ALGEBRA

Vorlesung an der
Universität Rostock

Prof. Dr. R. Knörr

Wintersemester 2004/2005

1 Lösungsformeln für Gleichungen vom Grad 3 oder 4

1.1 Bemerkung: *Standardform*

Sei $f(x) = x^3 + ax^2 + bx + c$ ein Polynom mit Koeffizienten aus einem Körper K; gesucht sind die Nullstellen von f. Substituiert man $x = y - \frac{a}{3}$, so erhält man ein Polynom $g(y) = y^3 + py + q$, d.h. ohne quadratischen Term. Wenn man die Nullstellen von g kennt, dann braucht man von diesen nur $\frac{a}{3}$ zu subtrahieren und hat auch die Nullstellen von f. Also kann man sich gleich auf Polynome ohne quadratischen Term beschränken, wenn man die Nullstellen eines Polynoms dritten Grades finden will. Entsprechend gilt für Polynome vierten Grades, dass man sich auf solche der Form $x^4 + px^2 + qx + r$ beschränken darf.

1.2 Bemerkung: *zur Berechnung der Nullstellen von $f(x) = x^3 + px + q$*

Wenn $p = 0$, findet man die Nullstellen als die dritten Wurzeln von $-q$; wir nehmen daher $p \neq 0$ an.
Ansatz: Sei $\alpha = u + v$ eine Nullstelle mit $3uv = -p$. Dann

$$0 = f(\alpha) = (u+v)^3 + p(u+v) + q = u^3 + v^3 + 3uv(u+v) + p(u+v) + q = u^3 + v^3 + q\ ,$$

also $u^3 + v^3 = -q$. Wir führen ein Hilfspolynom

$$h(z) = (z - u^3)(z - v^3) = z^2 - (u^3 + v^3)z + (uv)^3 = z^2 + qz - \frac{p^3}{27}$$

ein. Da dies ein quadratisches Polynom ist, lassen sich die beiden Nullstellen u^3 und v^3 auf bekannte Weise berechnen. Zieht man die dritten Wurzeln, so erhält man u und v. Genauer erhält man für beide je drei verschiedene Lösungen, die sich um dritte Einheitswurzeln unterscheiden. Diese müssen so gepaart werden, dass jeweils $3uv = -p$, d.h. $v = \frac{-p}{3u}$. Aus jedem solchen Paar erhält man dann durch Addition eine Nullstelle von f.

1.3 Beispiel: $f(x) = x^3 + 9x^2 + 24x - 9$

Standardform: $g(y) = f(y-3) = y^3 - 3y - 27$, d.h. $p = -3,\ q = -27$.
Hilfspolynom: $h(z) = z^2 + qz - \frac{p^3}{27} = z^2 - 27z + 1$
Nullstellen von h sind $u^3 = \frac{27}{2} + \sqrt{(\frac{27}{2})^2 - 1} = \frac{1}{2}(27 + 5\sqrt{29})$
und $v^3 = \frac{1}{2}(27 - 5\sqrt{29})$.

Drei Lösungen für u: $u_1 = \sqrt[3]{\frac{1}{2}(27 + 5\sqrt{29})},\ u_2 = \omega\sqrt[3]{\frac{1}{2}(27 + 5\sqrt{29})},\ u_3 = \overline{\omega}\sqrt[3]{\frac{1}{2}(27 + 5\sqrt{29})}$

Drei Lösungen für v: $v_1 = \sqrt[3]{\frac{1}{2}(27 - 5\sqrt{29})},\ v_2 = \omega\sqrt[3]{\frac{1}{2}(27 - 5\sqrt{29})},\ v_3 = \overline{\omega}\sqrt[3]{\frac{1}{2}(27 - 5\sqrt{29})}$
Dabei ist ω eine primitive dritte Einheitswurzel, d.h

$$\omega = -\frac{1}{2}(1 + i\sqrt{3})$$

Nullstellen von g: $\alpha_1 = u_1 + v_1$, $\alpha_2 = u_2 + v_3$, $\alpha_3 = u_3 + v_2$
Nullstellen von f: $\alpha_1 - 3$, $\alpha_2 - 3$, $\alpha_3 - 3$

1.4 **Bemerkung:** *zur Berechnung der Nullstellen von* $f(x) = x^4 + px^2 + qx + r$

Der Fall $q = 0$ führt zu einer biquadratischen Gleichung, aus der man sehr leicht erst x^2 und dann x berechnet. Wir nehmen daher $q \neq 0$ an; natürlich darf man auch $r \neq 0$ annehmen.
Ansatz: $f(x) = (x^2 + \frac{u}{2})^2 - (vx + w)^2 = x^4 + (u - v^2)x^2 - 2vwx + \frac{u^2}{4} - w^2$
Koeffizientenvergleich liefert:

$$\begin{array}{rcl} p &=& u - v^2 \quad \text{oder} \quad v^2 = u - p \\ q &=& -2vw \\ r &=& \frac{u^2}{4} - w^2 \quad \text{oder} \quad w^2 = \frac{u^2}{4} - r \end{array}$$

Es folgt

$$\begin{array}{rcl} q^2 &=& 4v^2w^2 \\ &=& 4(u-p)(\frac{u^2}{4} - r) \\ &=& (u-p)(u^2 - 4r) \ , \end{array}$$

also ist u eine Nullstelle von

$$h(z) = (z - p)(z^2 - 4r) - q^2 = z^3 - pz^2 - 4rz + 4pr - q^2 \ .$$

Dies ist ein Polynom dritten Grades, dessen Nullstellen wir berechnen können (s.o.). Hier reicht *eine* Nullstelle u. Setzt man

$$\begin{array}{rcll} v &=& \sqrt{u-p} & \text{und} \\ w &=& -\frac{q}{2v} & (\text{beachte} \quad v \neq 0, \quad \text{weil} \quad h(p) = -q^2 \neq 0, \ \text{also } u \neq p) \ , \end{array}$$

dann gelten die obigen Gleichungen für p, q und r. Folglich ist α genau dann eine Nullstelle von f, wenn $(\alpha^2 + \frac{u}{2})^2 = (v\alpha + w)^2$, d.h.

$$\begin{array}{rcl} \alpha^2 + \frac{u}{2} &=& v\alpha + w \qquad \text{oder} \\ \alpha^2 + \frac{u}{2} &=& -(v\alpha + w) \quad . \end{array}$$

Lösen dieser quadratischen Gleichungen gibt die vier (i.A. verschiedenen) Nullstellen von f, nämlich

$$\alpha_1, \ldots, \alpha_4 = \frac{1}{2}(\varepsilon v + \delta\sqrt{4\varepsilon w - u - p}) \ ,$$

wobei $\varepsilon, \delta \in \{1, -1\}$.
Das eben beschriebene Verfahren führt bei der Berechnung von w zu einem sehr unschönen Ausdruck, mit dem man dann weiter rechnen muss. Eleganter ist es, alle drei Lösungen u_1, u_2, u_3 von h zu berechnen. Weil

$$\begin{array}{rcl} z^3 - pz^2 - 4rz + 4pr - q^2 &=& h(z) = (z - u_1)(z - u_2)(z - u_3) \\ &=& z^3 - (u_1 + u_2 + u_3)z^2 + (u_1u_2 + u_1u_3 + u_2u_3)z - u_1u_2u_3 \ , \end{array}$$

folgt

$$\begin{array}{rcl} u_1 + u_2 + u_3 &=& p \\ u_1u_2 + u_1u_3 + u_2u_3 &=& -4r \\ u_1u_2u_3 &=& q^2 - 4pr \ . \end{array}$$

Wir setzen wie oben $v_i = \sqrt{u_i - p}$ (dafür gibt es jeweils zwei Möglichkeiten). Dann

$$(v_1v_2v_3)^2 = (u_1 - p)(u_2 - p)(u_3 - p) = -h(p) = q^2 \ ,$$

also ist $v_1v_2v_3 = q$ oder $v_1v_2v_3 = -q$. Wir wählen das Vorzeichen von v_3 so, dass $v_1v_2v_3 = -q$, also $v_3 = \frac{-q}{v_1v_2}$. Setze $A = v_1 + v_2 + v_3$ und $B = v_1v_2 + v_1v_3 + v_2v_3$. Dann

$$\begin{array}{rcl} A^2 &=& v_1^2 + v_2^2 + v_3^2 + 2B \\ &=& u_1 - p + u_2 - p + u_3 - p + 2B \\ &=& 2(B - p) \end{array}$$

und

$$\begin{aligned}
B^2 &= v_1^2v_2^2 + v_1^2v_3^2 + v_2^2v_3^2 + 2v_1v_2v_3(v_1+v_2+v_3) \\
&= (u_1-p)(u_2-p) + (u_1-p)(u_3-p) + (u_2-p)(u_3-p) - 2qA \\
&= u_1u_2 + u_1u_3 + u_2u_3 - 2p(u_1+u_2+u_3) + 3p^2 - 2qA \\
&= -4r - 2p^2 + 3p^2 - 2qA \\
&= p^2 - 4r - 2qA\ .
\end{aligned}$$

Daraus erhält man

$$\begin{aligned}
A^4 &= 4(B^2 + p^2 - 2pB) \\
&= 4(p^2 - 4r - 2qA + p^2 - 2pB) \\
&= 8(p^2 - 2r - qA - pB)\ .
\end{aligned}$$

Jetzt setzen wir $\alpha = \frac{A}{2}$ und berechnen

$$\begin{aligned}
f(\alpha) &= \alpha^4 + p\alpha^2 + q\alpha + r \\
&= \tfrac{1}{16}\,A^4 + p\,\tfrac{1}{4}\,A^2 + q\,\tfrac{1}{2}\,A + r \\
&= \tfrac{1}{2}\,(p^2 - 2r - qA - pB) + p\,\tfrac{1}{2}\,(B-p) + q\,\tfrac{1}{2}\,A + r \\
&= 0\ ,
\end{aligned}$$

also ist $\frac{1}{2}\,(v_1+v_2+v_3)$ eine Nullstelle von f.

