alpha] < \infty \Rightarrow \mathbb{K}[\alpha] = \mathbb{K}(\alpha)$ ist ein Körper. $\Rightarrow \frac{1}{\alpha} \in \mathbb{K}[A] \subset A$.

□

Definition 2.12.
Eine Körpererweiterung $\mathbb{L}/\mathbb{K}$ heißt **algebraisch**, wenn jedes $\alpha \in \mathbb{L}$ algebraisch über $\mathbb{K}$ ist.

Beispiel: Jede endliche Körpererweiterung ist algebraisch.

Satz 2.13.
Sei $\mathbb{L}/\mathbb{K}$ eine Körpererweiterung, die von über $\mathbb{K}$ algebraischen Elementen erzeugt wird. Dann ist die Erweiterung $\mathbb{L}/\mathbb{K}$ algebraisch.

Anders gesagt: Summen und Produkte von algebraischen Elementen sind wieder algebraisch.

Beweis:
Sei $\mathbb{L} = \mathbb{K}(a_i : i \in I)$ mit $\alpha_i/\mathbb{K}$ algebraisch $\forall\ i \in I$. Sei $\beta \in \mathbb{L}$. Es gibt $J \subset I$ endlich mit $\beta \in \mathbb{K}(\alpha_j : j \in J)$. O.E. also $\mathbb{L} = \mathbb{K}(\alpha_1, \ldots, \alpha_n)$ (d.h. $|I| < \infty$).
Betrachte den Körperturm $\mathbb{K} \subset \mathbb{K}(\alpha_1) \subset \mathbb{K}(\alpha_1, \alpha_2 \subset \ldots \subset \mathbb{K}(\alpha_1, \ldots, \alpha_n) = \mathbb{L}$.

Behaupte: $[\mathbb{K}(\alpha_1, \ldots, \alpha_{i+1}) : \mathbb{K}(\alpha_1, \ldots, \alpha_i)] = \deg \mathrm{MinPol}\,(\alpha_{i+1}/\mathbb{K}(\alpha_1, \ldots, \alpha_i)) < \infty$, denn α_{i+1} ist algebraisch über $\mathbb{K}$, und daher auch über $\mathbb{K}(\alpha_1, \ldots, \alpha_i)$.
Also ist $[\mathbb{L} : \mathbb{K}] < \infty \Rightarrow \mathbb{L}/\mathbb{K}$ ist algebraisch $\Rightarrow \beta \in \mathbb{L}$ ist algebraisch über $\mathbb{K}$.

□

Korollar 2.14.
Jede endlich erzeugte, algebraische Körpererweiterung ist endlich.

Korollar 2.15 (Transitivität)**.**
Seien $\mathbb{K} \subset \mathbb{L} \subset \mathbb{M}$ Körper mit $\mathbb{L}/\mathbb{K}$ und $\mathbb{M}/\mathbb{L}$ algebraisch. Dann ist auch $\mathbb{M}/\mathbb{K}$ algebraisch.

Beweis:
Sei $\alpha \in \mathbb{M}$. Sei $g(t) \in \mathbb{L}[t]$ das Minimalpolynom von $\alpha/\mathbb{L}$. Sei $\mathbb{L}_1 := \mathbb{K}(\mathit{Koeffizienten\ von}\ g(t))$.
$\Rightarrow \mathbb{K} \subset \mathbb{L}_1 \subset \mathbb{L}$, $\mathbb{L}_1/\mathbb{K}$ endlich erzeugt, $\mathbb{L}_1/\mathbb{K}$ ist algebraisch (da $\mathbb{L}/\mathbb{K}$ schon algebraisch ist).
$\Rightarrow [\mathbb{L}_1 : \mathbb{K}] < \infty$. Andererseits ist $[\mathbb{L}_1(\alpha) : \mathbb{L}_1] < \infty$.
$\Rightarrow [\mathbb{L}_1(\alpha) : \mathbb{K}] < \infty \Rightarrow [\mathbb{K}(\alpha) : \mathbb{K}] < \infty \Rightarrow \alpha$ ist algebraisch über $\mathbb{K}$.

□

Korollar 2.16.
Sei $\mathbb{L}/\mathbb{K}$ eine beliebige Körpererweiterung. Sei $\widetilde{\mathbb{K}}$ die Menge aller über $\mathbb{K}$ algebraischen Elemente in $\mathbb{L}$. Dann ist $\widetilde{\mathbb{K}}$ ein Teilkörper von $\mathbb{L}$. Man nennt $\widetilde{\mathbb{K}}$ den ***relativen algebraischen Abschluss von $\mathbb{K}$ in $\mathbb{L}$.***

Beweis:
siehe 2.13.

□

b. Adjunktion von Nullstellen

Sei $\mathbb{K}$ ein Körper, sei $f(t) \in \mathbb{K}[t]$. $f(x) = 0$ lösen?

Satz 2.17.
Sei $f \in \mathbb{K}[t]$ ein nicht-konstantes Polynom. Dann gibt es eine endliche Körpererweiterung $\mathbb{L}/\mathbb{K}$ und ein $\alpha \in \mathbb{L}$ mit $f(\alpha) = 0$.

Beweis:
Sei $g(t)$ ein irreduzibler Faktor von $f(t)$. Setze $\mathbb{L} := \mathbb{K}[t]/(g(t))$. Dies ist ein Oberkörper von $\mathbb{K}$ und in $\mathbb{L}$ hat $g(x) = 0$ eine Lösung: nämlich $x = \bar{t} = t + (g(t))$.
Klar, dass auch $f(\bar{t}) = 0$ in $\mathbb{L}$ ist.

□

Definition 2.18.
Sei $f \in \mathbb{K}[t]$ *irreduzibel*. Ein **Wurzelkörper** von f über $\mathbb{K}$ ist ein Oberkörper $\mathbb{L}$ von $\mathbb{K}$, so dass ein $\alpha \in \mathbb{L}$ existiert mit $f(\alpha) = 0$ und mit $\mathbb{L} = \mathbb{K}(\alpha)$.

Satz 2.19.
Sei $f \in \mathbb{K}[t]$ irreduzibel.

(a) *$\mathbb{K}[t]/(f)$ ist ein Wurzelkörper von f.*

(b) *Sind $\mathbb{L}_1, L_2$ zwei Wurzelkörper von f, so ist $\mathbb{L}_1 \cong_{\mathbb{K}} \mathbb{L}_2$.*
Genauer: sei $\alpha_i \in \mathbb{L}_i$ mit $\mathbb{L}_i = \mathbb{K}(\alpha_i)$ und $f(\alpha_i) = 0$ für $i = 1, 2$. Dann gibt es genau einen $\mathbb{K}$-Isomorphismus $\varphi : \mathbb{L}_1 \to_{\mathbb{K}} \mathbb{L}_2$ mit $\varphi(\alpha_1) = \alpha_2$.

Beweis:

(a) gerade gesehen.

(b) Ist $\mathbb{L} = \mathbb{K}(\alpha)$ ein Wurzelkörper von $f/\mathbb{K}$ (mit $f(\alpha) = 0$), so ist $\varphi : \mathbb{K}[t]/(f) \to_{\cong} \mathbb{L}$, $\varphi(\overline{g(t)}) := g(\alpha)$ ein $\mathbb{K}$-Isomorphismus, mit $\varphi(\bar{t}) = \alpha$.
Daraus folgt die Aussage durch Verknüpfung der Isomorphismen von $\mathbb{K}$ auf $\mathbb{L}_1$ bzw. $\mathbb{L}_2$.

□

Bemerkung 2.20.

1. Die Irreduzibilität von f ist wesentlich.

2. Sei $f \in \mathbb{K}[t]$ irreduzibel, sei $\mathbb{E}/\mathbb{K}$ eine Körpererweiterung. Sind $\alpha, \beta \in \mathbb{E}$ Nullstellen von f in $\mathbb{E}$, so ist also $\mathbb{K}(\alpha) \cong_{\mathbb{K}} \mathbb{K}(\beta)$ (beide sind Wurzelkörper von f). Die Körper $\mathbb{K}(\alpha)$ und $\mathbb{K}(\beta)$ sind algebraisch nicht unterscheidbar über $\mathbb{K}$, können aber sehr verschieden „aussehen“: sei etwa $\mathbb{K} = \mathbb{Q}$, $f(t) = t^4 - 2$ (irreduzibel nach Eisenstein). $\mathbb{E} = \mathbb{C}$, sei $\alpha := \sqrt[4]{2} = 1,189\ldots, \beta := i\alpha$ (mit $i := \sqrt{-1}$). Also $\mathbb{Q}(\alpha) \cong \mathbb{Q}(\beta)$. Aber $\mathbb{Q}(\alpha) \subset \mathbb{R}, \mathbb{Q}(\beta) \not\subset \mathbb{R}$!

Korollar 2.21.
Sei $f \in \mathbb{K}[t]$ irreduzibel sei $\mathbb{L} = \mathbb{K}(\alpha)$ ein Wurzelkörper von f, mit $f(\alpha) = 0$. Für jede Körpererweiterung $\mathbb{E}/\mathbb{K}$ haben wir eine Bijektion $\mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \mathbb{E}) \to \{\beta \in \mathbb{E} : f(\beta) = 0\}$, *nämlich* $(\varphi : \mathbb{L}_{\mathbb{K}} \to \mathbb{E}) \mapsto \varphi(\alpha)$.

Beweis:
Sei $\mathbb{L}_0 := \mathbb{K}[t]/(f), \alpha_0 := \bar{t} \in \mathbb{L}_0$.
Dann ist die Aussage klar: $\mathbb{K}[t]/(f) \to_{\mathbb{K}} \mathbb{E}$ ist nach dem Homomorphiesatz durch $\beta := \varphi(\bar{t}$ festgelegt, es ist $f(\beta) = 0$.
Umgekehrt gibt es zu jeden $\beta \in \mathbb{E}$ mit $f(\beta) = 0$ ein solches φ.
Daraus wegen 2.19 sofort auch der Fall von allgemeinem $\mathbb{L}$.

□

Definition 2.22.
Eine Körpererweiterung $\mathbb{L}/\mathbb{K}$ heißt **einfach**, wenn es ein $\alpha \in \mathbb{L}$ gibt mit $\mathbb{L} = \mathbb{K}(\alpha)$. Ein solches α heißt ein **primitives Element** für die Erweiterung $\mathbb{L}/\mathbb{K}$.

Bemerkung 2.23.
Ist $\alpha/\mathbb{K}$ algebraisch, so ist $\mathbb{L} = \mathbb{K}(\alpha)$ endlich über $\mathbb{K}$ und $\mathbb{L}$ ist ein Wurzelkörper von $f := \mathrm{MinPol}(\alpha/\mathbb{K})$ über $\mathbb{K}$. Ist $\alpha/\mathbb{K}$ transzendent, so ist $[\mathbb{K}(\alpha) : \mathbb{K}] = \infty$.

Bemerkung 2.24.
Sei $\mathbb{L} = \mathbb{K}(\alpha)$ eine einfache endliche Erweiterung von $\mathbb{K}$.
Kennt man $f(t) = \mathrm{MinPol}(\alpha/\mathbb{K}) = t^n + a_{n-1}t^{n-1} + \ldots + a_1 t + a_0$, so kann man im Körper $\mathbb{L}$ rechnen:
Eine $\mathbb{K}$-Basis von $\mathbb{L}$ ist (z.B.) $(1, \alpha, \alpha^2, \ldots, \alpha^{n-1})$. Die höheren Potenzen von α findet man durch Anwenden von $f(\alpha) = 0$.
Systematisches Vorgehen: die Abbildung $\mu_A : \mathbb{L} \to \mathbb{L}, x \mapsto \alpha x$, ist $\mathbb{K}$-linear und

hat bezüglich obiger Basis die Matrix $\begin{pmatrix} 0 & & & -a_0 \\ 1 & 0 & & -a_1 \\ & 1 & \ddots & \vdots \\ & & \ddots\ 0 & \\ & & 1 & -a_{n-1} \end{pmatrix} =: A$. In der i-ten Spalte von A^k $(k > 0)$ $(1 \le i \le n)$ stehen die Koeffizienten von α^{k+i-1}.

Jedes Element $\beta \in \mathbb{L}$ hat die Form $\beta = g(\alpha)$ mit $g \in \mathbb{K}[t]$. Dabei kann man $\det(g) < n$ erreichen; dann ist g eindeutig.
Das Inverse β^{-1} erhält man mit dem Euklidischen Algorithmus:
(sei $\beta \neq 0$) es ist ggT$(f, g) = 1$, Euklidischer Algorithmus gibt $p, 1 \in \mathbb{K}[t]$ mit $1 = pf + qg \Rightarrow$ (mit $t := \alpha$) $1 = q(\alpha) \cdot \underbrace{g(\alpha)}_{\beta} \Rightarrow q(\alpha) = \beta^{-1}$.

Um MinPol$(\beta/\mathbb{K})$ zu berechnen, berechne die Potenzen $1, \beta, \beta^2, \ldots$ (bis höchstens β^n) und schaue nach, wann sie linear abhängig werden.

Beispiel 2.25.
Sei $\mathbb{L} = \mathbb{Q}(\alpha)$ mit $\alpha^4 - 8\alpha^3 + 20\alpha^2 - 16\alpha + 2 = 0$.
Das Polynom ist irreduzibel nach Eisenstein.
$\Rightarrow (1, \alpha, \alpha^2, \alpha^3)$ ist eine $\mathbb{Q}$-Basis von $\mathbb{L}$. Sei $\beta := \alpha^2 - 4\alpha$. Berechne MinPol$(\beta/\mathbb{Q})$:
$\beta^2 = \alpha^4 - 8\alpha^3 + 16\alpha^2 = \ldots = -4\alpha^2 + 16\alpha - 2 = -4\beta - 2$.
$\Rightarrow$ MinPol$(\beta/\mathbb{Q}) = t^2 + 4t + 2$
$\Rightarrow$ erhalte auch β^{-1} wie folgt: $\beta^2 + 4\beta + 2 = 0 \Rightarrow \beta(\beta + 4) = -2$.
$\Rightarrow \beta^{-1} = -\frac{1}{2}(\beta + 4) = -\frac{1}{2}\alpha^2 + 2\alpha - 2$.

Sei $\mathbb{L}$ ein Wurzelkörper von f über $\mathbb{K}$, sei $\alpha \in \mathbb{L}$ mit $f(\alpha) = 0$. Habe $f(t) = (t - \alpha)g(t)$ mit $g \in \mathbb{L}(t)$.

Beispiel 2.26.
Der Faktor $g(t)$ in $\mathbb{L}(t)$ kann irreduzibel sein oder in mehrere Faktoren zerfallen:

(1) Sei p eine Primzahl, $\xi = e^{2\pi i/p} \in \mathbb{C}^*$.
$\Phi(t) := Min(\xi/\mathbb{Q}) = t^{p-1} + \ldots + t + 1$ (irreduzibel in $\mathbb{Q}[t]$).
Wir haben gesehen $\Phi_p(t) = (t - \xi) \cdot \ldots \cdot (t - \xi^{p-1})$.
Somit zerfällt das (irreduzible) Polynom über seinem Wurzelkörper $\mathbb{Q}(\xi)$ in Linearfaktoren.

(2) Sei $a \in \mathbb{Z}$, keine dritte Potenz, $f(t) = t^3 - a \in \mathbb{Q}[t]$. Sei $\alpha = \sqrt[3]{a}$ die reelle dritte Wurzel, sei $f(t) = t^3 - a = (t - \alpha)g(t)$ mit $\det(g(t)) = 2$, mit $g(t)$ irreduzibel in

$\mathbb{Q}(\alpha)$.
Denn $\mathbb{Q}(\alpha) \subset \mathbb{R}$, aber die Nullstellen von $g(t)$ sind nicht in $\mathbb{R}$.

Korollar 2.27.
Zu jeden nichtkonstanten Polynom $f(t) \in \mathbb{K}[t]$ gibt es eine Körpererweiterung $\mathbb{L}/\mathbb{K}$, so dass f über $\mathbb{L}$ in Linearfaktoren zerfällt. Dabei kann man $[\mathbb{L} : \mathbb{K}] \leq n!$ erreichen, $n := \deg(f)$.

Beweis:
Induktion nach n. Beginn $n = 1$: lineares Polynom zerfällt über $\mathbb{K}$. ✓
Sei $n > 1$, sei $g(t)$ ein irreduzibler Faktor von $f(t)$ in $\mathbb{K}[t]$, sei $\mathbb{K}_1$ ein Wurzelkörper von $g(t)$, sei $g(\alpha) = 0$ mit $\alpha \in \mathbb{K}$.
Es ist $[\mathbb{K}_1 : \mathbb{K}] = \deg(g) \leq n$, und $f(t) = (t - \alpha) \cdot h(t)$ mit einem $h \in \mathbb{K}_1[t]$, $\deg(h) = n - 1$. Nach Induktionsannahme gibt es $\mathbb{L}/\mathbb{K}_1$ mit $[\mathbb{L} : \mathbb{K}_1] \leq (n-1)!$, so dass $h(t)$ über $\mathbb{L}$ in Linearfaktoren zerfällt. Also zerfällt auch f über $\mathbb{L}$ in Linearfaktoren, $[\mathbb{L} : \mathbb{K}] = \underbrace{[\mathbb{L} : \mathbb{K}_1]}_{\leq (n-1)!} \cdot \underbrace{[\mathbb{K}_1 : \mathbb{K}]}_{\leq n} \leq n!$

□

Definition 2.28.
Sei $f \in \mathbb{K}[t]$, nicht konstant. Ein Oberkörper $\mathbb{L}$ von $\mathbb{K}$, über dem f in Linearfaktoren zerfällt und der von den Nullstellen von f (über $\mathbb{K}$) erzeugt wird, heißt ein **Zerfällungskörper** von f über $\mathbb{K}$.

Satz 2.29.
Sei $f \in \mathbb{K}[t]$, $\deg(f) = n \geq 1$:
Dann hat f einen Zerfällungskörper $\mathbb{L}$ über $\mathbb{K}$ mit $[\mathbb{L} : \mathbb{K}] \leq n!$. Je zwei Zerfällungskörper von f über $\mathbb{K}$ sind zueinander $\mathbb{K}$-isomorph.

Beweis:
Existenz von $\mathbb{L}$ und $[\mathbb{L} : \mathbb{K}] \leq n!$ siehe 2.27.

Bleibt: Eindeutigkeit bis auf $\cong_{\mathbb{K}}$.
Seien $\mathbb{L}_1, \mathbb{L}_2$ Zerfällungskörper von f über $\mathbb{K}$. Induktion über $n = \deg(f)$.
Sei $n = 1$: klar ($\mathbb{K}$ ist Zerfällungskörper).

Sei nun $n > 1$. Sei g ein irreduzibler Faktor von f in $\mathbb{K}[t]$. Es gibt $\alpha_i \in \mathbb{L}_i$ mit $g(\alpha_i) = 0$ für $i = 1, 2$.
Nach 2.19 gibt es einen $\mathbb{K}$-Isomorphismus $\varphi : \mathbb{K}(\alpha_1) \to_{\cong} \mathbb{K}(\alpha_2)$ mit $\varphi(\alpha_1) = \alpha_2$. Es

gibt $h_i \in \mathbb{K}(\alpha_i)[t]$ mit $f = (t - \alpha_i)h_i(t)$ für $i = 1, 2$.

Dann ist $\mathbb{L}_i$ ein Zerfällungskörper von h_i über $\mathbb{K}(\alpha_i)$ für $i = 1, 2$. Insbesondere ist auch $\mathbb{L}_2$ via die Inklusion $\mathbb{K}(\alpha_1) \to_{\cong,\varphi} \mathbb{K}(\alpha_2) \subset \mathbb{L}_2$ ein Zerfällungskörper von $h_1(t)$ über $\mathbb{K}(\alpha_1)$. Denn der Homomorphismus $\widetilde{\varphi} : \mathbb{K}(\alpha_1)[t] \to \mathbb{K}(\alpha_2)[t]$, der durch koeffizientenweises Anwenden von φ entsteht, bildet $h_1(t)$ auf $h_2(t)$ ab. Nach Induktionsannahme sind also die beiden Zerfällungskörper $\mathbb{K}(\alpha_1) \subset \mathbb{L}_1$ und $\mathbb{K}(\alpha_1) \to_{\varphi} \mathbb{K}_2(\alpha_2) \subset \mathbb{L}_2$ von $h_1(t)$ über $\mathbb{K}(\alpha_1)$ isomorph. Sei $\psi : \mathbb{L}_1 \to_{\mathbb{K}(\alpha_1)} \mathbb{L}_2$ ein solcher Isomorphismus. Dann ist ψ ein $\mathbb{K}$-Isomorphismus von $\mathbb{L}_1$ auf $\mathbb{L}_2$.

□

Notation 2.30.
Sei $f \in \mathbb{K}[t]$, $\deg(f) \geq 1$. Schreibe $\mathrm{Zfk}(f/\mathbb{K})$ für „den“ Zerfällungskörper von f über $\mathbb{K}$.

Beispiel 2.31.
Sei p eine Primzahl, sei $a \neq 0$ eine ganze Zahl, quadratfrei. Was ist $\mathbb{L} := \mathrm{Zfk}(t^p - a/\mathbb{Q})$?
Sei $\xi = e^{2\pi i/p} \in \mathbb{C}^*$, sei $\alpha \in \mathbb{C}$ mit $\alpha^p = a$. Dann ist $t^p - A = (t-\alpha)(t-\xi\alpha)\cdot\ldots\cdot(t-\xi^{p-1}\alpha)$.
Also $\mathrm{Zfk}(t^p - a/\mathbb{Q}) = \mathbb{Q}(\alpha, \xi d) = \mathbb{Q}(\alpha, \xi)$.

2.32.
Sei $\mathbb{L}/\mathbb{K}$ eine quadratische Erweiterung, d.h. $[\mathbb{L} : \mathbb{K}] = 2$, sei $\alpha \in \mathbb{L} \setminus \mathbb{K}$, dann ist $\mathbb{L} = \mathbb{K}(\alpha)$, sei $\mathrm{MinPol}(\alpha/\mathbb{K}) = t^2 + at + b$, $0 = \alpha^2 + a\alpha + b = (\alpha + \frac{a}{2})^2 + (b - \frac{a^2}{4})$. Hier haben wir $char(\mathbb{K}) \neq 2$ benutzt.
Setze $\beta := \alpha + \frac{a}{2}$, dann ist auch $\mathbb{L} = \mathbb{K}(\beta)$, und $\mathrm{MinPol}(\beta/\mathbb{K}) = t^2 - c$ mit $c := -b + \frac{a^2}{4}$ ist „einfacher“ als $\mathrm{MinPol}(\alpha/\mathbb{K})$. $\alpha = \beta - \frac{a}{2} \rightsquigarrow \alpha = \sqrt{c} - \frac{a}{2} = \frac{\sqrt{a^2-4b}-2a}{2}$.

Satz 2.33.
Sei $char(\mathbb{K}) \neq 2$. Jede quadratische Erweiterung von $\mathbb{K}$ hat die Form $\mathbb{L} = \mathbb{K}(\sqrt{c})$, mit $c \in \mathbb{K}^* \setminus \mathbb{K}^{*2}$.
Dabei gilt für $c, d \in \mathbb{K}^* \setminus \mathbb{K}^{*2}$: $\mathbb{K}(\sqrt{c}) \cong_{\mathbb{K}} \mathbb{K}(\sqrt{d}) \Leftrightarrow c\mathbb{K}^{*2} = d\mathbb{K}*2 \Leftrightarrow \frac{c}{d} \in \mathbb{K}^{*2}$.

Beweis:
$\mathbb{L} = \mathbb{K}(\sqrt{c})$ gerade gesehen. „$\Leftarrow$“ ist klar. $d = cb^2$ mit $b \in \mathbb{K}^* \Rightarrow \sqrt{d} = \sqrt{c} \cdot b \Rightarrow \mathbb{K}(\sqrt{c}) = \mathbb{K}(\sqrt{d})$.
„$\Rightarrow$“ Sei $c \in \mathbb{K}^* \setminus \mathbb{K}^{*2}$. Welche Elemente aus $\mathbb{K}$ werden in $\mathbb{K}(\sqrt{c})$ zu einem Quadrat?
$x, y \in \mathbb{K}$. $(x + y\sqrt{c})^2 = (x^2 + y^2c) + 2xy\sqrt{c} \in \mathbb{K} \Leftrightarrow 2xy = 0 \Leftrightarrow x = 0 \vee y = 0$.
Somit $\mathbb{K}^* \cap \mathbb{K}(\sqrt{c})^{*2} = \mathbb{K}^{*2} \cup c\mathbb{K}^{*2}$. Daraus folgt „$\Rightarrow$“.

□

Bemerkung 2.34.

1. Für $char(\mathbb{K}) \neq 2$ entsprechen also die ($\mathbb{K}$-Isomorphismus-Klassen von) quadratischen Erweiterungen von $\mathbb{K}$ genau den von $1\mathbb{K}^{*2}$ verschiedenen Klassen in $\mathbb{K}^*/\mathbb{K}^{*2} = \{a \cdot \mathbb{K}^{*2} : a \in \mathbb{K}^*\}$

2. Bsp. $\mathbb{K} = \mathbb{Q}$. Die quadratischen Erweiterungen von $\mathbb{Q}$ sind genau die folgenden: $\mathbb{Q}(\sqrt{-1})$ und die $\mathbb{Q}(\sqrt{n}), \mathbb{Q}(\sqrt{-n})$ mit $n > 1$ eine quadratfreie natürliche Zahl.

3. Allgemeiner kann man in jedem Grad folgendes machen:
   Ist $f(t) = t^n + a_{n-1}t^{n-1} + \ldots + a_1 t + a_0 \in \mathbb{K}[t]$ irreduzibel, so kann man durch Substitution $u := t + \frac{a_{n-1}}{n}$ erreichen, dass $a_{n-1} = 0$ wird (für $char(\mathbb{K}) \nmid n$).
   Weiter kommt man aber im Allgemeinen nicht.

Beispiel 2.35.
Sei $\mathbb{L}$ ein Wurzelkörper von $f(t) = t^3 - 4t + 1$ über $\mathbb{Q}$ (irreduzibel), $f(0) = 1, f(1) = -2, f(x) \to \pm\infty$ für $x \to \pm\infty$.
Dann hat f drei reelle Nullstellen.
Sei $\beta \in \mathbb{L} \setminus \mathbb{Q}$. Dann ist niemals $b := \beta^3 \in \mathbb{Q}$, denn sonst wäre $\mathbb{L} = \mathbb{Q}(\beta)$ und $\text{MinPol}(\beta/\mathbb{Q}) = t^3 - b$. $\Rightarrow \text{Hom}_{\mathbb{Q}}(\mathbb{L}; \mathbb{R}) \cong \{x \in \mathbb{R} : x^3 = b\}$: es gäbe nur eine $\mathbb{L} \to \mathbb{R}$.

Andererseits folgt aus $\mathbb{L}$ ist Wurzelkörper von $(f/\mathbb{Q})$: $\mathbb{L}$ hat drei Einbettungen nach $\mathbb{R}$.

c. Der algebraische Abschluss von $\mathbb{K}$

Lemma 2.36.
Für jeden Körper $\mathbb{K}$ sind äquivalent

(i) $\mathbb{K}$ *ist algebraisch abgeschlossen, d.h. jedes nichtkonstante Polynom in* $\mathbb{K}[t]$ *zerfällt in Linearfaktoren;*

(ii) $\mathbb{K}$ *hat keine von* $\mathbb{K}$ *verschiedene endliche Körpererweiterung.*

Beweis:
(i) $\Rightarrow$ (ii)
Sei $\mathbb{L}/\mathbb{K}$ endlich, sei $\alpha \in \mathbb{L}$. $f := Min(\alpha/\mathbb{K}) \Rightarrow f$ zerfällt nach Voraussetzung in Linearfaktoren, einer davon ist $(t - \alpha) \Rightarrow \alpha \in \mathbb{K} \Rightarrow \mathbb{L} = \mathbb{K}$.

(ii) $\Rightarrow$ (i)
klar aus Existenz eines Zerfällungskörpers.

□

Definition 2.37.
Sei $\mathbb{K}$ ein Körper. Ein Oberkörper $\mathbb{E}$ von $\mathbb{K}$ heißt ein **algebraischer Abschluss** von $\mathbb{K}$, wenn $\mathbb{E}/\mathbb{K}$ algebraisch und $\mathbb{E}$ algebraisch abgeschlossen ist.

Lemma 2.38.
Sei $\mathbb{L}/\mathbb{K}$ eine algebraische Erweiterung derart, dass jedes Polynom aus $\mathbb{K}[t]$ über $\mathbb{L}$ in Linearfaktoren zerfällt. Dann ist $\mathbb{L}$ ein algebraischer Abschluss.

Beweis:
Sei $\mathbb{F}/\mathbb{L}$ eine endliche Erweiterung. Dann ist auch $\mathbb{F}/\mathbb{K}$ algebraisch (2.15).
Sei $\alpha \in \mathbb{F}$, $Min(\alpha/\mathbb{K}) =: f$ zerfällt über $\mathbb{L}$ nach Voraussetzung.
$f(\alpha) = 0 \Rightarrow \alpha \in \mathbb{L} \Rightarrow \mathbb{F} = \mathbb{L}$.

□

Korollar 2.39.
Sei $\mathbb{E}/\mathbb{K}$ eine beliebige Körpererweiterung derart, dass jedes Polynom aus $\mathbb{K}[t]$ über $\mathbb{E}$ zerfällt. Dann ist der relative algebraische Abschluss $\widetilde{K}$ in $\mathbb{E}$ (2.16) ein algebraischer Abschluss von $\mathbb{K}$.

Beweis:
sofort aus 2.38.

□

Beispiel 2.40.
$\mathbb{C}$ ist ein algebraischer Abschluss von $\mathbb{R}$.
Der Körper $\widetilde{\mathbb{Q}} := \{\alpha \in \mathbb{C} : \alpha \text{ ist algebraisch über } \mathbb{Q}\}$ ist ein algebraischer Abschluss von $\mathbb{Q}$ nach 2.39.

Theorem 2.41 (Steinitz)**.**
Sei $\mathbb{K}$ ein Körper. Dann hat $\mathbb{K}$ einen algebraischen Abschluss. Je zwei algebraische Abschlüsse von $\mathbb{K}$ sind $\mathbb{K}$-isomorph.

Beweis:
Existenz:
Konstruiere eine Kette $\mathbb{K} = \mathbb{K}_0 \subset \mathbb{K}_1 \subset \mathbb{K}_2 \subset \ldots$ von Körpererweiterungen derart, dass jedes nichtkonstante Polynom $f \in \mathbb{K}_i[t]$ eine Nullstelle in $\mathbb{K}_{i+1}$ hat für $i = 0, 1, 2, \ldots$.
Ist dies erreicht, so sei $\mathbb{E} := \bigcup_{i \geq 1} \mathbb{K}_i$ ein Oberkörper von $\mathbb{K}$. Jedes nichtkonstante $f \in \mathbb{K}[t]$ zerfällt über $\mathbb{E}$ in Linearfaktoren.
Aus 2.39 folgt also dann die Existenz eines algebraischen Abschlusses von $\mathbb{K}$.

Also genügt es zu zeigen, dass es einen Oberkörper $\mathbb{K}_1$ von $\mathbb{K}$ gibt derart, dass jedes $f \in \mathbb{K}[t] \setminus \mathbb{K}$ in $\mathbb{K}$ eine Nullstelle hat. Sei

$$\mathcal{I} := \{f \in \mathbb{K}[t] : f \text{ ist normiert und irreduzibel}\}$$

Sei $A := \mathbb{K}[x_f : f \in \mathcal{I}]$, Polynomring in den (unendlich vielen!) Variablen $x_f, f \in \mathcal{I}$.
Sei I das in A von alles $f(x_f)$, $f \in \mathcal{I}$, erzeugte Ideal.
Behauptung: $I \neq A$.
Beweis: Wäre $1 \in I$, so gäbe es $f_1, \ldots, f_r \in \mathcal{I}$ und $a_1, \ldots, a_r \in A$ mit $1 = a_1 f_1(x_{f_1}) + \ldots + a_r f_r(x_{f_r})$ (*)
Sei $\mathbb{L}/\mathbb{K}$ eine endliche Erweiterung, so dass $f_1, \ldots, f_r$ jeweils eine Nullstelle in $\mathbb{L}$ haben (z.B. $\mathbb{L} = \mathrm{Zfk}(f_1, \ldots, f_k/\mathbb{K})$).
Sei $\alpha_i \in \mathbb{L}$ mit $f_i(\alpha_i) = 0$ für $i = 1, \ldots, r$. Definiere den $\mathbb{K}$-Homomorphismus $\varphi : A \to \mathbb{L}, \varphi(x_{f_i}) := \alpha_i$ für $i = 1, \ldots, r$ und $\varphi(x_f) := 0$ für $f \in \mathcal{I} \setminus \{f_1, \ldots, f_r\}$.
Anwendung von φ auf (*). $1 = \underbrace{\sum_{i=1}^{r} \varphi(a_i) \cdot \underbrace{f_i(\underbrace{\varphi(x_{f_i})}_{=\alpha_i})}_{=0}}_{=0} \to$ Widerspruch.

Also ist tatsächlich $I \neq A$. Nach 1.29 gibt es ein maximales Ideal $\mathfrak{m}$ in A mit $I \subset \mathfrak{m}$.
Setze $\mathbb{K}_1 := A/\mathfrak{m}$, ein Oberkörper von $\mathbb{K}$.

$\mathbb{K}_1$ hat die gewünschte Eigenschaft. Zu $f \in \mathcal{I}$ ist nämlich $\overline{x}_f = x_f + \mathfrak{m}$ eine Nullstelle von f in $\mathbb{K}_1$, denn $f(x_f) \in \mathfrak{m}$.

Bemerkung: Wir haben hier das Zorn'sche Lemma verwendet (Existenz von $\mathfrak{m}$).

Fortsetzung nach dem nächsten Satz ...

Satz 2.42.
Sei $\varphi : \mathbb{K} \to \Omega$ ein Homomorphismus von $\mathbb{K}$ in einen algebraisch abgeschlossenen Körper Ω. Sei $\mathbb{L}/\mathbb{K}$ eine algebraische Erweiterung. Dann lässt sich φ von $\mathbb{K}$ auf $\mathbb{L}$ fortsetzen:
$\mathbb{K} \hookrightarrow \mathbb{L}$, $\mathbb{K} \to_\varphi \Omega \Rightarrow \mathbb{L} \to_\psi \Omega$.
Also $\exists$ ein Homomorphismus $\psi : \mathbb{L} \to \Omega$ mit $\psi|_{\mathbb{K}} = \varphi$.

Beweis: *(Fortsetzung von 2.41)*
Eindeutigkeit aus 2.42:
$\mathbb{K}$, seien Ω_1, Ω_2 algebraische Abschlüsse von $\mathbb{K}$. 2.42 $\Rightarrow$ *ex* $\mathbb{K}$-Homomorphismus $\psi : \Omega_1 \to \Omega_2$.
ψ ist surjektiv, denn sei $\beta \in \Omega_2$, sei $f := \mathrm{MinPol}(\beta/\mathbb{K})$. Seien $\alpha_1, \ldots, \alpha_n \in \Omega_1$ die Nullstellen von f in Ω_1 ($n := \deg(f)$).
$\Rightarrow f(t) = \prod_{i=1}^{n}(t - \alpha_i) = \prod_{i=1}^{n}(t - \psi(\alpha_i))$. Also sind $\psi(\alpha_1), \ldots, \psi(\alpha_n)$ alle Nullstellen von $f(t)$ in Ω_2. Also ist $\beta = \psi(\alpha_i)$ für ein i.

□

Beweis: (von Satz 2.42)
Zunächst sei $\mathbb{L} = \mathbb{K}(\alpha)$ mit einem $\alpha \in \mathbb{L}$.
Sei $f := \mathrm{MinPol}(\alpha/\mathbb{K})$. Ω ist algebraisch abgeschlossen $\Rightarrow$ $\exists\, \beta \in \Omega$ mit $f(\beta) = 0$.
Also ist durch $\psi(\alpha) := \beta$ eine solche Fortsetzung definiert.
($\mathbb{L} = \mathbb{K}(\alpha)$, $\mathbb{K}(\beta)$ Wurzelkörper von f)

Nun sei $\mathbb{L}/\mathbb{K}$ beliebig (algebraisch).
Betrachte die Menge
$\mathfrak{X} := \{(E, \phi) : \mathbb{K} \subset \mathbb{E} \subset \mathbb{L}$ Zwischenkörper, $\phi \in \mathrm{Hom}(\mathbb{E}, \Omega), \phi|_{\mathbb{K}} = \varphi\}$.
$\mathfrak{X}$ ist eine geordnete Menge durch $(\mathbb{E}_1, \phi_1) \leq (\mathbb{E}_2, \phi_2) :\Leftrightarrow \mathbb{E}_1 \subset \mathbb{E}_2, \phi_2|_{\mathbb{E}_1} = \phi_1$.

Jede Kette in $\mathfrak{X}$ hat eine obere Schranke in $\mathfrak{X}$:
$\{(\mathbb{E}_i, \phi_i)\}_{i \in I}$ Kette.
$\Rightarrow (\mathbb{E}, \phi) := \bigcup_{i \in I}(\mathbb{E}_i, \phi_i)$.

Zorn'sches Lemma $\Rightarrow$ es gibt ein maximales $(\mathbb{E}, \phi)$ in $\mathfrak{X}$.

Behaupte: $\mathbb{E} = \mathbb{L}$. Andernfalls wähle $\alpha \in \mathbb{L} \setminus \mathbb{E}$. dann hat ϕ nach dem ersten Schritt eine Fortsetzung auf $\mathbb{E}(\alpha) \neq \mathbb{E}$, Widerspruch zu Maximalität.

□

Definition 2.43.
Mit $\overline{\mathbb{K}}$ wird ein algebraischer Abschluss von $\mathbb{K}$ bezeichnet.
(nach 2.41 sind je zwei solche $\mathbb{K}$-isomorph)

Bemerkung 2.44.
Für $\mathbb{K} = \mathbb{R}$ ist $\mathbb{C} = \mathbb{R}(\sqrt{-1})$ ein algebraischer Abschluss von $\mathbb{R}$. Ein anderer ist $\Omega = \mathbb{R}[t]/(t^2 + 1)$.
Es gibt zwei $\mathbb{R}$-Isomorphismen $\Omega \to_{\cong,\mathbb{R}} \mathbb{C}$, nämlich $\bar{t} \mapsto \pm\sqrt{-1}$. Keiner ist kanonischer als der andere.