1.5 Beispiel: $f(x) = x^4 - 4x^3 - 3x^2 + 29x - 29$

Standardform: $g(y) = f(y+1) = y^4 - 9y^2 + 15y - 6$, d.h. $p = -9,\ q = 15,\ r = -6$
Hilfspolynom: $h(z) = z^3 - pz^2 - 4rz + 4pr - q^2 = z^3 + 9z^2 + 24z - 9$
Die Nullstellen von h haben wir im vorigen Beispiel berechnet, nämlich

$$\begin{aligned}
u_1 &= -3 + \sqrt[3]{\tfrac{1}{2}(27+5\sqrt{29})} + \sqrt[3]{\tfrac{1}{2}(27-5\sqrt{29})} \\
u_2 &= -3 + \omega\,\sqrt[3]{\tfrac{1}{2}(27+5\sqrt{29})} + \overline{\omega}\,\sqrt[3]{\tfrac{1}{2}(27-5\sqrt{29})} \\
u_3 &= -3 + \overline{\omega}\,\sqrt[3]{\tfrac{1}{2}(27+5\sqrt{29})} + \omega\,\sqrt[3]{\tfrac{1}{2}(27-5\sqrt{29})}.
\end{aligned}$$

Daher

$$\begin{aligned}
v_1 &= \varepsilon_1\sqrt{6 + \sqrt[3]{\tfrac{1}{2}(27+5\sqrt{29})} + \sqrt[3]{\tfrac{1}{2}(27-5\sqrt{29})}} \\
v_2 &= \varepsilon_2\sqrt{6 + \omega\,\sqrt[3]{\tfrac{1}{2}(27+5\sqrt{29})} + \overline{\omega}\,\sqrt[3]{\tfrac{1}{2}(27-5\sqrt{29})}} \\
v_3 &= \varepsilon_3\sqrt{6 + \overline{\omega}\,\sqrt[3]{\tfrac{1}{2}(27+5\sqrt{29})} + \omega\,\sqrt[3]{\tfrac{1}{2}(27-5\sqrt{29})}}\ .
\end{aligned}$$

Wählt man die Vorzeichen ε_i so, dass $v_1v_2v_3 = -15$ (dafür gibt es vier Möglichkeiten), dann ist $\frac{1}{2}(v_1+v_2+v_3)$ eine Nullstelle von g, aus der man dann auch eine Nullstelle von f erhält. Man sieht schön, wie sie sich durch wiederholtes Wurzelziehen berechnen lässt (dies gilt ja auch für ω und $\overline{\omega} = \omega^2$).

1.6 Bemerkung:

Wir haben bei den obigen Berechnungen durch Potenzen von 2 und 3 geteilt. Das ist erlaubt, wenn in K gilt: $1+1 \neq 0$ und $1+1+1 \neq 0$ (z.B. $K = \mathbb{Q}$ oder $K = \mathbb{R}$). Dies muss also *vorausgesetzt* werden. Natürlich brauchen die Wurzeln, welche in den Lösungsformeln auftreten, nicht in K zu liegen (sondern erst in einem größern Körper).

1.7 Bemerkung:

Die Formeln zur Lösung der kubischen Gleichung sind als Cardano'sche Formeln bekannt (Girolamo Cardano, 1501-1576), stammen aber nicht von ihm, sondern von Scipione del Ferro (1465-1526). Den Ansatz für die Lösung der Gleichung vierten Grades verdanken wir Cardano's Schüler Lodovico Ferrari (1522-1565). Die Lösung der quadratischen Gleichung war zu diesem Zeitpunkt schon etwa 3000 Jahre bekannt. Was bei Polynomen vom Grad ≥ 5 geschieht, konnte im 19. Jahrhundert von Evariste Galois (1811-1832) und anderen geklärt werden.
Die Galois-Theorie ist der Inhalt dieser Vorlesung.

2 Gruppen und Homomorphismen

2.1 Definition: *Gruppe*

Eine Menge G mit einer Verknüpfung $G \times G \to G$, geschrieben als $(g,h) \mapsto gh$, heißt eine Gruppe, wenn die folgenden Axiome gelten:

(1) (Assoziativität) $(ab)c = a(bc) \quad \forall a,b,c \in G$

(2) (Neutrales Element) $\exists 1 \in G$ mit $1 \cdot g = g \cdot 1 = g \quad \forall g \in G$

(3) (Inverses) $\forall g \in G \; \exists h \in G$ mit $gh = hg = 1$

G heißt abelsch, falls zusätzlich $ab = ba \quad \forall a,b \in G$ (Kommutativität) gilt.

2.2 Bemerkung: *Gruppen*

Sei G eine Gruppe.

(i) Es gibt nur ein neutrales Element.
Denn wenn auch $1'$ ein neutrales Element ist, dann gilt $1' = 1 \cdot 1' = 1$.

(ii) Zu jedem g gibt es nur ein Inverses, geschrieben als g^{-1}.
Denn wenn auch h' ein Inverses von g ist, also auch $gh' = h'g = 1$ gilt, dann ist $h = h \cdot 1 = h(gh') = (hg)h' = 1 \cdot h' = h'$.

(iii) Es gelten die Kürzungsregeln: $ab = ac \Rightarrow b = c$ und $ba = ca \Rightarrow b = c$.
Beweis: $ab = ac \Rightarrow b = 1 \cdot b = (a^{-1}a)b = a^{-1}(ab) = a^{-1}(ac) =$
$= (a^{-1}a)c = 1 \cdot c = c$.
Analog beweist man die zweite Kürzungsregel.

(iv) Spezialfälle der Kürzungsregeln:

- $ab = a = a \cdot 1 \Rightarrow b = 1$
  analog: $ab = b \Rightarrow a = 1$
- $ab = 1 = aa^{-1} \Rightarrow b = a^{-1}$
  analog: $ab = 1 = b^{-1}b \Rightarrow a = b^{-1}$
- Insbesondere: $(a^{-1})^{-1} = a$, denn $a^{-1}(a^{-1})^{-1} = 1 = a^{-1}a$

2.3 Beispiel: *Gruppen: GL, SL, Aut, symmetrische, alternierende*

(i) $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$ mit der Multiplikation; ebenso $\mathbb{R}^*$

(ii) $(\mathbb{Z}, +)$

(iii) $GL(n,K) = \{n \times n$ -Matrizen A über K mit $\det A \neq 0\}$, wobei K ein Körper ist. Die Matrizenmultiplikation ist die Verknüpfung.
Dies nennt man die volle lineare Gruppe.

(iv) $SL(n,K) = \{A \in GL(n,K)$ und $\det A = 1\}$.
Dies heißt die spezielle lineare Gruppe.

(v) Ω sei eine Menge. Dann heißt $S_\Omega = \{\alpha : \Omega \to \Omega \mid \alpha$ bijektiv $\}$
die symmetrische Gruppe auf Ω.Ihre Elemente heißen *Permutationen* von Ω. Die Verknüpfung ist die Hintereinanderausführung.
Insbesondere: ist $\Omega = \{1, \ldots, n\}$, $(n \in \mathbb{N})$, dann schreibt man $S_\Omega = S_n$.

(vi) Sei K ein Körper und V ein K-Vektorraum.
$Aut(V) = \{\alpha : V \to V \mid \alpha$ bijektiv und linear$\}$ mit der Verknüpfung wie in (v) heißt die Automorphismengruppe von V.

(vii) $A_n = \{\pi \in S_n \mid \text{sign}(\pi) = 1\}$ heißt die alternierende Gruppe.

(viii) Die Drehgruppe des Würfels. Jede Drehung permutiert die 6 Flächen, also ist die Drehgruppe eine „Untergruppe" von S_6.

2.4 Definition: *Direktes Produkt*

Seien G und H Gruppen. Die Menge $G \times H$ ist mit komponentenweiser Verknüpfung wieder eine Gruppe, genannt das direkte Produkt von G und H. Diese Konstruktion ist nicht auf zwei Faktoren beschränkt: für die Gruppen G_i, $i \in I$, sei $\prod\limits_{i\in I}\!\times\, G_i =$
$\{\phi : I \to \bigcup\limits_{i\in I} G_i \mid \phi(i) \in G_i\}$ definiert mit der Verknüpfung $(\phi\psi)(i) = \phi(i)\psi(i) \in G_i$.

2.5 Definition: *Untergruppe*

Eine Teilmenge U einer Gruppe G heißt Untergruppe, geschrieben als $U \leq G$, falls U mit der Verknüpfung von G selbst eine Gruppe ist.

2.6 Beispiel: *Untergruppen*

(i) $\{1\}$, G sind Untergruppen in jeder Gruppe G.

(ii) Die geraden Zahlen $2\mathbb{Z} \leq \mathbb{Z}$. Allgemeiner: $n\mathbb{Z} \leq \mathbb{Z} \quad \forall n \in Z$

(iii) $SL(n, K) \leq GL(n, K)$

(iv) $A_n \leq S_n$

(v) $Aut(V) \leq S_V$

(vi) $\mathbb{R}_{>0} \leq \mathbb{R}^*$

2.7 Lemma: *Untergruppenkriterium*

Sei U eine Teilmenge der Gruppe G. Genau dann ist U eine Untergruppe von G, wenn:

(1) $U \neq \emptyset$ und

(2) $xy^{-1} \in U \quad \forall x, y \in U$

Falls U endlich ist, kann man (2) ersetzen durch

(2') $xy \in U \quad \forall x, y \in U$.