Korollar 2.45.
Sei $\overline{\mathbb{K}}$ ein algebraischer Abschluss von $\mathbb{K}$, sei $\mathbb{L}/\mathbb{K}$ eine algebraische Erweiterung. Dann gibt es eine $\mathbb{K}$-Einbettung $\mathbb{L} \to_{\mathbb{K}} \overline{\mathbb{K}}$.
(das ist 2.42)

Erinnerung 2.46.
Sei $\mathbb{E}/\mathbb{K}$ eine Körpererweiterung. Ein **$\mathbb{K}$-Automorphismus** von $\mathbb{E}$ ist ein bijektiver $\mathbb{K}$-Homomorphismus $\mathbb{E} \to_{\mathbb{K}} \mathbb{E}$.

Die Menge aller $\mathbb{K}$-Automorphismen von $\mathbb{E}$ bildet unter Komposition eine Gruppe, $Aut(\mathbb{E}/\mathbb{K})$.

Korollar 2.47.
Sei $\mathbb{K}$ ein Körper, sei $\overline{\mathbb{K}}$ ein algebraischer Abschluss von $\mathbb{K}$.

(a) Jeder $\mathbb{K}$-Homomorphismus $\overline{\mathbb{K}} \to_{\mathbb{K}} \overline{\mathbb{K}}$ ist bijektiv, also ein $\mathbb{K}$-Automorphismus.

(b) Sind $\mathbb{L}, \mathbb{L}'$ Zwischenkörper von $\overline{\mathbb{K}}/\mathbb{K}$, und ist $\varphi : \mathbb{L} \to_{\cong,\mathbb{K}} \mathbb{L}'$ ein $\mathbb{K}$-Isomorphismus, so lässt sich φ zu einem $\mathbb{K}$-Automorphismus ψ von $\overline{\mathbb{K}}$ fortsetzen.

Beweis:

(a) schon im Beweis der Eindeutigkeit in 2.41.

(b) folgt aus 2.42 (Homomorphismus) und (a) (Bijektivität).

□

Definition 2.48.
Zwei Elemente $\alpha, \beta \in \overline{\mathbb{K}}$ heißen zueinander $\mathbb{K}$**-konjugiert**, wenn es ein $\sigma \in \mathrm{Aut}(\overline{\mathbb{K}}/\mathbb{K})$ mit $\sigma(\alpha) = \beta$ gibt.

Korollar 2.49.
Genau dann sind $\alpha, \beta \in \overline{\mathbb{K}}$ $\mathbb{K}$-konjugiert, wenn $MinPol(\alpha/\mathbb{K}) = MinPol(\beta/\mathbb{K})$ ist.

Beweis:
Ist $\mathrm{MinPol}(\alpha/\mathbb{K}) = \mathrm{MinPol}(\beta/\mathbb{K}) =: f$, so gibt es nach 2.19 einen $\mathbb{K}$-Isomorphismus $\varphi : \mathbb{K}(\alpha) \to_{\cong} \mathbb{K}(\beta)$ mit $\varphi(\alpha) = \beta$.
Nach 2.47 (b) lässt sich φ zu einem $\sigma \in Aut(\overline{\mathbb{K}}/\mathbb{K})$ fortsetzen.

Umgekehrt sei $\sigma \in \mathrm{Aut}(\overline{K}/\mathbb{K})$, sei $\beta = \sigma(\alpha)$. Sei $\mathrm{MinPol}(\alpha/\mathbb{K}) = \sum a_i t^i$, dann $0 = \sum a_i \alpha^i = \sum a_i \underbrace{\sigma^i(\alpha)}_{=\beta} = \sum a_i \beta^i \Rightarrow \mathrm{MinPol}(\alpha/\mathbb{K}) = \mathrm{MinPol}(\beta/\mathbb{K})$.

□

Korollar 2.50.
Sei $\alpha \in \overline{K}$. Die $\mathbb{K}$-Konjugierten von α sind genau die Nullstellen von $MinPol(\alpha/\mathbb{K})$ in $\overline{\mathbb{K}}$.

Beispiele 2.51.

1. $\mathbb{K} = \mathbb{R}$, $\overline{\mathbb{K}} = \mathbb{C}$. Ist $\alpha \in \mathbb{C}, \alpha = a + bi$ mit $a, b \in \mathbb{R}$, so sind die $\mathbb{R}$-Konjugierten von α gerade α und $\overline{A} = a - bi$.
   $\mathrm{MinPol}(\alpha/\mathbb{R}) = t^2 - 2at + (a^2 + b^2) = (t - \alpha)(t - \overline{\alpha})$, falls $b \neq 0$.

2. Sei $\mathbb{K} = \mathbb{Q}$, sei p eine Primzahl, $\zeta = e^{2\pi i/p}$. Was sind die $\mathbb{Q}$-Konjugierten von ζ?
   Wegen $\mathrm{MinPol}(\zeta/\mathbb{Q}) = t^{p-1} + \ldots + t + 1 = \prod_{j=1}^{p-1} (t - \zeta^j)$ sind es genau $\zeta, \zeta^2, \ldots, \zeta^{p-1}$.

d. Separable Polynome und vollkommene Körper

Zählen von Nullstellen von Polynomen mit Vielfachheiten.

Definition 2.52.
Sei $f \in \mathbb{K}[t]$, $f \neq 0$, sei $c \in \mathbb{K}$.
Dann heißt die größte Zahl $e \geq 0$ mit $(t-c)^e \mid f$ die **Vielfachheit** der Nullstelle c von f.
Ist $e = 1$, so heißt c eine **einfache Nullstelle** von f.

Lemma 2.53.
Ein Polynom $f \in \mathbb{K}[t]$ vom Grad $n \geq 0$ hat höchstens n Nullstellen in $\mathbb{K}$, gezählt mit Vielfachheit.

Beweis:
klar aus Gradgründen, und wegen der eindeutigen Faktorzerlegung in $\mathbb{K}[t]$.
□

Definition 2.54.
Sei $f = a_n t^n + \ldots + a_1 t + a_0 \in \mathbb{K}[t]$.
Die (formale) Ableitung von f ist das Polynom
$f' = \frac{d}{dt} f = n a_n t^{n-1} + \ldots + a_1 = \sum_{i \geq 1} i a_i t^{i-1}$.

Höhere Ableitungen werden induktiv definiert durch $f^{(k)} = \left(f^{(k-1)}\right)'$ für $k = 1, 2, \ldots$.

Lemma 2.55.
Für $f, g \in \mathbb{K}[t]$ und $a, b \in \mathbb{K}$ gilt:

(a) $(af + bg)' = af' + bg'$;

(b) $(f \cdot g)' = f' \cdot g + f \cdot g'$;

(c) $(f \circ g)' = (f' \circ g) \cdot g'$.

Dabei sei $f \circ g$ das durch Einsetzen definierte Polynom: ist $f = \sum_{i \geq 0} a_i t^i$, so $f \circ g := \sum_{i \geq 0} a_i g^i$.

Beweis:
Aufgabe 25
□

Satz 2.56.
Sei $0 \neq f \in \mathbb{K}[t]$, sei $c \in \mathbb{K}$ eine Nullstelle von f von Vielfachheit $e \geq 1$.
Dann ist c eine Nullstelle von f' von Vielfachheit $\geq e-1$.
Dabei gilt Gleichheit genau dann, wenn char($\mathbb{K}$) kein Teiler von e ist (also z.B. stets für char($\mathbb{K}$) = 0).

Beweis:
$f = (t-c)^e \cdot g$ mit $g \in \mathbb{K}[t]$, $g(c) \neq 0$.
Ableiten $\Rightarrow f' = e(t-c)^{e-1} \cdot g(t) + (t-c)^e \cdot g'(t) = (t-c)^{e-1} \underbrace{(e \cdot g(t) + (t-c)g'(t))}_{=:h(t)}$.

$h(c) = e \cdot \underbrace{g(c)}_{\neq 0}$. Ist $e \neq 0$ in $\mathbb{K}$, so $h(c) \neq 0$, also die Vielfachheit $= e-1$; ist $e = 0$ in $\mathbb{K}$, so $h(c) = 0$, also Vielfachheit $\geq e$.

□

Satz 2.57.
Sei $f \in \mathbb{K}[t]$.

(a) Ist char($\mathbb{K}$) = 0, so gilt: $f' = 0 \Leftrightarrow f \in \mathbb{K}$.

(b) Sei char($\mathbb{K}$) = $p > 0$, so gilt $f' = 0 \Leftrightarrow f \in \mathbb{K}[t^p]$, d.h. $f = b_0 + b_1 t^p + b_2 t^{2p} + \ldots + b_m t^{mp}$ mit geeigneten $b_i \in \mathbb{K}$.

Beweis:
$f = \sum_{i \geq 0} a_i t^i$, $f' = \sum_{i \geq 1} i a_i t^{i-1}$.
Ist char($\mathbb{K}$) = 0, so $i \cdot a_i = 0 \Leftrightarrow a_i = 0$ für $i \geq 1$.
Ist char($\mathbb{K}$) = $p > 0$, so also $f' = 0 \Leftrightarrow a_i = 0$ für alle i mit $p \nmid i$.

□

Definition 2.58.
Sei $\mathbb{K}$ ein Körper. Ein Polynom $0 \neq f \in \mathbb{K}[t]$ heißt **separabel**, wenn f in $\overline{\mathbb{K}}$ (:= algebraischer Abschluss von $\mathbb{K}$) nur einfache Nullstellen hat. Andernfalls heißt f **inseparabel**.

Satz 2.59.
Für $0 \neq f \in \mathbb{K}[t]$ sind äquivalent:

(i) f ist separabel;

(ii) in jedem Oberkörper $\mathbb{E}$ von $\mathbb{K}$ hat f nur einfache Nullstellen;

(iii) $ggT(f, f') = 1$.

Beweis:
Zunächst:

Lemma 2.60.
Sei $\mathbb{E}/\mathbb{K}$ *eine Körpererweiterung. Seien* $f, g \in \mathbb{K}[t]$. *Ist* h *ein ggT von* f *und* g *in* $\mathbb{K}[t]$, *so ist* h *auch ein ggT von* f *und* g *in* $\mathbb{E}[t]$.

Beweis:
Der euklidische Algorithmus hängt nicht vom Grundkörper ab!

□

Sei nun $\overline{\mathbb{K}}$ ein algebraischer Abschluss von $\mathbb{K}$. Sei $f = c \cdot \prod_{i=1}^{n} (t-\alpha_i)^{e_i}$ mit $\alpha_1, \ldots, \alpha_n, c \in \overline{\mathbb{K}}$, $e_i \in \mathbb{N}$, und $\alpha_i \neq \alpha_j$ für $i \neq j$.
Ist f separabel, so folgt $e_i = 1$ für $i = 1, \ldots, n$, also $f'(\alpha_i) \neq 0 \ \forall\, i$.
Also $t - \alpha_i \nmid f'$ für $i = 1, \ldots, n$, somit ist $\mathrm{ggT}(f, f') = 1$ (über $\overline{\mathbb{K}}$, also auch über $\mathbb{K}$).
Ist f inseparabel, so ist $e_i \geq 2$ für ein i, also $f'(\alpha_i) = 0 \Rightarrow t - \alpha_i$ ist ein gemeinsamer Teiler von f und $f' \Rightarrow \mathrm{ggT}(f, f') \neq 1$ (über $\overline{\mathbb{K}}$, also auch über $\mathbb{K}$). Also (i) $\Leftrightarrow$ (iii).

Dann wegen 2.60 auch Äquivalenz zu (ii).

□

Beispiel 2.61.
Sei $f = t^2 + at + b \in \mathbb{K}[t]$.
$f' = 2t + a$. Euklidischer Algorithmus ergibt für $char(\mathbb{K}) \neq 2$: $f = \frac{1}{4}(2t+a) \cdot f' - \frac{a^2-4b}{4}$.
Also f separabel $\Leftrightarrow \mathrm{ggT}(f, f') = 1 \Leftrightarrow a^2 - 4b \neq 0$.
Die Zahl $D(f) := a^2 - 4b$ heißt **Diskriminante** von f.

Man sieht leicht, dass diese Charakterisierung auch für $char(\mathbb{K}) = 2$ richtig bleibt.

Sei $t^3 + at + b$. Dann findet man analog:
f separabel $\Leftrightarrow D(f) := 4a^3 + 27b^2 \neq 0$.

$f \in \mathbb{K}[t]$, $f = f_1^{e_1} \cdot \ldots \cdot f_r^{e_r}$, f_i irreduzibel, $f_i \nsim f_j$ für $i \neq j$.
klar: f separabel $\Rightarrow e_i = 1$.
Umkehrung?

Satz 2.62.
Sei $f \in \mathbb{K}[t]$ ein irreduzibles Polynom.

(a) ist $char(\mathbb{K}) = 0$, so ist f separabel;

(b) ist $char(\mathbb{K}) = p > 0$, so gilt:
f ist inseparabel $\Leftrightarrow f' = 0 \Leftrightarrow f$ is ein Polynom in t^p.

Beweis:
f separabel $\Leftrightarrow \mathrm{ggT}(f, f') = 1$.
$\deg(f') < \deg(f)$. Da f irreduzibel ist, folgt $\mathrm{ggT}(f, f') \neq 1 \Leftrightarrow f' = 0$.

□

Satz 2.63.
Sei A ein Ring und p eine Primzahl, es gelte $p = 0$ in A. Dann ist $(x + y)^p = x^p + y^p$ für alle $x, y \in A$.
Induktiv damit auch $(x + y)^{p^n} = x^{p^n} + y^{p^n}$ für alle $n \geq 1$.

Beweis:
$(x + y)^p = x^p + y^p + \sum_{i=1}^{p-1} \binom{p}{i} x^i p^{i-1}$.
Dabei ist $\binom{p}{i} = \frac{p(p-1)\cdot\ldots\cdot(p-i+1)}{i!}$ durch p teilbar für $i = 1, \ldots, p-1$.

□

Definition 2.64.
Sei $\mathbb{K}$ ein Körper, $char(\mathbb{K}) = p > 0$. Der Ringhomomorphismus $\varphi : \mathbb{K} \to \mathbb{K}, \varphi(x) = x^p$, heißt der **Frobenius** von $\mathbb{K}$.

Man schreibt $\mathbb{K}^p := \varphi(\mathbb{K}) = \{x^p : x \in \mathbb{K}\}$.

Bemerkungen 2.65.

1. $\mathbb{K}^p = \varphi(\mathbb{K})$ ist ein Teilkörper von $\mathbb{K}$, der zu $\mathbb{K}$ isomorph ist. Denn $\varphi : \mathbb{K} \to \mathbb{K}^p$ ist ein Isomorphismus.
2. Der Frobenius φ ist die Identität auf $\mathbb{F}_p = \{0, 1, \ldots, p-1\} \subset \mathbb{K}$.

Satz 2.66.
Sei $char(\mathbb{K}) = p > 0$, sei $f(t) = t^p - a$ mit $a \in \mathbb{K} \setminus \mathbb{K}^p$. Dann ist f irreduzibel in $\mathbb{K}[t]$, und inseparabel.

Beweis:
Sei $\alpha \in \overline{\mathbb{K}}$ mit $\alpha^p = a$, dann ist $f = t^p - a = (t-\alpha)^p$. Die Faktorzerlegungen von f in $\overline{\mathbb{K}}$ sind also die $(t-\alpha)^i \cdot (t-\alpha)^{p-i}$.
Zu zeigen also: $(t-\alpha)^i \notin \mathbb{K}[t]$ für $1 \leq i \leq p-1$.

Tatsächlich ist $\alpha^i \notin \mathbb{K}$:
wegen $p \nmid i$ ist $1 = s \cdot p + t \cdot i$ mit $s, t \in \mathbb{Z} \Rightarrow \alpha = \alpha^{sp+ti} = \underbrace{(\overset{s}{\alpha^p})}_{\in \mathbb{K}} \cdot (\alpha^i)^t$.

Wäre also $\alpha^i \in \mathbb{K}$, so auch $\alpha \in \mathbb{K} \rightarrow$ Widerspruch.

□

Beispiele 2.67.

1. Ist k ein beliebiger Körper mit $char(k) = p$ und $\mathbb{K} = k(x)$ (der rationale Funktionenkörper in der Variablen x), so ist $x \notin \mathbb{K}^p$. Also ist das Polynom $t^p - x \in \mathbb{K}[t]$ irreduzibel und inseparabel.

2. Ist $char(\mathbb{K}) = p > 0$, so hat jedes Element in $\overline{\mathbb{K}}$ nur *eine* p-te Wurzel.

Definition 2.68.
Ein Körper heißt **vollkommen**, wenn jedes irreduzible $f \in \mathbb{K}[t]$ separabel ist.

Satz 2.69.
Sei $\mathbb{K}$ ein Körper. Es sind äquivalent:

(i) $\mathbb{K}$ *ist vollkommen;*

(ii) $char(\mathbb{K}) = 0$ *oder* $char(\mathbb{K}) = p > 0$ *und* $\mathbb{K}^p = \mathbb{K}$.

Beweis:
Ist $char(\mathbb{K}) = 0$, so ist $\mathbb{K}$ vollkommen nach 2.62 (a).

Sei $char(\mathbb{K}) = p > 0$. Ist $\mathbb{K}^p \neq \mathbb{K}$, etwa $a \in \mathbb{K} \setminus \mathbb{K}^p$, so ist $t^p - a \in \mathbb{K}[t]$ irreduzibel und inseparabel, also $\mathbb{K}$ nicht vollkommen.
Sei nun $\mathbb{K}^p = \mathbb{K}$, sei $f \in \mathbb{K}[t]$ ein irreduzibles Polynom. Wäre f inseparabel, so wäre $f \in \mathbb{K}[t^p]$ etwa $f = \sum_{i=0}^{m} a_i t^{ip}$ (2.62 (b)).

Sei $b_i = \sqrt[p]{a_i} \in \mathbb{K}$ für $i = 0, \ldots, m$, dann $f = \left(\sum_{i=0}^{m} b_i t^i \right)^p$. $\rightarrow$ Widerspruch zu f

irreduzibel.

□

Beispiele 2.70.

1. Jeder Körper von Charakteristik 0 ist vollkommen.
   Jeder algebraisch abgeschlossene Körper ist vollkommen.
2. Jeder endliche Körper ist vollkommen. Denn der Frobenius $\varphi : \mathbb{K} \to \mathbb{K}, \varphi(x) = x^p$ ist injektiv, also auch surjektiv wegen $|\mathbb{K}| < \infty$.
3. Ist $char(\mathbb{K}) = p > 0$, so ist $\mathbb{K}(x) = \text{Quot } \mathbb{K}[x]$ nicht vollkommen.

Definition 2.71.
Sei $\mathbb{L}/\mathbb{K}$ eine algebraische Körpererweiterung.

(1) Sei $\alpha \in \mathbb{L}$. α heißt **separabel über** $\mathbb{K}$, wenn $\text{MinPol}(\alpha/\mathbb{K})$ separabel ist.

(2) Die Erweiterung $\mathbb{L}/\mathbb{K}$ heißt **separabel**, wenn jedes $\alpha \in \mathbb{L}$ separabel über $\mathbb{K}$ ist.

Korollar 2.72.
Ein Körper $\mathbb{K}$ ist genau dann vollkommen, wenn jede algebraische Erweiterung $\mathbb{L}/\mathbb{K}$ separabel ist.

Korollar 2.73.
Sei $\overline{\mathbb{K}}$ ein algebraischer Abschluss von $\mathbb{K}$, sie $\alpha \in \overline{\mathbb{K}}$. Sei $n := \deg(\alpha/\mathbb{K}) = [\mathbb{K}(\alpha) : \mathbb{K}]$ $(= \deg(MinPol))$. Dann sind äquivalent:

(i) α ist separabel;

(ii) α hat n verschiedene $\mathbb{K}$-Konjugierte in $\overline{\mathbb{K}}$;

(iii) $|\text{Hom}_{\mathbb{K}}(\mathbb{K}(\alpha), \overline{\mathbb{K}})| = n$.

Beweis:
$f := \text{MinPol}(\alpha/\mathbb{K})$. α separabel über $\mathbb{K} \Leftrightarrow f$ hat n verschiedene Nullstellen in $\mathbb{K}$. Diese sind die $\mathbb{K}$-Konjugierten von α in $\mathbb{K}$.

zu (iii):
$\mathbb{K}(\alpha) \dashrightarrow_{\varphi} \overline{\mathbb{K}} \hookleftarrow \mathbb{K} - - - \mathbb{K}(\alpha)$.

Nach 2.21 sind sie auch in Bijektion zu $\mathrm{Hom}_{\mathbb{K}}(\mathbb{K}(\alpha), \overline{\mathbb{K}})$.

□

e. Separable Körpererweiterungen, Satz vom primitiven Element

Definition 2.74.
Sei $\mathbb{L}/\mathbb{K}$ eine endliche Erweiterung. Man nennt $[\mathbb{L} : \mathbb{K}]_S := |\mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \overline{\mathbb{K}})|$ den **Separabilitätsgrad** von $\mathbb{L}/\mathbb{K}$.

Bemerkung 2.75.
Sei $\mathbb{L} = \mathbb{K}(\alpha)$ eine einfache Erweiterung. Dann sagt 2.73: $[\mathbb{K}(\alpha) : \mathbb{K}]_S \leq [\mathbb{K}(\alpha) : \mathbb{K}]$, mit Gleichheit genau dann, wenn α separabel /$\mathbb{K}$ ist.

Lemma 2.76.
Sei $\mathbb{L}/\mathbb{K}$ endlich, sei $\varphi : \mathbb{K} \to \Omega$ eine Einbettung mit Ω algebraisch abgeschlossen. Dann hat φ genau $[\mathbb{L} : \mathbb{K}]_S$ Fortsetzungen $\psi : \mathbb{L} \to \Omega$ (insbesondere hängt die Definition von $[\mathbb{L} : \mathbb{K}]_S$ nicht von der Wahl von $\overline{\mathbb{K}}$ ab).

Beweis:
Wir können annehmen: Ω ist algebraisch über $\varphi(\mathbb{K})$. Nach 2.42 gibt es einen Isomorphismus $\beta : \overline{\mathbb{K}} \to_{\cong} \Omega$ mit $\beta|_{\mathbb{K}} = \varphi$. Dann ist $\mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \overline{\mathbb{K}}) \to \{\psi : \mathbb{L} \to \Omega : \psi|_{\mathbb{K}} = \varphi\}$, $\Phi \mapsto \beta \cdot \Phi$ bijektiv, mit Umkehrabbildung $\psi \mapsto \beta^{-1} \cdot \psi$.
Also $[\mathbb{L} : \mathbb{K}]_S = |\{\psi : \mathbb{L} \to \Omega : \psi|_{\mathbb{K}} = \varphi\}|$.

□

Korollar 2.77.
Seien $\mathbb{K} \subset \mathbb{F} \subset \mathbb{L}$ endliche Erweiterungen: $[\mathbb{L} : \mathbb{K}]_S = [\mathbb{L} : \mathbb{F}]_S \cdot [\mathbb{F} : \mathbb{K}]_S$.

Beweis:
Es gibt $m := [\mathbb{F} : \mathbb{K}]_S$ $\mathbb{K}$-Einbettungen $\varphi_i : \mathbb{F} \to_{\mathbb{K}} \overline{\mathbb{K}}$ für $i = 1, \ldots, m$. Jedes φ_i hat genau $n := [\mathbb{L} : \mathbb{F}]_S$ Fortsetzungen ψ_{ij} für $j = 1, \ldots, n$ auf $\mathbb{L}$. Das gibt $m \cdot n = |\mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \overline{\mathbb{K}})| = [\mathbb{L} : \mathbb{K}]_S$.

□

Lemma 2.78.
Sei $\mathbb{L}/\mathbb{K}$ algebraisch, sei $\alpha \in \mathbb{L}$ separabel. Dann ist α auch separabel über jedem $\mathbb{F}$ mit $\mathbb{K} \subset \mathbb{F} \subset \mathbb{L}$.

Beweis:
Sei $f := \mathrm{MinPol}(\alpha/\mathbb{K})$, nach Voraussetzung ist f separabel. Sei $g := \mathrm{MinPol}(\alpha/\mathbb{F})$. Wegen $f(\alpha) = 0$, $f \in \mathbb{F}[t]$ folgt $g \mid f$. Damit ist auch g separabel.

□

Satz 2.79.
Sei $\mathbb{L}/\mathbb{K}$ *endlich. Dann ist* $[\mathbb{L} : \mathbb{K}]_S \leq [\mathbb{L} : \mathbb{K}]$, *und Gleichheit gilt genau dann, wenn* $\mathbb{L}/\mathbb{K}$ *separabel ist.*

Beweis:
$\mathbb{K} = \mathbb{K}_0 \subset \mathbb{K}(\alpha_1) \subset \mathbb{K}(\alpha_1, \alpha_2) \subset \ldots \subset \mathbb{K}(\alpha_1, \ldots, \alpha_n) = \mathbb{L}$, $\mathbb{K}_i = \mathbb{K}(\alpha_1, \ldots, \alpha_i)$ für $i = 0, \ldots, n$. Jeder Schritt $\mathbb{K}_{i-1} \subset \mathbb{K}_i = \mathbb{K}_{i-1}(\alpha_i)$ ist einfach.
Nach 2.75 folgt: $[\mathbb{K}_i : \mathbb{K}_{i-1}]_S \leq [\mathbb{K}_i : \mathbb{K}_{i-1}] \Rightarrow$ (weil beide multiplikativ sind) $[\mathbb{L} : \mathbb{K}]_S \leq [\mathbb{L} : \mathbb{K}]$.

Zweite Aussage:
Ist $[\mathbb{L} : \mathbb{K}]_S = [\mathbb{L} : \mathbb{K}]$, so ist auch $[\mathbb{F} : \mathbb{K}]_S = [\mathbb{F} : \mathbb{K}]$ für alle $\mathbb{K} \subset \mathbb{F} \subset \mathbb{L}$ (Multiplikativität + Ungleichung).
Sei $\alpha \in \mathbb{L}$, dann also $[\mathbb{K}(\alpha) : \mathbb{K}]_S = [\mathbb{K}(\alpha) : \mathbb{K}] \Rightarrow \alpha$ ist separabel (2.73, 2.75).

Umgekehrt sei $\mathbb{L}/\mathbb{K}$ separabel. Dann ist auch α_i über $\mathbb{K}_{i-1} = \mathbb{K}(\alpha_1, \ldots, \alpha_{i-1})$ separabel für $i = 1, \ldots, n$. $\Rightarrow$ wegen $\mathbb{K}_i = \mathbb{K}_{i-1}(\alpha_i)$ ist $[\mathbb{K}_i : \mathbb{K}_{i-1}]_S = [\mathbb{K}_i : \mathbb{K}_{i-1}]$ (2.73, 2.75) $\Rightarrow$ (Multiplikativität) $[\mathbb{L} : \mathbb{K}]_S = [\mathbb{L} : \mathbb{K}]$.

□

Korollar und Definition 2.80.
Sei $\mathbb{L}/\mathbb{K}$ *eine algebraische Erweiterung. Dann ist* $\mathbb{L}_S := \{\alpha \in \mathbb{L} : \alpha$ *ist separabel über* $\mathbb{K}\}$ *ein Zwischenkörper von* $\mathbb{L}/\mathbb{K}$, *genannt die* ***separable Hülle*** *von* $\mathbb{K}$ *in* $\mathbb{L}$.

Beweis:
Seien $\alpha, \beta \in \mathbb{L}_S : \mathbb{K} \subset \mathbb{K}(\alpha) \subset \mathbb{K}(\alpha, \beta)$. Wegen α separabel über $\mathbb{K}$ und β separabel über $\mathbb{K}$ ist $[\mathbb{K}(\alpha) : \mathbb{K}]_S = [\mathbb{K}(\alpha) : \mathbb{K}]$ und $[\mathbb{K}(\alpha), \beta : \mathbb{K}(\alpha)]_S = [\mathbb{K}(\alpha, \beta) : \mathbb{K}(\alpha)]$.
Multiplikativität: $[\mathbb{K}(\alpha, \beta) : \mathbb{K}]_S = [\mathbb{K}(\alpha, \beta) : \mathbb{K}]$.
Nach 2.79 ist also jedes Element von $\mathbb{K}(\alpha, \beta)$ separabel über $\mathbb{K}$.

□

Lemma 2.81.
Sei $char(\mathbb{K}) = p > 0$, *sei* $\mathbb{L}/\mathbb{K}$ *algebraisch.*
Für jedes $\alpha \in \mathbb{L}$ *gibt es ein* $r \geq 0$, *so dass* α^{p^r} *separabel über* $\mathbb{K}$ *ist.*

Beweis:
$f := \text{MinPol}(\alpha/\mathbb{K})$, irreduzibel. Sei $r := \max\{i \geq 0 : f \in \mathbb{K}[t^{p^i}]\}$.
Dann ist $f(t) = g(t^{p^r})$ mit $g \in \mathbb{K}[t]$ irreduzibel, und $g \notin \mathbb{K}[t^p]$, also g separabel. Es

ist $f(\alpha) = g(\alpha^{p^r}) = 0$, also ist α^{p^r} separabel über $\mathbb{K}$.

□

Definition 2.82.
Eine algebraische Erweiterung $\mathbb{L}/\mathbb{K}$ heißt **rein inseparabel**, wenn alle Elemente in $\mathbb{L} \setminus \mathbb{K}$ inseparabel (d.h. nicht separabel) über $\mathbb{K}$ sind.

Korollar 2.83.
Sei char$(\mathbb{K}) = p > 0$. *Dann:* $\mathbb{L}/\mathbb{K}$ *ist rein inseparabel* $\Leftrightarrow \ \forall\, \alpha \in \mathbb{L}\ \exists\, r \geq 0\ \alpha^{p^r} \in \mathbb{K}$.

Beweis:
$\mathbb{L}/\mathbb{K}$ rein inseparabel $\Rightarrow$ (nach 2.81) $\forall\, \alpha\ \exists\, r\ \alpha^{p^r} \in \mathbb{K}$.
Umgekehrt: sei $c := \alpha^{p^r} \in \mathbb{K}$, $r \geq 1$. $\Rightarrow \alpha$ ist eine Nullstelle von $t^{p^r} - c$, ein inseparables Polynom.

□

Satz 2.84.
$\mathbb{L}/\mathbb{K}$ *sei endlich. Dann* $\mathbb{L}/\mathbb{K}$ *rein inseparabel* $\Rightarrow [\mathbb{L} : \mathbb{K}]_S$.

Beweis:
Sei $[\mathbb{L} : \mathbb{K}]_S = 1$, sei $\alpha \in \mathbb{L} \setminus \mathbb{K}$. Es ist $[\mathbb{K}(\alpha) : \mathbb{K}]_S = 1 < [\mathbb{K}(\alpha) : \mathbb{K}] \Rightarrow \alpha$ ist inseparabel über $\mathbb{K}$. Also $\mathbb{L}/\mathbb{K}$ rein inseparabel.
Umgekehrt: sei $\mathbb{L}/\mathbb{K}$ rein inseparabel. Wir zeigen: es gibt nur eine Fortsetzung $\psi : \mathbb{L} \to_{\mathbb{K}} \overline{\mathbb{K}}$.
Sei $\alpha \in \mathbb{L}$, sei etwa $\alpha^{p^r} =: c \in \mathbb{K}$. $\Rightarrow \psi(\alpha^{p^r}) = \psi(\alpha)^{p^r} = c$.
Also muss $\psi(\alpha)$ eine p^r-te Wurzel von c in $\overline{\mathbb{K}}$ sein. Also gibt es nur eine solche $\Rightarrow$ $\psi(\alpha)$ ist eindeutig bestimmt $\Rightarrow$ ψ ist eindeutig bestimmt.

□

Korollar 2.85.
Sei $\mathbb{L}/\mathbb{K}$ *endlich, sei* $\mathbb{L}_S$ *die separable Hülle von* $\mathbb{K}$ *in* $\mathbb{L}$. *Dann ist* $[\mathbb{L} : \mathbb{K}]_S = [\mathbb{L}_S : \mathbb{K}]$. *Die Erweiterung* $\mathbb{L}/\mathbb{L}_S$ *ist rein inseparabel. Insbesondere ist* $[\mathbb{L} : \mathbb{K}]_S$ *ein Teiler von* $[\mathbb{L} : \mathbb{K}]$.

Beweis:
Ist *char*$(\mathbb{K}) = 0$: nichts zu zeigen.
Sei *char*$(\mathbb{K}) = p > 0$. Für jedes $\alpha \in \mathbb{L}$ gibt es nach 2.81 ein $r \geq 0$ mit $\alpha^{p^r} \in \mathbb{L}_S \Rightarrow$ (nach 2.83) $\mathbb{L}/\mathbb{L}_S$ ist rein inseparabel $\Rightarrow [\mathbb{L} : \mathbb{L}_S]_S = 1 \Rightarrow [\mathbb{L} : \mathbb{K}]_S = [\mathbb{L} : \mathbb{L}_S]_S \cdot \underbrace{[\mathbb{L}_S : \mathbb{K}]_S}_{1} =$

$[\mathbb{L}_S : \mathbb{K}]$.

□

Notation 2.86.
Sei $\mathbb{L}/\mathbb{K}$ eine feste Erweiterung, seien $\mathbb{L}_1, \mathbb{L}_2$ Zwischenkörper von $\mathbb{L}/\mathbb{K}$. Wir schreiben $\mathbb{L}_1\mathbb{L}_2$ für den von $\mathbb{L}_1$ und $\mathbb{L}_2$ erzeugten Teilkörper von $\mathbb{L}$.
Ist $\mathbb{L}/\mathbb{K}$ algebraisch, so ist $\mathbb{L}_1\mathbb{L}_2$ die Menge aller endlichen Summen $\sum_{i=1}^{r} \alpha_i\beta_i$ mit $\alpha_i \in \mathbb{L}_1, \beta_i \in \mathbb{L}_2$.

Satz 2.87.
Sei $\mathbb{E}/\mathbb{K}$ eine algebraische Erweiterung, seien $\mathbb{L}, \mathbb{M}$ Zwischenkörper von $\mathbb{E}/\mathbb{K}$.

(a) $\mathbb{E}/\mathbb{K}$ *ist separabel* $\Leftrightarrow$ $\mathbb{E}/\mathbb{L}$ *und* $\mathbb{L}/\mathbb{K}$ *sind separabel;*

(b) $\mathbb{L}\mathbb{M}/\mathbb{K}$ *ist separabel* $\Leftrightarrow$ $\mathbb{L}/\mathbb{K}$ *und* $\mathbb{M}/\mathbb{K}$ *sind separabel;*

(c) $\mathbb{L}/\mathbb{K}$ *ist separabel* $\Rightarrow$ $\mathbb{L}\mathbb{M}/\mathbb{M}$ *ist separabel.*

Beweis:
als Übung ...

□

Theorem 2.88 (Abel - Satz vom primitiven Element)**.**
Sei $\mathbb{L}/\mathbb{K}$ eine endliche Erweiterung, $\mathbb{L} = \mathbb{K}(\alpha_1, \ldots, \alpha_n)$; höchstens eines der α_i sei inseparabel über $\mathbb{K}$.
Dann hat $\mathbb{L}/\mathbb{K}$ ein primitives Element : $\exists\, \alpha \in \mathbb{L}\ \mathbb{L} = \mathbb{K}(\alpha)$.

Korollar 2.89.
Jede endliche separable Erweiterung hat ein separables Element.

Beweis: (von 2.88)
Ist $\mathbb{K}$ endlich ($\Rightarrow \mathbb{L}$ ist endlich), so ist $\mathbb{L}^*$ zyklisch $\Rightarrow$ nimm $\alpha :=$ Erzeuger von $\mathbb{L}^*$.
Sei also $|\mathbb{K}| = \infty$. Es genügt: $n = 2$.
Sei $\mathbb{L} = \mathbb{K}(\alpha, \eta)$, sei α separabel über $\mathbb{K}$. Sei $f(t) = \mathrm{MinPol}(\alpha/\mathbb{K})$, $g(t) = \mathrm{MinPol}(\beta/\mathbb{K})$.
Ansatz $\gamma = \beta + c \cdot \alpha$ mit $c \in \mathbb{K}$.
Seien $\alpha = \alpha_1, \ldots, \alpha_n$ die $\mathbb{K}$-Konjugierten von α in $\overline{\mathbb{K}}$,
seien $\beta = \beta_1, \ldots, \beta_n$ die $\mathbb{K}$-Konjugierten von β in $\overline{\mathbb{K}}$.
Es ist $f(t) = \prod_{i=1}^{n}(t - \alpha_i)$. Sei $c \in \mathbb{K}$ und $\gamma = \beta + c \cdot \alpha \Rightarrow \alpha$ ist Nullstelle von $f(t)$ und von $g(\gamma - ct) \in \mathbb{K}(\gamma)[t]$.
Angenommen, wir wissen, α ist die einzige gemeinsame Nullstelle dieser beiden Polynome. Dann ist der ggT von $g(t)$ und $g(\gamma - ct)$ (in $\mathbb{K}[t]$) gleich $t - \alpha$. Also auch in $\mathbb{K}(\gamma)[t] \Rightarrow \alpha \in \mathbb{K}(\gamma)$.

$\Rightarrow \beta = \gamma - c\alpha \in \mathbb{K}(\gamma) \Rightarrow \mathbb{L} = \mathbb{K}(\alpha, \beta) = \mathbb{K}(\gamma)$: fertig.

Bleibt zu zeigen: bei geeigneter Wahl von $c \in \mathbb{K}$ ist α die einzige gemeinsame Nullstelle von $f(t)$ und $g(\gamma - ct)$.
Ist auch $\alpha_i, i \geq 2$, eine gemeinsame Nullstelle, so $g(\gamma - ct) = 0 \Rightarrow \gamma - c\alpha_i = \beta_j$ für ein $j \in \{1, \ldots, n\}$.
$\Rightarrow$ solange $c \notin \left\{\frac{\beta_j - \beta}{\alpha - \alpha_i} : i = 2, \ldots, m; j = 1, \ldots, n\right\}$, können wir c nehmen.

□

Beispiel 2.90.
Sei $char(k) = p > 0$. Sei $\mathbb{K} := k(x, y)$. Sei $\mathbb{L} := \mathbb{K}(\sqrt[p]{x}, \sqrt[p]{y})$. Dann ist $[\mathbb{L} : \mathbb{K}] = p^2$.
Aber $\forall\ \alpha \in \mathbb{L}$ gilt $\alpha^p \in \mathbb{K}$, also $[\mathbb{K}(\alpha) : \mathbb{K}] \leq p$, also $\mathbb{K}(\alpha) \neq \mathbb{L}$.

f. Endliche Körper

Wir kennen: $\mathbb{F}_p = \mathbb{Z}/(p) = \mathbb{Z}/p\mathbb{Z}$ für p prim.