Beweis: Wenn U eine Untergruppe von G ist, dann gelten offenbar (1),(2) und (2'). Sei nun U eine Teilmenge, welche (1) und (2) erfüllt. Wegen (1) gibt es $x \in U$. Nach (2) mit $y = x$ ist dann $1 = xx^{-1} \in U$, d.h. U enthält das neutrale Element. Wendet man wieder (2) mit $x = 1$ und beliebigem $y \in U$ an, so folgt $y^{-1} = 1 \cdot y^{-1} \in U$, d.h. für jedes $y \in U$ ist auch $y^{-1} \in U$. Man kann also nochmals (2) anwenden für y ersetzt durch y^{-1} und erhält $xy = x(y^{-1})^{-1} \in U$, falls $x, y \in U$. Somit ist $(x, y) \mapsto xy$ eine Verknüpfung auf U. Trivialerweise gilt das Assoziativgesetz. Also ist U eine Gruppe, daher eine Untergruppe von G.
Sei schließlich U endlich und es gelte (1) und (2'). Um (2) zu zeigen, reicht der Nachweis, dass $y^{-1} \in U \quad \forall y \in U$. Dazu betrachtet man die Potenzen $y^1 = y$, $y^2 = y \cdot y$, $y^3 = y^2y, \ldots$. Diese gehören alle zu U nach (2') und einfacher Induktion. Da U endlich

ist, können sie nicht alle verschieden sein. Daher gibt es natürliche Zahlen $m < n$ mit $y^m = y^n = y^m y^{n-m}$. Die Kürzungsregel zeigt $1 = y^{n-m} = yy^{n-m-1}$ und daher $y^{-1} = y^{n-m-1}$. Als Potenz von y ist y^{-1} also auch in U.

2.8 **Korollar:** *Durchschnitte von Untergruppen*

Durchschnitte von Untergruppen sind wieder Untergruppen.

Beweis: Seien $U_i \leq G \quad \forall i \in I$. Dann $1 \in U_i \quad \forall i \in I$, also $1 \in \bigcap_i U_i \neq \emptyset$. Wenn $x, y \in \bigcap_i U_i$, dann $x, y \in U_i \quad \forall i \in I$, also $xy^{-1} \in U_i \quad \forall i \in I$ und daher $xy^{-1} \in \bigcap_i U_i$. Damit erfüllt $\bigcap_i U_i$ die Bedingungen von (2.7).

2.9 **Definition:** *Erzeugnis* $\langle T \rangle$

Sei $T \subseteq G$. Man nennt $\langle T \rangle = \bigcap_{T \subset U \leq G} U$ das Erzeugnis von T. Man schreibt einfach $\langle t \rangle$ für $\langle \{t\} \rangle$.
Es ist $\langle T \rangle$ die kleinste Untergruppe von G, welche T enthält.

2.10 **Definition:** *zyklisch*

Eine Untergruppe $U \leq G$ heißt zyklisch, falls ein $u \in G$ existiert mit $\langle u \rangle = U$. (Natürlich ist dann $u \in U$.)

2.11 **Beispiel:** *zyklische Gruppen*

$(\mathbb{Z}, +)$ ist zyklisch, nämlich $\langle 1 \rangle = \mathbb{Z}$; allgemeiner $\langle n \rangle = n\mathbb{Z}$ für $n \in \mathbb{Z}$.

2.12 **Definition:** *Ordnung eines Elementes*

Sei G eine Gruppe und $g \in G$. Dann heißt $o(g) = |\langle g \rangle|$ die Ordnung von g.

2.13 **Bemerkung:** *Ordnung eines Elementes*

Wenn g die endliche Ordnung n hat, dann ist n die kleinste natürliche Zahl mit $g^n = 1$.

Beweis: Sei $U = \langle g \rangle$. Dann sind mit einfacher Induktion alle Potenzen $g, g^2, g^3, \ldots$ in U. Da nach Voraussetzung U endlich ist, gibt es $l < m$ mit $g^l = g^m = g^l g^{m-l}$. Daher ist $g^{m-l} = 1$. Sei n_0 die kleinste natürliche Zahl mit $g^{n_0} = 1$. Dann sind $g, g^2, \ldots, g^{n_0} = 1$ alle verschieden (mit den Bezeichnungen von oben wäre sonst $m - l < n_0$). Offenbar ist $\{g, \ldots, g^{n_0}\}$ die kleinste Gruppe, welche g enthält, also gleich U. Daher $n = |U| = n_0$.

2.14 **Definition:** *Rechts- und Linksnebenklasse*

Sei U eine Untergruppe von G und $g \in G$. Man nennt dann $Ug = \{ug \mid u \in U\}$ eine Rechtsnebenklasse von U (in G). Entsprechend sind die Linksnebenklassen gU definiert.

2.15 **Lemma:** *Nebenklassen*

Sei $U \leq G$ und $g, h \in G$. Dann sind äquivalent:

(1) $Ug = Uh$

(2) $Ug \cap Uh \neq \emptyset$

(3) $h \in Ug$

(4) $\exists u \in U : h = ug$

(5) $hg^{-1} \in U$

Beweis:

(1)⇒(2) Es ist $g = 1 \cdot g \in Ug \neq \emptyset$.

(2)⇒(3) Sei $x \in Ug \cap Uh$, etwa $x = ug = vh$ mit $u, v \in U$. Dann ist $v^{-1}u \in U$, also $h = v^{-1}ug \in Ug$.

(3)⇒(4) trivial.

(4)⇒(5) trivial.

(5)⇒(1) Sei $u \in U$. Dann ist $uh = uhg^{-1}g \in Ug$, denn $uhg^{-1} \in U$ nach (5). Also folgt aus (5), dass $Uh \subseteq Ug$. Aber aus (5) folgt auch $gh^{-1} = (hg^{-1})^{-1} \in U$ und dann wie oben $Ug \subseteq Uh$. Daher ist $Ug = Uh$.

2.16 Lemma: *Vereinigung von Nebenklassen*

Sei $\mathcal{R} = \{Ug \mid g \in G\}$. Dann gilt $G = \dot{\bigcup\limits_{R \in \mathcal{R}}} R$ (disjunkte Vereinigung).

Beweis: Jedes $g \in G$ liegt in einer Rechtsnebenklasse, nämlich in $R = Ug$, aber auch nur in dieser, denn verschiedene Rechtsnebenklassen haben leeren Schnitt nach (2.15).

2.17 Lemma: *Bijektion zwischen Links- und Rechtsnebenklassen*

Sei R ein Rechtsnebenklasse von U in G. Dann ist $R^{-1} = \{r^{-1} \mid r \in R\}$ eine Linksnebenklasse von U in G. Die Abbildung $R \mapsto R^{-1}$ ist eine Bijektion von der Menge der Rechtsnebenklassen $\mathcal{R}$ auf die Menge der Linksnebenklassen $\mathcal{L}$.

Beweis: Sei $R = Ug$. Dann ist $R^{-1} = g^{-1}U$, also eine Linksnebenklasse. Ebenso wird aus einer Linksnebenklasse L eine Rechtsnebenklasse L^{-1}. Die so definierten Abbildungen $\mathcal{R} \to \mathcal{L}$ und $\mathcal{L} \to \mathcal{R}$ sind offenbar zueinander invers. Daher die Behauptung.

2.18 Definition: *Index*

Man nennt $|\mathcal{R}| = |\mathcal{L}|$ den Index von U in G und schreibt dafür auch $|G : U|$.

2.19 Beispiel: *Indizes*

(i) $|G : G| = 1$

(ii) $|G : 1| = |G|$

2.20 Satz: *Indexsatz*

Sei $U \leq H \leq G$. Dann ist $|G : U| = |G : H| \cdot |H : U|$.

Beweis: Sei $G = \dot{\bigcup\limits_{i \in I}} Hg_i$, (also $|G : H| = |I|$) und $H = \dot{\bigcup\limits_{j \in J}} Uh_j$ (also $|H : U| = |J|$). Wir zeigen $G = \dot{\bigcup\limits_{i \in I, j \in J}} Uh_jg_i$. (Es folgt dann $|G : U| = |I \times J| = |I| \cdot |J|$, also die Behauptung.) Wenn $g \in G$, dann $g = hg_i$ für ein $i \in I$ und $h \in H$. Aber $h = uh_j$ für ein $j \in J$ und $u \in U$, also $g = uh_jg_i \in Uh_jg_i$, daher $\bigcup\limits_{i,j} Uh_jg_i = G$. Diese Vereinigung ist disjunkt: Wenn $Uh_jg_i \cap Uh_{j'}g_{i'} \neq \emptyset$, dann $h_jg_ig_{i'}^{-1}h_{j'}^{-1} \in U \leq H$ nach 2.15, also $g_ig_{i'}^{-1} \in H$. Nach 2.15 folgt $Hg_i = Hg_{i'}$, also $i = i'$. Daher $h_jh_{j'}^{-1} \in U$, wieder nach 2.15 also $Uh_j = Uh_{j'}$, d.h. auch $j = j'$.

2.21 **Korollar:** *Index einer Untergruppe*

Sei $H \leq G$. Dann gilt $|G| = |G : H| \cdot |H|$.
Insbesondere: Wenn G endlich ist, dann sind Ordnung und Index einer Untergruppe Teiler der Gruppenordnung und ebenso die Ordnung eines jeden Gruppenelements.