Satz 2.91.
Sei $\mathbb{F}$ ein endlicher Körper. Dann ist $char(\mathbb{F}) = p > 0$, und $|\mathbb{F}| = p^n$ für ein $n \in \mathbb{N}$.

Beweis:
$char(\mathbb{F}) = p > 0$. $[\mathbb{F} : \mathbb{F}_p] =: n \Rightarrow |\mathbb{F}| = p^n$.

□

Wir haben gesehen: jeder endliche Körper $\mathbb{F}$ ist vollkommen.
Sei $\varphi : \mathbb{F} \to \mathbb{F}, \varphi(x) := x^p$ ($p := char(\mathbb{F})$), dann ist $\varphi \in \mathrm{Aut}(\mathbb{F})$ („Frobenius").

2.92.
Sei $\mathbb{F}$ ein Körper mit p^n Elementen.
$\Rightarrow \mathbb{F}^*$ ist eine abelsche (zyklische) Gruppe von Ordnung $p^n - 1$. Insbesondere ist $\alpha^{p^n-1} = 1 \ \ \forall\, \alpha \in \mathbb{F}^*$.
$\Rightarrow \alpha^{p^n} = \alpha \ \forall\, \alpha \in \mathbb{F}$.
Es ist also $\mathbb{F} = \mathrm{Zfk}(t^{p^n} - t/\mathbb{F}_p)$. Somit ist $\mathbb{F}$ bis auf Isomorphie eindeutig bestimmt (Eindeutigkeit von Zfk, 2.29).

Umgekehrt sei p^n eine gegebene Primzahlpotenz, konstruiere einen Körper mit p^n Elementen:
sei $\mathbb{F} := \mathrm{Zfk}(t^{p^n} - t/\mathbb{F}_p)$. Sei $\mathbb{F}_0 := \{\alpha \in \mathbb{F} : \alpha^{p^n} = \alpha\}$.
Sei $f := tp^n - t$, dann ist $f' = -1 \Rightarrow \mathrm{ggT}(f, f') = 1$. Also ist f separabel $\Rightarrow |\mathbb{F}_0| = p^n$.
Zu zeigen ist noch, dass $\mathbb{F}_0$ ein Körper ist:
seien $\alpha, \beta \in \mathbb{F}_0$, so ist $(\alpha + \beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} = \alpha + \beta$; ebenso $(\alpha \cdot \beta)^{p^n} = \alpha^{p^n} \cdot \beta^{p^n} = \alpha \cdot \beta$.
$\Rightarrow \mathbb{F}_0$ ist ein Teilring, also ein Teilkörper von $\mathbb{F} \Rightarrow \mathbb{F} = \mathbb{F}_0$.

Theorem 2.93.
Zu jeder Primzahlpotenz $q = p^n$ gibt es bis auf Isomorphie genau einen Körper mit $|\mathbb{F}| = q$, nämlich $\mathbb{F} = Zfk(t^q - t/\mathbb{F}_p)$.
Es gilt $\alpha^q = \alpha$ für alle $\alpha \in \mathbb{F}$.

Definition 2.94.
Ist q eine Primzahlpotenz, so schreibt man $\mathbb{F}_q$ für „den" Körper mit q Elementen.
(manchmal auch als $GF(q)$ in der Literatur)

Vorsicht:
$\mathbb{F}_p = \mathbb{Z}/(p)$, aber $\mathbb{F}_{p^n} \ncong \mathbb{Z}/(p^n)$ für $n \geq 2$ (nicht nullteilerfrei).

Satz 2.95.
Sei $\mathbb{F}$ ein Körper, $|\mathbb{F}| = q = p^n$.
Zu jedem Teiler d von n gibt es einen und nur einen Teilkörper $\mathbb{E}$ von $\mathbb{F}$ mit $|\mathbb{E}| = p^d$. Das sind alle Teilkörper von $\mathbb{F}$.

Also: Teilkörper von $\mathbb{F}_{p^n} \leftrightarrow$ Teiler von n.

Beweis:
Sei $\mathbb{E} \subset \mathbb{F}$ ein Teilkörper, $[\mathbb{F} : \mathbb{E}] = m$, dann $q^n = |\mathbb{F}| = |\mathbb{E}|^m \Rightarrow |\mathbb{E}| = q^{n/m} \Rightarrow m \mid n$, also $|\mathbb{E}| = p^d$ für $d = \frac{n}{m} \mid n$.

Umgekehrt sei $d \mid n$. Sei $\mathbb{E} := \{\alpha \in \mathbb{F} : \alpha^{p^d} = \alpha\}$. Behaupte, $\mathbb{E}$ ist ein Teilkörper von $\mathbb{F}$ mit $|\mathbb{E}| = p^d$. Zu zeigen ist also: das Polynom $t^{p^d} - t$ zerfällt über $\mathbb{F} = \mathbb{F}_{p^n}$.

Ist $\alpha^{p^d} = \alpha \Rightarrow$ (mit $n = de$) $\alpha^{p^n} = \alpha^{p^{d \cdot e}} = \left(\ldots \underbrace{\left(\left(\alpha^{p^d} \right)^{p^d} \right) \ldots}_{e-mal} \right)^{p^d} = \alpha.$

$\Rightarrow \alpha \in \mathbb{F}$: ✓.

□

Korollar 2.96.
Genau dann ist $\mathbb{F}_{p^m}$ in $\mathbb{F}_{p^n}$ einbettbar, wenn $m \mid n$ ist.

Korollar 2.97.
Sei $\mathbb{F} = \mathbb{F}_q$. Zu jedem $d \in \mathbb{N}$ gibt es eine, und bis auf $\mathbb{F}$-Isomorphie nur eine, Erweiterung $\mathbb{E}$ von $\mathbb{F}$ mit $[\mathbb{E} : \mathbb{F}] = d$, nämlich $\mathbb{E} = Zfk(t^{q^d} - t/\mathbb{F})$.

Beweis:
Nach Korollar 2.96 gibt es eine Erweiterung $\mathbb{E}/\mathbb{F}$ vom Grad d; $\mathbb{E} \cong \mathbb{F}_{q^d}$, und jedes solche $\mathbb{E} = \mathrm{Zfk}(t^{q^d}/\mathbb{F})$; daher sind je zwei solche Erweiterungen über $\mathbb{F}$ isomorph.
□

Korollar 2.98.
Sei q eine Primzahlpotenz, sei $n \in \mathbb{N}$.
Dann ist $t^{q^n} - t$ das Produkt aller normierten irreduziblen Polynome $f \in \mathbb{F}_q[t]$ mit

$\deg(f) \mid n$.

Beweis:
Sei $\mathbb{F} := \mathbb{F}_q$, sei $\mathcal{I} := \{f \in \mathbb{F}[t] : f \text{ ist normiert, irreduzibel, } \deg(f) \mid n\}$.
Sei $g := \prod_{f \in \mathcal{I}} f$. Zeige: g und $t^{q^n} - t$ teilen sich gegenseitig ($\Rightarrow$ fertig).

Sei $\mathbb{E} := \mathbb{F}_{q^n}$, sei $\alpha \in \mathbb{E}$. Dann ist $\mathbb{F} \subset \mathbb{F}(\alpha) \subset \mathbb{E}$, also $d := \deg(\alpha/\mathbb{F}) \mid [\mathbb{E} : \mathbb{F}] = n$.
Also ist $\text{MinPol}(\alpha/\mathbb{F}) \in \mathcal{I} \Rightarrow g(\alpha) = 0$.
$t^{q^n} - t = \prod_{\alpha \in \mathbb{E}} (t - \alpha) \Rightarrow (t^{q^n} - t) \mid g(t)$.

Umgekehrt sei $f \in \mathcal{I}$. Dann ist $\mathbb{F}[t]/(f)$ eine Erweiterung von $\mathbb{F}$ vom Grad $d := \deg(f) \mid n$. Also existiert eine $\mathbb{F}$-Einbettung $\mathbb{F}[t]/(f) \hookrightarrow \mathbb{E} \Rightarrow \exists\ \alpha \in \mathbb{E}$ mit $f(\alpha) = 0$. $\Rightarrow (t - \alpha)$ ist ein gemeinsamer Teiler von $f(t)$ und $t^{q^n} - t$ (in $\mathbb{E}[t]$). Also haben sie auch einen gemeinsamen Teiler in $\mathbb{F}[t]$. Da $f(t)$ irreduzibel in $\mathbb{F}[t]$ ist, folgt $f(t) \mid t^{q^n} - t$.

Also $g(t) = t^{q^n} - t$.

□

Theorem 2.99.
Sei $\mathbb{E}/\mathbb{F}$ eine Erweiterung endlicher Körper, sei $f(t) \in \mathbb{F}[t]$ irreduzibel. Hat $f(t)$ eine Nullstelle in $\mathbb{E}$, so zerfällt $f(t)$ schon über $\mathbb{E}$.

***Anders:** Der Wurzelkörper von f über $\mathbb{F}$ ist schon der Zerfällungskörper.*

Beweis:
Seien $\alpha_1, \ldots, \alpha_n$ ($n = \deg(f)$) die Nullstellen von $f(t)$ in $\mathbb{L} := \text{Zfk}(f/\mathbb{F})$.
Für jedes $i = 1, \ldots, n$ ist $[\mathbb{F}(\alpha_i) : \mathbb{F}] = n$
$\mathbb{L}$ - $\mathbb{F}(\alpha_1) = \ldots = \mathbb{F}(\alpha_1)$ - $\mathbb{F}$
Nach 2.95 ist also $\mathbb{F}(\alpha_1) = \ldots = \mathbb{F}(\alpha_1)$. Nach Voraussetzung liegt ein α_i in $\mathbb{E}$, also alle.

□

Satz 2.100.
Sei $\mathbb{E}/\mathbb{F}$ eine Erweiterung endlicher Körper, $[\mathbb{E} : \mathbb{F}] = n$. Dann ist $\sigma : \mathbb{E} \to \mathbb{E}$, $\sigma(x) := x^q$ mit $q := |\mathbb{F}|$ ein $\mathbb{F}$-Automorphismus von $\mathbb{E}$ von der genauen Ordnung n.

Beweis:
σ ist ein Homomorphismus und ist injektiv, also wegen $|\mathbb{E}| < \infty$ bijektiv, und

$\sigma|_{\mathbb{F}} = \mathrm{id}_{\mathbb{F}}$ ist klar.
Für alle $x \in \mathbb{E}$ ist $x = x^{q^n} = \underbrace{\sigma \circ \ldots \circ \sigma}_{n-mal}(x) = \sigma^n(x)$, also $\sigma^n = \mathrm{id}_{\mathbb{E}}$. Ist $d \mid n$, $d < n$, so gibt es ein $x \in \mathbb{E} = \mathbb{F}_{q^n}$ mit $x^{q^d} \neq x$.
($x \in \mathbb{F}_{q^n} = \mathbb{E}$ - $x \notin \mathbb{F}_{q^d}$ - $\mathbb{F}_q = \mathbb{F}$)

$\Rightarrow$ für dieses x ist $\sigma^d(x) \neq x$, also ist $\sigma^d \neq \mathrm{id}_{\mathbb{E}}$.

□

Korollar 2.101.
Sei $|\mathbb{F}| = q$, sei $f \in \mathbb{F}[t]$ irreduzibel vom Grad n. Ist $\alpha \in \mathbb{F}$ eine Nullstelle von f, so ist $f(t) = (t-\alpha)(t-\alpha^q)(t-\alpha^{q^2}) \cdot \ldots \cdot (t-\alpha^{q^{n-1}}) = \prod_{j=0}^{n-1} \left(t - \alpha^{q^j}\right)$.
Also sind $\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}$ genau die verschiedenen Nullstellen von $f(t)$.

Beweis:
$\mathbb{E} := \mathbb{F}(\alpha), [\mathbb{E} : \mathbb{F}] = n$. Jeder $\mathbb{F}$-Automorphismus (insbesondere σ) bildet α auf eine Nullstelle von $f(t)$ in $\mathbb{E}$ ab.
Also sind $\alpha, \sigma(\alpha), \sigma^2(\alpha), \ldots, \sigma^{n-1}(\alpha)$ Nullstellen von $f(t)$. Wegen $\mathbb{E} = \mathbb{F}(\alpha)$ und $\mathrm{ord}(\sigma) = n$ sind diese alle verschieden $\Rightarrow$ Behauptung.

□

Bemerkung 2.102.
Um den Körper $\mathbb{F}_{p^n}$ explizit zu beschreiben und dann zu rechnen verschafft man sich ein irreduzibles $f(t) \in \mathbb{F}_p[t]$ vom Grad n; dann ist $\mathbb{F}_{p^n} \cong \mathbb{F}_p[t]/(f)$.

Beispiele 2.103.
$p = 2, n = 2$: $t^2, t^2+1, t^2+t, t^2+t+1$.
$f(t) = t^2 + t + 1$ ist irreduzibel über $\mathbb{F}_2$.
Also ist $\mathbb{F}_4 \cong \mathbb{F}_2[t]/(f(t)) = \mathbb{F}_2(\alpha)$ mit $\alpha^2 = \alpha + 1$ (d.h. $f(\alpha) = 0$).
$\mathbb{F}_4 = \{0, 1, \alpha, \alpha+1\}$.
Es ist $f(t) = (t-\alpha)(t-\alpha^2) = (t-\alpha)(t-(\alpha+1))$, vgl. 2.101.

$p = 2, n = 3$: die irreduziblen kubischen Polynome über $\mathbb{F}_2$ sind $t^3 + t + 1$ und $t^3 + t^2 + 1$.
Benutze $f(t) = t^3 + t + 1$, das ergibt $\mathbb{F}_8 = \mathbb{F}_2(\beta)$ mit $\beta^3 = \beta + 1$:
$\mathbb{F}_8 = \{0, 1, \beta, \beta+1, \beta^2, \beta^2+1, \beta^2+\beta, \beta^2+\beta+1\}$.
$f(t) = (t-\beta)(t-\beta^2)(t-\beta^4)$.

g. Konstruktion mit Zirkel und Lineal

Lit: R. Hartshorne, Geometry: Euklid and Beyond.

Definition 2.104.
Gegeben sei eine Menge $\mathcal{P} \subset \mathbb{R}^2$ von Punkten, $|\mathcal{P}| \geq 2$. Wir erlauben die folgenden Konstruktionsschritte:

(1) Für je zwei schon kontruierte Punkte $P \neq Q$: Konstruktion der Geraden durch P und Q.

(2) Konstruktion des Kreises mit Mittelpunkt P durch Q.

(3) Konstruktion neuer Punkte durch Schneiden von bereits konstruierten Geraden oder Kreisen.

Durch (1) - (3) vergrößern wir die Menge $\mathcal{P}$.
Frage: Welche Punkte der Ebene sind aus $\mathcal{P}$ in endlich vielen Schritten (1) - (3) konstruierbar?

2.105.
Mit Descartes algebraisieren wir die Fragen wie folgt: wir identifizieren $\mathbb{R}^2$ mit $\mathbb{C}$ und normieren das Koordinatensystem so, dass $\{0, 1\} \subset \mathcal{P}$ gilt.
Sei $\Omega := \Omega(\mathcal{P})$ die Menge der aus $\mathcal{P}$ in endlich vielen Schritten (1) - (3) konstruierbaren Punkte, $\Omega \subset \mathbb{C}$.

Konstruktion 2.106.
Zu einer Geraden G und einem Punkt P: Konstruktion der Senkrechten zu G durch P.

1. Fall $P \notin G$:

- Wähle einen (konstruierbaren) Punkt $Q \in G$
- $\{Q, Q'\} := G \cap K_Q(P)$
- $\{P, P'\} := K_P(Q) \cap K_P(Q')$
- $\overline{PP'}$ ist die Senkrechte.

2. Fall $P \in G$:

- Wähle einen (konstruierbaren Punkt $P \neq Q \in G$

- $\{Q, Q'\} := G \cap K_Q(P)$
- $\{P', P''\} = K_Q(Q') \cap K_{Q'}(Q)$
- $\overline{PP'}$ ist die Senkrechte.

Konstruktion 2.107.
Konstruktion der zu Gerade G parallelen Geraden durch einen gegebenen Punkt P:
zweimal Senkrechte.

Konstruktion 2.108.
Zu einem Punt P auf einer Geraden G und Punkten Q, Q: Abtragen der Strecke $[QQ']$ auf G von P aus.

1. Fall $Q \notin G \vee Q' \notin G$:

- Gerade G' durch Q und P
- Parallele zu G' durch Q'
- Gerade G'' durch Q und Q'
- Parallele zu G'' durch P
- Schnittpunkt der Parallelen $\Rightarrow P'$
- Kreis um P durch P' schneidet G in $P'' \Rightarrow$ fertig.

2. Fall $Q, Q' \in G$:

- Wähle Hilfsgerade $G' \neq G$ durch P
- Trage $[Q, Q']$ erst auf G' von P aus ab
- Kreis um P schneidet G im gewünschten Punkt

Lemma 2.109.
Aus $w, z \in \mathbb{C}$ kann man $w \pm z$ konstruieren.

Beweis:
klar aus Parallelogramm mit Ecken $0, w, z, w + z$.

□

Lemma 2.110.
$z \in \mathbb{C}$ ist genau dann konstruierbar, wenn $Re(z), Im(z)$ konstruierbar sind.

BEWEIS: klar aus Senkrechten durch $\overline{0, Re(z)}, \overline{0, Im(z)}$.

□

LEMMA 2.111.
Aus $w, z \in \mathbb{C}$ kann man wz und $\frac{1}{z}$ (für $z \neq 0$) konstruieren.

BEWEIS:
Wegen 2.108 und 2.109 genügt für Produkte:
aus reellen Zahlen $x, y > 0$ können wir $x \cdot y$ konstruieren.

→ Strahlensatz ...

Für $z \neq 0, z \in \mathbb{C}$ genügt es zur Konstruktion von $\frac{1}{z}$ zu zeigen: zu jeder reellen Zahl $x > 0$ können wir $\frac{1}{x}$ konstruieren.

→ wieder Strahlensatz ...

□

LEMMA 2.112.
Man kann Quadratwurzeln konstruieren: zu $z \in \mathbb{C}$ kann man $\pm\sqrt{z}$ konstruieren.

BEWEIS:
Es genügt, Winkel zu halbieren und für reelle $x > 0$ die Wurzel $\sqrt{x}$ zu konstruieren.

Winkelhalbierende wie in der Schule.

Sei $x > 0$ eine reelle Zahl. Konstruiere $\sqrt{x}$:

- errichte den Kreis durch -1 und x mit Mittelpunkt $\frac{x-1}{2}$
- der Kreis schneidet imaginäre Achse in iz
- Dreieck mit Eckpunkten -1, x und iz ist nach Satz von Thales rechtwinklig
- Pythagoras: $(x+1)^2 = 1 + z^2 + x^2 + z^2 \Leftrightarrow 2x = 2z^2 \Rightarrow z = \sqrt{x}$.

□

Definition 2.113.
Ein Körper $\mathbb{K}$ heißt **quadratisch abgeschlossen**, wenn er keine quadratische Körpererweiterung hat.

Wir wissen: Ist *char* $\neq 2$, so ist das äquivalent dazu, dass $\mathbb{K}^* = \mathbb{K}^{*2}$, also jedes Element aus $\mathbb{K}$ ein Quadrat ist.

Die Menge $\Omega := \Omega(\mathcal{P})$ der aus $\mathcal{P}$ konstruierbaren Punkte in $\mathbb{C}$ ist also ein quadratische abgeschlossener Teilkörper von $\mathbb{C}$. Setze $\mathbb{K}_0 := \mathbb{Q}(\mathcal{P})$ (der von der von $\mathcal{P}$ in $\mathbb{C}$ erzeugte Körper)

Satz 2.114.
Ω ist der „quadratische Abschluss" von $\mathbb{K}_0$ in $\mathbb{C}$, d.h.: eine komplexe Zahl $\alpha \in \mathbb{C}$ liegt genau dann in Ω, wenn es eine Kette $\mathbb{K}_0 \subset \mathbb{K}_1 \subset \ldots \subset \mathbb{K}_n \subset \mathbb{C}$ von Körpern gibt, so dass $[\mathbb{K}_i : \mathbb{K}_{i-1}] = 2$ für $i = 1, \ldots, n$ ist, und $\alpha \in \mathbb{K}_n$ ist.

Beweis:
Sei $\Omega' = \{\alpha \in \mathbb{C} :$ es gibt $\mathbb{K}_0 \subset \mathbb{K}_1 \subset \ldots \subset \mathbb{K}_n$ wie oben mit $\alpha \in \mathbb{K}_n\}$ Seien $\alpha, \beta \in \Omega'$, seien $\mathbb{K}_0 \subset \mathbb{K}_1 \subset \ldots \subset \mathbb{K}_m \ni \alpha$, $\mathbb{K}_0 \subset \mathbb{L}_1 \subset \ldots \subset \mathbb{L}_n \ni \beta$ wie oben.
$\mathbb{K}_0 \subset \mathbb{K}_1 \subset \ldots \subset \mathbb{K}_m \subset K_m\mathbb{L}_1 \subset \ldots \subset \mathbb{K}_m\mathbb{L}_n = \Omega' \ni \{\alpha, \beta\}$ mit $[\mathbb{K}_m\mathbb{L}_i : \mathbb{K}_m\mathbb{L}i - 1] \leq 2$ (also quadratische Ergänzung oder Gleichheit).
$\Rightarrow \alpha, \beta \in \Omega'$; nach Konstruktion ist Ω' quadratisch abgeschlossen, also $\Omega' \subset \Omega$.

Umgekehrt müssen wir zeigen, dass die Konstruktionsschritte (1) - (3) nicht aus Ω' hinausführen:
sind $z_1, z_2 \in \mathbb{R}^2$ Punkte mit Koordinaten in einem Teilkörper $\mathbb{K}$ von $\mathbb{R}$, so hat die Verbindungsgerade durch die beiden Punkte wieder Koordinaten in $\mathbb{K}$, ebenso der Kreis um z_1 durch z_2.
$\Rightarrow$ Schnitt von zwei Geraden ergibt Punkt in $\mathbb{K}$;
Schnitt Gerade $\cap$ Kreis ergibt quadratische Erweiterung von $\mathbb{K}$;
Schnitt Kreis$_1 \cap$ Kreis$_2$: subtrahiere Gleichungen $\Rightarrow$ Gleichung vom Grad 2 $\Rightarrow$ quadratische Erweiterung.

□

Korollar 2.115.
Ist $\alpha \in \mathbb{C}$, so ist α höchstens dann aus $\mathcal{P}$ konstruierbar, wenn $[K_0(\alpha) : \mathbb{K}_0]$ eine 2er-Potenz ist.

2.116.
Die klassischen Konstruktionsprobleme der Antike:

(1) Dreiteilung eines gegebenen Winkels;

(2) „Delphisches Problem“ Verdopplung eines Würfels;

(3) Quadratur des Kreises: verwandle einen Kreis in ein Quadrat mit gleichem Flächeninhalt.

Alle drei sind mit Zirkel und Lineal unlösbar:

1. Sei $\alpha \in e^{i\Theta}$. Genau dann lässt sich Θ in 3 Teile teilen, wenn $e^{i\Theta/3} = \sqrt[3]{\alpha}$ aus $\mathbb{Q}(\alpha)$ konstruierbar ist. Das kann nur gehen, wenn $[\mathbb{Q}(\sqrt[3]{\alpha}) : \mathbb{Q}(\alpha)]$ eine 2er-Potenz ist, also nur dann, wenn $\sqrt[3]{\alpha} \in \mathbb{Q}(\alpha)$.
   Ist $\alpha/\mathbb{Q}$ transzendent, so ist $t^3 - \alpha$ irreduzibel über $\mathbb{Q}(\alpha)$, also der Winkel nicht drittelbar. Aber auch im Allgemeinen für $\alpha/\mathbb{Q}$ algebraisch nicht drittelbar:
   $\alpha = \cos(\Theta) + i\sin(\Theta)$, also $\sqrt[3]{\alpha} = \cos\left(\frac{\Theta}{3}\right) + i\sin\left(\frac{\Theta}{3}\right)$
   Äquivalent ist also die Konstruktion von $\cos\left(\frac{\Theta}{3}\right)$ aus $\mathbb{Q}(\cos(\Theta))$:
   $(\cos\eta + i\sin\beta)^3 \rightsquigarrow \cos(3\beta) = 4\cos^3(\beta) - 3\cos(\beta)$.
   Schreibe $c := \cos(\Theta)$, dann ist $\cos\left(\frac{\Theta}{3}\right)$ eine Nullstelle von $4t^3 - 3t - c = 0$.
   Substitution $u = 2t \Rightarrow u^3 - 3u - 2c = 0$.
   Diese Gleichung ist über $\alpha(c)$ im Allgemeinen irreduzibel, z.B. $\Theta = 120° = \frac{2\pi}{3}$:
   $\cos(\Theta) = -\frac{1}{2}$
   $u^3 - 3u + 1 = 0$ über $\mathbb{Q}$.
2. Unlösbar, da $t^3 - 2 = 0$ irreduzibel über $\mathbb{Q}$, also $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.
3. Konstruktion von $\sqrt{\pi}$ bzw. π aus $\mathbb{Q}$: ist unmöglich, da π nach Lindemann (1882) transzendent ist.

Konstruktion 2.117 (Regelmäßiges n-Eck)**.**
Für welche n ist dieses konstruierbar?
Spezialfall $n = p$ eine Primzahl: sei $\zeta = \zeta_p = e^{2\pi i/p}$.
$[\mathbb{Q}(\zeta) : \mathbb{Q}] = p - 1$. Ist also p nicht von der Form $p = 2^m + 1$, so ist das regelmäßige p-Eck nicht konstruierbar.
Regelmäßiges 5-Eck:

- Gerade durch $\frac{i}{2}$
- Kreis um $\frac{i}{2}$ durch i Gerade zwischen 1 und $\frac{i}{2}$
- Kreis um 1 durch Schnittpunkt schneidet Einheitskreis in ζ; ζ ist primitive 10-te Einheitswurzel.

3. Gruppentheorie

a. Grundbegriffe: Untergruppen, Normalteiler, Automorphismen, Zentrum

Gruppe $G = (G, \cdot)$, mit neutralem Element e.
$ex = x = xe \quad \forall\, x \in G$.

Beispiele:

(1) Matrixgruppen $GL_n(\mathbb{K})$ ($\mathbb{K}$ ein Körper) und ihre Untergruppen;

(2) Permutationsgruppen: die symmetrische Gruppe S_1 aller Bijektionen $\{1, \dots, n\} \to \{1, \dots, n\}$ und ihre Untergruppen.

3.1.
Zu jeder Untergruppe $H \leq G$ bilden wir die Nebenklassenmengen $G/H = \{gH : g \in G\}$, wobei $gH := \{gh : h \in H\}$ und $H\backslash G = \{Hg : g \in \Gamma\}$, wobei $Hg := \{hg : h \in H\}$.
Beide sind gleichmächtig: $G/H \to H \setminus G, xH \mapsto Hx^{-1}$ ist eine Bijektion. Man nennt $[G : H] := |G/H| = |H \setminus G|$ den **Index von** H **in** G.
Insbesondere $[G : \{e\}] = |G|$.

Lemma 3.2.
Seien $K \leq H \leq G$ Untergruppen. Dann gilt $[G : K] = [G : H] \cdot [H : K]$.

Beweis:
Sei $(x_i)_{i\in I}$ ein Vertretersystem für G/H, d.h. es sei $G = \bigcup_{i\in I} x_i H$ und $x_i H \cap x_j H = \emptyset$ für alle $i \neq j$.
Sei $(y_j)_{j\in J}$ ein Vertretersystem für H/K, also $H = \bigcup_{j\in J} y_j K$ und $y_j K \cap y_k K = \emptyset$ für alle $j \neq k$.
Also $|I| = [G : H], |J| = [H : K]$. Dann ist $(x_i y_j)_{(i,j)\in I\times J}$ ein Vertretersystem für G/K:
$\forall\, g \in G\ \exists\, (i, j)\ gK = x_i y_j K$, denn $\exists\, i \in I\ gH = x_i H$, etwa $g = x_i h$ mit $h \in H$; $\exists\, j \in J\ h = y_j K$. $\Rightarrow g = x_i y_j K$.

□

Bemerkung: Dieses Lemma hatten wir im Spezialfall $K = \{e\}$ schon gesehen:
$|G| = |H| \cdot [G : H]$ (Satz von Lagrange).

3.3.
Die Untergruppe $H \leq G$ heißt ein **Normalteiler** von G, in Zeichen $H \trianglelefteq G$, wenn gilt $\forall\, g \in G\ \forall\, h \in H$ gilt $ghg^{-1} \in H$ oder äquivalent: $\forall\, g \in G\ gH = Hg$.

Ist $H \trianglelefteq G$, so wird die Menge $G/H = H \setminus G$ zu einer Gruppe durch $(g_1H) \cdot (g_2H) := (g_1g_2)H$.
Die Abbildung $\pi : G \to G/H$, $\pi(g) = gH$ ist ein surjektiver Gruppenhomomorphismus. Homomorphiesatz:
Ist $\varphi : G_1 \to G_2$ ein surjektiver Gruppenhomomorphismus, so ist $\ker(\varphi) \trianglelefteq G_1$, und $\overline{\varphi} : G_1/\ker(\varphi) \to_{\cong} G_2$, $g \cdot \ker(\varphi) \mapsto \varphi(g)$ ist ein Isomorphismus.

Korollar 3.4.
Sei $N \trianglelefteq G$. Die Untergruppen von G/N sind genau die H/N, wobei $H \leq G$ mit $N \leq H$ ist. Dabei gilt:
$H/N \trianglelefteq G/N \Leftrightarrow H \trianglelefteq G$, und dann ist
$(G/N)/(H/N) \cong G/H$.

Beweis:
Die erste Aussage ist klar.
Normalität: sei $N \leq H \leq G$.
$H/N \trianglelefteq G/N \Leftrightarrow\ \forall\, g \in G\ \forall\, h \in H$: $(gN)\cdot(hN)\cdot(gN)^{-1} = (ghg^{-1})N \in H/N \Leftrightarrow ghg^{-1} \in H$.
Also $H/N \trianglelefteq G/N \Leftrightarrow H \trianglelefteq G$.

Für die letzte Aussage sei $H \trianglelefteq G$, $N \leq H$.
Betrachte den Homomorphismus $G/N \to G/H$, $gN \mapsto gH$. Dieser ist surjektiv und hat den Kern $\{gN \in G/N : gH = eH = H\} = \{gN \in G/N : g \in H\} = H/N$.
Aus dem Homomorphiesatz folgt: $G/H \cong (G/N)/(H/N)$.

□

Satz 3.5.
Sei $H \leq G, N \trianglelefteq G$.

(a) $HN = NH(:= \{hn : h \in H, n \in N\})$ ist eine Untergruppe von G;

(b) $H \cap N \trianglelefteq H$, und $H/(H \cap N) \cong (HN)/N$;

(c) $H \trianglelefteq G \Rightarrow HN \trianglelefteq G$, $H \cap N \trianglelefteq G$.

Beweis:

(a) $HN \neq \emptyset$. $(hn) \cdot (h'n') = \underbrace{\underbrace{hh'}_{\in H} \cdot \underbrace{(h')^{-1}nh'}_{\in N} n'}_{\in N} \in HN$.

$(hn)^{-1} = n^{-1}h^{-1} = h^{-1} \cdot \underbrace{hn^{-1}h^{-1}}_{\in N} \in HN$.

(b) Sei $n \in H \cap N, h \in H \Rightarrow hnh^{-1} \in H \cap N$.
$\Rightarrow H \cap N \trianglelefteq H$. Betrachte den Homomorphismus $H \to (HN)/N$, $h \mapsto hN \in (HN)/N$. Dieser ist surjektiv: $(hn)N = hN$ und hat als Kern genau $\{h \in H : hN = eN = N\} = \{h \in H : h \in N\} = H \cap N$.
Aus dem Homomorphiesatz folgt die $H/H \cap N \cong (HN)/N$.

(c) Seien $H \trianglelefteq G, N \trianglelefteq G$.
Produkt: $g(HN) = (gH)N = (Hg)N = H(gN) = HNg \Rightarrow HN \trianglelefteq G$.
Durchschnitt: $x \in H \cap N, g \in G \Rightarrow gxg^{-1} \in H \cap N \Rightarrow H \cap N \trianglelefteq G$.

□

Beispiel 3.6.
Sind $H_1, H_2 \leq G$ nicht normal, so gilt im Allgemeinen $H_1H_2 \neq H_2H_1$, ist also im Allgemeinen keine Untergruppe.
Beispiel: $G = S_3$, $H_1 = \langle(12)\rangle$, $H_2 = \langle(13)\rangle$.

Lemma 3.7.
Ist G eine Gruppe, $H \leq G$ mit $[G : H] = 2$, so ist $H \trianglelefteq G$.

Beweis:
Übungsaufgabe auf Blatt 9.

□

Lemma 3.8.
Ist G eine Gruppe mit $x^2 = e \; \forall \; x \in G$, so ist G abelsch.

Beweis:
$xyxy = (xy)^2 = e = x^2y^2 = xxyy$.
Kürzen $\Rightarrow yx = xy$.

□

Bemerkung 3.9.
$\trianglelefteq$ ist im Allgemeinen *nicht* transitiv: aus $H \trianglelefteq N$ und $N \trianglelefteq G$ folgt im Allgemeinen

nicht $H \trianglelefteq G$.
Beispiel: $G := \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a, b \in \mathbb{R}, a \neq 0 \right\} \leq GL_2(\mathbb{R})$, $N := \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{R} \right\} \trianglelefteq G$.
$N \cong \mathbb{R}$ ist abelsch. Es ist $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & ac \\ 0 & 1 \end{pmatrix}$.
N hat viele Untergruppen $\{e\} \neq H \trianglelefteq \neq N$, z.B. $H = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{Z} \right\}$. Diese sind alle nicht normal in G.

3.10.
Sei G eine Gruppe, $X \subset G$ eine Teilmenge. Dann bezeichnet $\langle X \rangle := \bigcap_{H \leq G, X \subset H} H$ die von X erzeugte Untergruppe von G.
Speziell: ist $X = \{x_1, \ldots, x_n\}$, so schreibt man $\langle x_1, \ldots, x_n \rangle := \langle X \rangle$.

Sei $X = \{x_1, \ldots, x_n\}$. Dann besteht $\langle x_1, \ldots, x_n \rangle$ aus allen „Wörter“ in $x_1^{\pm 1}, \ldots, x_n^{\pm 1}$, also allen endlichen Produkten $x_{i_1}^{e_1} x_{i_2}^{e_2} \cdot \ldots \cdot x_{i_r}^{e_r}$, $e_\nu \in \mathbb{Z}, r \geq 0, i_\nu \in \{1, \ldots, n\}$.
Die Gruppe G heißt zyklisch, wenn $\exists\, g \in G$ mit $G = \langle g \rangle$.

Wir schreiben in Zukunft $C_n := \{z \in \mathbb{C}^* : z^n = 1\}$ für „die“ zyklische Gruppe von Ordnung n, multiplikativ geschrieben ($C_n \cong \mathbb{Z}/n$).

3.11.
Die Menge $\mathrm{Aut}(G)$ aller Automorphismen von G ist eine Gruppe unter Komposition. $(\varphi \circ \psi)(g) = \varphi(\psi(g))$.

Für jedes $g \in G$ ist $\mathrm{int}_g : G \to G$, $\mathrm{int}_g(x) := gxg^{-1}$ ein Automorphismus von G:
$\mathrm{int}_g(xy) = g(xy)g^{-1} = gxg^{-1} \cdot gyg^{-1} = \mathrm{int}_g(x)\mathrm{int}_g(y)$.
$\mathrm{int}_{g^{-1}} \circ \mathrm{int}_g = id = \mathrm{int}_g \circ \mathrm{int}_{g^{-1}}$. Allgemeiner gilt:
$(\mathrm{int}_g \circ \mathrm{int}_h)(x) = g(hxh^{-1})g^{-1} = (gh)x(gh)^{-1} = \mathrm{int}_{gh}$.

Wir haben also gezeigt:

Satz 3.12.
Die Abbildung $G \to \mathrm{Aut}(G)$, $g \mapsto int_g$, ist ein Gruppenhomomorphismus.

Definition 3.13.
Automorphismen der Form $\mathrm{int}_g : x \mapsto gxg^{-1}$ (mit $g \in G$) von G heißen die **inneren**

Automorphismen von G. Man nennt int_g auch die **Konjugation** mit g.

Zwei Elemente $x, y \in G$ (oder: zwei Untergruppen $H, K \leq G$) heißen **zueinander konjugiert**, wenn es ein $g \in G$ gibt mit $y = gxg^{-1}$ (bzw. $K = gHg^{-1}$).

Definition 3.14.
Der Kern des Homomorphismus $\mathrm{int} : G \to \mathrm{Aut}(G)$ ist $Z(G) := \{g \in G : \forall\, x \in G\ gx = xg\}$.
Man nennt $Z(G)$ das **Zentrum** von G.

Bemerkungen und Beispiele 3.15.

1. $Z(G)$ ist ein abelscher Normalteiler von G.
   Dasselbe gilt für jede Untergruppe von $Z(G)$.

2. Ist G abelsch, so ist die Identität der einzige innere Automorphismus und $Z(G) = G$.
   Jedes Element ist zu sich selbst konjugiert.

3. Die Automorphismen der zyklischen Gruppen haben wir schon bestimmt: $\mathrm{Aut}(\mathbb{Z}) = \{\pm id\}$; $\mathrm{Aut}(C_n) = (\mathbb{Z}/n)^*$ (siehe Aufgabe 17).
   $(C_n = \langle z\rangle;\ k \in (\mathbb{Z}/n)^* \rightsquigarrow \varphi_k : z^i \mapsto z^{ki})$

4. Sei $\mathbb{K}$ ein Körper, betrachte $GL_n(\mathbb{K})$.
   Es ist $Z(GL_n(\mathbb{K})) = \mathbb{K}^* I = \{cI : c \in \mathbb{K}^*\}$ (siehe LA I, Blatt 5; Idee: sei $S \in Z$, vergleiche $i \neq j$ $S(I + E_{ij})$ und $(I + E_{ij})S$).
   Zwei Matrizen $S, T \in GL_n(\mathbb{K})$ sind genau dann zueinander konjugiert, wenn sie ähnlich sind, also $S \approx T$: $[\ \exists\, U \in GL_n(\mathbb{K})\ T = USU^{-1}]$.