Beweis: Verwende Indexsatz (2.20) mit $U = \{1\}$.
Es folgt $|G| = |G : 1| = |G : H||H : 1| = |G : H||H|$ (vergleiche. 2.19).
Wenn $g \in G$, dann ist $o(g) = |\langle g\rangle|$ die Ordnung einer Untergruppe von G.
Die Behauptungen sind jetzt klar.

2.22 **Definition:** *Normalteiler, konjugiertes Element, Normalisator*

Ein Normalteiler N von G, geschrieben $N \triangleleft G$, ist eine Untergruppe N mit der Eigenschaft, dass $n^g := g^{-1}ng \in N \quad \forall n \in N, g \in G$. Man nennt n^g das zu n unter g konjugierte Element und die Abbildung $x \mapsto x^g$ Konjugation mit g.
Wenn $X \subseteq G$ und $g \in G$, dann ist per Definition $X^g = \{x^g \mid x \in X\}$ und $N_G(X) = \{g \in G \mid X^g = X\}$. Man nennt $N_G(X)$ den Normalisator von X in G.

2.23 **Bemerkung:** *Normalisator*

(i) Aus dem Untergruppenkriterium folgt leicht, dass $N_G(X)$ für jedes $X \subseteq G$ eine Untergruppe ist.

(ii) Wenn $X = U \leq G$ selbst eine Untergruppe ist, dann $U \leq N_G(U)$ und sogar $U \triangleleft N_G(U)$.

2.24 **Beispiel:** *Normalteiler*

(i) In einer abelschen Gruppe ist jede Untergruppe ein Normalteiler.

(ii) $G \triangleleft G$ und $\{1\} \triangleleft G$.

(iii) In der S_3 gibt es 3 Untergruppen der Ordnung 2. Keine von diesen ist normal. Es gibt auch eine Untergruppe der Ordnung 3. Diese ist normal.

(iv) $A_n \triangleleft S_n$

(v) In der Gruppe $Q_8 = \left\langle \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \right\rangle$ (eine Untergruppe von $GL(2, \mathbb{C})$) ist jede Untergruppe normal, aber Q_8 ist nicht abelsch.

(vi) Wenn $N \triangleleft G$, $M \triangleleft G$, dann $N \cap M \triangleleft G$ und $NM := \{nm \mid n \in N, m \in M\} \triangleleft G$.

(vii) Allgemeiner: Wenn $U \leq G$ und $N \triangleleft G$, dann $UN \leq G$. Vorsicht: Das Produkt von zwei Untergruppen ist im Allgemeinen keine Untergruppe!

(viii) Wenn $N \triangleleft G$, $U \leq G$, dann $N \cap U \triangleleft U$.

(ix) Seien N_1 und N_2 Gruppen. In der Gruppe $G = N_1 \times N_2$ sind dann $N_1 \times 1 = \{(n_1, 1) \mid n_1 \in N_1\}$ und analog $1 \times N_2$ Normalteiler.

2.25 Bezeichnung/Bemerkung: *Produkte von Teilmengen*

Wenn $A, B \subseteq G$, dann bezeichnet man als ihr Produkt die Teilmenge $AB := \{ab \mid a \in A, b \in B\}$.
Diese Multiplikation ist assoziativ: $(AB)C = A(BC)$, da die Multiplikation in der Gruppe G assoziativ ist.

2.26 Lemma: *Produkt von Nebenklassen*

Sei $N \triangleleft G$. Dann ist $Ng = gN \quad \forall g \in G$ und $(Ng)(Nh) = Ngh \quad \forall g, h \in G$.
Das Produkt zweier Nebenklassen ist also wieder eine Nebenklasse.
<u>*Beweis:*</u>

(1) Es ist $N^g \subseteq N \quad \forall g \in G$ (nach Definition des Normalteilers). Die Linksmultiplikation mit g ergibt $Ng \subseteq gN$. Dies gilt auch für g^{-1}, also $Ng^{-1} \subseteq g^{-1}N$. Durch Multiplikation mit g von links und rechts folgt $gN \subseteq Ng$. Daher $Ng = gN$.

(2) $(Ng)(Nh) = N(gN)h \overset{(1)}{=} (NN)gh = Ngh$.

2.27 Satz/Definition: *Faktorgruppe*

Sei $N \triangleleft G$. Mit der Verknüpfung $(Ng, Nh) \mapsto NgNh \quad g, h \in G$ wird ${}^{G}\!/_{N} := \{Ng \mid g \in G\}$ zu einer Gruppe, genannt die <u>Faktorgruppe</u> von G nach N.

<u>*Beweis:*</u>

(1) Assoziativität folgt aus 2.25.

(2) Das neutrale Element ist $N = N \cdot 1$, wie man aus 2.26(2) sieht.

(3) Damit folgt auch, dass Ng^{-1} das Inverse zu Ng ist.

2.28 Satz: *Untergruppen und Faktorgruppen*

Sei $N \triangleleft G$. Die Abbildung $U \mapsto \overline{U} := {}^{U}\!/_{N}$ ist eine Bijektion zwischen den Untergruppen U von G, welche N enthalten, und den Untergruppen $\overline{U}$ von $\overline{G} = {}^{G}\!/_{N}$. Außerdem gelten für Untergruppen U und V oberhalb von N:

(1) $U \leq V \Leftrightarrow \overline{U} \leq \overline{V}$

(2) $\overline{U \cap V} = \overline{U} \cap \overline{V}$

(3) $\overline{\langle U, V \rangle} = \langle \overline{U}, \overline{V} \rangle$

(4) $\overline{N_G(U)} = N_{\overline{G}}(\overline{U})$

(5) $U \triangleleft G \Leftrightarrow \overline{U} \triangleleft \overline{G}$

<u>*Beweis:*</u> Die Umkehrabbildung ist $\overline{U} \mapsto \{g \in G \mid gN \in \overline{U}\}$, wie man leicht sieht. Offenbar erhalten beide Abbildungen Inklusionen. Daher gilt (1). Aus (1) folgen (2) und (3), denn $U \cap V$ ist die größte Untergruppe, welche in U und V enthalten ist, und $\langle U, V \rangle$ ist die kleinste Untergruppe, welche U und V enthält.
Weil $\overline{U}^{\overline{g}} = \overline{U^g}$ ist, gilt (4). Aus (4) folgt (5), denn $U \triangleleft G \Leftrightarrow N_G(U) = G$.

2.29 Definition: *Gruppenhomomorphismus, isomorph*

Seien die Gruppen G und H multiplikativ geschrieben. Ein Gruppenhomomorphismus von G nach H ist eine Abbildung $\alpha : G \to H$ mit $\alpha(g_1 g_2) = \alpha(g_1)\alpha(g_2) \quad \forall g_1, g_2 \in G$. Monomorphismus, Epimorphismus, Isomorphismus und Automorphismus seien definiert wie üblich.
G heißt isomorph zu H, geschrieben $G \cong H$, wenn ein Isomorphismus $\alpha : G \to H$ existiert.

2.30 Bemerkung/Beispiel: *Gruppenhomomorphismen*

(i) Wenn $\alpha : G \to H$ und $\beta : H \to K$ Homomorphismen (Isomorphismen) sind, dann auch $\beta\alpha : G \to K$.

(ii) $\mathrm{id} : G \to G$ ist ein Automorphismus von G.

(iii) Wenn $\alpha : G \to H$ ein Isomorphismus ist, dann existiert die Umkehrabbildung $\alpha^{-1} : H \to G$. Diese ist auch ein Homomorphismus.
Beweis: Seien $h_1, h_2 \in H$, dann ist

$$\alpha\left[\alpha^{-1}(h_1 h_2)\right] = h_1 h_2 = \alpha\left[\alpha^{-1}(h_1)\right]\alpha\left[\alpha^{-1}(h_2)\right] = \alpha\left[\alpha^{-1}(h_1)\alpha^{-1}(h_2)\right],$$

denn α ist ein Homomorphismus. Da α injektiv ist , folgt $\alpha^{-1}(h_1 h_2) = \alpha^{-1}(h_1)\alpha^{-1}(h_2)$. Dies zeigt, dass auch α^{-1} ein Homomorphismus ist.

(iv) Aus (i),(ii) und (iii) folgt, dass *„Isomorphie"* transitiv, reflexiv und symmetrisch ist.

(v) Die Menge der Automorphismen von G bildet mit der üblichen Verknüpfung von Abbildungen eine Gruppe, genannt die Automorphismengruppe von G, geschrieben als „$Aut(G)$".

(vi) Sei $g \in G$ fest. Für $x \in G$ sei $x\gamma_g = x^g$. Es gilt $(xy)\gamma_g = (xy)^g = x^g y^g = (x\gamma_g)(y\gamma_g)$. Also ist γ_g ein Homomorphismus $G \to G$. Außerdem ist offenbar $\gamma_1 = \mathrm{id}_G$ und $x(\gamma_g\gamma_h) = (x\gamma_g)\gamma_h = (x^g)\gamma_h = (x^g)^h = x^{gh} = (x)\gamma_{gh}$. Also ist $\gamma_g\gamma_h = \gamma_{gh}$ (*). Insbesondere $\gamma_g\gamma_{g^{-1}} = \gamma_{gg^{-1}} = \gamma_1 = \mathrm{id}$. Daher ist γ_g bijektiv, also $\gamma_g \in Aut(G)$. Nach (*) ist die Abbildung $\gamma : G \to Aut(G)$, definiert durch $\gamma : g \mapsto \gamma_g$, ein Homomorphismus.