5. Die Konjugiertheit von Elementen in G ist eine Äquivalenzrelation. Man nennt daher die Menge $\{gx^{-1}g : g \in G\}$ (der zu x konjugierten Elemente) die Konjugationsklassen von $x \in G$.

b. Direkte und semidirekte Produkte

3.16 (Direkte Produkte von Gruppen)**.**
Seien $G_1, \ldots, G_n$ Gruppen. Dann ist $G_1 \times \ldots \times G_n$ gemäß $(x_1, \ldots, x_n) \cdot (y_1, \ldots, y_n) := (x_1 y_2, \ldots, x_n y_n)$ für $x_i, y_i \in G_i$ und $i = 1, \ldots, n$ selbst eine Gruppe, genannt das direkte Produkt von $G_1, \ldots, G_n$. Neutrales Element ist $(e, \ldots, e)$. Die Abbildungen $\pi_i : G_1 \times \ldots \times G_n \to G_i$, $\pi_i(x_1, \ldots, x_n) := x_i$ für $i = 1, \ldots, n$ sind Homomorphismen.

Interne Charakterisierung:
Ist G eine Gruppe und sind $G_1, \ldots, G_n \leq G$ Untergruppen, so nennt man G das (**interne**) **direkte Produkt** von $G_1, \ldots, G_n$, wenn die Abbildung $G_1 \times \ldots \times G_n \to G$, $(g_1, \ldots, g_n) \mapsto g_1 \cdot \ldots \cdot g_n$ ein Gruppenisomorphismus ist. Man schreibt dann einfach $G = G_1 \times \ldots \times G_n$.

Hier die Charakterisierung für $n = 2$:

Satz 3.17.
Sei G eine Gruppe, seien $H, K \leq G$. Genau dann ist G das interne direkte Produkt von H und K, wenn gelten:

(1) $H \trianglelefteq G, K \trianglelefteq G$;

(2) $HK = G$;

(3) $H \cap K = \{e\}$.

Beweis:

„$\Rightarrow$“ ist klar: ist $\varphi : H \times K \to G$, $(h, k) \to hk$ ein Isomorphismus, so identifizieren sich H bzw. K mit $H \times \{e\}$ bzw. $\{e\} \times K$ in $H \cdot K$.

„$\Leftarrow$“ Gelte (1) - (3). Für $h \in H, k \in K$ ist $\underbrace{(hkh^{-1})}_{\in K} k^{-1} = hkh^{-1}k^{-1} = h\underbrace{(kh^{-1}k^{-1})}_{\in H} \in H \cap K = \{e\} \Rightarrow hk = kh$.
Damit ist die Abbildung φ ein Homomorphismus:
$\varphi((h_1, k_1) \cdot (h_2, k_2)) = \varphi(h_1 h_2, k_1 k_2) = h_1 h_2 k_1 k_2 = h_1 k_1 h_2 k_2 = \varphi(h_1, k_1) \cdot \varphi(h_2, k_2)$.
φ ist surjektiv wegen (2). φ ist auch injektiv: ist $(h, k) \in \ker(\varphi)$ ^{2} $hk = e \Rightarrow k = h^{-1} \in H \cap K = \{e\} \Rightarrow (h, k) = (e, e)$.

□

Beispiele 3.18.

1 Sie G eine endliche Gruppe, seien $H, K \trianglelefteq G$ mit $|G| = |H| \cdot |K|$ und $H \cap K = \{e\}$. Dann ist $G = H \times K$. Beachte: ist $\mathrm{ggT}(|H|, |K|) = 1$, so ist $H \cap K = \{e\}$ automatisch erfüllt!

2 Sei $G = GL_n(\mathbb{R})$, sei $Z = Z(G) = \mathbb{R}^* \cdot I$. Ist n ungerade, so ist $GL_n(\mathbb{R}) = SL_n(\mathbb{R}) \times Z \cong SL_n(\mathbb{R}) \times \mathbb{R}^*$.

Lemma und Definition 3.19.
Sei $N \trianglelefteq G$, sei $H \leq G$. Es sind äquivalent:

(i) $NH = G$ *und* $N \cap H = \{e\}$;

(ii) der Homomorphismus $H \to G/N$, $h \mapsto hN$, *ist bijektiv;*

(iii) die Abbildung $N \times H \to G$, $(n, h) \mapsto n \cdot h$, *ist bijektiv.*

Sind diese erfüllt, so heißt H ein ***Komplement*** *von N in G.*

Beweis:
(i) $\Leftrightarrow$ (ii) klar!

In (iii) ist Surjektivität gerade äquivalent zu $NH = G$, die Injektivität zu $N \cap H = \{e\}$: $nh = n'h' \Leftrightarrow \underbrace{h(h')^{-1}}_{\in H} = \underbrace{n^{-1}n'}_{\in N}$.

□

Bemerkungen und Beispiele 3.20.

1. Jedes Komplement H von N in G ist zu G/N isomorph.
2. Ist $G = G_1 \times G_2$ ein direktes Produkt, so ist G_1 ein Komplement von G_2 und umgekehrt.
3. Ist $|G| < \infty$ und $N \trianglelefteq G$, $H \leq G$, so ist zu (i) - (iii) auch äquivalent:

(iv) $|N \cap H| = 1$ *und* $|N| \cdot |H| = |G|$.

4. Der Normalteiler A_n von S_n hat ein Komplement, nämlich z.B. $H = \langle \tau \rangle$ für jede Transposition τ.
5. Sei $G = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, b, c \in \mathbb{K}, ac \neq 0 \right\} \leq GL_2(\mathbb{K})$, $N := \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{K} \right\}$, $N \trianglelefteq G$. Dann ist $H := \left\{ \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} : a, c \in \mathbb{K}^* \right\}$ ein Komplement von N in G.

6. In der Regel gibt es zu $N \trianglelefteq G$ *kein* Komplement H in G. Denn G braucht gar keine zu G/N isomorphe Untergruppe zu haben. Beispiel:
   $G = \mathbb{Z}$, $N \leq G$ mit $N \neq \{0\}, \neq G$. Dann hat N kein Komplement in G. Denn G/N ist endlich zyklisch, $|G/N| > 1$.

Bemerkung 3.21.
Sei H ein Komplement von N in G. Übertrage die Multiplikation der Gruppe G via (iii) nach $N \times H$:
$g = n \cdot h$, $g' = n'h'$ mit $n, n' \in N, h, h' \in H \Rightarrow gg' = nh \cdot n'h' = (\underbrace{n \cdot hn'h^{-1}}_{\in N}) \cdot (\underbrace{hh'}_{\in H})$. (*)
Für $h \in H$ schreibe $\alpha_h := (\mathrm{int}_h)|_N \in \mathrm{Aut}(N)$, also $\alpha_h(x) = hxh^{-1}$ für $x \in N$. Damit wird (*) zu $nh \cdot n'h' = (n \cdot \alpha_h(n')) \cdot (hh')$.
Wir haben also G rekonstruiert aus N, H und aus $\alpha : H \to \mathrm{Aut}(N), h \mapsto \alpha_h$
(Beachte: α ist ein Gruppenhomomorphismus)
Dies ist die Idee des semidirekten Produkts:

3.22 (Semidirektes Produkt)**.**
Seien N, H Gruppen, sei $\alpha : H \to \mathrm{Aut}(N)$ ein Homomorphismus. Das semidirekte Produkt $N \rtimes_\alpha H$ von N mit H via α ist wie folgt definiert:
als Menge ist $N \rtimes_\alpha H := N \times H$, die Multiplikation ist $(n_1, h_1) \cdot (n_2, h_2) := (n_1 \cdot \alpha_{h_1}(n_2), h_1 h_2)$.
Dann ist $G := N \rtimes_\alpha H$ eine Gruppe (nachrechnen!) mit neutralem Element (e, e) und Inversen $(n, h)^{-1} = (\alpha_h^{-1}(n)^{-1}, h^{-1})$. In G ist $N \cong N \times \{e\} \trianglelefteq G$, $H \cong \{e\} \times H \leq G$, und dabei ist $\{e\} \times H$ ein Komplement von $N \times \{e\}$ in G. Es gilt $(n, h) = (n, e) \cdot (e, h)$.

Korollar 3.23.
Sei G eine Gruppe, $N \trianglelefteq G$ und $H \leq G$ ein Komplement von N in G. Dann gibt es einen natürlichen Isomorphismus

$$N \rtimes_\alpha H \to G, (n, h) \mapsto nh$$

wobei $\alpha : H \to \mathrm{Aut}(N)$ gegeben ist durch $\alpha_h = (int_h)|_N$.

Also: Ein Normalteiler N von G hat genau dann ein Komplement in G, wenn G zu einem semidirekten Produkt $N \rtimes H$ isomorph ist.

Bemerkungen und Beispiele 3.24.

1. Notation: statt $N \rtimes_\alpha H$ schreibt man häufig $N \rtimes H$, wenn α nicht wichtig, oder klar ist.
   Das Dreieck in $\rtimes$ deutet an, dass N die Rolle des Normalteilers spielt.

2. Ist α trivial, also $\alpha_h = id_N$ für alle $h \in H$, so ist $N \rtimes_\alpha H = N \times H$, das direkte Produkt.

3. $S_n = A_n \rtimes C_2$ (in vielen Weisen, siehe oben).

4. Sei $\mathbb{K}$ ein Körper, sei $GA_n(\mathbb{K})$ die Gruppe der Affinitäten von $\mathbb{K}^n$, also aller Abbildungen $f = f_{A,u} : \mathbb{K}^n \to \mathbb{K}^n$, $f(x) = Ax + u$ mit $A \in GL_n(\mathbb{K})$ und $u \in \mathbb{K}^n$.
Es ist $GA_n(\mathbb{K}) = \left\{ \begin{pmatrix} 1 & 0 & \dots & 0 \\ u_1 & & & \\ \vdots & & A & \\ u_n & & & \end{pmatrix} \right\} \leq GL_{n+1}(\mathbb{K})$, $\left(\begin{array}{c|ccc} 1 & 0 & \dots & 0 \\ \hline u_1 & & & \\ \vdots & & A & \\ u_n & & & \end{array}\right)\left(\begin{array}{c} 1 \\ \hline x_1 \\ \vdots \\ x_n \end{array}\right) = \left(\begin{array}{c} 1 \\ \hline \\ f_{A,u}(x) \\ \\ \end{array}\right)$
Es ist $G := GA_n(\mathbb{K}) \cong \mathbb{K}^n \rtimes_\alpha GL_n(\mathbb{K})$, wie folgt:
sei $T := \{f_{I,u} : u \in \mathbb{K}^n\}$ der Normalteiler aller Translationen in G; $H := \{f_{A,o} : A \in GL_n(\mathbb{K})\}$ die Untergruppe aller linearen Abbildungen in G.
Dann ist H ein Komplement von T in G, denn jedes $f \in G$ zerlegt sich eindeutig $f = t \circ h$ mit $t \in T, h \in H$. Dabei ist α wie folgt: für $A \in GL_n(\mathbb{K})$, $u \in \mathbb{K}^n$ ist $\alpha_h(t) = \underbrace{f_{A,o}}_{=:h \in H} \circ \underbrace{f_{I,u}}_{=:t \in T} \circ \underbrace{f_{A^{-1},o}}_{\in H} : x \mapsto A(A^{-1}x + u) = x + (Au)$.
Also ist α die natürliche Operation von $GL_n(\mathbb{K})$ auf $\mathbb{K}^n$.

c. Operation von Gruppen auf Mengen

Definition 3.25.
Sei G eine Gruppe und M eine Menge. Eine **Operation** von G auf M (von links) ist eine Abbildung $G \times M \to M$, $(g, x) \mapsto g \cdot x = gx$ mit folgenden Eigenschaften:

(1) $e \cdot x = x \ \forall\ x \in M$;

(2) $g \cdot (h \cdot x) = (gh) \cdot x \ \forall\ g, h \in G \ \forall\ x \in M$.

Eine G**-Menge** ist eine Menge M zusammen mit einer Operation von G auf M. Eine Abbildung $f : M_1 \to M_2$ von G-Mengen heißt eine G**-Abbildung**, wenn gilt

$$f(g \cdot x) = g \cdot f(x) \ \ \forall\ g \in G, \ \forall\ x \in M_1$$

Ist f bijektiv, so ist auch f^{-1} eine G-Abbildung und man nennt f einen Isomorphismus der G-Mengen M_1 und M_2.

Definition und Satz 3.26.
Sei M eine G-Menge, sei $x \in M$.

(a) $G_x := Stab_G(x) := \{g \in G : g \cdot x = x\}$ *ist eine Untergruppe von G, genannt die* ***Standgruppe*** *(oder:* ***Stabilisator****) von x.*

(b) Die Menge $Gx := \{gx : g \in G\}$ heißt die ***Bahn*** *(oder der* ***Orbit****) von x unter G. Die Abbildung $G/G_x \to Gx$, $gG_x \mapsto g \cdot x$ ist eine (wohldefinierte) Bijektion.*

(c) Für $g \in G$ ist $Stab(gx) = g \cdot Stab(x) \cdot g^{-1}$.

Beweis:

(a) klar: $g, h \in G_x \Rightarrow (gh^{-1})x = (gh^{-1})(hx) = gx = x$.

(b) $g \cdot x = h \cdot x \Leftrightarrow (h^{-1}g)x = x \Leftrightarrow h^{-1}g \in G_x \Leftrightarrow gG_x = hG_x$.

(c) $h \cdot (gx) = gx \Leftrightarrow g^{-1}hg \cdot x = x \Leftrightarrow g^{-1}hg \in \mathrm{Stab}(x) \Leftrightarrow h \in g \cdot \mathrm{Stab}(x) \cdot g^{-1}$.

□

Korollar 3.27.
Ist G endlich, so gilt $|Gx| = [G : G_x]$; also $|G| = |Gx| \cdot |G_x|$.

Lemma 3.28.
Sei M eine G-Menge, seien $x, y \in M$. Dann gilt: $Gx = Gy$ oder $Gx \cap Gy = \emptyset$.

Beweis: □

Bemerkung 3.29.
Jede Operation von G auf M definiert einen Homomorphismus $\varphi : G \to \mathrm{Sym}(M)$, $g \mapsto \left(\varphi_g : M \to M, x \mapsto gx\right)$. φ_g ist eine Bijektion, denn $\varphi_{g^{-1}}$ ist die Umkehrabbildung.
$\varphi_g \circ \varphi_h = \varphi_{gh} : g(hx) = (gh)x$.
Umgekehrt gibt jeder Homomorphismus $\varphi : G \to \mathrm{Sym}(M)$ eine Operation von G auf M.
Dabei ist $\ker(\varphi) = \{g \in G : \ \forall\, x \in M\ g \cdot x = x\} = \bigcap\limits_{x \in M} G_x$:

Definition 3.30.
Man nennt $K_M := \ker(\varphi) = \{g \in G : g \cdot x = x\}$ den **Kern** der Operation von G auf M.
Man nennt die Operation **treu**, wenn $K_M = \{e\}$ ist, also wenn gilt: $\forall\ e \neq g \in G\ \exists\, x \in M\ g \cdot x \neq x$.

In jedem Fall operiert die Faktorgruppe G/K_M auf M durch $\overline{g} \cdot x = g \cdot x$, und diese Operation ist treu.

Beispiele 3.31.

1. Die symmetrische Gruppe S_n operiert auf $\{1, \ldots, n\} : (\sigma, i) \mapsto \sigma(i)$. Die Standgruppen $\mathrm{Stab}_{S_n}(i) \cong S_{n-1}$.
   Allgemeiner: $\forall$ Mengen M operiert $\mathrm{Sym}(M)$ auf M.

2. Jede Gruppe G operiert auf sich selbst durch Translation:
   $G \times G \to G, (g, x) \mapsto gx$.
   Ist $|G| = n < \infty$, so erhalten wir einen injektiven Homomorphismus $\varphi : G \to \mathrm{Sym}(G) \cong S_n$ (die Operation ist treu und hat sogar triviale Standgruppen).

Satz 3.32 (von Cayley)**.**
Jede Gruppe der Ordnung $n < \infty$ ist zu einer Untergruppe von S_n isomorph.

Beispiel 3.33.
Ist $H \leq G$, so operiert insbesondere H auf G durch Translation: $H \times G \to G, (h, x) \mapsto hx$.

Die Bahnen sind genau die Nebenklassen Hx ($x \in G$).

3.34.
Es existiert eine zweite (wichtigere) Operation von G aus sich, durch Konjugation:

$$G \times G \to G, (g, x) \mapsto gxg^{-1}$$

Die Bahnen sind genau die Konjugationsklassen der Elemente von G. Insbesondere ist G die disjunkte Vereinigung seiner Konjugationsklassen.

Standgruppen?
Für $x \in G$ ist $\text{Stab}(x) = \{g \in G : gxg^{-1} = x\} = \{g : gx = xg\} =: C_G(x)$, der **Zentralisator** von x in G.
$C_G(x)$ ist die größte Untergruppe von G, in deren Zentrum x liegt.

Lemma 3.35.
Die Anzahl der Konjugierten von x ist $[G : C_G(x)]$.

Beweis:
Anwendung von 3.27:
$|\{Konjugierte\ von\ x\}| = |Bahn(x)| = [G : \text{Stab}(x)] = [G : C_G(x)]$.

□

3.36.
Sei $\text{Subg}(x)$ die Menge aller Untergruppen von G. Dann operiert G auf $\text{Subg}(G)$ durch Konjugation: $(g, H) \mapsto gHg^{-1}$. Die Standgruppe von $H \leq G$ ist $\{g \in G : gHg^{-1} = H\} = \{g \in G : gH = Hg\} = N_G(H)$ der **Normalisator** von H in G: dies ist die größte Untergruppe von G, in der H normal ist.

Lemma 3.37.
Die Anzahl der zu $H \leq G$ konjugierten Untergruppen von G ist $[G : N_G(H)]$.

Bemerkung 3.38.
Eine **Rechts-Operation** der Gruppe G auf der Menge M ist eine Abbildung $M \times G \to M, (x, g) \mapsto x \cdot g$, mit

(1) $x \cdot e = x$,

(2) $(x \cdot g) \cdot h = x \cdot (gh)$ $\forall\ x \in M,\ \forall\ g, h \in G$.

Alles über Links-Operationen Gesagte gilt analog für Rechts-Operationen. Man kann jede Rechts-Operation in eine Links-Operation verwandeln:
ist $(x, g) \mapsto xg$ eine Operation von rechts, so ist $(g, x) \mapsto xg^{-1}$ eine Operation von links (gleiche Bahnen, Standgruppen, ...)

Definition 3.39 (transitiv)**.**
Eine Operation von G auf M heißt **transitiv**, wenn $M \neq \emptyset$ und gilt $\forall\, x, y \in M$: $\exists\, g \in G, y = g \cdot x$.
Oder äquivalent: wenn es nur eine G-Bahn gibt (und $M \neq \emptyset$ ist).

Bemerkung 3.40.

(1) Ist M eine transitive G-Menge, so sind alle Standgruppen G_x für $x \in M$ zueinander konjugiert, also isomorph, nach 3.26 (c).

(2) Beispiel einer transitiven Operation: sei G eine Gruppe, $H \leq G$ eine Untergruppe, sei $M := G/H = \{gH : g \in G\}$. Auf M operiert G durch $G \times (G/H) \to G/H$, $(g, xH) \mapsto (gx)H$ transitiv: $(yx^{-1})xH = yH$.

Standgruppen?
$\mathrm{Stab}(eH) = \{g \in G : g \cdot e \cdot H = eH\} = H$.

Satz 3.41.

(a) Sei M eine transitive G-Menge. Sei $x \in M$. Dann ist die Abbildung $\varphi : G/G_x \to M$, $gG_x \mapsto g \cdot x$ ein Isomorphismus der G-Mengen.

(b) Seien $H, K \leq G$. Dann gilt:
$G/H \cong G/K$ (als G-Mengen) $\Leftrightarrow\ \exists\, g \in G$ mit $K = gHg^{-1}$.

Beweis:

(a) bijektiv wissen wir schon (3.26).
Es ist eine G-Abbildung $(ag)x = \varphi(a \cdot gG_x) = a \cdot \varphi(gG_x) = a(gx)\ \ \forall\, a, g \in G$.

(b) Sind M, N isomorphe transitive G-Mengen, so sind ihre Standgruppen dieselbe Konjugationsklasse.
Das zeigt „$\Rightarrow$“.

„⇐“ Ist $K = gHg^{-1}$, so gibt es in G/H einen Punkt x mit Standgruppe K, nämlich $x = gH$. Also ist nach (a) $G/H \cong G/G_x = G/K$.

□

Fazit 3.42.
Bis auf Isomorphie sind die transitiven G-Mengen also genau die G/H mit der Standardoperation (für $H \leq G$). Dabei entsprechen die Isomorphieklassen solcher G-Mengen gerade den Konjugationsklassen der Untergruppen von G.

Andererseits ist jede G-Menge eine disjunkte Vereinigung von transitiven G-Mengen, nämlich von ihren Bahnen.

Beispiele 3.43.

1 Die Gruppe $GL_n(\mathbb{K})$ operiert auf $\mathbb{K}^n$ (= Vektorraum der Spaltenvektoren) durch $(g, x) \mapsto gx$.
Es gibt genau 2 Bahnen, nämlich $\{0\}$ und $\mathbb{K}^n \setminus \{0\}$. Die Operation auf $\mathbb{K}^n \setminus \{0\}$ ist also transitiv und treu.
Die Standgruppen sind isomorph zur affinen Gruppe $AG_n(\mathbb{K})$ (Gruppe aller Abbildungen $x \mapsto Ax + u$); das sieht man für $x = e_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$:

$$G_x = \left\{ \left(\begin{array}{c|c} 1 & * \\ \hline 0 & \\ \vdots & * \\ 0 & \end{array} \right) \right\}.$$

2 Der n-dimensionale projektive Raum $\mathbb{P}^n(\mathbb{K})$ ist definiert als die Menge der 1-dimensionalen Untervektorräume von $\mathbb{K}^{n+1}$: für $0 \neq x \in \mathbb{K}^{n+1}$ schreibe $\mathbb{K}_x =: [x]$, dann gilt also: $[x] = [y] \Leftrightarrow \exists\, \lambda \in \mathbb{K}^*$ mit $y = \lambda x$, $\mathbb{P}n(\mathbb{K}) = \{[x] : 0 \neq x \in \mathbb{K}^{n+1}\}$.
Die Operation von $GL_{n+1}(\mathbb{K})$ auf $\mathbb{K}^{n+1}$ induziert ein Operation auf $\mathbb{P}(\mathbb{K})$ durch $g, [x]) \mapsto [gx]$. Der Kern dieser Operation ist $Z := \{\lambda I : \lambda \in \mathbb{K}^*\} \leq GL_{n1}(\mathbb{K})$ (es ist auch $Z = Z(GL_n + 1(\mathbb{K}))$).
Die Faktorgruppe $PGL_{n+1}(\mathbb{K}) = GL_{n+1}(\mathbb{K})/Z$ operiert also treu auf $\mathbb{P}^n(\mathbb{K})$ durch $(gZ, [x]) \mapsto [gx]$.

3 Betrachte den Fall $n = 1$ näher:
die projektive Gerade $\mathbb{P}^1(\mathbb{K})$ kann man mit $\mathbb{K} \cup \{\infty\}$ identifizieren:

$\left[\begin{pmatrix} x \\ y \end{pmatrix}\right] \mapsto \frac{x}{y}$ mit $\frac{x}{0} := \infty$.

Bijektion $\mathbb{P}^1(\mathbb{K}) \to \mathbb{K} \cup \{\infty\}, \left[\begin{pmatrix} x \\ y \end{pmatrix}\right] \mapsto \frac{x}{y}$.

Unter dieser Identifikation operiert $GL_2(\mathbb{K})$ auf $\mathbb{P}^1(\mathbb{K}) = \mathbb{K} \cup \{\infty\}$ durch $\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, x\right) \mapsto \frac{ax+b}{cx+d}, x \in K \cup \{\infty\}$ (mit $\frac{*}{0} := \infty$).

Definition 3.44.
Sei M eine G-Menge. Dann heißt $M^G := \{x \in M : \forall\, g \in G\ g \cdot x = x\} = \{x \in M : G_x = G\}$ die Menge der G**-Fixpunkte** in M.

3.45.
Sei M eine endliche G-Menge, seien $M_i = Gx_i$ für $i = 1, \ldots, r$ die verschiedenen Bahnen.
Dann ist $M = \bigcup_{i=1}^{r} M_i$ (disjunkte Vereinigung) $\Rightarrow |M| = |M_1| + \ldots + |M_r| = \sum_{i=1}^{r} [G : G_{x_i}]$.
Diese Identität heißt die **Bahnengleichung** der Operation. Sie hat wichtige Anwendungen:

Definition 3.46.
Eine endliche Gruppe G heißt eine p**-Gruppe** (p sei eine Primzahl), wenn $|G|$ eine Potenz von p ist.

Satz 3.47.
Sei G eine p-Gruppe und M eine endliche G-Menge.
Dann ist $|M^G| \equiv |M| \mod p$.

Insbesondere: ist $|M|$ nicht durch p teilbar, so ist $M^G \neq \emptyset$.

Beweis:
Seien $M_1, \ldots, M_r$ die verschiedenen Bahnen. Die $|M_i|$ sind Teiler von $|G| = p^n$, also $|M_i| = p^{n_i}$ mit $0 \leq n_i \leq n$. Lies die Bahnengleichung $|M| = \sum_{i=1}^{r} |M_i|$ modulo $(p) \Rightarrow |M| \equiv |M^G| \mod p$.

□

3.48.
Wichtiger Spezialfall der Bahnengleichung:
G operiere auf sich durch Konjugation, d.h. $G \times G \to G, (g, x) \mapsto gxg^{-1}$. Die Bahnen

sind die Konjugationsklassen in G. Sei $|G| < \infty$, seien $C_1, \ldots, C_r$ die Konjugationsklassen in G. Die Gleichung $|G| = \sum_{i=1}^{r} |C_i|$ heißt die **Klassengleichung** von G.
Die Fixpunkte der Operation sind genau die Elemente in $Z(G)$. Es folgt:

Korollar 3.49.
Ist $G \neq \{e\}$ eine p-Gruppe, so ist $Z(G) \neq \{e\}$.

Beweis:
$|Z(G)| \equiv |G| \equiv 0 \mod p$ nach 3.47.

□

Liste von Gruppen kleiner Ordnung:

Lemma 3.50.
Ist $|G| = p$ prim, so ist G zyklisch: $G \cong C_p$.
Denn: sei $e \neq g \in G$, dann $|\langle g \rangle| \mid |G| = p \Rightarrow \langle g \rangle = G$.

Korollar 3.51.
Ist $|G| = p^2$ mit p prim, so ist G abelsch, also $G \cong C_{p^2}$ oder $G \cong C_p \times C_p$.

Beweis:
Nach 3.49 ist $|Z(G)| \neq 1$. Angenommen, $|Z(G)| = p \Rightarrow |G/Z(G)| = p$. Also ist $G/Z(G)$ zyklisch nach 3.50.
Nach Aufgabe 33 folgt G ist abelsch.
($G/Z(G)$ zyklisch $\Rightarrow$ G abelsch: nach Voraussetzung $\exists\ g \in G$ mit $g/Z = \langle gZ \rangle$. D.h. jedes $x \in G$ schreibt sich $x = g^n z$ mit $n \in \mathbb{Z}$, $z \in Z$. Je zwei solche Elemente kommutieren: $x' = g^m \cdot z' \Rightarrow xx' = x'x$.)

□

Satz 3.52.
Jede Gruppe von Ordnung 6 ist zyklisch oder zu S_3 isomorph.

Beweis:
Sei G nicht zyklisch, also auch nicht abelsch. Es gibt ein $g \in G$ mit $\mathrm{ord}(g) = 3$.
(Denn aus $g^2 = e\ \forall\ g \in G$ folgt nach Lemma 3.8: G ist abelsch)
Sei $h \in G$ mit $\mathrm{ord}(h) = 3$, sei $H = \langle h \rangle$. Dann ist $[G : H] = 2 \Rightarrow H \trianglelefteq G$ (nach 3.7).
Sei $g \in G \setminus H$. Behaupte: $\mathrm{ord}(g) = 2$ *(denn 2 | ord(g) wegen $ord_{G/H}(gH) = 2$).*

Also ist $\langle g \rangle$ ein Komplement von H in G, d.h. $G = H \rtimes_\alpha \langle g \rangle \cong C_3 \rtimes_\alpha C_2$ mit einem $\alpha : \langle g \rangle \to Aut(H) \cong Aut(C_3) \cong C_2$.
α ist nicht trivial, denn sonst wäre G abelsch. Also ist α der Isomorphismus. Also ist $G \cong S_3$.

□

Bemerkung 3.53.
Gruppen kleiner Ordnung:

n	G mit $\lvert G\rvert = n$
1	$\{e\}$
2	C_2
3	C_3
4	$C_4, C_2 \times C_2$
5	C_5
6	C_6, S_3
7	C_7
8	$C_8, C_4 \times C_2, C_2 \times C_2 \times C_2$ und weitere (?)
9	$C_9, C_3 \times C_3$

Beispiel 3.54.
Beispiel einer Gruppe von Ordnung 8:
Betrachte die Matrizen $u := \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, v := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in GL_2(\mathbb{C})$ ($i = \sqrt{-1}$).
Die **Quaternionengruppe** Q ist $\mathbb{Q} := \langle u, v \rangle \leq GL_2(\mathbb{C})$.
$w := uv = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, vu = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} = -w.$
Außerdem haben u, v, w die Ordnung 4; $u^2 = -I = v^2 = w^2$. Also ist $Q = \{\pm I, \pm u, \pm v, \pm w\}$.
Also ist Q nichtabelsch, $|Q| = 8$.

Die Untergruppen von Q sind: $\{I\} - - \{-I\} = Z(Q) - - \left\{ \begin{matrix} \langle u \rangle \\ \langle v \rangle \\ \langle v \rangle \end{matrix} \right\} - - Q.$

Beachte: alle Untergruppen von Q sind Normalteiler, obwohl Q nicht abelsch ist!
Klassengleichung von Q:
$|Q| = 8 = 1 + 1 + 2 + 2 + 2$. (Die Konjugationsklasse $\not\subset Z(Q)$ sind $\{\pm u\}, \{\pm v\}, \{\pm w\}$.)

Beispiel 3.55.
Sei $n \geq 3$. Sei $\zeta = e^{2\pi i/n} \in \mathbb{C}$, sei $P := \{1, \zeta, \zeta^2, \ldots, \zeta^{n-1}\} \subset \mathbb{C}$ (Eckpunkte des regelmäßigen n-Ecks).

Sei D_n die Gruppe aller Bewegungen des $\mathbb{R}^2$, die P in sich überführen. Alle Elemente von D_n lassen den Nullpunkt fest, sind also linear, d.h. in $O(2)$. Also ist $D_n = \{f \in O(2) : f(P) = P\}$.

Sei $D_n^+ := D_n \cap SO(2)$. Die Gruppe D_n^+ der Drehungen in D_n ist zyklisch, erzeugt von der Drehung σ um $\frac{2\pi}{n}$.
Die Elemente in $D_n \setminus D_n^+$ sind die Spiegelungen an Ursprungsgeraden, die durch einen Eckpunkt und/oder einen Seitenmittelpunkt gehen: n Stück.
Es ist $|D_n| = 2n$.

Definition 3.56.
Die so definierte Gruppe D_n heißt die **Diedergruppe** (der Ordnung 2n).

3.57.
Die Operation von D_n auf der Menge P der Eckpunkte ist transitiv und treu.
Das bedeutet (wegen $|P| = n$): wir haben einen injektiven Homomorphismus $D_n \hookrightarrow S_n$ (nummeriere die Eckpunkte als $1, \ldots, n$).
$n = 3$: $|D_3| = G = |S_3| \Rightarrow D_3 \cong S_3$.
$n \geq 4$: D_n ist eine echte Untergruppe von S_n.

Die Untergruppe $D_n^+ = D_n \cap SO(2)$ ist normal in D_n, $[D_n : D_n^+] = 2$. Alle Elemente in $D_n \setminus D_n^+$ haben als Spiegelungen die Ordnung 2.
Sei τ eine dieser Spiegelungen, sei $\langle\sigma\rangle = D_n^+$. Es ist also $D_n = \langle\sigma\rangle \rtimes \langle\tau\rangle$.
Wie operiert τ auf $\langle\sigma\rangle$? Für alle $k \in \mathbb{Z}$ ist $\tau\sigma^k$ ebenfalls eine Spiegelung, also ist $e = (\tau\sigma^k)^2 = \tau\sigma^k\tau\sigma^k \Rightarrow \sigma^{-k} = \tau\sigma^k\tau = \tau\sigma^k\tau^{-1} \quad \forall\, k \in \mathbb{Z}$.
Damit ist die Struktur von D_n völlig aufgedeckt:
$D_n = \langle\sigma, \tau\rangle$ mit $\sigma^n = \tau^2 = (\sigma\tau)^2 = e$.

Die Elemente von D_n sind also genau die folgenden:
$\sigma^k, \sigma^k\tau$ für $k = 0, \ldots, n-1$.
$\sigma^k \cdot \sigma^l\tau = \sigma^{k+l}\tau$; $\sigma^k \underbrace{\tau\sigma^l\tau}_{=\sigma^{-l}} = \sigma^{k-l}$.

Bemerkung 3.58.
Konjugationsklassen in D_n?

1. *Drehungen:* zueinander konjugierte Drehungen müssen bis auf das Vorzeichen denselben Drehwinkel haben. Umgekehrt sind die Drehungen um $\pm\alpha$ auch zueinander konjugiert ($\sigma^{-k} = \tau\sigma^k\tau^{-1}$).

2. *Spiegelungen:*

- n gerade: zwei Typen von Spiegelachsen $\widehat{=}$ 2 Konjugationsklassen
- n ungerade: nur ein Typ $\widehat{=}$ 1 Konjugationsklasse.

Bemerkung 3.59.
Die Gruppen D_4 und Q sind beide nichtabelsch von Ordnung 8, sie sind aber nicht isomorph.
Zum Beispiel gibt es in Q nur ein Element von Ordnung 2, in D_4 aber fünf solche Elemente.

Satz 3.60.
Bis auf Isomorphie gibt es genau fünf Gruppen der Ordnung 8: $C_8, C_4 \times C_2, C_2 \times C_2 \times C_2$ *und* Q *und* D_4.

Beweis:
Sei $|G| = 8$, G nicht abelsch. Es gibt ein $g \in G$ mit $\operatorname{ord}(g) = 4$. Also $\langle g \rangle \trianglelefteq G$.
Sei $h \in G$ mit $h \notin \langle g \rangle$, also $G = \langle g, h \rangle$. Es ist $hgh^{-1} \neq g$ (sonst wäre G abelsch).
Also ist $hgh^{-1} = g^{-1}$. Ist $\operatorname{ord}(h) = 2$, so ist $G \cong D_4$. Ist $\operatorname{ord}(h) = 4$, so ist $G \cong Q$.

□

d. Permutationen

Erinnerung 3.61.
S_n symmetrische Gruppe auf $\{1,\dots,n\}$, $|S_n| = n!$.
r-Zykel: $(i_1 i_2 \dots i_r)$, $i_1,\dots,i_r$ paarweise verschieden in $\{1,\dots,n\}$.

Jedes $\sigma \in S_n$ hat im Wesentlichen eine eindeutige Darstellung $\sigma = \sigma_1 \circ \dots \circ \sigma_t$ mit σ_i ein r_i-Zykel, σ_i paarweise disjunkt.
Disjunkte Zykel kommutieren! Sortieren wir die $\sigma_1,\dots,\sigma_t$ so, dass $r_1 \geq r_2 \geq \dots r_t$ ist (r_i = Länge des Zykels σ_i) und ist $k = |Fix(\sigma)|$, so ist $r_1 + \dots + r_t + \underbrace{1 + \dots + 1}_{k-mal} = n$.
Also ist $(r_1,\dots,r_t,1,\dots,1) =: \text{typ}(\sigma)$ eine Partition von n. Wir nennen typ(σ) den **Typ** von σ.

Beispiel:
$n = 6, \sigma = (143)(56)$ hat Typ $(3,2,1)$.

Ist σ ein r-Zykel, so ist ord(σ) = r. Allgemeiner: ist $\sigma = \sigma_1 \circ \dots \circ \sigma_t$ mit disjunkten Zykeln σ_i von Länge r_i für $i = 1,\dots,t$, so gilt:

Lemma 3.62.
ord$(\sigma) = kgV(r_1,\dots,r_t)$.

Beweis:
$\sigma^k = id \Leftrightarrow \sigma_i^k = id \;\forall\; i = 1,\dots,t$
$\Rightarrow$ Behauptung.

□

Bemerkung 3.63.
Rechnen mit Zykeln ist sehr bequem:
Invertieren: $(i_1 \dots i_r) = (i_r i_{r-1} \dots i_1)$
Konjugation: $\sigma \circ ((i_1 \dots i_r) \circ (j_1 \dots j_s)) \circ \sigma^{-1} = (\sigma(i_1) \dots \sigma(i_r)) \circ (\sigma(j_1) \dots \sigma(j_s))$.

Anwendung: Konjugierte Permutationen haben denselben Typ.
Umkehrung gilt auch: haben ρ, σ denselben Typ, so gibt es $\tau \in S_n$ mit $\sigma = \tau\rho\tau^{-1}$:

Beispiel:
$\rho = (1342)(76), \sigma = (4571)(23) \in S_7$.

$\Rightarrow \tau := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 1 & 5 & 7 & 6 & 3 & 2 \end{pmatrix}$ macht dies.

Satz 3.64.
Zwei Permutationen σ, τ in S_n sind genau dann konjugiert, wenn sie denselben Typ haben.

Insbesondere stehen die Konjugationsklassen in S_n in Bijektion zu den Partitionen von n.

Erinnerung 3.65.
S_n wird von den Transpositionen erzeugt:
$\sigma = \tau_1 \dots \tau_k$ mit τ_i Transpositionen. Dabei ist $(-1)^k =: \operatorname{sgn}(\sigma)$ eindeutig bestimmt und heißt **Signum** von σ.
$A_n := \{\sigma \in S_n : \operatorname{sgn}(\sigma) = +1\}$ ist ein Normalteiler in S_n vom Index 2. Also $|A_n| = \frac{1}{2}n!$.
Ist $\sigma = \sigma_1 \circ \dots \circ \sigma_t$ eine Zykelzerlegung, σ_i ein r_i-Zykel, $\operatorname{sgn}(\sigma) = \prod_i \operatorname{sgn}(\sigma_i) = \prod_i (-1)^{r_i - 1} = (-1)^{r_1 + \dots + r_t - t}$.

Betrachte nun Permutationsgruppen kleiner Ordnung:

$S_1 = A_1 = A_2 = \{e\}$, $|S_2| = 2$.