(vii) $\mathrm{sign} : S_n \to \{1, -1\}$ ist ein Homomorphismus, denn
$\mathrm{sign}(\sigma\tau) = \mathrm{sign}(\sigma)\mathrm{sign}(\tau) \quad \forall \sigma, \tau \in S_n$.
Wenn $n \neq 1$ ist, so ist sign sogar ein Epimorphismus.

(viii) $\det : GL(n, K) \to K^*$ ist ein Homomorphismus, da $\det(AB) = \det(A)\det(B)$ (Produktsatz für Determinanten). Diese Abbildung ist auch surjektiv, da (z.B.)
$$\begin{pmatrix} a & & & \\ & 1 & 0 & \\ & 0 & \ddots & \\ & & & 1 \end{pmatrix}$$ die Determinante a hat.

(ix) Sei $N \triangleleft G$ und $\kappa : G \to {}^{G}/_{N}$ definiert durch $\kappa(g) = Ng$. Diese Abbildung ist offenbar surjektiv. Nach Lemma 2.26 ist κ ein Homomorphismus. Man nennt κ den kanonischen Epimorphismus von G auf ${}^{G}/_{N}$.

(x) Sei $z \in \mathbb{Z}$. Die Abbildung $\mu_z : \mathbb{Z} \to \mathbb{Z}$ sei definiert durch $\mu_z(x) = z \cdot x$. Dann ist $\mu_z(x+y) = z(x+y) = zx + zy = \mu_z(x) + \mu_z(y)$. Also ist μ_z ein Homomorphismus $(\mathbb{Z}, +) \to (\mathbb{Z}, +)$.
Wenn $z \neq 0$, ist μ_z injektiv. Wenn $z = \pm 1$, ist μ_z sogar bijektiv.

(xi) $\log : (\mathbb{R}_{>0}, \cdot) \to (\mathbb{R}, +)$ ist ein Homomorphismus, denn $\log(ab) = \log(a) + \log(b)$. Es ist sogar ein Isomorphismus. Die Umkehrabbildung ist die Exponentialfunktion.

(xii) Wenn $G = N_1 \times N_2$ ein direktes Produkt ist, dann ist $N_1 \cong N_1 \times 1$ (vergleiche 2.4).

2.31 Bemerkung: *$\alpha(1) = 1$ und $\alpha(g)^{-1} = \alpha(g^{-1})$*

Sei $\alpha : G \to H$ ein Homomorphismus.
Dann ist $\alpha(1_G) = 1_H$ und $\alpha(g)^{-1} = \alpha(g^{-1}) \quad \forall g \in G$.

<u>*Beweis:*</u> $\alpha(1_G) = \alpha(1_G \cdot 1_G) = \alpha(1_G)\alpha(1_G)$. Die Behauptung folgt durch Kürzen von $\alpha(1_G)$. Weiterhin ist $\alpha(g)\alpha(g)^{-1} = 1_H = \alpha(1_G) = \alpha(gg^{-1}) = \alpha(g)\alpha(g^{-1})$. Wieder durch Kürzen folgt $\alpha(g)^{-1} = \alpha(g^{-1}) \quad \forall g \in G$.

2.32 Definition: *Kern und Bild*

Sei $\alpha : G \to H$ ein Homomorphismus. Man nennt $\mathrm{Ker}\,(\alpha) := \{g \in G \mid \alpha(g) = 1_H\}$ den <u>Kern</u> von α und $\mathrm{Im}\,(\alpha) := \{h \in H \mid \exists g \in G : \alpha(g) = h\}$ das <u>Bild</u> von α.

2.33 Lemma: *Kern und Bild*

(1) $\mathrm{Im}\,(\alpha) \leq H$

(2) $\mathrm{Ker}\,(\alpha) \triangleleft G$

(3) $\mathrm{Im}\,(\alpha) = H \Leftrightarrow \alpha$ ist Epimorphismus.

(4) $\mathrm{Ker}\,(\alpha) = \{1_G\} \Leftrightarrow \alpha$ ist Monomorphismus.

<u>*Beweis:*</u> $\alpha(1_G) = 1_H \Rightarrow 1_G \in \mathrm{Ker}\,(\alpha) \neq \emptyset$ und $1_H \in \mathrm{Im}\,(\alpha) \neq \emptyset$.

(1) Sei $x, y \in \mathrm{Im}\,(\alpha)$, etwa $x = \alpha(g_x)$ und $y = \alpha(g_y)$. Dann ist $xy^{-1} = \alpha(g_x)\alpha(g_y)^{-1} = \alpha(g_x g_y^{-1}) \in \mathrm{Im}\,(\alpha)$. Aus dem Untergruppenkriterium 2.7 folgt dann die Behauptung.

(2) Wenn $x, y \in \mathrm{Ker}\,(\alpha)$, dann ist $\alpha(xy^{-1}) = \alpha(x)\alpha(y)^{-1} = 1_H 1_H^{-1} = 1_H$ und somit $xy^{-1} \in \mathrm{Ker}\,(\alpha)$. Daher $\mathrm{Ker}\,(\alpha) \leq G$. Wenn $g \in G$ und $x \in \mathrm{Ker}\,(\alpha)$, dann $\alpha(x^g) = \alpha(g^{-1}xg) = \alpha(g)^{-1}\alpha(x)\alpha(g) = \alpha(g^{-1})\alpha(g) = 1_H$, also ist $x^g \in \mathrm{Ker}\,(\alpha)$.
Daher gilt (2).

(3) ist trivial.

(4) „$\Rightarrow$“ Sei $\alpha(x) = \alpha(y)$. Dann ist $1_H = \alpha(x)\alpha(y)^{-1} = \alpha(xy^{-1})$, also $xy^{-1} \in \mathrm{Ker}\,(\alpha) = \{1_G\}$, d.h. $xy^{-1} = 1_G$, daher $x = y$. Dies zeigt, dass α injektiv ist.
„$\Leftarrow$“ Sei $x \in \mathrm{Ker}\,(\alpha)$. Dann ist $\alpha(x) = 1_H = \alpha(1_G)$. Aus der Injektivität von α folgt $x = 1_G$. Daher $\mathrm{Ker}\,(\alpha) = \{1_G\}$.

2.34 Beispiel: *Kern*

(i) Der kanonische Epimorphismus $\kappa : G \to {}^{G}/_{N}$ hat den Kern $\mathrm{Ker}\,(\kappa) = N$, denn $1_{G/N} = N$ und $\kappa(g) = Ng = N \Leftrightarrow g \in N$.

(ii) $\mathrm{Ker}\,(\mathrm{sign}) = A_n$

(iii) $\mathrm{Ker}\,(\det) = SL(n, K)$

(iv) Sei $\gamma : G \to Aut(G)$ definiert wie in 2.30(vi). Es ist $g \in \mathrm{Ker}\,(\gamma) \Leftrightarrow \gamma_g = \mathrm{id} \Leftrightarrow x = x\gamma_g = x^g = g^{-1}xg \quad \forall x \in G \Leftrightarrow gx = xg \quad \forall x \in G$.

2.35 Definition: *Zentrum*

Man nennt $\mathrm{Ker}\,(\gamma) = \{g \in G \mid gx = xg \quad \forall x \in G\}$ das <u>Zentrum</u> von G und schreibt dafür $Z(G)$.
(Offenbar ist $Z(G) \lhd G$ und $Z(G) = G \Leftrightarrow G$ abelsch.)

2.36 Erster Isomorphiesatz

Sei $\alpha : G \to H$ ein Homomorphismus. Dann gilt

$$\mathrm{Im}\,(\alpha) \cong {}^{G}/_{\mathrm{Ker}\,(\alpha)}.$$

<u>*Beweis:*</u> Sei $\sigma : {}^{G}/_{\mathrm{Ker}\,(\alpha)} \to \mathrm{Im}\,(\alpha)$ definiert durch $\sigma(g\mathrm{Ker}\,(\alpha)) = \alpha(g) \in \mathrm{Im}\,(\alpha)$. Dann ist σ wohldefiniert, denn: $g\mathrm{Ker}\,(\alpha) = g'\mathrm{Ker}\,(\alpha) \Rightarrow g^{-1}g' \in \mathrm{Ker}\,(\alpha) \Rightarrow 1 = \alpha(g^{-1}g') = \alpha(g)^{-1}\alpha(g') \Rightarrow \alpha(g) = \alpha(g')$.
σ ist Homomorphismus, denn: $\sigma\,[(g_1\mathrm{Ker}\,(\alpha))(g_2\mathrm{Ker}\,(\alpha))] = \sigma(g_1g_2\mathrm{Ker}\,(\alpha)) = \alpha(g_1g_2) = \alpha(g_1)\alpha(g_2) = \sigma(g_1\mathrm{Ker}\,(\alpha))\sigma(g_2\mathrm{Ker}\,(\alpha))$.
Wenn $g\mathrm{Ker}\,(\alpha) \in \mathrm{Ker}\,(\sigma)$, dann $1 = \sigma(g\mathrm{Ker}\,(\alpha)) = \alpha(g)$, daher $g \in \mathrm{Ker}\,(\alpha)$ und $g\mathrm{Ker}\,(\alpha) = \mathrm{Ker}\,(\alpha) = 1 \in {}^{G}/_{\mathrm{Ker}\,(\alpha)}$. Also ist $\mathrm{Ker}\,(\sigma) = \{1\}$, das heißt σ ist injektiv. Wenn $x \in \mathrm{Im}\,(\alpha)$, dann $\exists g \in G : x = \alpha(g) = \sigma(g\mathrm{Ker}\,(\alpha))$, also $x \in \mathrm{Im}\,(\sigma)$. Daher ist σ surjektiv.

2.37 Zweiter Isomorphiesatz

Sei $N \lhd G$ und $U \leq G$. Dann ist

$$ {}^{UN}/_{N} \cong {}^{U}/_{U \cap N}.$$

<u>*Beweis:*</u> Sei $\kappa : G \to {}^{G}/_{N}$ der kanonische Epimorphismus und $\alpha := \kappa_{|U} : U \to {}^{G}/_{N}$ die Einschränkung. Dann ist α ein Homomorphismus mit
$\mathrm{Im}\,(\alpha) = \{\alpha(u) = uN \mid u \in U\} = {}^{UN}/_{N}$ und
$\mathrm{Ker}\,(\alpha) = U \cap N$, denn $u \in \mathrm{Ker}\,(\alpha) \Leftrightarrow uN = N \Leftrightarrow u \in U \cap N$. Die Behauptung folgt jetzt aus dem Ersten Isomorphiesatz.

2.38 Dritter Isomorphiesatz

Seien $N, M \lhd G$ und $M \leq N$. Dann ist ${}^{N}/_{M} \lhd {}^{G}/_{M}$ und es gilt

$$ {}^{({}^{G}/_{M})}/_{({}^{N}/_{M})} \cong {}^{G}/_{N}.$$

<u>*Beweis:*</u> Sei $\alpha : {}^{G}/_{M} \to {}^{G}/_{N}$ definiert durch $\alpha(gM) = gN$. Da $M \leq N$, ist α wohldefiniert. Dann ist α ein Homomorphismus und offenbar surjektiv. Außerdem
$gM \in \mathrm{Ker}\,(\alpha) \Leftrightarrow g \in N \Leftrightarrow gM \in {}^{N}/_{M}$, also $\mathrm{Ker}\,(\alpha) = {}^{N}/_{M}$.
Die Behauptung folgt jetzt aus dem Ersten Isomorphiesatz.

2.39 Satz: *Radikal*

Sei $\mathcal{E}$ eine Gruppeneigenschaft (d.h. $\mathcal{E}$ vererbt sich auf isomorphe Gruppen), für die gilt:

(1) $\{1\}$ hat $\mathcal{E}$.

(2) Wenn eine Gruppe die Eigenschaft $\mathcal{E}$ hat, dann auch jede Untergruppe.

(3) (Endliche) direkte Produkte von Gruppen mit $\mathcal{E}$ haben wieder die Eigenschaft $\mathcal{E}$.

Dann gibt es in jeder (endlichen) Gruppe G einen kleinsten Normalteiler $N^{\mathcal{E}}$ derart, dass ${}^{G}/_{N^{\mathcal{E}}}$ die Eigenschaft $\mathcal{E}$ hat.

<u>*Beweis:*</u> Sei $\mathcal{N} = \{M \triangleleft G \mid {}^{G}/_{M}$ hat die Eigenschaft $\mathcal{E}\}$. Da $\{1\} \cong {}^{G}/_{G}$ nach der Voraussetzung (1) die Eigenschaft $\mathcal{E}$ hat, ist $G \in \mathcal{N} \neq \emptyset$. Sei $N = \bigcap_{M \in \mathcal{N}} M$. Wir zeigen $N \in \mathcal{N}$ (es ist dann offenbar N das kleinste Element von $\mathcal{N}$). Dazu betrachten wir das direkte Produkt $P = \prod_{M \in \mathcal{N}} \times {}^{G}/_{M}$. Nach Voraussetzung (3) hat P die Eigenschaft $\mathcal{E}$, da dies für jedes ${}^{G}/_{M}$ gilt (und da $\mathcal{N}$ endlich ist, wenn G endlich ist). Nach (2) hat auch jede Untergruppe von P die Eigenschaft $\mathcal{E}$. Sein nun $\alpha : G \to P$ definiert durch $\alpha(g)(M) = gM$. Dies ist offenbar ein Homomorphismus. Es ist $g \in \operatorname{Ker}(\alpha) \Leftrightarrow gM = \alpha(g)(M) = 1_{{}^{G}/_{M}} = M \quad \forall M \in \mathcal{N} \Leftrightarrow g \in M \quad \forall M \in \mathcal{N} \Leftrightarrow g \in N$, also $\operatorname{Ker}(\alpha) = N$. Da $\operatorname{Im}(\alpha) \leq P$, hat $\operatorname{Im}(\alpha)$ die Eigenschaft $\mathcal{E}$. Nach dem Ersten Isomorphiesatz (2.36) ist ${}^{G}/_{N} \cong \operatorname{Im}(\alpha)$, also hat ${}^{G}/_{N}$ die Eigenschaft $\mathcal{E}$. Daher ist $N \in \mathcal{N}$.

3 G-Mengen

3.1 Definition: *G-Menge, Bahn, transitiv, Stabilisator*

Sei Ω eine Menge und G eine Gruppe. Man nennt Ω eine G-Menge, falls eine Abbildung $\Omega \times G \to \Omega$ gegeben ist, geschrieben $(\omega, g) \mapsto \omega g$ mit

(1) $\omega 1 = \omega \quad \forall \omega \in \Omega$

(2) $(\omega g)h = \omega(gh) \quad \forall \omega \in \Omega;\ g, h \in G.$

Wenn Ω eine G-Menge ist und $\omega \in \Omega$, dann heißt $\omega G = \{\omega g \mid g \in G\}$ die Bahn von ω (unter G). Falls ein $\omega \in \Omega$ existiert mit $\omega G = \Omega$, dann heißt Ω eine transitive G-Menge. Man nennt $G_\omega = \{g \in G \mid \omega g = \omega\}$ den Stabilisator von ω (in G).

3.2 Bemerkung: *Bahnen*

Durch $\omega \approx \omega' \Leftrightarrow \omega G = \omega' G$ wird ein Äquivalenzrelation auf Ω definiert. Die Äquivalenzklassen sind genau die Bahnen von G auf Ω.
Es gilt $\omega G = \omega' G \Leftrightarrow \exists g \in G : \omega g = \omega'$. Wenn $\omega g = \omega'$, dann ist $G_{\omega'} = (G_\omega)^g$, denn $x \in G_{\omega'} \Leftrightarrow \omega g = \omega' = \omega' x = \omega g x \Leftrightarrow \omega = \omega g x g^{-1} \Leftrightarrow g x g^{-1} \in G_\omega \Leftrightarrow x \in G_\omega^g$. Offenbar ist G_ω eine Untergruppe von G.

3.3 Bezeichnung/Beispiel: *transitiv, Konjugierten-Klassen, Zentralisator, Normalisator*

(i) Auf $\Omega = \{1, \ldots, n\}$ operiert $G = S_n$ transitiv. Es ist $G_n = S_{n-1}$.

(ii) Eine beliebige Gruppe G operiert auf $\Omega = G$ durch $g \circ h = gh$ transitiv. Es ist $G_1 = \{1\}$.

(iii) Eine beliebige Gruppe G operiert auf $\Omega = G$ durch $g \circ h = g^h$. Die Bahnen heißen die Konjugierten-Klassen von G. Es ist $G_g = C_G(g) = \{x \in G \mid xg = gx\}$ der Zentralisator von g.

(iv) Eine beliebige Gruppe G operiert auf $\Omega = \{\text{Untergruppen von } G\}$ durch Konjugation, d.h. $U \circ g = U^g$.
Die Bahnen sind die Klassen von konjugierten Untergruppen und $G_U = N_G(U)$ der Normalisator von U.

(v) Für eine beliebige Untergruppe U operiert G auf $\Omega = \{Ug \mid g \in G\}$, der Menge der Rechtsnebenklassen, durch $(Ug) \circ h = Ugh$ transitiv. Offenbar ist $G_{Ug} = U^g$.

(vi) Sei $\phi : G \to H$ ein Homomorphismus und Ω eine H-Menge. Dann wird Ω zu einer G-Menge durch $\omega \circ g = \omega \phi(g)$.

(vii) Sei Ω eine G-Menge. Dann sind auch $\Omega^k = \{(\omega_1, \ldots, \omega_k) \mid \omega_i \in \Omega\}$ und $\Omega^{(k)} = \{T \subseteq \Omega \mid |T| = k\}$ auf natürliche Weise G-Mengen.

3.4 Satz: *Hauptsatz über G-Mengen*

Sei Ω eine G-Menge und $\omega \in \Omega$. Die Abbildung $f : G_\omega g \mapsto \omega g$ ist eine Bijektion von der Menge der Rechtsnebenklassen des Stabilisators G_ω auf die Bahn ωG von ω.

Beweis: Wenn $G_\omega g = G_\omega h$, dann ist $h = xg$ für ein $x \in G_\omega$, also $\omega h = \omega x g = \omega g$. Daher ist f wohldefiniert.

Wenn $\alpha \in \omega G$, etwa $\alpha = \omega g$, dann ist $\alpha = f(G_\omega g)$, also ist f surjektiv.
Wenn $f(G_\omega g) = f(G_\omega h)$, dann ist $\omega g = \omega h$, also $\omega g h^{-1} = \omega$. Aber dann $gh^{-1} \in G_\omega$ und $G_\omega g = G_\omega h$ nach (2.15). Damit ist f auch injektiv.

3.5 Korollar: *Bahnlänge gleich Index des Stabilisators*

Es ist $|\omega G| = |G : G_\omega|$, d.h. die Bahnlänge ist gleich dem Index des Stabilisators.