3.66.
$n = 3$: S_3: Konjugationsklassen

K	σ	$\operatorname{ord}(\sigma)$	$\lvert K\rvert$
K_1	id	1	1
K_2	(12)	2	$\binom{3}{2} = 3$
K_3	(123)	3	2

3.67.
$n = 4$: S_4: $|S_4| = 24$ Konjugationsklassen

K	σ	$\operatorname{ord}(\sigma)$	$\lvert K\rvert$
K_1	id	1	1
K_2^a	(12)	2	$\binom{4}{2} = 6$
K_3	(123)	3	$4 \cdot 2 = 8$
K_4	(1234)	4	$3! = 6$
K_2^b	(12)(34)	2	$\frac{1}{2}\binom{4}{2} = 3$

Klassengleichung: $24 = 1 + 3 + 6 + 6 + 8$.

Außer $S_4, A_4, \{e\}$ gibt es einen weiteren Normalteiler in S_4, nämlich
$V_4 := \{id, (12)(34), (13)(24), (14)(23)\} \cong C_2 \times C_2$, die **Kleinsche Vierergruppe**.

Aus der Klassengleichung folgt, dass es keine weiteren Normalteiler in S_4 gibt. Denn jeder solche ist Vereinigung von Konjugationsklassen, also ist $|N|$ eine Teilsumme der Klassengleichung, in der 1 ($\widehat{=}\{e\}$) vorkommt. Außerdem ist $|N|$ ein Teiler von $|G| = |S_4| = 24$; wir können hier aber keine anderen solchen Teilsummen mehr finden!

Transitive Untergruppen von S_4? (d.h. transitiv auf $\{1, 2, 3, 4\}$).
S_4, A_4, V_4, außerdem die von einem 4-Zykel σ erzeugte $C_4 = \langle\sigma\rangle$ (3 Stück), sowie die D_4 (3 Stück), die Normalisatoren der C_4 (z.B. ist $N_{S_4}(\langle 1234\rangle) = \langle(1234), (13)\rangle$).
Behaupte, das sind alle transitiven Untergruppen von S_4. Das Inklusionsdiagramm ihrer Konjugationsklassen ist (siehe Aufschrieb).

3.68.
Untersuche jetzt die A_4: $|A_4| = 12$.
Klassengleichung? In A_4 sind K_1, K_2^b, K_3 der S_4 enthalten.
In wie viele Teilklassen zerfallen diese in A_4?

Lemma 3.69.
Sei $M \cong G/H$ eine transitive G-Menge, sei $N \trianglelefteq G$. Dann besteht M als N-Menge aus genau $[G : NH]$ N-Bahnen, die alle dieselbe Länge $[N : N \cap H] = [NH : H]$ haben.

Beweis:
Für $x = gH, x' = g'H \in M$ gilt:
$Nx = Nx' \Leftrightarrow NgH = Ng'H \Leftrightarrow gNH = g'NH$.
Also entsprechen die N-Bahnen in G/H genau den Elementen von G/NH.

Ihre Länge ist $[N : N_x] = [N : N \cap gHg^{-1}] = [N : N \cap H]$.

□

Bemerkung 3.70.
Die Aussage ist im Allgemeinen falsch, falls $N \not\trianglelefteq G$!

Korollar 3.71.
Sei $N \trianglelefteq G$, sei $g \in N$. Sei $K_G(g) := \{xgx^{-1} : x \in G\}$ die Konjugationsklasse von g in G. Dann zerfällt $K_G(g)$ in genau $[G : C_G(g)N]$ N-Konjugationsklassen derselben Länge.

Beweis:
Wende Lemma 3.69 an auf die Operation von G auf G durch Konjugation: $K_G(g)$ ist gerade die G-Bahn von g.

□

3.72 (Zurück zur A_4)**.**
Für $\sigma = (1234)$ ist $C_{S_4}(\sigma) = \langle\sigma\rangle \Rightarrow K_3$ zerfällt in $[S_4 : \underbrace{\langle\sigma\rangle A_4}_{A_4}] = 2$ Konjugationsklassen K_3^I und K_3^{II} in A_4, aus je 4 Elementen.
Dagegen bleibt $K_2 b$ eine volle Konjugationsklasse in A_4.

Also hat A_4 die Klassengleichung $12 = 1 + 3 + 4 + 4$.
Außer V_4 gibt es also keine echten Normalteiler in A_4.

3.73 (Die Gruppe S_5)**.**
$|S_5| = 120$. Konjugationsklassen:

K	σ	ord(σ)	$\lvert K\rvert$
K_1	id	1	1
K_2^a	(12)	2	$\binom{5}{2} = 10$
K_2^b	(12)(34)	2	$5 \cdot 3 = 15$
K_3	(123)	3	$2 \cdot 10 = 20$
K_4	(1234)	4	$5 \cdot 6 = 30$
K_5	(12345)	5	24
K_6	(123)(45)	6	$10 \cdot 2 = 20$

Klassengleichung: $120 = 1 + 10 + 15 + 20 + 20 + 24 + 30$.

Betrachte transitive Untergruppen von S_5:
$S_5, A_5, C_5 = \langle\sigma\rangle$ mit σ ein 5-Zykel, D_5 (6 Stück) und $GA_1(\mathbb{F}_5) = \{ax + b : a, b \in \mathbb{F}_5, a \neq 0\} \cong C_5 \rtimes C_4$ (6 Stück). Das sind alle!

3.74.
Betrachte A_5, $|A_5| = 60$:
Die Klassen K_1, K_2^b, K_3, K_5 sind in A_5 enthalten. Analog z oben stellt man fest: K_5 zerfällt in A_5 in zwei Konjugationsklassen aus je 12 Elementen, während K_2^b, K_3 je eine volle Konjugationsklasse in A_5 bleiben $\Rightarrow$ Klassengleichung: $60 = 1 + 12 + 12 + 15 + 20$.

Definition 3.75.
Eine Gruppe G heißt **einfach**, wenn es außer $\{e\}$ und G keine Normalteiler von G

gibt.

Beispiele:
Jede zyklische Gruppe von Primzahlordnung ist einfach.

Satz 3.76.
Die alternierende Gruppe A_5 ist einfach.

Beweis:
Direkt aus Klassengleichung! □

Die nichtabelschen einfachen Gruppen sind schwer zu verstehen ...

Theorem 3.77.
Die alternierende Gruppen A_n sind für $n \neq 4$ einfache Gruppen.

Beweis:
Für $n \leq 3$ ist es trivial (Primzahlordnung). Beweis für $n \geq 5$ durch Induktion nach n, der Induktionsbeginn ist 3.76. Sei also $n > 5$.

Annahme: es gibt $N \trianglelefteq A_n$, $N \neq \{e\}$, $N \neq A_n$.

1. Schritt: Zeige für alle $id \neq \sigma \in N$: σ hat keinen Fixpunkt.
Angenommen, $\sigma(i) = i$. Dann liegt σ in $H := (A_n)_i = \{\tau \in A_n : \tau(i) = i\} \cong A_{n-1}$.
Wegen $id \neq \sigma \in N \cap H \trianglelefteq H$ und H einfach folgt $N \cap H = H \Rightarrow H \leq N$. Damit enthält N alle Stabilisatoren $(A_n)_j$ für $j = 1, \ldots, n$, da diese zu H konjugiert (in A_n) sind. Diese erzeugen aber ganz A_n, denn: A_n wird von allen 3-Zykeln erzeugt (Übungsaufgabe LA I, Blatt 10) $\Rightarrow N = A_n$.

2. Schritt: Sei $\sigma \neq \mathrm{id}$ in N, sei $\sigma(1) =: i$ für $i \neq 1$. Betrachte die Elemente ρ von A_n mit $\rho(1) = 1$, $\rho(i) = i$.
Dann ist $(\rho\sigma^{-1}\rho^{-1}\sigma)(1) = 1$, und $\rho\sigma^{-1}\rho^{-1}\sigma \in N$.
Also $\rho\sigma^{-1}\rho^{-1}\sigma = id$ wegen dem 1. Schritt $\Rightarrow \rho\sigma = \sigma\rho$.
Aber es ist leicht, ein ρ mit $\rho\sigma \neq \sigma\rho$ und $\rho(1) = 1, \rho(i) = i$ in A_n zu finden. $\Rightarrow$ Widerspruch.

□

Lemma 3.78.
A_n wird von allen 3-Zykeln erzeugt.

Beweis:
Es genügt, zu zeigen, dass jedes Produkt von zwei Transpositionen in S_n ein Produkt von 3-Zykeln ist.
Es gilt: (12)(23) = (123) und (12)(34) = (143)(123). Also OK.

□

Nachtrag:
($\{id\} \neq N \trianglelefteq A_n, \neq A_n, n \geq 5$)
$\forall$ *is* $\neq \sigma \in N$ ist fixpunktfrei.
Sei $\sigma \in N$, $\sigma \neq id$, $\sigma(1) =: i$.
$\exists\ \rho \in A_n : \rho(1) = 1, \rho(i) = i$ mit $\rho\sigma \neq \sigma\rho$, denn:

1. Fall $\sigma(i) = 1$, dann $\sigma(1i) \cdot \sigma'$ mit σ' fixpunktfrei auf $\{2, \ldots, n\} \setminus \{i\}$.
Wähle ρ so, dass $\rho(1) = 1, \rho(i) = i$ und $\rho\sigma' \neq \sigma'\rho$.

2. Fall $\sigma(i) = j \neq 1$: $\sigma = (1ij, \ldots)(\ldots)$.
Nimm ρ mit $\rho(1) = 1$, $\rho(i) = i$, $\rho(j) \neq j$.
$\rho\sigma\rho^{-1} = (1i\rho(i)\ldots)(\ldots) \neq \sigma$

Korollar 3.79.
Für alle $n \neq 4$ gilt:

(a) Die einzigen Normalteiler von S_n sind $\{id\}, A_n, S_n$.

(b) Für jede Untergruppe $H < S_n$ mit $H \neq A_n$ ist $[S_n : H] \geq n$.

Beweis: Für $n \leq 3$ ist das klar. Sei $n \geq 5$.

1. Fall Sei $N \trianglelefteq S_n$ mit $N \neq S_n, N \neq A_n, N \neq \{id\}$.
Dann ist $N \cap A_n \trianglelefteq A_n$, und $N \cap A_n \neq A_n$, also $N \cap A_n = \{id\}$ wegen A_n einfach.
$N \hookrightarrow S_n/A_n = \{\pm 1\} \Rightarrow |N| = 2$, also $N = \{id, \sigma\}$ mit $\sigma^2 = id$, und $\sigma \in Z(S_n)$.
Widerspruch wegen $Z(S_n) = \{id\}$.

2. Fall Sei $H < S_n$ mit $[S_n : H] = m < n$, sei $H \neq A_n$. Betrachte die Operation von S_n auf S_n/H (durch $(\sigma, \tau H) \mapsto \sigma\tau H$).
Diese Operation ist treu: denn der Kern der Operation ist ein Normalteiler von S_n, der in H enthalten ist, ist also gleich $\{id\}$ nach (a).

Das bedeutet: $S_n \to \mathrm{Sym}(S_n/H)$ ist injektiv.
Aber $\mathrm{Sym}(S_n/H) \cong S_m$ mit $m = [S_n : H] < n$; Widerspruch zur Injektivität.

□

Bemerkung 3.80.
Beide Aussagen von 3.79 sind falsch für $n = 4$:
$V_4 \trianglelefteq S_4$ und $D_4 < S_4$ hat Index $3 < 4$.

e. Die Sätze von Sylow und Anwendungen

Sei G eine endliche Gruppe. Fragen: Sei d ein Teiler von $|G|$.

(a) hat G eine Untergruppe von Ordnung d?

(b) hat G sogar ein Element von Ordnung d, also eine zyklische Untergruppe?

Antwort auf (b) ist im Allgemeinen nein (z.B. $d = |G|$: nur für G zyklisch). Antwort auf (a) im Allgemeinen nein: in A_4 ($|A_4| = 12$) gibt es keine Untergruppe von Ordnung 6.

Lemma 3.81.
Sei G eine endliche abelsche Gruppe. Zu jedem Teiler d von $|G|$ gibt es $H \leq G$ mit $|H| = d$.

Beweis:
$G \cong G_1 \times \ldots \times G_r$ mit zyklischen Gruppen, $|G_i| = n_i$. $|G| = n_1 \cdot \ldots \cdot n_r$. Schreibe $d = d_1 \cdot \ldots \cdot d_r$ mit $d_i \mid n_i$.
Sei H_i ein (die) Untergruppe von G_i mit $|H_i| = d_i$ für $i = 1, \ldots, r$. Dann hat $H := H_1 \times \ldots \times H_r$ die Ordnung $|H| = d$.

□

Satz 3.82.
Sei G eine p-Gruppe, $|G| = p^r$.

(a) Zu jedem $0 < i \leq r$ gibt es ein $H \leq G$ mit $|H| = p^i$.

(b) Für alle $H \leq G, H \neq G$, ist $N_G(H) \supsetneq H$; es gibt also zu jeder echten Untergruppe H von G ein Element, das nicht in H liegt und H normalisiert.

(c) Jede Untergruppe $H < G$ mit $[G : H] = p$ ist normal in G.

Beweis:

(a) Induktion nach r, $r = 1$ trivial.
$r - 1 \to r \geq 2$. Nach 3.49 ist $Z(G) \neq \{e\}$. Nach 3.81 gibt es in $Z(G)$ ein $z \in Z(G)$ mit $\operatorname{ord}(z) = p$. Für $G/\langle z \rangle =: G_1$ gilt $|G_1| = p^{r-1}$, also gibt es in G_1 eine Untergruppe $H/\langle z \rangle$ der Ordnung p^{i-1} (nach Induktionsannahme) $\Rightarrow |H| = p^i$.

(b) Sei $H \lneq G$. Betrachte die Operation $H \times (G/H) \to G/H$, $(h, xH \mapsto hxH$. Was sind die Fixpunkte=
$H \cdot xH = xH \Leftrightarrow x^{-1}Hx = H \Leftrightarrow x \in N_G(H)$.
Aus 3.47 folgt: $[N_G(H) : H]$ = die Anzahl der H-Fixpunkte $\equiv [G : H] \equiv \mod p$.
$\Rightarrow N_G(H) \neq H$.

(c) Spezialfall von (b).

□

Definition 3.83 (Sylowgruppe)**.**
Sei G eine endliche Gruppe, sei p eine Primzahl. Eine Untergruppe $S \leq G$ heißt eine **p-Sylowgruppe** von G, wenn S eine p-Gruppe ist und $[G : S] \not\equiv 0 \mod p$ ist. Sei $\mathrm{Syl}_p(G)$ die Menge aller p-Sylowgruppen von G, und $s_p(G) := |\mathrm{Syl}_p(G)|$ ihre Anzahl.

Bemerkungen 3.84.

1. Ist $|G| = p^r m$ mit $p \nmid m$, so sind die p-Sylowgruppen von G genau die Untergruppen von Ordnung p^r in G.
($|G| = [G : S] \cdot |S|$).

2. Ist G abelsch, so hat G für jede Primzahl $p \mid |G|$ genau eine p-Sylowgruppe, nämlich $S = \{x \in G : ord(x)$ ist eine Potenz von $p\}$.

3. $G = S_n$ hat eine 3-Sylowgruppe (A_3) und drei 2-Sylowgruppen (die Transpositionen).

4. $G = A_4$, $|A| = 12 = 2^2 \cdot 3$: eine 2-Sylowgruppe (V_4), vier 3-Sylowgruppen.

5. Jede zu einer p-Sylowgruppe von G konjugierte Untergruppe ist wieder eine p-Sylowgruppe von G.

Theorem 3.85 (Sylowsche Sätze)**.**
Sei G eine endliche Gruppe, p eine Primzahl.

(a) Jede p-Untergruppe von G ist in einer p-Sylowgruppe von G enthalten.

(b) Je zwei p-Sylowgruppen von G sind zueinander konjugiert.

(c) $s_p(G) \equiv 1 \mod p$. Insbesondere gibt es mindestens eine p-Sylowgruppe.

Korollar 3.86.
Sei $|G| = p^r \cdot m$ *mit* $m \not\equiv 0 \mod p$. *Dann hat* G *für jedes* $i = 0, 1, \ldots, r$ *eine Untergruppe der Ordnung* p^i.

Beweis:
Klar: nimm eine p-Sylowgruppe S und wende darauf Satz 3.82 an.

□

Bemerkung:
Der Fall $i = 1$ heißt der **Satz von Cauchy**: für jeden Primteiler p von G gibt es in G ein Element der Ordnung p.

Korollar 3.87.
Hat G *eine normale* p*-Sylowgruppe* ($S \trianglelefteq G$), *so ist diese die einzige* p*-Sylowgruppe (sofort aus 3.85 (b) und Normalteiler ist die einzige zu sich selbst konjugierte Untergruppe).*

Korollar 3.88.
Sei $|G| = p^r \cdot m$ *mit* $m \not\equiv 0 \mod p$.
Für die Anzahl $s_p = s_p(G)$ *gilt* $s_p \equiv 1 \mod p$ *und* $s_p \mid m$.

Beweis:
Alls p-Sylowgruppen sind zueinander konjugiert. Sei S eine von ihnen, dann ist also $s_p = |\{\text{zu } s \text{ konjugierte Untergruppen}\}| = [G : N_G(S)]$.
s ist $S \leq N_G(S) \leq G \Rightarrow s_p$ teilt m (da $[G : S] = m$).

□

Beweis: *(der Sylowschen Sätze 3.85)*
Sei $|G| = p^r \cdot m := n$ mit $m \not\equiv 0 \mod p$. Es ist also $\mathrm{Syl}_p(G)$ die Menge der p^r-elementigen Untergruppen von G.
Wir zeigen zunächst $\mathrm{Syl}_p(G) \neq \emptyset$: sei X die Menge aller p^r-elementigen *Teilmengen* von G. Auf X operiert G durch $G \times X \to X$, $(g, A) \mapsto gA$.
Wir wollen die Bahnengleichung anwenden.

Behaupte: $\binom{n}{p^r} = |X| \equiv m \mod p$.

$$\underbrace{(1+t)^n}_{=\sum_{i=0}^{n}\binom{n}{i}t^i} = ((1+t)^{p^r})^m \equiv (1+t^{p^r})^m = \sum_{j=0}^{m}\binom{m}{j}t^{p^r j} \mod p.$$

Betrachte darin die Koeffizienten von t^{p^r}: $\binom{n}{p^r} \equiv \binom{m}{1} = m \mod p$.
Wegen $|X| \equiv m \not\equiv 0 \mod p$ gibt es also eine Menge $A \in X$, deren G-Bahn in X eine

nicht durch p teilbare Länge hat. Sei $G_A := \{g \in G : gA = A\}$, dann $[G : G_A] \equiv m \not\equiv 0 \mod p$.
Andererseits ist aber $|G| \leq |A| = p^r$. Daraus folgt $|G_A = p^r$: $p^r \cdot m = n = |G| = \underbrace{|G_A|}_{\leq p^r} \cdot \underbrace{[G : G_A]}_{\text{Teiler von } m}$.
Also ist G_A eine p-Sylowgruppe.

Sei jetzt S eine p-Sylowgruppe von G und $H \leq G$ eine p-Untergruppe von G. Dann $\exists\, g \in G : H \leq gSg^{-1}$. *(Damit (a) und (b) gezeigt)*
Betrachte die Operation von H auf G/S: $(h, gS) \mapsto hgS$. Wegen $[G : S] = m \not\equiv 0 \mod p$ gibt es einen Fixpunkt: also ein gS mit $HgS = gS \Leftrightarrow g^{-1}Hg \leq S$.

Beweis von (c):
Sei $Y := \mathrm{Syl}_p(G)$, sei S eine p-Sylowgruppe, S operiere auf Y durch Konjugation $(s, P) \mapsto sPs^{-1}$. Seien $S = P_1, P_2, \ldots, P_k$ Vertreter der verschiedenen S-Bahnen in Y. Behaupte: die von $\{P_1 = S\}$ verschiedenen Bahnen haben Länge $\equiv 0 \mod p$ (oder: S ist der einzige Fixpunkt unter der Operation). Denn: sei $P \neq S$ eine andere p-Sylowgruppe. Angenommen, $S \leq N_G(P)$: dann hätte $N_G(P)$ mindestens zwei verschiedene p-Sylowgruppen S und P, von denen eine, P normal ist: Widerspruch zu Folgerung (s.o.) aus (b).

Somit ist $s_p \equiv 1 \mod p$.

□

3.89 (Gruppen der Ordnung pq)**.**
Seien $p < q$ zwei Primzahlen. Sei G eine Gruppe mit $|G| = pq$. Dann ist $s_q(G) \equiv 1 \mod q$ und $s_q(G) \mid p \Rightarrow s_q(G) = 1$.
Sei T die (normale) q-Sylowgruppe von G, also $T \cong C_q$.

Ist $q \not\equiv 1 \mod p$, so ist auch $s_p(G) = 1$, also ist dann $G \cong C_p \times C_q = C_{pq}$.

Sei $q \equiv 1 \mod p$, und sei $s_p(G) = q$. Sei $S \in \mathrm{Syl}_p(G)$. Dann ist $G = T \rtimes S$ ($T \cap S = \{e\}$, wegen $|T|, |S|$ teilerfremd).
$G \cong C_q \rtimes C_p$. Was ist $C_p \to \mathrm{Aut}(C_q)$?
$\mathrm{Aut}(C_q) \cong (Z/q\mathbb{Z})^* \cong C_{q-1}$. Da C_{q-1} genau eine Untergruppe der Ordnung p hat, gibt es bis auf Wechsel des Erzeugers von C_p genau eine nichttriviale Operation von C_p auf C_q.

Also haben wir gezeigt:

Satz 3.90.
Seien $p < q$ zwei Primzahlen. Es gibt, bis auf $\cong$, höchstens zwei Gruppen der Ordnung pq:

(1) C_{pq};

(2) nur falls $q \equiv 1 \mod p$*: die nichtabelsche Gruppe* $C_q \rtimes C_p = \langle x \rangle \rtimes \langle y \rangle$*, wobei* y *auf* $\langle x \rangle$ *durch* $yxy^{-1} = x^s$ *mit einer primitiven p-Einheitswurzel* $\mod q$ *(d.h.* $s^p \equiv 1 \not\equiv s \mod q$*).*

Bemerkung 3.91.

1. Sei $q = kp + 1$ mit $k \in \mathbb{N}$. Die Gruppe (2) aus Satz 3.90 ist isomorph zur Untergruppe $\left\{ \begin{pmatrix} a^k & b \\ 0 & 1 \end{pmatrix} : a, v \in \mathbb{F}_q, a \neq 0 \right\}$ von $GL_2(\mathbb{F}_q)$.
2. Jede Gruppe der Ordnung 15, 33, 35, 51, ... ist also zyklisch.

Beispiel 3.92.
Eine typische Anwendung der Sylow-Sätze ist, zu zeigen, dass eine Gruppe eine normale Sylowgruppe hat. Siehe Aufgabe 47 für Beispiele. Hier ist ein explizites Beispiel:

Betrachten wir eine Gruppe G mit $|G| = 30 = 2 \cdot 3 \cdot 5$.
Behaupte: G hat eine normale 3- oder 5- Sylowgruppe.
$s_2 \in \{1, 3, 5, 15\}, s_3 \in \{1, 10\}, s_5 \in \{1, 6\}$.
Angenommen, $s_3 \neq 1, s_5 \neq 1 \Rightarrow \underbrace{s_3 = 10}_{\text{von Ordnung 3}}$, $\underbrace{s_5 = 6}_{\text{von Ordnung 5}}$.
Dies ergibt $10 \cdot 2 = 20$ Elemente der Ordnung 3 und $6 \cdot 4 = 24$ Elemente der Ordnung 5 $\Rightarrow |G| \geq 44 \rightarrow$ Widerspruch.

3.93 (Gruppen kleiner Ordnung?)**.**
Bis Ordnung 15 (außer Ordnung 12) sind oben bereits behandelt.

Satz 3.94.
Es gibt genau fünf Gruppen der Ordnung 12: die abelschen Gruppen C_{12} *und* $C_6 \times C_2$ *und die nichtabelschen Gruppen* A_4, D_6 *und* $C_3 \rtimes C_4$ *(dabei gibt es nur eine Weise, dieses* $\rtimes$ *so zu bilden, dass es kein* $\times$ *ist:* $C_3 \rtimes C_4 = \langle x \rangle \rtimes \langle y \rangle$ *mit* $yxy^{-1} = x^{-1}$*).*

Beweis:
Sei $|G| = 12$, G nichtabelsch.
$12 = 2^2 \cdot 3$: $s_2 \in \{1, 3\}, s_3 = \{1, 4\}$. Wegen G nichtabelsch ist $s_2 > 1$ oder $s_3 > 1$.

1. Fall $s_3 = 4$: G operiert auf der 4-elementigen Menge $\mathrm{Syl}_3(G)$ durch Konjugation (transitiv). Wegen $s_3 = 4 = [G : N_G(S)]$ für $S \in \mathrm{Syl}_3(G)$ ist $N_G(S) = S \Rightarrow G$ operiert treu.
Also ist G eine 12-elementige Untergruppe von $S_4 \Rightarrow G \cong A_4$.

2. Fall $s_3 = 1, s_2 = 3$: Sei $U \trianglelefteq G$ die 3-Sylowgruppe, sei V eine 2-Sylowgruppe: $U \cong C_3$, $V \cong C_4$ oder $V \cong C_2 \times C_2$. $G = U \rtimes V$:
ist $V = C_4$, so ist $G = C_3 \times C_4$; ist $V = C_2 \times C_2$, so ist $G = D_6$.

□

Ziel: A_5 ist die kleinste nichtzyklische einfache Gruppe.

Satz 3.95.
Seien p, q, r verschiedene Primzahlen. Jede Gruppe G von Ordnung pq oder p^2q oder pqr hat eine normale Sylowgruppe.

Beweis:
pq: Satz 3.90, die anderen: Aufgabe 47.

□

Satz 3.96.
Es gibt keine nichtzyklische einfache Gruppe von Ordnung kleiner als 60.

Beweis:
Angenommen, $|G| = n < 60$, G einfach, nicht zyklisch.
Nach Satz 3.95 folgt: $n \in \{24, 36, 40, 48, 54, 56\}$ Jede dieser Ordnungen ergibt einen Widerspruch:

$n = 24, 48$: sei $S \in \mathrm{Syl}_2(G)$. Operation von G auf G/S: $|G/S| = 3$ ergibt einen Homomorphismus $G \to \mathrm{Sym}(G/S) \cong S_3$. Dieser ist nicht konstant, also injektiv wegen G einfach. $\Rightarrow G \hookrightarrow S_3 \to$ Widerspruch, wegen $|S_3| = 6$.

$n = 36$: analog mit $S \in \mathrm{Syl}_3(G)$: $|G/S| = 4$: $G \hookrightarrow S_4 \rightarrow$ Widerspruch, wegen $|S_4| = 24$.

$n = 40$: $40 = 2^3 \cdot 5 \Rightarrow s_5 = 1 \Rightarrow$ normale Sylowgruppe.

$n = 54$: $54 = 2 \cdot 3^3 \Rightarrow s_3 = 1$.

$n = 56$: $56 = 2^3 \cdot 7 \Rightarrow s_7 = 1$ ($\Rightarrow$ normal) oder $s_7 = 8$. Ist $s_7 = 8$, so gibt es $8 \cdot (7-1) = 48$ Elemente der Ordnung 7 $\Rightarrow s_2 = 1$ ($\Rightarrow$ normal).

□

Theorem 3.97.
A_5 ist die einzige einfache nichtzyklische Gruppe von Ordnung kleiner oder gleich 60.

Beweis:
Sei $|G| \leq 60$, G einfach, nicht zyklisch. $\Rightarrow |G| = 60$ (nach 3.96).
Sei $H \lneqq G$, $[G : H] = m$. Dann ergibt die Operation von G auf G/H einen injektiven Homomorphismus $G \hookrightarrow \mathrm{Sym}(G/H) \cong S_m$. Also ist $m \geq 5$, und aus $m = 5$ folgt $[S_5 : G] = 2 \Rightarrow G \cong A_5$. Also genügt es, zu zeigen, G hat eine Untergruppe $H \neq G$ vom Index ≤ 5.
Angenommen, dies ist falsch, d.h. $[G : H] \geq 6 \ \forall \ H < G$. Zähle Sylowgruppen: $s_p = [G : N_G(S)] \geq 6 \ \forall \ p = 2, 3, 5$.
$\Rightarrow s_2 = 15$, $\underbrace{s_3 = 10}_{\Rightarrow 10 \cdot 2 = 20 \text{ Elemente}}$, $\underbrace{s_5 = 6}_{\Rightarrow 6 \cdot 4 = 24 \text{ Elemente}}$.
Seien $P_1 \neq P_2 \in \mathrm{Syl}_2(G)$. $|P_1| = |P_2| = 4$. Sei $H := \langle P_1 \cup P_2 \rangle \leq G$.
$\Rightarrow H = G$ (wegen $[G : H] \geq 6$ sonst).
P_1, P_2 sind beide abelsch. Falls $P_1 \cap P_2 =: P \neq \{e\}$, so $|P| = 2$. P zentralisiert P_1 und P_2, also $P \subset Z(G)$: Widerspruch.
$\Rightarrow$ es gibt in den 2-Sylowgruppen $15 \cdot 3 = 45$ Elemente.

Insgesamt gibt es also zu viele Elemente, $\rightarrow$ Widerspruch.

□

f. Auflösbare Gruppen

Definition 3.98.
Sei G eine endliche Gruppe.

(a) Eine Folge
$G = H_0 \gneqq H_1 \gneqq H_2 \gneqq \ldots \gneqq H_n = \{e\}$ (*)
von Untergruppen von G heißt eine **Kompositionsreihe** von G, wenn gilt:

(i) $H_i \trianglelefteq H_{i-1}$ für $i = 1, \ldots, n$;

(ii) die Faktorgruppen H_{i-1}/H_i für $i = 1, \ldots, n$ sind einfache Gruppen (evtl. zyklisch).

(b) Die H_{i-1}/H_i für $i = 1, \ldots, n$ heißen die **Kompositionsfaktoren** der Reihe (*).

Bemerkungen 3.99.

1. Ist $N \trianglelefteq G$, und ist $N = K_0 < \ldots < K_r = \{e\}$ eine Kompositionsreihe von N und $G/N = L_0/N < \ldots < L_S/N = N/N$ eine Kompositionsreihe von G/N, so ist $G = L_0 > L_1 > \ldots < L_S = N = K_0 > \ldots > K_r = \{e\}$ eine Kompositionsreihe von G.

2. Jede endliche Gruppe $G \neq \{e\}$ hat eine Kompositionsreihe:
ist G einfach, so ist $G > \{e\}$ eine Kompositionsreihe. Andernfalls gibt es ein $\{e\} \neq N \trianglelefteq G$ (mit $G \neq N$). Per Induktion können wir annehmen, dass N und G/N Kompositionsreihen haben. Mit 1. erhalte eine von G.

Satz 3.100 (Jordan-Hölder)**.**
Seien $G = H_0 > H_1 > \ldots > H_r = \{e\}$ und $G = K_0 > K_1 > \ldots > K_s = \{e\}$ zwei Kompositionsreihen von G.
Dann gilt $r = s$ und es gibt eine Permutation π von $\{1, \ldots, r\}$ mit $H_{i-1}/H_i \cong K_{\pi(i)-1}/K_{\pi(i)}$ für $i = 1, \ldots, r$.

Beweis:
Induktion nach $|G|$. Ist G einfach, so hat G nur die Kompositionsreihe $G > \{e\}$.
Ist $H_1 = K_1$, so fertig nach Induktion.
Sei $H_1 \neq K_1$. Wegen $H \lneqq H_1K_1 \trianglelefteq G$ ist $H_1K_1 = G$. Also $G/H_1 = (H_1K_1)/H_1 \cong K_1/(H_1 \cap K_1)$ und $G/K_1 = (H_1K_1)/K_1 \cong H_1/H_1 \cap K_1$.

Sei $H_1 \cap K_1 = M_0 > M_1 > \ldots < M_t = \{e\}$.
Dann sind
$H_1 > M_0 > M_1 > \ldots > M_t = \{e\}$ (I)

$K_1 > M_0 > M_1 > \ldots > M_t = \{e\}$ (II)
Kompositionsreihen.

Induktionsvoraussetzung anwenden auf H_1 und auf K_1:
$(G/H_1, H_1/H_2, \ldots, H_{r-1}/H_r) = (G/H_1, H_1/M_0, M_0/M_1, \ldots, M_{t-1}/M_t)$ (bis auf Permutation)
$(G/K_1, K_1/K_2, \ldots, K_{r-1}/K_r) = (G/K_1, K_1/M_0, M_0/M_1, \ldots, M_{t-1}/M_t)$ (bis auf Permutation)

Da $G/H_1 \cong K_1/M_0$ und $G/K_1 \cong H_1/M_0$, folgt die Behauptung.

□

Korollar 3.101.
Ist G eine endliche Gruppe, ist $G = H_0 > H_1 > \ldots > H_{r-1} > H_r = \{e\}$ mit $H_i \trianglelefteq H_{i-1}$ für $i = 1, \ldots, r$, so sind die Kompositionsfaktoren von G (mit Vielfachheit) genau die Vereinigung der Kompositionsfaktoren von $H_0/H_1, H_1/H_2, \ldots, H_{r-1}/H_r$ (mit Vielfachheit).

Definition 3.102 (auflösbare Gruppe)**.**
Eine endliche Gruppe G heißt **auflösbar**, wenn alle Kompositionsfaktoren von G (prim-)zyklisch sind.

Beispiele 3.103.

1. $S_n, n \geq 5$: eine Kompositionsreihe von S_n ist $S_n > A_n > \{id\}$; die Kompositionsfaktoren von S_n sind also C_2 und A_n. Also ist S_n für $n \geq 5$ nicht auflösbar; ebenso ist A_n für $n \geq 5$ nicht auflösbar.

   Für $n = 4$ ist $S_4 > A_4 > V_4 > C_2 > \{id\}$ eine Kompositionsreihe von S_4. Die Kompositionsfaktoren von S_4 sind also C_2, C_2, C_2, C_3, also ist S_4 auflösbar.

2. Jede Gruppe G mit $|G| < 60$ ist auflösbar. Denn alle Kompositionsfaktoren von G haben Ordnung < 60, sind also primzyklisch nach Satz 3.96.

Satz 3.104.
Sei G eine auflösbare endliche Gruppe, sei $|G| = p_1 \cdot \ldots \cdot p_r$ mit Primzahlen p_i. Dann sind die Kompositionsfaktoren von G genau $C_{p_1}, \ldots, C_{p_r}$.

Beweis:
Die Kompositionsfaktoren von G sind primzyklisch und das Produkt ihrer Ordnungen ist $|G|$.

□

Definition 3.105.
Sei G eine beliebige Gruppe.

(a) Für $x, y \in G$ heißt $[x, y] := xyx^{-1}y^{-1} \in G$ der **Kommutator** von x und y.

(b) Die von allen $[x, y]$ ($x, y \in G$) erzeugte Untergruppe von G heißt die Kommutatorengruppe von G und wird mit G' oder $[G, G]$ bezeichnet.
(manchmal kommt in der Literatur auch $[x, y] := x^{-1}y^{-1}xy$ *vor)*

Bemerkung 3.106.
$xy = [x, y] \cdot yx$. Also gilt: $[x, y] = e \Leftrightarrow xy = yx$.
$[x, y]$ als „Maß“ für die (Nicht-)Vertauschbarkeit von x und y.
Insbesondere: G ist abelsch $\Leftrightarrow G' = \{e\}$.

Satz 3.107.
$G' \trianglelefteq G$, und die Faktorgruppe $G^{ab} := G/G'$ ist abelsch.

Beweis:
$[gx, g^{-1}, gyg^{-1}] = gxg^{-1} \cdot gyg^{-1} \cdot gx^{-1}g^{-1}\dot{g}y^{-1}g^{-1} = g \cdot xyx^{-1}y^{-1}g^{-1} = g[x, y]g^{-1}$.
Also ist die Menge aller Kommutatoren stabil unter Konjugation mit beliebigen $g \in G$. Die von ihnen erzeugte Untergruppe G' also ebenfalls. $\Rightarrow G' \trianglelefteq G$.

Lies $xy = \underbrace{[x, y]}_{\in G'} \cdot yx$ in G/G':

$\overline{xy} = \overline{yx}$ in G/G' $\quad \forall\ \overline{x}, \overline{y} \in G/G'$.

□

Bemerkungen 3.108.

1. $G^{ab} = G/G'$ heißt auch die abelsch gemachte Gruppe G (oder Abelianisierung von G), aus folgendem Grund: G^{ab} ist „die größte“ abelsche Faktorgruppe von G in folgendem Sinn: für jeden Normalteiler N von G mit G/N abelsch gilt $G' \leqq N$, d.h. G/N ist ein epimorphes Bild von $G/G' = G^{ab}$.
2. Ist $f : G \to A$ ein Homomorphismus von G in eine abelsche Gruppe A, so ist $G' \leq \ker(f)$, denn $f[x, y] = [f(x), f(y)] = e$.

Definition 3.109.
Die höheren Kommutatorgruppen sind induktiv definiert durch $G^{(0)} := G$, $G^{(1)} := G' = [G, G]$, $G^{(i+1)} := (G^{(i)})' = [G^{(i)}, G^{(i)}]$.

Es gilt $G \geq G' \geq G^{(2)} \geqq \ldots$

Bemerkungen 3.110.

1. Ist $H \leq G$, so auch $H^{(n)} \leq G^{(n)}$ für alle $n \geq 1$. Beweis durch Induktion nach n.
2. Ist $N \trianglelefteq G$, so ist $(G/N)' = (G'N)/N$, allgemeiner $(G/N)^{(n)} = G^{(n)}N/N \ \forall\, n \geq 1$. Beweis durch Induktion nach n. $n = 1$: $(G/N)' = \left\langle \underbrace{[xN, yN]}_{=[x,y]N} : x, y \in G \right\rangle = \langle [x, y]N : x, y \in G \rangle = (G'N)/N \leq G/N$.

Satz 3.111.
Für jede endliche Gruppe G gilt: G ist auflösbar $\Leftrightarrow \ \exists\, n \in \mathbb{N}$ *mit* $G^{(n)} = \{e\}$.

Beweis:
(i) $\Rightarrow$ (ii): sei $G = H_0 > H_1 > \ldots > H_r = \{e\}$ eine Kompositionsreihe von G, wir beweisen durch Induktion nach r.
G/H_1 ist zyklisch $\Rightarrow G' \leq H_1$. Da H_1 auflösbar ist gibt es $m \in \mathbb{N}$ mit $(H_1)^{(m)} = \{e\} \Rightarrow G^{(m+1)} = (G')^{(m)} = \{e\}$.