Beweis: Klar.

3.6 Definition: *p-Gruppe*

Eine endliche Gruppe G heißt p-Gruppe, wenn $|G|$ eine Potenz der Primzahl p ist.

3.7 Satz: *Schnitt von Zentrum und Normalteiler in einer p-Gruppe*

Sei G ein p-Gruppe und $1 \neq N \triangleleft G$. Dann ist $N \cap Z(G) \neq 1$.

Beweis: N ist eine G-Menge durch Konjugation. Jede Bahnlänge ist nach 3.5 und Voraussetzung eine Potenz von p. Diese ist 1 genau dann, wenn die Bahn aus einem Element in $N \cap Z(G)$ besteht. Da $|N| > 1$ eine p-Potenz ist, kann es nicht nur eine Bahn der Länge 1 geben, also gibt es $1 \neq n \in N \cap Z(G)$, was zu zeigen war.

3.8 Korollar: *p-Gruppe hat Zentrum*

Jede p-Gruppe $G \neq \{1\}$ hat ein nicht-triviales Zentrum.

Beweis: Das ist der Spezialfall $N = G$ von (3.7).

3.9 Satz: *Normalisator in einer p-Gruppe*

Sei G eine p-Gruppe und U eine echte Untergruppe (d.h. $U \neq G$). Dann ist $N_G(U) > U$.

Beweis: Klar ist $U \leq N_G(U)$. Die Rechtsnebenklassen $\Omega = \{Ug \mid g \in G\}$ bilden eine G-, also eine U-Menge. Daher sind die Bahnlängen Potenzen von p. Da $|\Omega| = |G : U|$ teilbar ist durch p, kann $\{U\}$ nicht die einzige Bahn der Länge 1 sein. Also gibt es $g \in G \setminus U$ mit $Ugu = Ug \quad \forall u \in U$. Das heißt $gug^{-1} \in U$ nach (2.15), also $u \in U^g \quad \forall u \in U$ und damit $U \subseteq U^g$. Es folgt $g \in N_G(U) \setminus U$ wie behauptet.

3.10 Korollar: *Kleine p-Gruppen sind abelsch*

Sei $|G| = p^2$ mit einer Primzahl p. Dann ist G abelsch.

Beweis: Es ist zu zeigen, dass $x \in Z(G) \quad \forall x \in G$.
Wenn $o(x) = 1$, dann ist dies klar. Wenn $o(x) = p^2$, dann $\langle x \rangle = G$, und als zyklische Gruppe ist G abelsch. Es bleibt $o(x) = p$. Dann $\langle x \rangle < G$, also $N_G(\langle x \rangle) > \langle x \rangle$ nach (3.9). Weil $|G : \langle x \rangle| = p$, ist $N_G(\langle x \rangle) = G$, also $\langle x \rangle \triangleleft G$. Daher $Z(G) \cap \langle x \rangle \neq \{1\}$ nach (3.7). Weil $|\langle x \rangle| = p$, ist $x \in \langle x \rangle \leq Z(G)$.

4 Die Sylow'schen Sätze

4.1 Satz: *Existenz von Untergruppen in zyklischen Gruppen*

Sei G eine zyklische Gruppe der Ordnung $n \in \mathbb{N}$. Dann gibt es zu jedem Teiler $t \mid n$ genau eine Untergruppe der Ordnung t, und diese ist wieder zyklisch.

Beweis: Übungsaufgabe.

4.2 Satz: *Untergruppen und Primzahlpotenzen*

Sei G eine endlich Gruppe und p^a eine Primzahlpotenz, welche $|G|$ teilt. Sei $A_G(p^a)$ die Anzahl der Untergruppen der Ordnung p^a in G. Dann gilt:

$$A_G(p^a) \equiv 1 \pmod{p}.$$

Insbesondere gibt es Untergruppen der Ordnung p^a in G.

Beweis: Sei $|G| = p^a m$. Wir betrachten die G-Menge $\Omega = \{T \subseteq G \mid |T| = p^a\}$ mit der Verknüpfung $T \circ g = Tg$. Also $|\Omega| = \binom{|G|}{p^a} = \binom{p^a m}{p^a} = \sum_{i \in I} |B_i| \quad (*)$, wenn B_i die Bahnen von G auf Ω sind. Sei $T_i \in B_i$ und $U_i = G_{T_i}$ der Stabilisator. Wenn $t \in T_i$, dann $tU_i \subseteq T_i U_i = T_i$; also ist T_i eine Vereinigung von Linksnebenklassen von U_i, und es folgt $|U_i| \mid |T_i| = p^a$, also $|U_i| = p^{b_i}$ für ein $b_i \leq a$, d.h. $|B_i| = |G : U_i| = mp^{a-b_i}$. Wenn $b_i = a$, dann ist U_i eine der $A_G(p^a)$ gesuchten Untergruppen und T_i eine der m Linksnebenklassen von U_i und umgekehrt. Also gibt es genau $m \cdot A_G(p^a)$ Elemente $T \in \Omega$, welche in Bahnen der Länge m liegen. Alle anderen liegen in Bahnen, deren Länge durch pm teilbar ist. Aus $(*)$ folgt also $\binom{p^a m}{p^a} \equiv mA_G(p^a) \pmod{pm}$. Dies gilt auch für die zyklische Gruppe mit der Ordnung $p^a m$. In diesem Fall ist $A_G(p^a) = 1$ nach 4.1, also $\binom{p^a m}{p^a} \equiv m \pmod{pm}$. Aus den beiden letzten Kongruenzen ergibt sich $m\,(A_G(p^a) - 1) \equiv 0 \pmod{pm}$ und daher $A_G(p^a) \equiv 1 \pmod{p}$ wie behauptet.

4.3 Satz: *Elementordnung und Primteiler*

Wenn p ein Primteiler der Gruppenordnung $|G|$ ist, dann gibt es ein $g \in G$, so dass $o(g) = p$.

Beweis: Nach 4.2 gibt es eine Untergruppe $U \leq G$ mit $|U| = p$. Jedes $1 \neq g \in U$ hat die Ordnung p, da seine Ordnung die Untergruppenordnung teilen muß.

4.4 Definition: *p-Sylow-Gruppe*

Sei G eine endliche Gruppe, p eine Primzahl und p^a die größte p-Potenz, welche $|G|$ teilt. Jede Untergruppe der Ordnung p^a heißt dann eine p-Sylow-Gruppe von G.

4.5 Satz: *Sylow*

Sei G eine endliche Gruppe und p eine Primzahl. Dann gilt:

(1) G hat p-Sylow-Gruppen.

Sei P eine solche.

(2) Für jede p-Untergruppe Q gibt es ein $g \in G$ mit $Q^g \leq P$.

(3) Alle p-Sylow-Gruppen sind zueinander konjugiert.

(4) Die Anzahl der p-Sylow-Gruppen ist $|G : N_G(P)|$. Dies ist ein Teiler von $|G : P|$ und kongruent zu $1 \pmod p$.

Beweis:

(1) Klar nach 4.2.

(2) Die Menge $\Omega = \{Pg \mid g \in G\}$ ist eine G-Menge, also eine Q-Menge. Die Bahnlängen sind also Potenzen von p. Da $|\Omega| = |G : P| = |G|/|P|$ nicht durch p teilbar ist, gibt es eine Bahn mit Länge 1, also $PhQ = Ph$, d.h. $PhQh^{-1} = P$, also $hQh^{-1} \leq P$. Setzt man $g = h^{-1}$, folgt die Behauptung.

(3) Verwende (2) für eine p-Sylow-Gruppe Q. Dann gibt es $g \in G$ mit $Q^g \leq P$. Weil $|Q^g| = |Q| = |P|$, folgt $Q^g = P$, also die Behauptung.

(4) Nach (3) ist $\{P^g \mid g \in G\}$ die Menge der p-Sylow-Gruppen. Wegen (3.5) ist deren Anzahl also $|G : N_G(P)|$. Wegen $G \geq N_G(P) \geq P$ und dem Indexsatz ist $|G : N_G(P)|$ ein Teiler von $|G : P|$. Dass die Anzahl kongruent zu $1 \pmod p$ ist, steht schon in 4.2.

4.6 Definition: *Charakteristische Untergruppe*

Sei $U \leq G$. Man nennt U eine charakteristische Untergruppe von G (geschrieben $U \operatorname{char} G$), falls $\alpha(U) = U \quad \forall \alpha \in Aut(G)$.

4.7 Bemerkung: *Charakteristische Untergruppen*

(i) Jede charakteristische Untergruppe ist normal.

(ii) Charakteristische Untergruppen von Normalteilern sind wieder normal.

Beweis:

(i) ist ein Spezialfall von (ii).

(ii) Sei $U \operatorname{char} N \lhd G$. Da dann U bei jedem Automorphismus von N festbleibt, gilt dies auch für die Konjugation von N mit einem $g \in G$, denn $N^g = N$. Also ist $U^g = U \quad \forall g \in G$ und daher $U \lhd G$.

4.8 Korollar: *„normal“ heißt „charakteristisch“ für p-Sylow-Gruppe*

Sei P eine p-Sylow-Gruppe von G. äquivalent sind:

(1) $P \lhd G$.

(2) P ist die einzige p-Sylow-Gruppe von G.

(3) $P \operatorname{char} G$.

Beweis:

(1)⇒(2) Sei auch Q eine p-Sylow-Gruppe von G. Nach 4.5(3) gibt es ein $g \in G$ mit $Q = P^g$. Da $P \lhd G$, ist $P = P^g = Q$.