(ii) $\Rightarrow$ (i): habe die Reihe $G \geq G' \geq G^{(2)} \geq \ldots \geq G^{(n)} = \{e\}$.
Alle Faktorgruppen $G^{(i)}/G^{(i-1)}$ dieser Reihe sind abelsch, haben also zyklische Kompositionsfaktoren $\Rightarrow G$ hat zyklische Kompositionsfaktoren (Korollar 3.101). □

Definition 3.112 (Verallgemeinerung von auflösbar auf beliebige Gruppen)**.**
Eine Gruppe G heißt **auflösbar**, falls $\exists\, n \in \mathbb{N}$ mit $G^{(n)} = \{e\}$.

Korollar 3.113.
Sei G eine Gruppe.

(a) G ist auflösbar, $H \leq G \Rightarrow$ *H ist auflösbar;*

(b) G ist auflösbar, $N \trianglelefteq G \Rightarrow G/N$ *ist auflösbar.*

Beweis:

(a) $G^{(n)} = \{e\} \Rightarrow H^{(n)} \leq G^{(n)} = \{e\}$.

(b) $G^{(n)} = \{e\} \Rightarrow (G/N)^{(n)} = (G^{(n)}N)/N = N/N = \{e\}$.

□

Beispiele 3.114.

1. Jede endliche p-Gruppe (p eine Primzahl) ist auflösbar. Denn $\exists\, N \trianglelefteq G$ mit $G/N \cong C_p$ (Satz 3.82). Iteriere dies $\Rightarrow$ G hat Kompositionsreihe mit lauter Faktoren C_p.

2. Sei $G = D_n$, Diedergruppe, $|D_n| = 2n$.
   $G = \langle \sigma, \tau : \sigma^n = \tau^2 = (\sigma\tau)^2 = e \rangle = \langle \sigma \rangle \rtimes \langle \tau \rangle \cong C_n \rtimes C_2$.
   Kommutatoren: $G = \{\sigma^i, \sigma^i\tau : i = 0, \ldots, n-1\}$; $[\sigma^i, \sigma^j\tau] = \sigma^i \cdot \sigma^j\tau \cdot \sigma^{-i} \cdot (\sigma^j\tau)^{-1} = \sigma^{i+j+i-j} = \sigma^{2i}$
   $[x, y] = [y, x]^{-1}$
   $[\sigma^i\tau, \sigma^j\tau] = \ldots = \sigma^{2(i-j)}$.

   Also ist $G' = \left\langle \sigma^{2i} : i = 0, \ldots, n-1 \right\rangle$, also ist $[D_n, D_n] = \langle \sigma^2 \rangle = \begin{cases} \langle \sigma \rangle \cong C_n & \text{, falls } n \text{ ungerade;} \\ \langle \sigma^2 \rangle \cong C_{\frac{n}{2}} & \text{, falls } n \text{ gerade.} \end{cases}$

3. für $\mathbb{K}$ ein Körper sei $G = GA_1(\mathbb{K}) = \{\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a, b \in \mathbb{K}, a \neq 0\} \cong \{(x \mapsto ax + b, \mathbb{K} \to \mathbb{K}) : a, b \in \mathbb{K}, a \neq 0\} = \mathbb{K} \rtimes \mathbb{K}^*$. Diese Gruppe ist auflösbar mit $G^{(2)} = \{e\}$, denn die Reihe $G \trianglerighteq K \times \{1\} \trianglerighteq \{e\}$ hat die abelschen Faktorgruppen $\mathbb{K}^*, \mathbb{K}$.

4. $[S_n, S_n] =?$
   $[S_n, S_n] = A_n$ für $n \geq 5$; $S_n^{ab} = C_2$.
   Das stimmt auch für $n \leq 4$ (Übung!).

Definition 3.115 (elementar-abelsche p-Gruppe)**.**
Eine **elementar-abelsche p-Gruppe** (p eine Primzahl) ist eine abelsche Gruppe, die zu $\underbrace{C_p \times \ldots \times C_p}_{n-mal} \cong \underbrace{(\mathbb{Z}/p) \oplus \ldots \oplus (\mathbb{Z}/p)}_{n-mal}$ für ein $n \geq 0$ isomorph ist.

Lemma 3.116.
Sei G eine endliche auflösbare Gruppe, und $N \trianglelefteq G$ ein minimaler Normalteiler ($\neq \{e\}$) von G. Dann ist N eine elementar-abelsche p-Gruppe (für ein p).

Beweis:
N ist auflösbar, also $N' \neq N \Rightarrow N' \trianglelefteq G$.

(Übung: $N \trianglelefteq G \Rightarrow N' \trianglelefteq G$).
Wegen N minimal folgt $N' = \{e\}$, d.h. N ist abelsch. Jede Sylowgruppe von N ist Normalteiler von N ist normal in G. Wegen N minimal folgt N ist eine (abelsche) p-Gruppe.
Sei $A := \{x \in N : x^p = e\}$ $A \trianglelefteq G$, $A \leq N$, $A \neq \{e\} \Rightarrow A = N$ (wegen N minimal).

□

Theorem 3.117 (Galois)**.**
*Sei p eine Primzahl, sei G eine **transitive** Untergruppe von S_p. Es sind äquivalent:*

(i) *G ist auflösbar;*

(ii) *G ist konjugiert (in S_p) zu einer Untergruppe von $GA_1(\mathbb{F}_p) = \{(\mathbb{F}_p \to \mathbb{F}_p, x \mapsto ax + b) : a, b \in \mathbb{F}_p, a \neq 0\}$.*

(iii) *G hat eine normale p-Sylowgruppe;*

(iv) *es gibt $x \neq y$ in $\{1, \ldots, p\}$ mit $G_x \cap G_y = \{e\}$.*
$[G_x := \{g \in G : gx = x\}]$

Sind (i) bis (iv) erfüllt, so gilt (iv) sogar für beliebige $x \neq y$.

Beweis:
Sei $N \neq \{e\}$ ein minimaler Normalteiler von G. $\Rightarrow p \mid |N|$:
seien $x, y \in \{1, \ldots, p\} \Rightarrow$ $\exists\, g \in G$ mit $y = gx$ (wegen S_p transitiv) $\Rightarrow Ny = Ngx = g(Nx)$.
$\Rightarrow |Ny| = |Nx| \Rightarrow$ alle N-Bahnen haben die selbe Länge, und diese teilt $p \Rightarrow$ wegen $N \neq \{e\}$ ist auch N transitiv auf $\{1, \ldots, p\} \Rightarrow p \mid |N|$

(i) $\Rightarrow$ (iii): sei G auflösbar. Jeder minimale Normalteiler von G ist eine elementarabelsche p-Gruppe nach eben und nach Lemma 3.116.
Wegen $p^2 \nmid |S_p| = p!$ ist also N zyklisch von Ordnung $p \Rightarrow N$ ist eine (die einzige) p-Sylowgruppe von G.

(iii) $\Rightarrow$ (ii): sei $N = \langle g \rangle$ die normale p-Sylowgruppe, dann ist g ein p-Zykel.
Wir können annehmen: $g = (123 \ldots p)$. Also: g ist die Abbildung $x \mapsto x + 1$ von $F := \mathbb{F}_p$ in sich.
Sei $h \in G$. Wegen $N \trianglelefteq G$ $\exists\, a \in \{1, \ldots, p-1\}$ mit $hgh^{-1} = g^a \Rightarrow hg = g^a h$.
$\Rightarrow$ für $x \in F$: $h(x+1) = hg(x) = g^a h(x) = h(x) + a \Rightarrow h(1) = h(0) + a$, $h(2) = h(0) + 2a$ usw. $\Rightarrow h(x) = \underbrace{h(0)}_{=:b} + ax \;\; \forall\, x$.

(ii) $\Rightarrow$ (iv): für $g \neq e$ in $GA(\mathbb{F}_p)$ hat g höchstens einen Fixpunkt in $\mathbb{F}_p$: $g = (x \mapsto ax+b)$, $x = ax + b, y = ay + b \Rightarrow (a-1)(x-y) = 0$ OK

(iv) $\Rightarrow$ (iii): es gebe $x \neq y$ mit $G_x \cap G = \{e\}$. Die Abbildung $G_x \to \{1, \ldots, p\} \setminus \{x\}, g \mapsto gy$ ist dann injektiv. ($g, h \in G_x$, $gy = hy \Rightarrow (h^{-1}g)y = y \Rightarrow h^{-1}g \in G_x \cap G_y = \{e\}$)
$\Rightarrow |G_x| \leq p-1$; $[G : G_x] = p \Rightarrow |G| \leq p(p-1)$.
Angenommen, es gäbe zwei verschiedene p-Sylowgruppen P, Q: dann ist $P \cap Q = \{e\} \Rightarrow |\{pq : p \in P, q \in Q\}| = p^2 \to$ Widerspruch zu $|G| \leq p(p-1)$.

(iii) $\Rightarrow$ (i): G habe eine normale p-Sylowgruppe N: $|N| = p$.
$\Rightarrow C_G(N) = N$. Denn: in S_p gibt es $\frac{p!}{p} = (p-1)!$ p-Zykel. Diese sind alle zueinander konjugiert.
$\Rightarrow$ sie sind alle selbstzentralisierend: $\sigma \in S_p$ ein p-Zykel $\Rightarrow C_{S_p}(\sigma) = \langle\sigma\rangle$.
Also ist der Homomorphismus $G/N \to \mathrm{Aut}(N), gN \mapsto \mathrm{int}_g \,|_N$ injektiv (wegen $(\mathrm{int}_g)\,|_N = id_N \Leftrightarrow \forall\, x \in N\ gxg^{-1} = x \Rightarrow g \in C_G(N)$).
$\mathrm{Aut}(N) = (\mathbb{Z}/p)^* \cong C_{p-1}$ ist abelsch $\Rightarrow G/N$ ist abelsch; außerdem ist N abelsch $\Rightarrow$ G ist auflösbar (mit $G^{(2)} = \{e\}$).

□

4. Körpertheorie II (Galoistheorie)

Erinnerung 4.1.
Sei $\mathbb{L}/\mathbb{K}$ eine algebraische Körpererweiterung. Jedes $\alpha \in \mathbb{L}$ erfüllt die Identität $\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_0 = 0$ ($a_i \in \mathbb{K}$).
Das normierte $f(t) \in \mathbb{K}[t]$ von kleinstem Grad mit $f(\alpha) = 0$ heißt $f = \mathrm{MinPol}(\alpha/\mathbb{K})$, ist irreduzibel mit $d := \deg(f) = \deg(\alpha/\mathbb{K}) = [\mathbb{K}(\alpha) : \mathbb{K}]$.
Kennt man $f = \mathrm{MinPol}(\alpha/\mathbb{K})$, so kann man in $\mathbb{K}(\alpha)$ rechnen: $\mathbb{K}[t]/(f) \to_\sim \mathbb{K}(A)$: Elemente in $\mathbb{K}(\alpha)$ haben eine eindeutige Darstellung $b_0 + b_1\alpha + \ldots + b_{d-1}\alpha^{d-1} = g(\alpha)$ mit $b_i \in \mathbb{K}$.
$g_1(\alpha) \cdot g_2(\alpha) = (g_1 g_2)(\alpha)$. Dividiere durch f mit Rest, um dieses Element auf obige Form zu bringen.

Sei $\overline{\mathbb{K}}$ der algebraische Abschluss von $\mathbb{K}$.
Es gibt eine Bijektion von $\{\beta \in \overline{\mathbb{K}} : f(\beta) = 0\}$ auf $\mathrm{Hom}_{\mathbb{K}}(\mathbb{K}(\alpha), \overline{\mathbb{K}})$: $(\beta = \varphi(\alpha)) \leftarrow\!\shortmid (\varphi : \mathbb{K}(\alpha) \to_{\mathbb{K}} \overline{\mathbb{K}})$.
Die Nullstellen von $f(t)$ in $\overline{\mathbb{K}}$ heißen die $\mathbb{K}$-Konjugierten von α. Es gibt davon also höchstens d Stück in $\overline{\mathbb{K}}$.
Dies sind genau die $\beta = \sigma(\alpha)$ mit $\sigma \in \mathrm{Aut}(\overline{\mathbb{K}}/\mathbb{K})$.

α heißt separabel, wenn $f(t)$ d verschiedene Nullstellen in $\overline{\mathbb{K}}$ hat. Das kann höchstens für $char(\mathbb{K}) = p > 0$ schiefgehen: irreduzibles $f(t) \in \mathbb{K}[t]$ ist inseparabel $\Leftrightarrow$ $f \in \mathbb{K}[t^p]$.

($\mathbb{L}/\mathbb{K}$ algebraisch): $\mathbb{L}_s = \{\alpha \in \mathbb{L} : \alpha/\mathbb{K}$ ist separabel$\}$ ist ein Zwischenkörper.
$[\mathbb{L}_s : \mathbb{K}] = [\mathbb{L} : \mathbb{K}]_s = |\mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \overline{\mathbb{K}})|$
$(\mathbb{L} \underbrace{\dashleftarrow\dashrightarrow}_{\text{rein inseparabel}} \mathbb{L}_s \underbrace{\dashleftarrow\dashrightarrow}_{\text{separabel}} \mathbb{K}$.

Satz vom primitiven Element: $\mathbb{L}/\mathbb{K}$ separabel, $[\mathbb{L} : \mathbb{K}] < \infty \Rightarrow \exists\ \alpha \in \mathbb{L}$ mit $\mathbb{L} = \mathbb{K}(\alpha)$.

$\mathbb{L}/\mathbb{K}$ sei eine endliche Körpererweiterung. $\overline{\mathbb{K}}$ = der algebraische Abschluss von $\mathbb{K}$, der $\mathbb{L}$ enthält.
$\mathrm{Aut}(\overline{\mathbb{K}}/\mathbb{K}) = \{\sigma : \overline{\mathbb{K}} \to_\sim \overline{\mathbb{K}} : \sigma|_{\mathbb{K}} = id\}$.

Satz 4.2.
Es sind äquivalent für $\mathbb{L}/\mathbb{K}$*:*

(i) Für jede Erweiterung $\mathbb{E}/\mathbb{L}$ *und jeden* $\mathbb{K}$*-Homomorphismus* $\varphi : \mathbb{L} \to_{\mathbb{K}} \mathbb{E}$ *gilt*

$\varphi(\mathbb{L}) = \mathbb{L}$;

(ii) $\forall\, \sigma \in \mathrm{Aut}(\overline{\mathbb{K}}/\mathbb{K})$ *ist* $\sigma(\mathbb{L}) = \mathbb{L}$;

(iii) $\forall\, \alpha \in L$ *liegen alle* $\mathbb{K}$*-Konjugierten von* α *in* $\mathbb{L}$;

(iv) jedes irreduzible $f \in \mathbb{K}[t]$*, welches eine Nullstelle in L hat, zerfällt über* $\mathbb{L}$;

(v) $\exists\, f \in \mathbb{K}[t]$ *(evtl. reduzibel) mit* $\mathbb{L} = Zfk(f/\mathbb{K})$.

Beweis:
(i) $\Rightarrow$ (ii): klar. ($\mathbb{E} := \overline{\mathbb{K}}, \varphi := \sigma\,|_i$)

(ii) $\Rightarrow$ (iii): die $\mathbb{K}$-Konjugierten von α sind die $\sigma(\alpha)$ mit $\sigma \in \mathrm{Aut}(\overline{\mathbb{K}}/\mathbb{K})$.

(iii) $\Rightarrow$ (iv): sei $f \in \mathbb{K}[t]$ irreduzibel, sei $\alpha \in \mathbb{L}$ mit $f(\alpha) = 0$, sei $f = (t-\alpha)(t-\alpha_2) \cdot \ldots \cdot (t-\alpha_n)$, $\alpha_i \in \overline{\mathbb{K}}$; die $\alpha_2, \ldots, \alpha_n$ sind die $\mathbb{K}$-Konjugierten von α, liegen also in $\mathbb{L}$ nach (iii).

(iv) $\Rightarrow$ (v): sei $\mathbb{L} = \mathbb{K}(\alpha_1, \ldots, \alpha_n)$, sei $f_i := \mathrm{MinPol}(\alpha_i/\mathbb{K})$, $f := f_1 \cdot \ldots \cdot f_n$: $\mathbb{L} = Zfk(f_1 \cdot \ldots \cdot f_n)$ nach (iv).

(v) $\Rightarrow$ (i): sei $\mathbb{L} = \mathrm{Zfk}(f/\mathbb{K})$: $f(t) = (t-\alpha_1) \cdot \ldots \cdot (t-\alpha_n)$, also $\mathbb{L} = \mathbb{K}(\alpha_1, \ldots, \alpha_n)$. $\varphi(a_1), \ldots, \varphi(\alpha_n) \in \mathbb{E}$ sind Nullstellen von $f(t)$ in $\mathbb{E} \Rightarrow \{\varphi(\alpha_1), \ldots, \varphi(\alpha_n)\} = \{\alpha_1, \ldots, \alpha_n\} \subset \mathbb{L} \Rightarrow \varphi(\mathbb{L}) \subset \mathbb{L}$.

□

Definition 4.3.
Man nennt $\mathbb{L}/\mathbb{K}$ eine **normale Erweiterung**, wenn die Bedingungen (i) bis (v) gelten.

Satz 4.4.
Sei $\mathbb{E}/\mathbb{K}$ *eine endliche Erweiterung, seien* $\mathbb{L}, \mathbb{M}$ *Zwischenkörper von* $\mathbb{E}/\mathbb{K}$.

(a) $\mathbb{L}/\mathbb{K}, \mathbb{M}/\mathbb{K}$ *normal* $\Rightarrow \mathbb{L}\mathbb{M}/\mathbb{K}, (\mathbb{L} \cap \mathbb{M})/\mathbb{K}$ *normal;*

(b) $\mathbb{E}/\mathbb{K}$ *normal* $\Rightarrow \mathbb{E}/\mathbb{L}$ *normal;*

(c) $\mathbb{L}/\mathbb{K}$ *normal* $\Rightarrow \mathbb{L}\mathbb{M}/\mathbb{M}$ *normal.*

Beweis:
Leicht aus 4.2: (a) aus (ii); (b) und (c) aus (v).

□

Beispiele 4.5.

1. Sei $[\mathbb{L} : \mathbb{K}] = 2$. Dann ist $\mathbb{L}/\mathbb{K}$ normal: sei $\alpha \in \mathbb{L} \setminus \mathbb{K} \Rightarrow \mathbb{K}(\alpha)$, sei $f = \mathrm{MinPol}(\alpha/\mathbb{K})$: $\deg(f) = 2$, $f = (t-\alpha)(t-\beta)$ mit $\beta \in \mathbb{L} \Rightarrow \mathbb{L} = \mathrm{Zfk}(f/\mathbb{K})$.

2. Sei $\mathbb{K} = \mathbb{Q}$, $\mathbb{L} = \mathbb{Q}(\alpha)$, $\alpha = \sqrt[4]{2} \in \mathbb{R}$, $\alpha^4 = 2$.
   $\mathbb{Q}(\alpha)/\mathbb{Q}$ ist nicht normal. Denn die $\mathbb{Q}$-Konjugierten von α sind $\alpha, -\alpha, i\alpha, -i\alpha$ ($i = \sqrt{-1}$); $\mathbb{Q}(\alpha) \subset \mathbb{R}$, also $\pm i\alpha \notin \mathbb{Q}(\alpha)$.
   Es ist $\mathbb{Q}(i\alpha)/\mathbb{Q}$ ebenfalls nicht normal, denn $\mathbb{Q}(i\alpha) \cong_{\mathbb{Q}} \mathbb{Q}(\alpha)$.
   Die Eigenschaft normal für $\mathbb{L}/\mathbb{K}$ hängt nur von der $\mathbb{K}$-Isomorphieklasse von $\mathbb{L}$ ab.
   Deswegen macht es Sinn, zu sagen, „$\mathbb{Q}\sqrt[4]{2}/\mathbb{Q}$ ist nicht normal“ ohne zu sagen, welche vierte Wurzel man meint.

3. $\mathbb{Q} \underbrace{\subset}_{\text{Grad } 2} \mathbb{Q}(\sqrt{2}) \underbrace{\subset}_{\text{Grad } 2} \mathbb{Q}(\alpha)$: jede der beiden Teilerweiterungen ist (nach 1.) normal, aber die zusammengesetzte Erweiterung (nach 2.) nicht. Normalität ist also nicht transitiv.

Lemma 4.6.
Sei $\mathbb{L}/\mathbb{K}$ eine normale Erweiterung, sei $\mathbb{K} \subset \mathbb{F} \subset \mathbb{L}$ ein Zwischenkörper, sei $\varphi : \mathbb{F} \to \overline{\mathbb{K}}$ ein $\mathbb{K}$-Homomorphismus. Dann ist $\varphi(\mathbb{F}) \subset \mathbb{L}$, und $\exists\, \sigma \in \mathrm{Aut}(\mathbb{L}/\mathbb{K})$ mit $\varphi = \sigma|_{\mathbb{F}}$.

Beweis:
φ lässt sich fortsetzen zu einem $\widetilde{\varphi} : \mathbb{L} \to \overline{\mathbb{K}}$ (nach 2.45). $\mathbb{L}/\mathbb{K}$ normal $\Rightarrow \widetilde{\varphi}(\mathbb{L}) \subset \mathbb{L}$, also $\widetilde{\varphi} \in \mathrm{Aut}(\mathbb{L}/\mathbb{K})$, $\sigma := \widetilde{\varphi}$.

□

Satz 4.7.
Sei $\mathbb{L}/\mathbb{K}$ endlich. Dann sind äquivalent:

(i) $\mathbb{L}/\mathbb{K}$ *ist separabel und normal;*

(ii) $\forall\, \alpha \in \mathbb{L}$ *zerfällt MinPol*$(\alpha/\mathbb{K})$ *über* $\mathbb{L}$ *in verschiedene Linearfaktoren;*

(iii) $\exists$ *ein separables* $f \in \mathbb{K}[t]$ *mit* $\mathbb{L} = Zfk(f/\mathbb{K})$*;*

(iv) wie (iii), zusätzlich f ist irreduzibel;

(v) $|\mathrm{Aut}(\mathbb{L}/\mathbb{K})| = [\mathbb{L} : \mathbb{K}]$.

Beweis: (i) $\Leftrightarrow$ (ii) klar.

(i) $\Rightarrow$ (iv): $\exists\, \alpha \in \mathbb{L}$ mit $\mathbb{L} = \mathbb{K}(\alpha)$ (Satz vom primitiven Element);
$f := \mathrm{MinPol}(\alpha/\mathbb{K})$ ist irreduzibel und separabel.
$\mathbb{L} = \mathrm{Zfk}(f/\mathbb{K})$.

(iv) $\Rightarrow$ (iii): klar.

(iii) $\Rightarrow$ (i) klar (4.2, 2.80).

In den Fällen (i) bis (iv) hat $\mathbb{L}$ ein primitives Element α: $\mathbb{L} = \mathbb{K}(\alpha)$, und α hat $n := [\mathbb{L} : \mathbb{K}]$ verschiedene $\mathbb{K}$-Konjugierte $\alpha = \alpha_1, \ldots, \alpha_n \in \mathbb{L}$.
Für $i = 1, \ldots, n$ habe $\sigma_i : \mathbb{L} \to_{\mathbb{K}} \mathbb{L}$ mit $\sigma_i(\alpha) = \alpha_i \Rightarrow |\mathrm{Aut}(\mathbb{L}/\mathbb{K})| \geq n$.

(v) $\Rightarrow$ (i): ist $|\mathrm{Aut}(\mathbb{L}/\mathbb{K})| = n$, so ist $[\mathbb{L} : \mathbb{K}]_S = |\mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \overline{\mathbb{K}})| = |\mathrm{Aut}(\mathbb{L}/\mathbb{K})| = n \Rightarrow$ $\mathbb{L}/\mathbb{K}$ ist separabel. Also $\mathbb{L} = \mathbb{K}(\alpha)$ (primitives Element) und $\mathrm{MinPol}(\alpha/\mathbb{K}) =: f = \prod_{\sigma \in \mathrm{Aut}(\mathbb{L}/\mathbb{K})} (t - \sigma(\alpha)) \Rightarrow \mathbb{L} = \mathrm{Zfk}(f/\mathbb{K})$.

□

Definition 4.8.
$\mathbb{L}/\mathbb{K}$ heißt **galoissch** (oder **Galois-Erweiterung**), wenn (i) bis (v) aus 4.7 gelten.

In diesem Fall heißt $\mathrm{Gal}(\mathbb{L}/\mathbb{K}) := \mathrm{Aut}(\mathbb{L}/\mathbb{K})$ die **Galoisgruppe** von $\mathbb{L}/\mathbb{K}$.
Es ist also $|\mathrm{Gal}(\mathbb{L}/\mathbb{K})| = [\mathbb{L} : \mathbb{K}]$.

Bemerkung 4.9.
Die zu Satz 4.4 analogen Eigenschaften gelten für „galoissch“ statt „normal“

(a) $\mathbb{L}/\mathbb{K}, \mathbb{M}/\mathbb{K}$ galoissch $\Rightarrow \mathbb{L}\mathbb{M}/\mathbb{K}, (\mathbb{L} \cap \mathbb{M})/\mathbb{K}$ galoissch;

(b) $\mathbb{E}/\mathbb{K}$ galoissch $\Rightarrow \mathbb{E}/\mathbb{L}$ galoissch;

(c) $\mathbb{L}/\mathbb{K}$ galoissch $\Rightarrow \mathbb{L}\mathbb{M}/\mathbb{M}$ galoissch.

Denn: normal siehe 4.4, separabel siehe 2.87.

a. Der Hauptsatz der Galoistheorie

4.10. Sei $\mathbb{L}/\mathbb{K}$ eine Galois-Erweiterung, sei $G := \mathrm{Gal}(\mathbb{L}/\mathbb{K})$.
$\mathrm{Zwk}(\mathbb{L}/\mathbb{K}) := \{\mathbb{F} : \mathbb{K} \subset \mathbb{F} \subset \mathbb{L} \text{ ist Zwischenkörper}\}$.
$\mathrm{Subg}(G) := \{H : H \leq G\}$.

$\mathbb{F} \in \mathrm{Zwk}(\mathbb{L}/\mathbb{K}) \rightsquigarrow \mathbb{F}^0 := \mathrm{Aut}(\mathbb{L}/\mathbb{F}) = \{\sigma \in G : \sigma|_{\mathbb{F}} = id\}$
$H \in \mathrm{Subg}(G) \rightsquigarrow H^0 := \mathrm{Fix}(H) = \{\alpha \in \mathbb{L} : \ \forall\, \sigma \in H\ \sigma(\alpha) = \alpha\}$

Theorem 4.11 (Hauptsatz der Galoistheorie)**.**
Die Abbildungen $Zwk(\mathbb{L}/\mathbb{K}) \to Subg(G), \mathbb{F} \mapsto \mathbb{F}^0$
und $Subg(G) \to Zwk(\mathbb{L}/\mathbb{K}), H \mapsto H^0$
sind zueinander inverse Bijektionen:
$\mathbb{F}^{00} = \mathbb{F}, H^{00} = H\ \forall\, \mathbb{F},\ \forall\, H.$

Darüber hinaus gelten (seien $\mathbb{F}, \mathbb{F}_1, \mathbb{F}_2 \in Zwk(\mathbb{L}/\mathbb{K})$, $H = \mathbb{F}^0, H_1 = F_1^0, H_2 = \mathbb{F}_2 0 \in Subg(G)$*):*

(a) *Die Bijektionen sind inklusionsumkehrend:*

$$\mathbb{F}_1 \subset \mathbb{F}_2 \Rightarrow H_1 \supseteq H_2.$$

(b) *Die Bijektionen sind indexerhaltend: für* $\mathbb{F}_1 \subset \mathbb{F}_2$ *ist* $[\mathbb{F}_2 : \mathbb{F}_1] = [H_1 : H_2]$.

(c) *Die Bijektionen erhalten die Normalität: für* $\mathbb{F}_1 \subset \mathbb{F}_2$ *gilt:* $\mathbb{F}_2/\mathbb{F}_1$ *normal* $\Leftrightarrow H_2 \trianglelefteq H_1$.

Ist $\mathbb{F}_2/\mathbb{F}_1$ *normal, so ist* $Gal(\mathbb{F}_2/\mathbb{F}_1) \cong H_1/H_2$.

(d) *Die Bijektionen sind verträglich mit Konjugation: für* $\sigma \in G$ *ist* $\sigma(\mathbb{F})^0 = \sigma\mathbb{F}^0\sigma^{-1}$ *für* $\mathbb{F} \in Zwk(\mathbb{L}/\mathbb{K})$ *bzw.* $(\sigma H \sigma^{-1})^0 = \sigma(H^0)$ *für* $H \in Subg(G)$.

(e) *Insbesondere ist* $\mathbb{L}/\mathbb{F}$ *galoissch mit* $Gal(\mathbb{L}/\mathbb{F}) = \mathbb{F}^0$.

Beweis:
In mehrere Schritte:

(1) Sei $\mathbb{F} \in \mathrm{Zwk}(\mathbb{L}/\mathbb{K}) \Rightarrow \mathbb{L}/\mathbb{F}$ galoissch.
$\mathrm{Gal}(\mathbb{L}/\mathbb{F}) = \mathbb{F}^0$ gilt nach Definition. Also (e) gezeigt.

(2) Also $[\mathbb{L} : \mathbb{F}] = |F^0|$.

(3) $\mathbb{F}^{00} \supset \mathbb{F}$ klar nach Definition. Sei $\alpha \in \mathbb{L}, \alpha \notin \mathbb{F}$. Wegen $\mathbb{L}/\mathbb{F}$ separabel gibt es ein $\mathbb{F}$-Konjugiertes $\alpha' \neq \alpha$ von α. Wegen $\mathbb{L}/\mathbb{F}$ normal $\exists\, \sigma \in \mathbb{F}^0 = \mathrm{Gal}(\mathbb{L}/\mathbb{F})$ mit $\sigma(\alpha) = \alpha' \Rightarrow \alpha \notin \mathbb{F}^{00} = \mathrm{Fix}(F^0)$.

(4) Sei $H \leq G$, sei $\mathbb{F} := H^0 = \mathrm{Fix}(H)$. Wir wollen zeigen $H = H^{00} = \mathbb{F}^0$.
Klar: $H \leq H^{00} = \mathrm{Aut}(\mathbb{L}/\mathbb{F})$.
Nach dem Satz vom primitiven Element $\exists\, \beta \in \mathbb{L}$ mit $\mathbb{L} = \mathbb{F}(\beta)$. Sei $g(t) := \prod_{\sigma \in H} (t - \sigma(\beta))$. Für $\rho \in H$ sei $\widetilde{\rho} : \mathbb{L}[t] \to \mathbb{L}[t]$ der induzierte Automorphismus (koeffizientenweise) $\Rightarrow dt\rho(g(t)) = g(t) \Rightarrow$ die Koeffizienten von $g(t)$ sind fix unter H, also $g(t) \in \mathbb{F}[t]$.
Es ist $g(\beta) = 0$, also $\mathrm{MinPol}(\beta/\mathbb{F}) \mid g(t)$.

$\Rightarrow |H| = \deg(g) \geq \deg(\mathrm{MinPol}(\beta/\mathbb{F})) = [\mathbb{L} : \mathbb{F}]$.
Andererseits $[\mathbb{L} : \mathbb{F}] = |F^0| = |H^{00}|$ nach (2).
$\Rightarrow |H| \geq |H^{00}|$. Wegen $H \leq H^{00}$ folgt $H = H^{00}$.

(5) Inklusionsumkehrend: klar nach Definitionen.

(6) (b) folgt aus (2) wegen Multiplikativität $[\mathbb{F}_2 : \mathbb{F}_1] = \frac{[\mathbb{L}:\mathbb{F}_1]}{[\mathbb{L}/\mathbb{F}_2]} = \frac{|H_1|}{|H_2|} = [H_1 : H_2]$.

(7) Beweis von (c): für $\alpha \in \mathbb{L}$ ist $\alpha \in (\sigma H \sigma^{-1})^0 = \mathrm{Fix}(\sigma H \sigma^{-1})$
$\Leftrightarrow\ \forall\, h \in H\ \sigma h \sigma^{-1}(\alpha) = \alpha$
$\Leftrightarrow\ \forall\, h \in H\ h(\sigma^{-1}(\alpha)) = \sigma^{-1}(\alpha)$
$\Leftrightarrow \sigma^{-1}(\alpha) \in \mathrm{Fix}(H) = H^0$
$\Leftrightarrow \alpha \in \sigma(H^0)$.

(8) (c): $\mathbb{F}_2/\mathbb{F}_1$ ist separabel.
$\mathbb{F}_2/\mathbb{F}_1$ ist normal $\Leftrightarrow\ \forall\, \sigma \in \mathrm{Aut}(\mathbb{L}/\mathbb{F}_1) = \mathbb{F}_1^0\ \sigma(\mathbb{F}_2) = F_2$ (nach Lemma 4.6)
$\Leftrightarrow\ \forall\, \sigma \in \mathbb{F}_1^0\ \sigma(\mathbb{F}_2)^0 = \mathbb{F}_2^0$

Nach (d) ist $\sigma(\mathbb{F}_2)^0 = \sigma \mathbb{F}_2^0 \sigma^{-1}$,
also $\mathbb{F}_2/\mathbb{F}_1$ ist normal $\Leftrightarrow\ \forall\, \sigma \in \mathbb{F}_1^0\ \sigma \mathbb{F}_2 \sigma^{-1} = \mathbb{F}_2^0 \Rightarrow \mathbb{F}_2^0 \trianglelefteq \mathbb{F}_1^0$.

□

Bemerkung 4.12.
Die Bijektion aus Theorem 4.11 wird als **Galoiskorrespondenz** bezeichnet. Sie ist ein **Anti-Isomorphismus** der Verbände, damit ist gemeint:
Unter $(-)^0$ entsprechen sich Durchschnitt mit Erzeugnis:
$\forall\, H_1, H_2 \in \mathrm{Subg}(G)$: $\langle H_1 \cup H_2 \rangle^0 = H_1^0 \cap H_2^0$, $(H_1 \cap H_2)^0 = H_1^0 H_2^0$
$\forall\, \mathbb{F}_1, \mathbb{F}_2 \in \mathrm{Zwk}(\mathbb{L}/\mathbb{K})$: $(\mathbb{F}_1 \mathbb{F}_2)^0 = \mathbb{F}_1^0 \cap \mathbb{F}_2^0$, $(\mathbb{F}_1 \cap \mathbb{F}_2)^0 = \left\langle \mathbb{F}_1^0 \cup \mathbb{F}_2^0 \right\rangle$.
Dies folgt aus Bijektivität und Inklusionsumkehr!

b. Erste Anwedungen - Galoisgruppe eines Polynoms

4.13.
Sei $f \in \mathbb{K}[t]$ ein *separables* Polynom, sei $\mathbb{L} = \mathrm{Zfk}(f/\mathbb{K})$, also $\mathbb{L}/\mathbb{K}$ galoissch.
Sei $f = (t-\alpha_1)\cdot\ldots\cdot(t-\alpha_n)$, $\alpha_i \in \mathbb{L}$, dann operiert $G = \mathrm{Gal}(\mathbb{L}/\mathbb{K})$ auf $W := \{\alpha_1, \ldots, \alpha_n\}$:

Satz 4.14.

(a) Gal$(\mathbb{L}/\mathbb{K})$ *operiert treu auf* W.

(b) Genau dann ist die Operation transitiv, wenn f *irreduzibel ist.*

Beweis:
$G := \mathrm{Gal}(\mathbb{L}/\mathbb{K})$: $\sigma \in G, \alpha \in W$.
$f(\sigma(\alpha) = \sigma(\underbrace{f(\alpha)}_{=0}) = 0 \Rightarrow \sigma(\alpha) \in W$.
Wegen $\mathbb{L} = \mathbb{K}(\alpha_1, \ldots, \alpha_n)$ ist die Operation treu.

Ist f irreduzibel, so gibt es für jedes $i = 1, \ldots, n$ ein $\sigma_i \in G$ mit $\sigma_i(\alpha_1) = \alpha_i$, also G transitiv.
Ist f nicht irreduzibel, dann gibt es $\alpha, \beta \in W$ mit $\mathrm{MinPol}(\alpha/\mathbb{K}) \neq \mathrm{MinPol}(\beta/\mathbb{K}) \Rightarrow$ α, β nicht in derselben G-Bahn, denn $\forall\ \alpha \in W\ \forall\ \sigma \in G$ haben α und $\sigma(\alpha)$ dasselbe MinPol.

□

Definition 4.15.
Man nennt $\mathrm{Gal}(f/\mathbb{K}) := \mathrm{Gal}(\mathbb{L}/\mathbb{K})$ die **Galoisgruppe des** (separablen!) **Polynoms** f.
Die Operation auf $W = \{\text{Wurzeln von } f\}$ identifiziert $\mathrm{Gal}(f/\mathbb{K})$ mit einer Untergruppe von $\mathrm{Sym}(W)$, oder - bis auf Konjugation - einer Untergruppe von S_n, $n := \deg(f)$.

Bemerkung 4.16.

1. $|\mathrm{Gal}(f/\mathbb{K})| = [\mathrm{Zfk}(f/\mathbb{K}) : \mathbb{K}]$.
2. f irreduzibel $\Rightarrow \mathrm{Gal}(f/\mathbb{K})$ ist eine transitive Untergruppe von S_n, $n := \deg(f)$:
   Listen der transitiven Untergruppen:
   $n = 2$: $G = S_2$;
   $n = 3$:
   $n = 4$:

$n = 5$:
$n = 6$:
$n = 7$:
$n = 8$:

siehe Gruppentheorie ...

c. Erste Anwedungen - Beispiele für die Galoiskorrespondenz

Beispiel 4.17.
Sei $[\mathbb{L} : \mathbb{K}] = 2, \mathbb{L}/\mathbb{K}$ separabel.
$\Rightarrow \mathbb{L}/\mathbb{K}$ galoissch $\Rightarrow G := \mathrm{Gal}(\mathbb{L}/\mathbb{K}) = C_2$. Ist $char(\mathbb{K}) \neq 2$, so $\mathbb{L} = \mathbb{K}(\sqrt{d})$. Dann ist $\langle\sigma\rangle = G$ mit $\sigma(x + y\sqrt{d}) = x - y\sqrt{d}$.
(Zum Beispiel ist die komplexe Konjugation $z \mapsto \bar{z}$ der Erzeuger von $Gal(\mathbb{C}/\mathbb{R})$)

Beispiel 4.18.
$[\mathbb{L} : \mathbb{K}] = 3 \Rightarrow$ im Allgemeinen nicht mehr normal. Betrachte $f = t^3 - a$ mit $a \in \mathbb{K}$, f sei irreduzibel ($a \notin \mathbb{K}^{*3}$).
Sei α mit $\alpha^3 = a$ ($\alpha \in \overline{\mathbb{K}}$), sei $\zeta \neq 1$ eine 3-te Einheitswurzel (d..h. $\zeta^2 + \zeta + 1 = 0$) ($char(\mathbb{K}) \neq 3$) $\Rightarrow f = t^3 - a = (t - \alpha)(t - \zeta\alpha)(t - \zeta^2\alpha)$.

1. Fall: $\zeta \in \mathbb{K} \Rightarrow f(t)$ zerfällt über $\mathbb{K}(\alpha) = \mathbb{L}$.
$\Rightarrow |\mathrm{Gal}(f/\mathbb{K})| = 3, G := \mathrm{Gal}(\mathbb{L}/\mathbb{K}) = \langle\sigma\rangle$, und
$\sigma(x + y\alpha + z\alpha^2) = x + y\zeta\alpha + z\zeta^2\alpha^2$
$\sigma^2(x + y\alpha + z\alpha^2) = x + y\zeta^2\alpha^2 + z\zeta\alpha$.

2. Fall: $\zeta \notin \mathbb{K}$ (z.B. $\mathbb{K} = \mathbb{Q}$):
Dann ist $[\mathbb{K}(\zeta) : \mathbb{K}] = 2$, also $\zeta \notin \mathbb{K}(\alpha)$ wegen $[\mathbb{K}(\alpha) : \mathbb{K}] = 3$.
$\Rightarrow \mathbb{L} := \mathrm{Zfk}(f/\mathbb{K}) = \mathbb{K}(\alpha, \zeta)$ hat $[\mathbb{L} : \mathbb{K}] = 6$.
$G := \mathrm{Gal}(f/\mathbb{K})$ ist eine Untergruppe von S_3 mit $|G| = [\mathbb{L} : \mathbb{K}] = 6 \Rightarrow G = S_3$.

G erzeugt von $\sigma(\alpha) = \zeta\alpha, \sigma(\zeta) = \zeta, \tau(\alpha) = \alpha, \tau(\zeta) = \zeta^2 = \zeta^{-1}$:

$\mathbb{K}$ entspricht $G = S_3$
$\mathbb{K}(\zeta)$ entspricht $\langle\sigma\rangle$
$\mathbb{L} = \mathbb{K}(\alpha, \zeta)$ entspricht $\{id\}$
$\mathbb{K}(\alpha)$ entspricht $\langle\tau\rangle$
$\mathbb{K}(\zeta^2\alpha)$ entspricht $\langle\sigma\tau\rangle$
$\mathbb{K}(\zeta\alpha)$ entspricht $\langle\sigma^2\tau\rangle$

Beispiel 4.19.
$f := t^4 - 2 \in \mathbb{Q}[t]$ ist irreduzibel nach Eisenstein. Sei $\alpha = \sqrt[4]{2}$ (eine 4-te Wurzel aus 2), $f = (t - \alpha)(t + \alpha)(t - i\alpha)(t + i\alpha)$, $i = \sqrt{-1}$.
$\Rightarrow \mathbb{L} = \mathrm{Zfk}(f/\mathbb{Q}) = \mathbb{Q}(\alpha, \sqrt{-1}) = \mathbb{Q}(\alpha, i) \Rightarrow [\mathbb{L} : \mathbb{Q}] = 8$, $G := \mathrm{Gal}(f/\mathbb{Q})$ ist eine (transitive) Untergruppe von S_4, $|G| = 8 \Rightarrow G \cong D_4$.

$\mathbb{F} := \mathbb{Q}(i), H := \mathrm{Gal}(\mathbb{L}/\mathbb{Q}(i)), |H| = [\mathbb{L} : \mathbb{Q}(i)] = 4.$
$\Rightarrow H = \{id, \sigma, \sigma^2, \sigma^3\} = \langle\sigma\rangle$ mit $\sigma : \alpha \mapsto i\alpha, \sigma(i) = i.$

$\mathbb{F} := \mathbb{Q}(\alpha), \widetilde{H} := \mathrm{Gal}(\mathbb{L}/\mathbb{Q}(\alpha)), |\widetilde{H}| = [\mathbb{L} : \mathbb{Q}(\alpha)] = 2.$
$\Rightarrow \widetilde{H} = \langle\tau\rangle = \{id, \tau\}$ mit $\tau : \alpha \mapsto -\alpha, i \mapsto -i.$

$\Rightarrow G = \mathrm{Gal}(\mathbb{L}/\mathbb{Q}) = \langle\sigma, \tau\rangle$
Operation auf den vier Wurzeln von f:
$\{1, 2, 3, 4\} \longleftrightarrow \{i\alpha, -\alpha, -i\alpha, \alpha\}$
$\nu \longleftrightarrow i^\nu\alpha$
$\sigma \longleftrightarrow (1234), \tau \longleftrightarrow (13).$

Man sieht zum Beispiel: $\mathbb{Q}(i, \sqrt{2})/\mathbb{Q}$ ist galoissch mit Gruppe $C_2 \times C_2$; $\mathbb{L}/\mathbb{Q}(i)$ ist galoissch mit Gruppe C_4; usw.

d. Erste Anwedungen - Der Translationssatz

Satz 4.20.
Sei $\mathbb{E}/\mathbb{K}$ *eine beliebige Körpererweiterung, seien* $\mathbb{L}, \mathbb{M}$ *Zwischenkörper von* $\mathbb{E}/\mathbb{K}$*, mit* $\mathbb{L}/\mathbb{K}$ *galoissch.*
Dann ist auch $\mathbb{LM}/\mathbb{M}$ *galoissch, und* $Gal(\mathbb{LM}/\mathbb{M}) \to Gal(\mathbb{L}/\mathbb{K}), \sigma \mapsto \sigma|_{\mathbb{L}}$ *ist ein injektiver Homomorphismus mit Bild* $Gal(\mathbb{L}/\mathbb{L} \cap \mathbb{M})$ *von* $Gal(\mathbb{L}/\mathbb{K})$.
Insbesondere ist $Gal(\mathbb{LM}/\mathbb{M}) \cong Gal(\mathbb{L}/\mathbb{L}\cap\mathbb{M})$*, und* $[\mathbb{LM} : \mathbb{M}]$ *ist ein Teiler von* $[\mathbb{L} : \mathbb{K}]$.

Beweis:
$\mathbb{LM}/\mathbb{M}$ ist galoissch nach 4.9. Für $\sigma \in \mathrm{Gal}(\mathbb{LM}/\mathbb{M})$ ist $\sigma(\mathbb{L}) \subset \mathbb{L}$ wegen $\mathbb{L}/\mathbb{K}$ normal. $\Rightarrow \sigma|_{\mathbb{L}} \in \mathrm{Gal}(\mathbb{L}/\mathbb{L} \cap \mathbb{M})$.
Dieser Homomorphismus $\mathrm{Gal}(\mathbb{LM}/\mathbb{M}) \to \mathrm{Gal}(\mathbb{L}/\mathbb{L} \cap \mathbb{M})$ ist injektiv (ein σ im Kern ist die Identität auf $\mathbb{M}$ und $\mathbb{L}$, also auf $\mathbb{LM}$).

Sei $H := im(\mathrm{Gal}(\mathbb{LM}/\mathbb{M}) \to \mathrm{Gal}(\mathbb{L}/\mathbb{L} \cap \mathbb{M}))$.
Ist $\alpha \in \mathbb{L} \cap \mathrm{Fix}(H)$, so ist α fix unter $\mathrm{Gal}(\mathbb{LM}/\mathbb{M}) \Rightarrow \alpha \in \mathbb{M}$, also $\alpha \in \mathbb{L} \cap \mathbb{M}$.
Also $\mathrm{Fix}(H) = \mathbb{L} \cap \mathbb{M}$, also $H = \mathrm{Gal}(\mathbb{L}/\mathbb{L} \cap \mathbb{M})$.

□

Bemerkung 4.21.
Satz 4.20 heißt Translationssatz, da er eine (ordnungstreue) Bijektion $\mathrm{Zwk}(\mathbb{LM}/\mathbb{M}) \to_{\cong} \mathrm{Zwk}(\mathbb{L}/\mathbb{L} \cap \mathbb{M})$ induziert: $\mathbb{F}' \mapsto \mathbb{F} \cap \mathbb{L}$, bzw. umgekehrt $\mathbb{F} \mapsto \mathbb{FM}$.

Satz 4.22.
Seien $\mathbb{L}_1/\mathbb{K}$, $\mathbb{L}_2/\mathbb{K}$ *Galoiserweiterungen. Dann ist* $\mathbb{L}_1\mathbb{L}_2/\mathbb{K}$ *galoissch, und der Homomorphismus*

$$\begin{aligned} Gal(\mathbb{L}_1\mathbb{L}_2/\mathbb{K}) &\to Gal(\mathbb{L}_1/\mathbb{K}) \times Gal(\mathbb{L}_2/\mathbb{K}) \\ \sigma &\mapsto (\sigma\mid_{\mathbb{L}_1}, \sigma\mid_{\mathbb{L}_2}) \end{aligned}$$

ist injektiv. Ist $\mathbb{L}_1 \cap \mathbb{L}_2 = \mathbb{K}$*, so ist er sogar bijektiv, also* $Gal(\mathbb{L}_1\mathbb{L}_2/\mathbb{K}) \cong Gal(\mathbb{L}_1/\mathbb{K}) \times Gal(\mathbb{L}_2/\mathbb{K})$.

Beweis:
$\mathbb{L}_1\mathbb{L}_2/\mathbb{K}$ galoissch (selbes Argument wie oben: „tatsächlich trivial“).

Sei $\mathbb{L}_1 \cap \mathbb{L}_2 = \mathbb{K}$. Dann ist $[\mathbb{L}_1\mathbb{L}_2 : \mathbb{K}] = \underbrace{[\mathbb{L}_1\mathbb{L}_2 : \mathbb{L}_2]}_{=[\mathbb{L}_1:\mathbb{K}] \text{ nach } 4.20} \cdot [\mathbb{L}_2 : \mathbb{K}] = [\mathbb{L}_1 : \mathbb{K}] \cdot [\mathbb{L}_2 : \mathbb{K}] =$

|rechte Gruppe| $\Rightarrow$ Behauptung.

□

e. Erste Anwedungen - die galoissche Hülle einer separablen Erweiterung

4.23.
Sei $\mathbb{F}/\mathbb{K}$ eine endliche Erweiterung. Wann gibt es eine Galoiserweiterung $\mathbb{L}/\mathbb{K}$ mit $\mathbb{F} \subset \mathbb{L}$?
Notwendig: $\mathbb{F}/\mathbb{K}$ separabel. Das genügt schon: dann ist $\mathbb{F} = \mathbb{K}(\alpha)$ für ein $\alpha \in \mathbb{F}$ (primitives Element), sei $f = \text{MinPol}(\alpha/\mathbb{K})$. Dann ist $\mathbb{L} := \text{Zfk}(f/\mathbb{K})$ galoissch über $\mathbb{K}$, $\mathbb{K} \subset \mathbb{F} \subset \mathbb{L}$, und $\mathbb{L}$ ist minimal.

Andere Beschreibung von $\mathbb{L}$: seien $\sigma_1, \ldots, \sigma_n : \mathbb{F} \to_{\mathbb{K}} \overline{\mathbb{K}}$ die $\mathbb{K}$-Einbettungen von $\mathbb{F}$ in $\overline{\mathbb{K}}$ für $n = [\mathbb{F} : \mathbb{K}]_S = [\mathbb{F} : \mathbb{K}]$.
Dann ist $\mathbb{L} = \sigma_1(\mathbb{F}) \cdot \ldots \cdot \sigma_n(\mathbb{F})$ (Kompositum)

Definition 4.24.
$\mathbb{L}$ (wie oben) heißt die **galoissche Hülle** von $\mathbb{F}$ über $\mathbb{K}$.

4.25.
Angenommen, wir haben ein (große) Galoiserweiterung $\mathbb{E}/\mathbb{K}$ mit $\mathbb{K} \subset \mathbb{F} \subset \mathbb{E}$. Dann kann man die galoissche Hülle $\mathbb{L}$ von $\mathbb{F}/\mathbb{K}$ in $\mathbb{E}$ wie folgt ablesen:

die zu $\mathbb{L}$ gehörende Untergruppe $\mathbb{L}^0 = \mathrm{Gal}(\mathbb{E}/\mathbb{L})$ von G ist $\bigcap_{\sigma\in G} \sigma H\sigma^{-1}$ = der größte in $H = \sigma_1 H \sigma_1^{-1}$ enthaltene Normalteiler von G.

Beispiel 4.26.
Man kann die galoissche Hülle verwenden, um auch für nicht-normale (separable!) $\mathbb{F}/\mathbb{K}$ Informationen über die Zwischenkörper zu erhalten:
sei $f(t) = t^4 + t - 1 \in \mathbb{Q}[t]$, irreduzibles Polynom. Es ist $\mathrm{Gal}(f/\mathbb{Q}) = S_4$.

Sei α mit $f(\alpha) = 0$. Dann ist $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$, aber es gibt kein $\mathbb{Q} \subset \mathbb{F} \subset \mathbb{Q}(\alpha)$ mit $[\mathbb{F} : \mathbb{Q}] = 2$; denn $\mathbb{Q}(\alpha)^0 = S_3 < S_4$, es gibt keine Zwischengruppe $S_3 < H < S_4$ mit $[S_4 : H] = 2$.

f. Erste Anwedungen - Galoistheorie endlicher Körper

Satz 4.27.
Sei $\mathbb{E}/\mathbb{F}$ eine Erweiterung endlicher Körper, sei $|\mathbb{F}| = q$, $[\mathbb{E} : \mathbb{F}] = n$.

(a) $\mathbb{E}/\mathbb{F}$ ist galoissch;

(b) $Gal(\mathbb{E}/\mathbb{F}) = \langle\sigma\rangle$ ist zyklisch, erzeugt von $\sigma : \mathbb{E} \to \mathbb{E}, \sigma(x) = x^q$.

Beweis:
Wir wissen (a) schon (2.99: normal, 2.70: separabel).

Aus 2.100: $\sigma \in \mathrm{Aut}(\mathbb{E}/\mathbb{F})$ von genauer Ordnung n ($\sigma^n = id$).
$\Rightarrow \langle\sigma\rangle = \mathrm{Gal}(\mathbb{E}/\mathbb{F})$ wegen $n = |\mathrm{Gal}(\mathbb{E}/\mathbb{F})|$.

□

g. Erste Anwedungen - Konstruktion mit Zirkel und Lineal

$\mathcal{P} \subset \mathbb{C}, \mathbb{K}_0 := \mathbb{Q}(\mathcal{P})$. Hatten gesehen: ein $\alpha \in \mathbb{C}$ ist genau dann aus $\mathcal{P}$ mit Zirkel und Lineal konstruierbar, wenn es eine Kette $\mathbb{K}_0 \subset \mathbb{K}_1 \subset \ldots \subset \mathbb{K}_r$ gibt mit $\alpha \in \mathbb{K}_r$ und $[\mathbb{K}_i : \mathbb{K}_{i-1}] = 2 \; \forall \; i$.

Satz 4.28.
Sei $\alpha \in \mathbb{C}$ algebraisch über $\mathbb{K}_0$. Genau dann ist α aus $\mathcal{P}$ mit Zirkel und Lineal konstruierbar, wenn für die galoissche Hülle $\mathbb{L}$ von $\mathbb{K}_0(\alpha)/\mathbb{K}_0$ gilt: $[\mathbb{L} : \mathbb{K}_0]$ ist eine Potenz von 2.

Das folgt aus folgendem Lemma:

Lemma 4.29.
Sei G eine endlich Gruppe, $H \leq G$. Dann sind äquivalent:

(i) $\exists$ *Kette* $H = H_0 < H_1 < \ldots < H_r = G$ *mit* $[H_i : H_{i-1}] = 2 \; \forall \; i$;

(ii) $\exists \; N \trianglelefteq G$ *mit* $N \leq H, [G : N] =$ *Potenz von 2.*

Beweis:
(ii) $\Rightarrow$ (i): $G/N \geq H/N$, falls $H \neq G$.
$N_G(H) > H \Rightarrow \; \exists \, H < K \leq G$ mit $[K : H] = 2$.

(i) $\Rightarrow$ (ii): zeige zuerst: sind $K_1, \ldots, K_n \leq G$ vom Index 2, dann gilt $[G : \bigcap_{i=1}^{n} K_i]$ ist eine 2-Potenz. Denn $G/\bigcap_{i=1}^{n} K_i \to (G/K_1) \times \ldots \times (G/K_n), \overline{g} \mapsto (gK_1, \ldots, gK_n)$ ist injektiv.

$G = H_0 \leq H_1 \leq \ldots \leq H_r = H$ mit $[H_i : H_{i+1}] = 2$.

Sei $N_i :=$ der größte in H_i enthaltene Normalteiler von G, also $N_i = \bigcap_{g \in G} g H_i g^{-1}$.
Zeige: N_i/N_{i+1} ist eine 2-Gruppe $\; \forall \; i$ ($\Rightarrow$ fertig).
Für jede zu H_i konjugierte Untergruppe xH_ix^{-1} von G ist $[N_{i-1} : N_{i-1} \cap xH_ix^{-1}] = [N_{i-1} : N_{i-1} \cap H_i] = [N_{i-1}H_i : H_i] \leq 2$ wegen $H_i \leq N_{i-1}H_i \leq H_{i-1}$. ($N_i = \bigcap_{x \in G} \left(N - i - 1 \cap xH_ix^{-1}\right)$
(Index ≤ 2 in N_{i-1})

$\Rightarrow [N_{i-1} : N_i] =$ 2-Potenz.

□

Satz 4.30 (Fundamentalsatz der Algebra)**.**
Der Körper $\mathbb{C}$ ist algebraisch abgeschlossen.

Beweis:
Verwende über $\mathbb{R}$:

(1) $\mathbb{C} = \mathbb{R}(i), i^2 = -1$;

(2) jede positive reelle Zahl in $\mathbb{R}$ ist ein Quadrat;

(3) jedes Polynom in $\mathbb{R}[t]$ von ungeradem Grad hat eine Nullstelle in $\mathbb{R}$.

1. Schritt: $\mathbb{C}$ hat keine quadratische Erweiterung:
sei $w = u + iv \in \mathbb{C}$ mit $u, v \in \mathbb{R}$. Ansatz $w = (x + iy)^2$ führt auf $u = x^2 - y^2, v = 2xy$. Ohne Einschränkung $v \neq 0 \Rightarrow y = \frac{v}{2x} \rightsquigarrow 2x^2 = u \pm \sqrt{u^2 + v^2}$.
Rechte Seite > 0 für positive Wurzel $\Rightarrow \exists\, x \in \mathbb{R}$ mit $2x^2 = u + \sqrt{u^2 + v^2}$.
Einsetzen bestätigt: $w = (x + y)^2$ OK.

2. Schritt: Sei jetzt $\mathbb{L}/\mathbb{C}$ eine endliche Erweiterung. ObdA: $\mathbb{L}/\mathbb{R}$ ist galoissch (bilde galoissche Hülle über $\mathbb{R}$).
Sei $G := \mathrm{Gal}(\mathbb{L}/\mathbb{R})$, sei S eine 2-Sylowgruppe. Dann ist $[\mathrm{Fix}(S) : \mathbb{R}]$ ungerade.
Nach (3) folgt $\mathrm{Fix}(S) = \mathbb{R}$, also $S = G$, also ist G eine 2-Gruppe.

Wäre $\mathbb{L} \neq \mathbb{C}$, so betrachte $H := \mathrm{Gal}(\mathbb{L}/\mathbb{C}) \leq G$. Dann wäre $H \neq \{e\}$, also hätte H eine Untergruppe $\widetilde{H}$ vom Index 2 (nach 3.82). Dann wäre $[\mathrm{Fix}(\widetilde{H}) : \mathbb{C}] = 2$, Widerspruch zum 1. Schritt.

□

h. Symmetrische Polynome

Sei $\mathbb{K}$ ein Körper.

Definition 4.31.
S_n operiert auf $\mathbb{K}[t_1, \ldots, t_n]$:

$$^{\pi}f = f(t_{\pi(1)}, \ldots, t_{\pi(n)}) \text{ für } f \in \mathbb{K}[t_1, \ldots, t_n], \pi \in S_n.$$

S_n operiert auf $\mathbb{K}(t_1, \ldots, t_n)$:

$$^{\pi}\left(\frac{f}{g}\right) = \frac{^{\pi}f}{^{\pi}g} \text{ für } f, g \in \mathbb{K}[t_1, \ldots, t_n], g \neq 0$$

(wohldefiniert: für $\sigma, \rho \in S_n$ ist $^{\sigma}(^{\rho}f) = ^{\sigma\rho} f$; Einbettung: $\rho : S_n \hookrightarrow \mathrm{Aut}(\mathbb{K}(t_1, \ldots, t_n))$, $\pi \mapsto \rho_\pi : f \mapsto ^{\pi} f$).

Definition 4.32 (Symmetrische Funktionen)**.**
$f \in \mathbb{K}(t_1, \ldots, t_n)$ heißt **symmetrisch** in den Variablen $t_1, \ldots, t_n$, wenn $^{\pi}f = f$ $\forall\ \pi \in S_n$.
$\mathbb{K}(t_1, \ldots, t_n)^{\mathrm{Sym}} = \mathrm{Fix}_{\mathbb{K}(t_1,\ldots,t_n)}(S_n) = \{f \in \mathbb{K}(t_1, \ldots, t_n) :^{\pi} f = f\ \forall\ \pi \in S_n\}$
$\mathbb{K}[t_1, \ldots, t_n]^{\mathrm{Sym}} = \{f \in \mathbb{K}[t_1, \ldots, t_n] :^{\pi} f = f\ \forall\ \pi \in S_n\}$.

Satz 4.33.
$\mathbb{K}(t_1, \ldots t_n)/\mathbb{K}(t_1, \ldots, t_n)^{Sym}$ ist eine endlich Galoiserweiterung mit Galoisgruppe S_n.

Beweis:
folgt aus folgendem allgemeinerem Satz.

□

Satz 4.34 (E. Artin)**.**
Seien $\mathbb{E}$ ein Körper und $G \leq \mathrm{Aut}(\mathbb{E})$ eine endliche Untergruppe. Sei $\mathbb{F} = Fix_{\mathbb{E}}(G) = \{x \in \mathbb{E} : \sigma(x) = x\ \forall\ \sigma \in G\}$ der Fixkörper von G.
Dann ist $\mathbb{E}/\mathbb{F}$ eine endliche Galoiserweiterung mit Galoisgruppe G.

Beweis:

(1) Jedes $a \in \mathbb{E}$ ist algebraisch und separabel über $\mathbb{F}$ und es gilt $[\mathbb{F}(a) : \mathbb{F}] \leq |G|$:
Sei $a \in \mathbb{E}$. $H := \{\sigma \in G : \sigma(a) = a\} \leq G$. Für $\sigma, \sigma' \in G$ gilt $\sigma H = \sigma' H \Leftrightarrow$

$\sigma(a) = \sigma'(a)$.
Sei $G = \bigcup_{i=1} r$ eine disjunkte Zerlegung mit $\sigma_1, \ldots, \sigma_r \in G$.
Setze $f(T) = \prod_{i=1}^{r}(T - \sigma_i(a)) \in \mathbb{E}[T]$. Das Polynom $f(T)$ hängt nicht von der speziellen Wahl der $\sigma_1, \ldots, \sigma_r$ ab!
Insbesondere: ${}^{\sigma}f(T) = \prod_{i=1}^{n}(T - \sigma\sigma_i(a)) = f(T) \ \forall\ \sigma \in G$.
D.h. f hat seine Koeffizienten in $\mathrm{Fix}_{\mathbb{E}}(G) = \mathbb{F}$, d.h. $f(T) \in \mathbb{F}[T]$.

f ist separabel und $f(a) = 0$. Damit ist a algebraisch und separabel über $\mathbb{F}$.
$[F(a) : \mathbb{F}] \leq \deg f \leq |G|$.

(2) $\mathbb{E}/\mathbb{F}$ ist endlich und separabel mit $[\mathbb{E} : \mathbb{F}] \leq |G|$.
Aus (1) folgt: $\mathbb{E}/\mathbb{F}$ ist algebraisch und separabel.
Angenommen,$[\mathbb{E} : \mathbb{F}] > |G|$. Dann $\exists\ a_1, \ldots, a_m \in \mathbb{E}$ mit $[\mathbb{F}(a_1, \ldots, a_m) : \mathbb{F}]\ |G|$.
$\Rightarrow \mathbb{F}(a_1, \ldots, a_m) = \mathbb{F}(a)$ für ein primitives Element $a \in \mathbb{E}$.
$\Rightarrow [\mathbb{F}(a) : \mathbb{F}] > |G| \rightarrow$ Widerspruch zu (1).

(3) $G \leq \mathrm{Aut}(\mathbb{E}/\mathbb{F})$ und $|\mathrm{Aut}(\mathbb{E}/\mathbb{F})| \leq [\mathbb{E} : \mathbb{F}] \leq |G| < \infty \Rightarrow \mathrm{Aut}(\mathbb{E}/\mathbb{F}) = G \Rightarrow \mathbb{E}/\mathbb{F}$ ist galoissch mit $\mathrm{Gal}(\mathbb{E}/\mathbb{F}) = G$.

□

Korollar 4.35.
Zu jeder endlichen Gruppe G gibt es eine endliche Galoiserweiterung $\mathbb{E}/\mathbb{F}$ *und Gal*$(\mathbb{E}/\mathbb{F}) = G$.

Beweis:
Wähle eine Einbettung $\Psi : G \hookrightarrow S_n \hookrightarrow_{\varphi} \mathrm{Aut}(\mathbb{E})$ mit $\mathbb{E} = \mathbb{K}(t_1, \ldots, t_n)$.
($\exists\ \Psi$ nach Vorlesung, z.B. mit $n = |G|$)
Damit gilt für $\mathbb{F} = \mathrm{Fix}_{\mathbb{E}}(G')$ mit $G' = \Psi(G)$: $G \cong_{\Psi} G' = \mathrm{Aut}(\mathbb{E}/\mathbb{F})$ und $\mathbb{E}/\mathbb{F}$ galoissch.

□

Bemerkung 4.36.
Für einen gegebenen Körper $\mathbb{K}$ kann es schwierig sein, zu sagen, welche endlichen Gruppen Galoisgruppen $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ von einer endlichen Galoiserweiterung $\mathbb{L}/\mathbb{K}$ sind.

z.B.: $\mathbb{K} = \mathbb{R}$: nur $\{e\}$ und C_2.
$\mathbb{K} = \mathbb{Q}$: noch nicht so richtig gelöst $\Rightarrow$ Übungsaufgabe ...

4.37.
$\mathbb{E} = \mathbb{K}(t_1, \ldots, t_n)$, $\mathbb{F} = \mathbb{K}(t_1, \ldots, t_n)^{\mathrm{Sym}}$.
Betrachte $f(T) = \prod_{i=1}^{n}(T - t_i) \in \mathbb{F}[T]$ (da symmetrisch in $t_1, \ldots, t_n$).
$f(T)$ heißt das **allgemeine Polynom vom Grad** n.
Damit $\mathbb{E} = \mathrm{Zfk}(f/\mathbb{F})$. Damit gilt $\mathrm{Gal}(f/\mathbb{F}) = \mathrm{Gal}(\mathbb{E}/\mathbb{F}) = S_n$.
Da S_n auf den Wurzeln von $f(T)$ transitiv operiert, ist $f(T)$ irreduzibel in $\mathbb{F}[T]$.

4.38.
Für $k = 1, \ldots, n$ heißt $s_k(t_1, \ldots, t_n) = \sum_{1 \le i_1 < \ldots < i_k \le n} t_{i_1} \cdot \ldots \cdot t_{i_k} \in \mathbb{K}[t_1, \ldots, t_n]^{\mathrm{Sym}}$ das k**-te elementarsymmetrische Polynom in** $t_1, \ldots, t_n$.

$f(T) = \prod_{i=1}^{n}(T - t_i) = T^n - s_1 T^{n-1} + \ldots + (-1)^{n-1} s_{n-1} T + (-1)^n s_n = \sum_{k=0}^{n} (-1)^k s_k T^{n-k}$, wobei $s_0 = 1$.

Offensichtlich gilt $s_1, \ldots, s_n \in \mathbb{K}(t_1, \ldots, t_n)^{\mathrm{Sym}}$. Wir wollen nun zeigen: $\mathbb{K}(t_1, \ldots, t_n)^{\mathrm{Sym}} = \mathbb{K}(s_1, \ldots, s_n)$.

Theorem 4.39.

(a) *Jedes $f \in \mathbb{K}[t_1, \ldots, t_n]^{Sym}$ ist von der Form $f = p(s_1, \ldots, s_n)$ für ein eindeutig bestimmtes Polynom $p \in \mathbb{K}[t_1, \ldots, t_n]$.*

(b) *Jedes $f \in \mathbb{K}(t_1, \ldots, t_n)^{Sym}$ ist von der Form $f = p(s_1, \ldots, s_n)$ für eine eindeutig bestimmte rationale Funktion $p \in \mathbb{K}(t_1, \ldots, t_n)$.*

Beweis:
$\mathbb{Z}_+ = \mathbb{N} \cup \{0\}$, $\mathbb{Z}_+^n = \mathbb{Z}_+ \times \ldots \times \mathbb{Z}_+$, $\mathbb{Z}_+^n \ni a = (a_1, \ldots, a_n)$.
Auf $\mathbb{Z}_+^n$ definieren wir die Lexikographische Ordnung $\le$:

$$a \le b \Leftrightarrow a = b \text{ oder es gibt } k \in \{1, \ldots, n\} \text{ mit } a_1 = b_1 \wedge \ldots \wedge a_{k-1} = b_{k-1} \wedge a_k < b_k$$

$\le$ ist eine totale Ordnung und sogar eine Wohlordnung (es gibt ein „kleinstes“ Element).
$\le$ ist mit der Addition verträglich: $a \le b \Rightarrow a + c \le b + c$.

Für $f \in \mathbb{K}[t_1, \ldots, t_n]$ sei $f = \sum c_a t^a$ mit $t^a := t_1^{a_1} \cdot \ldots \cdot t_n^{a_n}$ und *f.f.a.* $c_a = 0$.

Für $f \in \mathbb{K}[t_1, \ldots, t_n] \setminus \{0\}$ sei $l(f) := \max\{a \in \mathbb{Z}_+^n | c_a \neq 0\} \in \mathbb{Z}_+^n$ (wobei $f = \sum c_a t^a$) der Lexikographische Grad von f.
Für $f, g \in \mathbb{K}[t_1, \ldots, t_n] \setminus \{0\}$ gilt: $l(f \cdot g) = l(f) + l(g)$ und $l(f + g) \leq \max\{l(f), l(g)\}$ und sogar Gleichheit, falls $l(f) \neq l(g)$.

Für $a \in \mathbb{Z}_+^n$ sei $s^a = s_1^{a_1} \cdot \ldots \cdot s_n^{a_n}$. $l(s_k) = l(t_1 \cdot \ldots \cdot t_k) = (1, \ldots, 1, 0, \ldots, 0)$.
$l(s^a) = l(s_1^{a_1}) + \ldots + l(s_n^{a_n}) = b$ mit $b_i = a_i + \ldots + a_n$ (*).
$\Rightarrow (s^a : a \in \mathbb{Z}_+^n)$ ist $\mathbb{K}$-linear unabhängig.
Zu $b \in \mathbb{Z}_+^n$ gibt es (genau) ein $a \in \mathbb{Z}_+^n$ mit $l(s^a) = b$ (da (*) eindeutig lösbar ist).

(a) Sei $f \in \mathbb{K}[t_1, \ldots, t_n]^{\mathrm{Sym}}$ gegeben. Sei $b = l(f)$. Sei a bestimmt mit $l(s^a) = b$.
$f = \sum c_a t^a \rightsquigarrow (f - c_b s^a) < l(f) = b$ und $f - c_b \cdot s^a$ ist symmetrisch in $t_1, \ldots, t_n$.
Durch Iteration erhalten wir damit (konstruktiv) das Polynom p mit $f = p(s_1, \ldots, s_n)$.

(b) Existenz von p bedeutet gerade, dass $\mathbb{K}(s_1, \ldots, s_n) = \mathbb{K}(t_1, \ldots, t_n)^{\mathrm{Sym}} = \mathbb{F}$.
$\mathbb{L} = \mathbb{K}(s_1, \ldots s_n) \subset \mathbb{F} \subset \mathbb{E} = \mathbb{K}(t_1, \ldots, t_n)$. Außerdem $[\mathbb{E} : \mathbb{F}] = n!$.

$\mathbb{E} = \mathrm{Zfk}(f(T)/\mathbb{L})$, denn $f(T) = \prod_{i=1}^{n}(T - t_i) = \sum_{k=0}^{n}(-1)^k s_k T^{n-k} \in \mathbb{L}[T]$.
$\Rightarrow [\mathbb{E} : \mathbb{L}] \leq (\deg f)! = n! = [\mathbb{E} : \mathbb{F}]$.
$\Rightarrow \mathbb{L} = \mathbb{F}$.

□

4.40.
Sei $f(T) = c \cdot (T^n + a_1 T^{n-1} + \ldots + a_{n-1} T + a_n) \in \mathbb{K}[T]$ (mit $c \neq 0$), $f(T) = c \cdot \prod_{i=1}^{n}(T - \alpha_i) \in \overline{\mathbb{K}}[T]$
mit den Wurzeln $\alpha_1, \ldots, \alpha_n \in \overline{\mathbb{K}}$.
Sei $I_f = h(\alpha_1, \ldots, \alpha_n)$ für ein $h \in k[t_1, \ldots, t_n]^{\mathrm{Sym}}$ mit $k \subset \mathbb{K}$ ein Teilkörper.
Dann gibt es $p \in k[t_1, \ldots, t_n]$ mit $I_f = p(a_1, \ldots, a_n)$.
Denn: $a_k = (-1)^k \cdot s_k(\alpha_1, \ldots, \alpha_n)$.

Beispiel 4.41.
Diskriminante von f: $D(f) = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2 \in \overline{\mathbb{K}}$
$\Rightarrow D(f)$ ist ein Polynom in den Koeffizienten $a_1, \ldots, a_n$, insbesondere $D(f) \in \mathbb{K}$.

Bemerkung 4.42.
$D(f) \neq 0 \Leftrightarrow f$ ist separabel.

Beispiel 4.43.
$f = t^2 + at + b = (t - \alpha_1)(t - \alpha_2) = t^2 - (\alpha_1 + \alpha_2)t + \alpha_1\alpha_2$.
$D(f) = (\alpha_1 - \alpha_2)^2 = \underbrace{(\alpha_1 + \alpha_2)}_{=-a}^2 - 4\ \underbrace{\alpha_1\alpha_2}_{=b} = a^2 - 4b$

Satz 4.44.
Sei char$\mathbb{K} \neq 2$, *sei* $f \in \mathbb{K}[t]$ *separabel mit* $\deg f = n$. *Dann gilt bekanntlich* $Gal(f/\mathbb{K}) \leq S_n$.
Es gilt $Gal(f/\mathbb{K}) \leq A_n \Leftrightarrow D(f)$ *ist ein Quadrat in* $\mathbb{K}$.

Beweis:
$\mathbb{L} = \mathrm{Zfk}(f/\mathbb{K})$, $f = c \cdot \prod_{i=1}^{n}(t - \alpha_i)$ in $\overline{\mathbb{K}}[t]$.
Sei $\delta := \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j) \in \overline{\mathbb{K}}$.
Also $D(f) \in \mathbb{K}^2 \Leftrightarrow \delta \in \mathbb{K} \Leftrightarrow \sigma(\delta) = \delta\ fa\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{K})$, wegen $\mathbb{L}/\mathbb{K}$ galoissch.

Aber: $\sigma(\delta) = (-1)^r \cdot \delta$, wobei $r_\sigma = |\{1 \leq i \leq n : \sigma(\alpha_i) \neq \alpha_i\}|$.
D.h. $D(f) \in \mathbb{K} \Leftrightarrow r_\sigma$ gerade $\forall\ \sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{K}) \leq S_n \Leftrightarrow \mathrm{Gal}(\mathbb{L}/\mathbb{K}) \leq A_n$.

□

Bemerkungen 4.45.

1. Für *char*$\mathbb{K} = 2$ gilt immer $D(f) \in \mathbb{K}^2$, aber nicht immer $\mathrm{Gal}(f/\mathbb{K}) \leq A_n$.
2. $D(f) \notin \mathbb{K}^2$. Dann ist $\mathbb{K}(\sqrt{D(f)}) \subset \mathrm{Zfk}(f/\mathbb{K})$ gerade der Fixkörper von $\mathrm{Gal}(f/\mathbb{K}) \cap A_n$.

i. Kreisteilungskörper

Sei immer $\mathbb{K}$ *ein Körper,* $n \in \mathbb{N}$ *mit* $n \geq 1$.

Definition 4.46.
$\mu_n(\mathbb{K}) = \{\zeta \in \mathbb{K} : \zeta^n = 1\} \leq \mathbb{K}^*$ heißt die Gruppe der n**-ten Einheitswurzeln** in $\mathbb{K}$.
Ein $\zeta \in \mu_n(\mathbb{K})$ heißt **primitive** n**-te Einheitswurzel**, falls $\mathrm{ord}(\zeta) = n$; $\mu_n^*(\mathbb{K}) = \{\zeta \in \mu_n(\mathbb{K}) : \mathrm{ord}(\zeta) = n\} \subset \mu(\mathbb{K})$.

Satz 4.47.

(a) $\mu_n(\mathbb{K})$ *ist eine endliche zyklische Gruppe, deren Ordnung n teilt.*

(b) Gilt $char(\mathbb{K}) \nmid n$ *(z.B.* $char\mathbb{K} = 0$*), so gilt* $|\mu_n(\overline{\mathbb{K}})| = n$.

(c) Ist $char(\mathbb{K}) = p > 0$ *und* $n = p^r \cdot m$ *mit* $p \nmid m$, *so ist* $\mu_n(\mathbb{K}) = \mu_m(\mathbb{K})$ *und* $|\mu_n(\overline{\mathbb{K}})| = m$.

Beweis:

(a) Die Elemente von $\mu_n(\mathbb{K})$ sind die Nullstellen von $t^n - 1$ in $\mathbb{K} \Rightarrow |\mu_n(\mathbb{K})| \leq n < \infty$. Wegen $\mu_n(\mathbb{K}) \leq \mathbb{K}^*$ ist $\mu_n(\mathbb{K})$ zyklisch.
Sei $\zeta \in \mu_n(\mathbb{K})$ ein erzeugendes Element. Dann gilt $|\mu_n(\mathbb{K})| = \mathrm{ord}\zeta \mid n$ (denn $\zeta^n = 1$).

(b) Da $t^n - 1$ bei $char\mathbb{K} \nmid n$ separabel ist, hat $t^n - 1$ in $\overline{\mathbb{K}}$ genau n Nullstellen. $\Rightarrow$ $|\mu_n(\overline{\mathbb{K}})| = n$.

(c) $n = p^r \cdot m, p = char\mathbb{K}$. Dann $\zeta \in \mu_n(\mathbb{K}) \Leftrightarrow \zeta$ ist Nullstelle von $t^{p^r \cdot m} - 1 = (t^m - 1)^{p^r}$ $\Leftrightarrow \zeta$ ist Nullstelle von $t^m - 1 \Leftrightarrow \zeta \in \mu_m(\mathbb{K})$.
Insbesondere $|\mu_n(\overline{\mathbb{K}})| = |\mu_m(\overline{\mathbb{K}})| = m$.

□

Bemerkung 4.48.
$char(\mathbb{K}) \nmid n \Leftrightarrow \mu_n(\overline{\mathbb{K}}) = n \Leftrightarrow \mu_n^*(\overline{\mathbb{K}}) \neq \emptyset$ (d.h. es gibt eine primitive n-te Einheitswurzel in $\overline{\mathbb{K}}$).

Sei $char\mathbb{K} \nmid n$. Dann gilt $|\mu_n^*(\overline{\mathbb{K}})| = \varphi(n)$ ($\varphi(n)$: Eulersche φ-Funktion)
(denn mit $\zeta \in \mu_n^*(\overline{\mathbb{K}})$ ist $\mu_n^*(\overline{\mathbb{K}}) = \{\zeta^k : 1 \leq k < n, \mathrm{ggT}(k, n) = 1\}$.

Beispiel:
$\mathbb{K} = \mathbb{C}$: $\mu_n(\mathbb{C}) = \{e^{\frac{2k\pi i}{n}} : 0 \le k < n\}$; $\mu_n^*(\mathbb{C}) = \{e^{\frac{2k\pi i}{n}} : 0 < k < n \wedge \mathrm{ggT}(k,n) = 1\}$.

Definition 4.49.
$\Phi_n(t) := \prod_{\zeta \in \mu_n^*(\mathbb{C})} (t - \zeta) \in \mathbb{C}[t]$ heißt das n**-te Kreisteilungspolynom**.

- $\Phi_n(t)$ ist normiert und $\deg \Phi_n(t) = |\mu_n^*(\mathbb{C})| = \varphi(n)$.

Lemma 4.50.
$t^n - 1 = \prod_{d|n} \Phi_d(t)$ *in* $\mathbb{C}[t]$.

Beweis:
$$t^n - 1 = \prod_{\zeta \in \mu_n(\mathbb{C})} (t - \zeta) = \prod_{d|n} \underbrace{\prod_{\zeta \in \mu_n(\mathbb{C}):\mathrm{ord}(zeta)=d} (t - \zeta)}_{=\Phi_d(t)} = \prod_{d|n} \underbrace{\prod_{\zeta \in \mu_d^*(\mathbb{C})} (t - \zeta)}_{\Phi_d(t)}.$$
□

Korollar 4.51.

(a) $\Phi_n(t) \in \mathbb{Z}[t] \ \ \forall\, n \ge 1$.

(b) Für einen beliebigen Körper $\mathbb{K}$ *mit* $\mathrm{char}\mathbb{K} \nmid n$ *gilt* $\Phi_n(t) = \prod_{\zeta \in \mu_n^*(\overline{\mathbb{K}})} (t - \zeta)$.

Beweis:

(a) Induktion nach n: $\Phi_1(t) = t - 1 \in \mathbb{Z}[t]$.
Sei $\Phi_d(t) \in \mathbb{Z}[t]$ (und normiert) $\forall\, d < n$.
$$\underbrace{t^n - 1}_{\in \mathbb{Z}[t],\ \text{normiert}} = \underbrace{\prod_{d|n, d \ne n} \Phi_d}_{\in \mathbb{Z}[t],\ \text{normiert}} \cdot \Phi_n(t) \Rightarrow \text{nach dem Gauß'schen Lemma ist auch } \Phi_n(t) \in \mathbb{Z}[t].$$

(b) Sei $\widetilde{\Phi}_n(t) = \prod_{\zeta \in \mu_n^*(\overline{\mathbb{K}})} (t - \zeta)$. Wie in 4.50 folgt $t^n - 1 = \prod_{d|n} \widetilde{\Phi}_d(t)$ in $\overline{\mathbb{K}}[t] \Rightarrow$
$\prod_{d|n} \Phi_d(t) = t^n - 1 = \prod_{d|n} \widetilde{\Phi}_d(t) \ \ \forall\, n \ge 1$.
$\Rightarrow \Phi_n(t) = \widetilde{\Phi}_n(t) \ \ \forall\, n \ge 1$ (Induktion nach n).

□

Lemma 4.52.
Sei p eine Primzahl und $n \geq 1$.

(a) $\Phi_p(t) = t + \ldots + t + 1$.

(b) $p \mid n \Rightarrow \Phi_{pn}(t) = \Phi_n(t^p)$.

(c) $p \nmid n \Rightarrow \Phi_{pn}(t) = \frac{\Phi_n(t^p)}{\Phi_n(t)}$.

(d) *n ist ungerade* $\Rightarrow \Phi_{2n}(t) = \Phi_n(-t)$.

Beweis:

(a) $t^p - 1 = \Phi_1(t) \cdot \Phi_p(t) = (t-1) \cdot \Phi_p(t) \Rightarrow$ Behauptung.

(b) Es gilt: $\zeta \in \mu^*_{pn}(\mathbb{C}) \Rightarrow \zeta^p \in \mu^*_n(\mathbb{C})$.
$\Rightarrow \Phi_{pn}(t) = \prod_{\zeta \in \mu^*_{pn}(\mathbb{C})} (t - \zeta) \mid \Phi_n(t^p)$.
Da beide Polynome normiert sind und $\deg \Phi_{pn}(t) = \underbrace{\varphi(p \cdot n) = p \cdot \varphi(n)}_{\text{wegen } p \mid n} =$ $\deg \Phi_n(t^p)$ folgt die Behauptung.

(c) $p \nmid n$. Dann gilt für $\zeta \in \mathbb{C}$: $\zeta \in \mu^*_n(\mathbb{C}) \Leftrightarrow \zeta^p \in \mu^*_n(\mathbb{C})$.
$\Rightarrow \Phi_n(t) = \prod_{\zeta \in \mu^*_n(\mathbb{C})} (t - \zeta) \mid \Phi_n(t^p)$.
Für $\zeta \in \mu^*_{pn}(\mathbb{C})$ gilt $\zeta^p \in \mu^*_n(\mathbb{C})$, d.h. ζ ist eine Nullstelle von $\Phi_n(t^p)$, aber nicht von $\Phi_n(t)$.
$\Phi_{pn}(t) = \prod^{(}_{\zeta \in \mu^*_{pn}(\mathbb{C})} t - \zeta) \mid \frac{\Phi_n(t^p)}{\Phi_n(t)}$.
Da beide Seiten normiert sind und $\deg \Phi_{pn}(t) = \underbrace{\varphi(pn) = (p-1)\varphi(n)}_{\text{wegen } p \nmid n} = \deg \frac{\Phi_n(t^p)}{\Phi_n(t)}$
folgt die Behauptung.

(d) $\zeta \in \mathbb{C}, 2 \nmid n$: $\zeta \in \mu^*_{2n}(\mathbb{C}) \Leftrightarrow -\zeta \in \mu^*_n(\mathbb{C})$.
$\Rightarrow$ Behauptung (Zitat: „Jetzt blick ich nicht mehr durch - das ist ganz einfach ...“)

□

Beispiele 4.53.

n	$\Phi_n(t)$
1	$t-1$
2	$t+1$
3	t^2+t+1
4	t^2+1
5	$t^4\ldots+t+1$
6	t^2-t+1

Satz 4.54.
$\Phi_n(t)$ ist irreduzibel in $\mathbb{Q}[t]$ für alle $n \geq 1$.

Beweis:
Angenommen, $\Phi_n(t) = f(t)\cdot g(t)$ mit $f, g \in \mathbb{Z}[t]$ normiert, $f(t)$ irreduzibel, $g(t)$ nicht konstant.
Dann gibt es ein $\zeta \in \mu_n^*(\mathbb{C})$ mit $f(\zeta) = 0$ und $g(\zeta^p) = 0$ für eine Primzahl $p \nmid n$.
(Denn: wähle $\xi \in \mu_n^*(\mathbb{C})$ und $f(\xi) = 0$; sei dann $m \leq 1$ minimal mit $g(\xi^m) = 0$; $m \neq 1$, da $\Phi_n(t)$ separabel, und $ggT(m,n) = 1 \Rightarrow$ $\exists$ eine Primzahl p mit $p \mid m \rightsquigarrow m = p\cdot m'$. Sei $\zeta = \xi^{m'} \Rightarrow$ (wegen m minimal) $f(\zeta) = 0$ und $g(zeta^p) = g(\xi^m) = 0$ und $p \nmid n$)

$f(t) = \mathrm{MinPol}(\zeta/\mathbb{Q}) \mid g(t^p)$ in $\mathbb{Z}[t]$.
In $\mathbb{F}_p[t]$ folgt: $\overline{f}(t) \mid \overline{g}(t^p) = \overline{g}(t)^p$.
Also sind $\overline{f}(t)$ und $\overline{g}(t)$ nicht teilerfremd. $\Rightarrow \overline{\Phi}(t) = \overline{f}(t)\cdot\overline{g}(t)$ ist nicht separabel.
Jedoch gilt $\overline{\Phi}(t) \mid t^n - 1$ und $t^n - 1$ ist auch über $\mathbb{F}_p$ separabel, da $p \nmid n$.
$\Rightarrow$ Widerspruch.

□

Korollar 4.55.
Sei $\zeta_n \in \mathbb{C}$ eine n-te primitive Einheitswurzel. Dann gilt $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \underbrace{\deg MinPol(\zeta_n/\mathbb{Q})}_{\Phi_n(t)} = \varphi(n)$.

Satz 4.56.
Sei $\mathbb{K}$ ein Körper, sei $n \in \mathbb{N}$ mit $char(\mathbb{K}) \nmid n$. Sei $\zeta_n \in \overline{\mathbb{K}}$ eine primitive n-te Einheitswurzel, sei $\mathbb{K}_n := \mathbb{K}(\zeta)$.

(a) $\mathbb{K}_n = Zfk(t^n - 1/\mathbb{K})$ *und ist galoissch über* $\mathbb{K}$.

(b) Für jedes $\sigma \in G = Gal(\mathbb{K}_n/\mathbb{K})$ gibt es ein eindeutiges $j = j(\sigma) \in \{1,\ldots,n\}$ mit $ggT(j,n) = 1$ und $\sigma(\zeta) = \zeta^{j(\sigma)}$ $\forall\ \zeta \in \mu_n(\mathbb{K})$.

(c) *Die Abbildung* $\chi_n : G = Gal(\mathbb{K}_n/\mathbb{K}) \to (\mathbb{Z}/n)^*$, $\chi_n(\sigma) := j(\sigma) \mod n$, *ist ein injektiver Gruppenhomomorphismus.*

(d) *Insbesondere ist* $Gal(\mathbb{K}_n/\mathbb{K})$ *eine Untergruppe von* $(\mathbb{Z}/n)^*$ *und ist somit abelsch.*

Beweis:

(a) Klar: $\mathbb{K}_n/\mathbb{K}$ ist galoissch als Zerfällungskörper des separablen Polynoms $t^n - 1$.

(b) $\sigma \in \Gamma$ muss ζ_n wieder auf eine primitive n-te Einheitswurzel abbilden. $\Rightarrow \sigma(\zeta_n) = \sigma_n^{j(\sigma)}$ mit $j(\sigma)$ teilerfremd zu n, eindeutig modulo n. Für alle $\zeta \in \mu_n(\mathbb{K})$ ist damit $\sigma(\zeta) = \zeta^{j(\sigma)}$ *(denn* $\zeta = \zeta_n^k$ *mit* $k \in \mathbb{N} \Rightarrow \sigma(\zeta) = \sigma(\zeta_n^k) = \sigma(\zeta_n)^k = \zeta^{j(\sigma)}$*).*

(c) $\chi_n : \sigma \mapsto j(\sigma) \mod n$ ist injektiv, da ζ_n die Erweiterung $\mathbb{K}_n/\mathbb{K}$ erzeugt.
Homomorph: ist auch $\tau \in G = \mathrm{Gal}(\mathbb{K}_n/\mathbb{K})$, so gilt $\sigma \circ \tau(\zeta_n) = \sigma(\tau(\zeta_n)) = \sigma(\zeta_n^{j(\tau)}) = \sigma(\zeta_n)^{j(\tau)} = (\zeta_n^{j(\sigma)})^{j(\tau)} = \zeta_n^{j(\sigma)\cdot j(\tau)}$, also $j(\sigma \circ \tau) = j(\sigma) \cdot j(\tau) \mod n$.

(d) aus (c).

□

Der Körper $\mathbb{K}_n = \mathbb{K}(\zeta_n)$ heißt der n-te **Kreisteilungskörper** über $\mathbb{K}$, und der Homomorphismus $\chi_n : \mathrm{Gal}(\mathbb{K}_n/\mathbb{K}) \hookrightarrow (\mathbb{Z}/n)^*$ heißt der n-te **zyklotomische Charakter**.

Korollar 4.57.
($\mathbb{K} = \mathbb{Q}$)
Sei ζ *eine primitive n-te Einheitswurzel in* $\mathbb{C}$*. Der Kreisteilungskörper* $\mathbb{Q}_n = \mathbb{Q}(\zeta_n)$ *hat die Galoisgruppe* $(\mathbb{Z}/n)^*$*.*

Beweis:
$[\mathbb{Q}_n : \mathbb{Q}] = \deg(\Phi_n(t))$ (nach 4.54: $\Phi_n/\mathbb{Q}$ irreduzibel)
$\deg(\Phi_n(t)) = \varphi(n) = (\mathbb{Z}/n)^*$.
$\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \leq (\mathbb{Z}/n)^*$ mit voller Mächtigkeit $\Rightarrow$ Behauptung.

□

4.58. [Anwendung auf Konstruktion regelmäßiger n-Ecke mit Zirkel und Lineal]
Hatten gesehen (4.28): $\alpha \in \mathbb{C}$ ist aus $0, 1$ konstruierbar $\Leftrightarrow$ galoissche Hülle von $\mathbb{Q}(\alpha)/\mathbb{Q}$ hat 2-Potenzgrad.

Das regelmäßige n-Eck ist konstruierbar $\Leftrightarrow$ die galoissche Hülle von $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ hat 2-Potenzgrad.
Wegen $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ galoissch vom Grad $\varphi(n)$ folgt:

Genau dann, wenn $\varphi(n)$ eine 2-Potenz ist, ist das regelmäßige n-Eck konstruierbar.

Ist $n = \prod_i p_i^{e_i}$ (mit p_i prim, paarweise verschieden), gilt $\varphi(n) = \prod_i (p_i - 1)p_i^{e_i - 1}$. Es folgt:

Theorem 4.59.
Genau dann ist das regelmäßige n-Eck mit Zirkel und Lineal konstruierbar, wenn $n = 2^k \cdot p_1 \cdot \ldots \cdot p_r$ *mit Primzahlen* $p_1 < \ldots < p_r$ *mit* $p_i - 1$ *eine 2-Potenz für* $i = 1, \ldots, r$.

Welche Zahlen der Form $2^s + 1$ sind prim?

Lemma 4.60.
$2^s + 1$ *ist prim* $\Rightarrow$ s *ist eine Potenz von* 2.

Beweis:
$s = 2^k \cdot t$ mit $t > 1$ ungerade.
$x^t + 1 = (x + 1) \cdot (x^{t-1} - x^{t-2} \pm \ldots \pm 1)$
Setze $x := 2^{2^k} \Rightarrow x^t + 1 = (2^{2^k})^t + 1 = 2^{2^k \cdot t} + 1 = 2^s + 1$ ist durch $2^{2^k} + 1$ teilbar.

□

4.61.

n	$2^{2^n} + 1$	
0	3	*prim*
1	5	*prim*
2	17	*prim*
3	257	*prim*
4	65537	*prim*
5	4294967297	$= 641 \cdot 6700417$

Vermutung (von Fermat): $F_n := 2^{2^n} + 1$ ist prim für alls n.
Die Vermutung ist falsch: Euler fand die obige Zerlegung von F_5.

Definition 4.62.
Eine Primzahl der Form $F_n = 2^{2^n}$ heißt **Fermatsche Primzahl**.

Bemerkung 4.63.
F_0, F_1, F_2, F_3, F_4 sind die einzigen bekannten Fermatschen Primzahlen.
Man weiß für $5 \leq n \leq 32$, dass F_n zusammengesetzt ist.
Unbekannt ist, ob es eine Fermatsche Primzahl F_n mit $n \geq 5$ gibt!

Theorem 4.64 (von Gauß)**.**
Sei $n \geq 3$. Das regelmäßige n-Eck ist genau dann mit Zirkel und Lineal konstruierbar, wenn $n = 2^k \cdot p_1 \cdot \ldots \cdot p_r$ mit Fermatschen Primzahlen $p_1, \ldots, p_r$.

j. Auflösung von Gleichungen durch Radikale

4.65.
Sei $\mathbb{K}$ ein Körper. Wir studieren zunächst Gleichungen der Form $x^n = a$.

Ist $char(\mathbb{K}) = p > 0$ und $p \mid n$, so ist $t^n - a$ inseparabel. Setze daher stets $char(\mathbb{K}) \nmid n$ voraus.
Dann ist $t^n - a$ mit $a \in \mathbb{K}^*$ separabel. Ist $\alpha \in \overline{\mathbb{K}}$ eine Nullstelle von $t^n - a$, d.h. $\alpha^n = a$ und ist $\zeta \in \overline{\mathbb{K}}$ eine primitive n-te Einheitswurzel, so ist $t^n - a = \prod_{j=0}^{n-1}(t - \alpha\zeta^j)$.
Sei $\mathbb{L} := \mathrm{Zfk}(t^n - a/\mathbb{K})$, also $\mathbb{L} = \mathbb{K}(\alpha, \zeta)$.

Satz 4.66.
$char(\mathbb{K}) \nmid n$, $a \in \mathbb{K}^*$.
Dann ist $Gal(t^n - a/\mathbb{K})$ eine Untergruppe der Gruppe $GA_1(n) := \left\{ \begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix} : c, d \in \mathbb{Z}/n, c \in (\mathbb{Z}/n)^* \right\}$ $(\leq GL_2(\mathbb{Z}/n))$.
Insbesondere ist $Gal(t^n - a/\mathbb{K})$ auflösbar.

Beweis:
Sei $\sigma \in G := \mathrm{Gal}(t^n - a/\mathbb{K}) \Rightarrow$ habe $\sigma(\alpha) = \zeta^d\alpha$ mit $d \in \mathbb{Z}$, und $\sigma(\zeta) = \zeta^c$ mit $c \in \mathbb{Z}, \mathrm{ggT}(c, n) = 1$.
Dann ist $\sigma(\zeta^j\alpha) = \zeta^{cj+d}\alpha$. Die Abbildung $G \to GA_1(n), \sigma \mapsto \begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix}$ ist ein Gruppenhomomorphismus: ist $\sigma' \in G$ mit $\sigma'(\zeta^j\alpha) = \zeta^{c'j+d'}\alpha$, so ist
$(\sigma' \circ \sigma)(\zeta^j\alpha) = \sigma'(\zeta^{cj+d}\alpha) = \zeta^{c'(cj+d)+d'}\alpha = \zeta^{c'ch+(c'd+d')}\alpha$.
$\Rightarrow \begin{pmatrix} c' & d' \\ 0 & 1 \end{pmatrix}\begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} c'c & c'd + d' \\ 0 & 1 \end{pmatrix} \Rightarrow$ homomorph.
Injektiv ist klar. Die Gruppe $GA_1(n)$ (und damit auch G ist auflösbar: $N := \left\{ \begin{pmatrix} 1 & d \\ 0 & 1 \end{pmatrix} : d \in \mathbb{Z}/n \right\} \trianglelefteq GA_1(n)$.
$GA_1(n)/N \cong ((\mathbb{Z}/n)^*, \cdot), N \cong (\mathbb{Z}/n, +)$. (hier also $G \trianglerighteq N \trianglerighteq \{e\}$)
□

Definition 4.67.
Eine Körpererweiterung $\mathbb{L}/\mathbb{K}$ heißt auflösbar (bzw. abelsch, zyklisch), wenn $\mathbb{L}/\mathbb{K}$ galoissch ist und $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ auflösbar (bzw. abelsch, zyklisch) ist.

Korollar 4.68.
$char(\mathbb{K}) \nmid n$, sei $|\mu_n(\mathbb{K})| = n$ (d.h. $\mathbb{K}$ enthalte die n-ten Einheitswurzeln).

Dann ist für $a \in \mathbb{K}^*$ die Erweiterung Zfk$(t^n - a/\mathbb{K})$ zyklisch über $\mathbb{K}$ und der Grad teilt n.

Beweis:
$G := \mathrm{Gal}(t^n - a/\mathbb{K})$.
$G \hookrightarrow GA_1(n)$, $\sigma \mapsto \begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix}$: hier ist $c = 1$; stets also $G \leq \left\{ \begin{pmatrix} 1 & d \\ 0 & 1 \end{pmatrix} : d \in \mathbb{Z}/n \right\} \cong \mathbb{Z}/n$.

□

Definition 4.69.
Eine Gleichung der Form $x^n = a$ mit $a \in \mathbb{K}^*$ heißt eine reine Gleichung.

Nebenbemerkung: $\mu_n(\mathbb{K})| = n \Leftrightarrow char(\mathbb{K}) \nmid n$ und $\mathbb{K}$ enthält eine (alle) primitive n-te Einheitswurzel(n).

Wir haben gesehen: ist $|\mu_n(\mathbb{K})| = n$, so ist der Zerfällungskörper jeder reinen Gleichung zyklisch über $\mathbb{K}$.
Umkehrung:

Theorem 4.70.
Sei $|\mu_n(\mathbb{K})| = n$. Jede zyklische Erweiterung von $\mathbb{K}$ vom Grad n ist Wurzelkörper einer reinen irreduziblen Gleichung $t^n - a$ mit $a \in \mathbb{K}^*$.

Das folgt aus folgender genaueren Version:

Satz 4.71.
Sei $|\mu_n(\mathbb{K})| = n$, sei $\mathbb{L}/\mathbb{K}$ zyklisch vom Grad n, sei etwa $Gal(\mathbb{L}/\mathbb{K}) = \langle\sigma\rangle$. Für jedes $\alpha \in \mathbb{L}^*$ sind äquivalent:

(i) $\mathbb{L} = \mathbb{K}(\alpha)$ und $\alpha^n \in \mathbb{K}$;

(ii) es gibt eine primitive n-te Einheitswurzel $\zeta \in \mathbb{K}$ mit $\sigma(\alpha) = \alpha \cdot \zeta$.

Es gibt ein $\alpha \in \mathbb{L}^*$ mit (i) und (ii). Für jedes solche α ist $(1, \alpha, \ldots, \alpha^{n-1})$ eine $\mathbb{K}$-Basis des $\mathbb{K}$-Vektorraums $\mathbb{L}$.

Nebenbemerkung zu (a): $a := \alpha^n \in \mathbb{K}$, α ist Nullstelle von $t^n - a = 0 \Rightarrow \mathbb{L} = \mathrm{Wkp}(t^n - a/\mathbb{K})$.

Beweis:
σ ist ein Endomorphismus des $\mathbb{K}$-Vektorraums $\mathbb{L}$.
$\sigma^n = id \Rightarrow$ MinPol$(\sigma/\mathbb{K})$ teilt $t^n - 1$. $\Rightarrow$ alle Eigenwerte von σ sind n-te Einheitswurzeln.
Für $\zeta \in \mu_n(\mathbb{K})$ sei $\mathbb{L}_\zeta := \text{Eig}(\sigma; \zeta)$. Dann ist $\mathbb{L}_{\zeta_1} \cdot \mathbb{L}_{\zeta_2} = \mathbb{L}_{\zeta_1\zeta_2} : \alpha_i \in \mathbb{L}_{\zeta_i}$
$\Rightarrow \sigma(\alpha_1\alpha_2) = \sigma(\alpha_1) \cdot \sigma(\alpha_2) = \zeta_1\alpha_1 \cdot \zeta_2\alpha_2 = (\zeta_1\zeta_2)(\alpha_1\alpha_2)$.
Behaupte, σ ist diagonalisierbar über $\mathbb{K}$: $\sigma^n = id$ und $char\mathbb{K} \nmid n$ impliziert, dass kein Jordankästchen der Größe ≥ 2 vorkommen kann.

Es ist $\dim_{\mathbb{K}}(\mathbb{L}_\zeta) \leq 1$ für alle $\zeta \in \mu_n(\mathbb{K})$. Denn seien $0 \neq \alpha, \beta \in \mathbb{L}_\zeta \Rightarrow \sigma(\frac{\alpha}{\beta}) = \frac{\sigma(\alpha)}{\sigma(\beta)} = \frac{\zeta\alpha}{\zeta\beta} = \frac{\alpha}{\beta} \Rightarrow \frac{\alpha}{\beta} \in \mathbb{K}$.
Es folgt: $\dim_{\mathbb{K}}(\mathbb{L}_\zeta) = 1 \ \ \forall\, \zeta \in \mu_n(\mathbb{K})$.

(i) $\Rightarrow$ (ii): $\mathbb{L} = \mathbb{K}(\alpha)$, $\alpha^n =: a \in \mathbb{K}$.
$\Rightarrow (\frac{\sigma(\alpha)}{\alpha})^n = \frac{\sigma(\alpha^n)}{\alpha^n} = \frac{a}{a} = 1$.
$\Rightarrow \sigma(\alpha) = \zeta \cdot \alpha$ für eine n-te Einheitswurzel ζ.
Wäre $\zeta^m = 1$ für $1 \leq m < n$, so wäre $\sigma^m(\alpha) = \zeta^m\alpha = \alpha$, also $\sigma^m = id$ wegen $\mathbb{L} = \mathbb{K}(\alpha)$ $\rightarrow$ Widerspruch.

(ii) $\Rightarrow$ (i): klar: $\sigma(\alpha^n) = \sigma(\alpha)^n = \zeta^n\alpha^n = \alpha^n \Rightarrow \alpha^n \in \mathbb{K}$.
Wäre $\mathbb{L} \supsetneq \mathbb{K}(\alpha) \supset \mathbb{K}$ mit $[\mathbb{K}(\alpha) : \mathbb{K}] = m < n$, so wäre $\sigma^m(\alpha) = \alpha$, aber $\sigma^m(\alpha) = \zeta^m\alpha \neq \alpha$ wegen $\zeta^m \neq 1 \rightarrow$ Widerspruch.

□

Definition 4.72.
Eine endliche Erweiterung $\mathbb{L}/\mathbb{K}$ heißt eine Radikalerweiterung, wenn es eine Kette $\mathbb{K} = \mathbb{K}_0 \subset \mathbb{K}_1 \subset \ldots \subset \mathbb{K}_r$ mit $\mathbb{L} \subset \mathbb{K}_r$ und $\mathbb{K}_i$ aus $\mathbb{K}_{i-1}$ durch Adjunktion einer Nullstelle einer reinen Gleichung über $\mathbb{K}_{i-1}$ ($t^{n_i} - a_{i-1}$ mit $a_{i-1} \in \mathbb{K}_{i-1}$ entsteht.

Man sagt auch: ein $\alpha \in \overline{\mathbb{K}}$ ist durch Radikale ausdrückbar über $\mathbb{K}$, wenn $\mathbb{K}(\alpha)/\mathbb{K}$ eine Radikalerweiterung ist.

Beispiele 4.73.

1. Jede zyklotomische Erweiterung $\mathbb{K}(\zeta_n)/\mathbb{K}$ (ζ_n eine primitive n-te Einheitswurzel) ist eine Radikalerweiterung.

2. Seien $\mathbb{L}, \mathbb{M}$ endlich Erweiterungen von $\mathbb{K}$ in $\overline{\mathbb{K}}$.

   (a) $\mathbb{L}/\mathbb{K}$ ist Radikalerweiterung $\Rightarrow \mathbb{M}\mathbb{L}/\mathbb{M}$ ist auch eine Radikalerweiterung.

(b) Ist $\mathbb{L} \subset \mathbb{M}$, sind $\mathbb{L}/\mathbb{K}$ und $\mathbb{M}/\mathbb{L}$ Radikalerweiterungen $\Rightarrow$ auch $\mathbb{M}/\mathbb{K}$ ist eine Radikalerweiterung.

3. Jede zyklische Erweiterung $\mathbb{L}/\mathbb{K}$ (bei $char\mathbb{K} = 0$) ist eine Radikelerweiterung: ist $[\mathbb{L} : \mathbb{K}] = n$, so ist $\mathbb{L}(\zeta_n)/\mathbb{K}(\zeta_n)$ zyklisch (Grad teilt n). Nach Lagrange ist $\mathbb{L}(\zeta_n)/\mathbb{K}(\zeta_n)$ eine Radikalerweiterung $\Rightarrow$ auch $\mathbb{L}/\mathbb{K}$ ist eine Radikalerweiterung.

Sei ab jetzt immer $char\mathbb{K} = 0$.

Theorem 4.74.
Sei $\mathbb{L}/\mathbb{K}$ *eine endliche Erweiterung. Dann gilt:* $\mathbb{L}/\mathbb{K}$ *ist eine Radikalerweiterung* $\Leftrightarrow$ *für die galoissche Hülle* $\mathbb{E}$ *von* $\mathbb{L}/\mathbb{K}$ *gilt:* $Gal(\mathbb{E}/\mathbb{K})$ *ist auflösbar.*

Beweis:

„$\Leftarrow$“ Sei zunächst $Gal(\mathbb{E}/\mathbb{K})$ auflösbar. Dann gibt es eine Kompositionsreihe mit zyklischen Faktorgruppen. Sei $\mathbb{K} = \mathbb{K}_0 \subset \mathbb{K}_1 \subset \ldots \subset \mathbb{K}_n = \mathbb{E}$ die zugehörige Kette der Fixkörper.
Die $\mathbb{K}_i/\mathbb{K}_{i-1}$ sind zyklisch, also Radikalerweiterungen nach 4.73 3. $\Rightarrow$ auch $\mathbb{E}/\mathbb{K}$ ist eine Radikalerweiterung $\Rightarrow$ auch $\mathbb{L}/\mathbb{K}$ ist eine Radikalerweiterung.

„$\Rightarrow$“ Sei $\mathbb{K} = \mathbb{K}_0 \subset \mathbb{K}_1 \subset \ldots \subset \mathbb{K}_r$ mit $\mathbb{L} \subset \mathbb{K}_r$ mit $\mathbb{K}_i = \mathbb{K}_{i-1}(\alpha_i)$ mit $\alpha_i^{n_i} \in \mathbb{K}_{i-1}$ für $i = 1, \ldots, r$.
Sei $\mathbb{E}_1$ = die galoissche Hülle von $\mathbb{K}_1/\mathbb{K}_0 = \mathbb{K}$. Dann ist $Gal(\mathbb{E}_1/\mathbb{K})$ auflösbar: $\mathbb{K}_1 = \mathbb{K}(\alpha_1), \alpha_1^n = a \in \mathbb{K}$; haben gesehen: $Gal(t^n - a/\mathbb{K})$ ist auflösbar.
Nun sei $\mathbb{E}_2$ = die galoissche Hülle von $E_1\mathbb{K}_2$ über $\mathbb{E}_1$.
$\vdots$
$\mathbb{E}_r$ = die galoissch Hülle von $\mathbb{E}_{r-1}\mathbb{K}_r$ über $\mathbb{E}_{r-1}$.
Jeder Schritt $\mathbb{E}_i/\mathbb{E}_{i-1}$ ist galoissch mit auflösbarer Gruppe.
Sei $\mathbb{F}$:= die galoissche Hülle von $\mathbb{E}_r/\mathbb{K}$. Dann ist $Gal(\mathbb{F}/\mathbb{K})$ auflösbar $\Rightarrow$ auch Gal(gal. Hülle von $\mathbb{L}/\mathbb{K}$) ist auflösbar nach folgendem Lemma:

□

Lemma 4.75.
Sei G *eine Gruppe,* $H = H_r \leq H_{r-1} \leq \ldots \leq H_1 \leq G$ *so dass gelten:*

(1) $H_i \trianglelefteq H_{i-1}$ $\forall$ i;

(2) H_{i-1}/H_i *auflösbar* $\forall$ i.

Sei $N := \bigcap_{g \in G} gHg^{-1}$ *(der größte in H enthaltene Normalteiler von G).*
Dann ist G/N *auflösbar.*

Beweis:
Aufgabe 51.

□

Bemerkung 4.76.
Achtung: Betrachte die Gleichung die Gleichung $x^4 + x^3 + x^2 + x + 1 = 0$ über $\mathbb{Q}$. Schreibe $x = \sqrt[5]{1}$, oder $(\sqrt[10]{1})^2$.
Das ist problematisch, da das Symbol „$\sqrt[5]{1}$“ über $\mathbb{Q}$ keinen eindeutigen algebraischen Sinn hat: denn das Polynom $t^5 - 1$ ist reduzibel über $\mathbb{Q}$ und hat Nullstellen, die nicht zueinander über $\mathbb{Q}$ konjugiert sind, also verschiedene Gleichungen erfüllen.

Satz 4.77.
Sei $\mathbb{L}/\mathbb{K}$ *eine Radikalerweiterung. Dann gibt es eine Kette* $\mathbb{K} = \mathbb{K}_0 \subset \mathbb{K}_1 \subset \ldots \subset \mathbb{K}_r$ *mit* $\mathbb{L} \subset \mathbb{K}$ *und* $\mathbb{K}_i = \mathbb{K}_{i-1}(\alpha_i)$ *mit* $\alpha_i^{n_i} =: c_i \in \mathbb{K}_{i-1}$ *derart, dass das Polynom* $t^{n_i} - c_i \in \mathbb{K}_{i-1}[t]$ *irreduzibel ist* $\forall$ *i.*
(man sagt: $\mathbb{K}_r$ *entsteht aus* $\mathbb{K}$ *durch Adjunktion von irreduziblen Radikalen)*

Beweis:
durch Induktion - siehe Skript Scheiderer.

□

Korollar 4.78 (Galois 1830)**.**
Ist $f \in \mathbb{K}[t]$ *ein separables Polynom, so lassen sich die Nullstellen von* f *genau dann durch iterierte (irreduzible) Radikale über* $\mathbb{K}$ *ausdrücken, wenn Gal*$(f/\mathbb{K})$ *auflösbar ist.*

Das ist für $\deg(f) \leq 4$ *stets der Fall, für* $\deg(f) \geq 5$ *dagegen im Allgemeinen nicht.*

Dass sich Gleichungen vom Grad 5 im Allgemeinen nicht auflösen lassen, wussten schon Ruffini (1799) und Abel (1824).

Gibt es Gleichungen $f \in \mathbb{K}[t]$ mit vorgegebener $\mathrm{Gal}(f/\mathbb{K}) = G$?
Z.B. $G = S_n$: $\mathbb{K}(x_1, \ldots x_n)/\mathbb{K}(x_1, \ldots, x_n)^{\mathrm{Sym}}$ ist galoissch, Gruppe S_n.

Fixiert man aber $\mathbb{K}$, so ist es im Allgemeinen nicht wahr, dass jede endliche Gruppe G als $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ vorkommt. $\mathbb{K} = \mathbb{Q}$?

Theorem 4.79 (Galois)**.**
Sei p eine Primzahl, $f \in \mathbb{K}[t]$ irreduzibel, $\deg(f) = p$. Dann sind äquivalent:

(i) $f(x) = 0$ *ist durch Radikale auflösbar;*

(ii) $Gal(f/\mathbb{K})$ *ist in* S_p *zu einer Untergruppe von* $GA_1(\mathbb{F}_p)$ *konjugiert;*

(iii) es gibt $\alpha, \beta \in \overline{\mathbb{K}}$ *mit* $f(\alpha) = f(\beta) = 0$ *derart, dass* f *über* $\mathbb{K}(\alpha, \beta)$ *zerfällt.*

Beweis:
Siehe Theorem 3.117: $G \leq S_p$ transitiv: auflösbar $\Leftrightarrow$ (ii) $\Leftrightarrow$ jedes $\sigma \neq id$ in G hat höchstens einen Fixpunkt.
$\{1, \ldots, p\} \longleftrightarrow \{\alpha_1, \ldots, \alpha_p\}$ (α_i Nullstellen von f). $\sigma(\alpha_1) = \alpha_1$, $\sigma(\alpha_2) = \alpha_2$
$\Rightarrow$ (iii).

□

Korollar 4.80.
Sei $f \in \mathbb{Q}[t]$ irreduzibel, $\deg(f) = p$ prim. Es habe f mindestens zwei reelle und mindestens eine nichtreelle Nullstelle. Dann ist $Gal(f/\mathbb{Q})$ nicht auflösbar.

Beweis:
Sei $\mathbb{L} := \mathrm{Zfk}(f/\mathbb{Q})$. Seien $\alpha \neq \beta$ reelle Nullstellen von f. Dann ist $\mathbb{Q}(\alpha, \beta) \subset \mathbb{R}$, aber $\mathbb{L} \not\subset \mathbb{R} \Rightarrow \mathbb{Q}(\alpha, \beta) \neq \mathbb{L}$.

□

Beispiel:
$p \geq 5$, $f = t^p - apt + bp$ mit $a, b \notin \mathbb{N}$, $p \nmid b \Rightarrow$ irreduzibel nach Eisenstein.
Ist $pb < (p-1)a \Rightarrow$ genau 3 reelle Nullstellen.

Lemma 4.81.
Sei p eine Primzahl, $G \leq S_p$ transitiv. Enthält G eine Transposition, so ist $G = S_p$.

Beweis:
Wegen G transitiv und p prim $\Rightarrow$ $\exists$ p-Zykel in G.

O.E. $(1\,2\,\ldots\,p) \in G$. Nach Voraussetzung $\exists\ \tau = (ab) \in G$. $\Rightarrow$ konjugiere mit σ^a $(1 \mapsto a)$: $\exists\ \tau' = (1\,b') \in G$. $\Rightarrow \sigma^{b'} = (1\,b'\,\ldots) \in G$.
$\Rightarrow G = S_p$ (siehe Übung).

□