(2)⇒(3) Wenn $\alpha \in Aut(G)$, dann ist $\alpha(P)$ eine p-Sylow-Gruppe, also $\alpha(P) = P$, da P die einzige p-Sylow-Gruppe ist. Daher ist P charakteristisch.

(3)⇒(1) folgt aus 4.7(i).

4.9 Satz: *Frattini-Argument*

Sei $N \lhd G$ und P eine p-Sylow-Gruppe von N. Dann ist $G = N_G(P)N$.

Beweis: Sei $g \in G$. Dann ist P^g eine p-Sylow-Gruppe von $N^g = N$, also gibt es nach 4.5(3) ein $n \in N$ mit $P^g = P^n$, d.h. $P^{gn^{-1}} = P$ und damit $gn^{-1} \in N_G(P)$, also $g \in N_G(P)n \subseteq N_G(P)N$. Daher die Behauptung.

4.10 Satz: *Normalisator-Gleichheit*

Sei P eine p-Sylow-Gruppe von G und $N_G(P) \leq U \leq G$. Dann ist $N_G(U) = U$.

Beweis: Es ist $U \lhd N_G(U)$ und P eine p-Sylow-Gruppe von U. Nach 4.9 (mit $N = U$ und $G = N_G(U)$) folgt $N_G(U) = N_{N_G(U)}(P)U$. Aber $N_{N_G(U)}(P) \leq N_G(P) \leq U$ nach Voraussetzung. Daher ist $N_G(U) = U$.

4.11 Satz: *Sylowgruppen und Normalteiler*

Sei $N \lhd G$ und sei P ein p-Sylow-Gruppe von G. Dann gilt:

(1) $N \cap P$ ist eine p-Sylow-Gruppe von N, und jede p-Sylow-Gruppe von N erhält man so.

(2) ${}^{PN}/_{N}$ ist eine p-Sylow-Gruppe von ${}^{G}/_{N}$, und jede p-Sylow-Gruppe von ${}^{G}/_{N}$ erhält man so.

(3) $N_{G/N}\left({}^{PN}/_{N}\right) = {}^{N_G(P)N}/_{N}$.

Beweis:

(1) Sei Q ein p-Sylow-Gruppe von N. Nach 4.5(2) gibt es $g \in G$ mit $Q^g \leq P$, also $Q \leq P^{g^{-1}} \cap N$. Weil $P^{g^{-1}} \cap N$ eine p-Untergruppe von N ist und Q eine p-Sylow-Gruppe von N, folgt die Gleichheit. Also ist Q der Schnitt einer p-Sylow-Gruppe von G mit N. Offenbar ist auch $Q^g = P \cap N^g = P \cap N$ eine p-Sylow-Gruppe von N.

(2) Nach dem Zweiten Isomorphiesatz (siehe 2.37) ist $\left|{}^{PN}/_{N}\right| = |P : P \cap N|$ eine p-Potenz, also ${}^{PN}/_{N}$ eine p-Untergruppe von ${}^{G}/_{N}$. Andererseits ist $\left|{}^{G}/_{N} : {}^{PN}/_{N}\right| = |G : PN|$, also ein Teiler von $|G : P|$ nach dem Indexsatz 2.20, und daher nicht durch p teilbar, da P eine p-Sylow-Gruppe von G ist. Also ist ${}^{PN}/_{N}$ eine p-Sylow-Gruppe von ${}^{G}/_{N}$. Wenn Q eine beliebige p-Sylow-Gruppe von ${}^{G}/_{N}$ ist, dann ist $Q = \left({}^{PN}/_{N}\right)^{gN}$ für ein geeignetes $gN \in {}^{G}/_{N}$ nach 4.5(3). Also ist $Q = \left({}^{PN}/_{N}\right)^{gN} = {}^{P^g N}/_{N}$ von der behaupteten Form.

(3) Nach 2.28(4) ist $N_{G/N}\left({}^{PN}/_{N}\right) = {}^{N_G(PN)}/_{N}$. Es genügt daher, $N_G(PN) = N_G(P)N$ zu zeigen.
Dies folgt aus dem Frattini-Argument: Weil P eine p-Sylow-Gruppe von $PN \lhd N_G(PN)$ ist, gilt nach (4.9): $N_G(PN) = N_G(P)PN = N_G(P)N$. (Für beliebige Untergruppen $U \leq G$ gilt nur $N_G(U)N \leq N_G(UN)$.)

5 Kompositionsreihen

5.1 Definition: *einfach*

Eine Gruppe $G \neq \{1\}$ heißt einfach, falls sie nur die Normalteiler $\{1\}$ und G besitzt.

5.2 Beispiel: *einfache Gruppen*

Jede endliche Gruppe mit Primzahlordnung ist einfach.

5.3 Lemma: *untere Schranke für die Fakultät*

Seien $t, m \in \mathbb{N}, m \geq 2$ und $(t, m) \neq (1,2), (1,3), (1,4), (2,2)$. Dann ist

$$(tm)! > 2t \cdot t! \cdot m^{t+1}. \qquad (*)$$

Beweis: Für $t = 1$ ist die Behauptung gerade $m! > 2m^2$ oder $(m-1)! > 2m$. Dies gilt offenbar für $m = 5$. Für $m > 5$ gilt nun per Induktion $(m-1)! = (m-2)!(m-1) > 2(m-1)2 = 2(m-1) + 2(m-1) > 2(m-1) + 2 = 2m$.
$(*)$ gilt also für $t = 1$, wenn $m \geq 5$. Wenn $t > 1$, dann kann man nun per Induktion über t annehmen, dass entweder $(t-1, m)$ einer der Fälle $(1,2), (1,3), (1,4), (2,2)$ ist (also $(t, m) \in \{(2,2), (2,3), (2,4), (3,2)\}$; in den letzten drei Fällen ist $(*)$ leicht zu verifizieren) oder dass $(*)$ für $(t-1, m)$ gilt. Dann ist

$$\begin{aligned}
(tm)! &= [(t-1)m]!(tm-m+1) \cdot \ldots \cdot (tm-1)tm \\
&> 2(t-1)(t-1)! \cdot m^t (tm-m+1) \cdot \ldots \cdot (tm-1)tm \\
&= 2t \cdot t! \cdot m^{t+1}(t-1)(tm-m+1) \cdot \ldots \cdot (tm-2)\frac{tm-1}{t} \\
&\geq 2t \cdot t! \cdot m^{t+1} \quad .
\end{aligned}$$

5.4 Lemma: *Zentralisator in der S_n*

Sei $x \in S_n$ ein Element, welches aus t Zyklen der Länge m besteht (also $tm = n$). Dann gilt $|C_{S_n}(x)| = t!m^t$.

Beweis: Übungsaufgabe.

5.5 Satz: *Alternierende Gruppen sind einfach*

Die Alternierenden Gruppen A_n sind einfach, ausgenommen $n = 1, 2, 4$.

Beweis: Wegen $|A_n| = \frac{1}{2}n!$ für $n > 1$ und $A_1 = \{1\}$ sind $A_1 = A_2 = \{1\}$ nicht einfach und A_3 hat die Ordnung 3, ist also einfach. In A_4 gibt es den Normalteiler $\{(1), (12)(34), (13)(24), (14)(23)\}$. Daher ist A_4 nicht einfach.

Zur Vorbereitung: Der Stabilisator von n in A_n besteht genau aus den geraden Permutationen von $\{1, \ldots, n-1\}$, ist also die A_{n-1}. Die zu A_{n-1} konjugierten Untergruppen von A_n sind also genau die Stabilisatoren der Punkte $i \in \{1, \ldots, n\}$. Insbesondere ist $x \in \bigcap_{g \in A_n} A_{n-1}^g \Leftrightarrow x$ stabilisiert alle Punkte $\Leftrightarrow x = 1$.

$n=5$: Sei $N \lhd A_5$. Wenn $N \leq A_4$, dann auch $N = N^g \leq A_4^g \quad \forall g \in A_5$, also $N \leq \bigcap_{g \in A_5} A_4^g = \{1\}$. Wenn $N \not\leq A_4$, dann $A_5 \geq NA_4 > A_4$. Weil $|A_5 : A_4| = 5$ eine Primzahl ist, folgt aus dem Indexsatz (2.20), dass $NA_4 = A_5$. Daher ist $5 \mid |NA_4| = |N||A_4 : A_4 \cap N|$. Da $|A_4| = 12$, folgt $5 \mid |N|$. Folglich enthält N eine 5-Sylowgruppe, also alle 24 Elemente der Ordnung 5. Daher ist $|N| = 30$ oder $|N| = 60$. In jedem Fall $3 \mid |N|$, und wie oben enthält N auch alle 20 Elemente der Ordnung 3. Daher $|N| \geq 24 + 20$, d.h. $|N| = 60$, also $N = A_5$.

$n > 5$: Wieder sei $N \lhd A_n$. Dann ist $N \cap A_{n-1} \lhd A_{n-1}$, also (per Induktion) (1) $N \cap A_{n-1} = A_{n-1}$ oder (2) $N \cap A_{n-1} = \{1\}$.

(1): Es ist $N \geq A_{n-1}$, also auch $N = N^g \geq A_{n-1}^g \quad \forall g \in A_n$, d.h. N enthält alle geraden Permutationen, welche wenigstens einen Fixpunkt haben. Sei nun $x \in A_n$ eine beliebige Permutation. Dann ist $x = \tau_1\tau_2 \cdot \ldots \cdot \tau_{2m-1}\tau_{2m}$ ein Produkt einer geraden Anzahl von Transpositionen. Per Induktion über m sieht man, dass $x \in N$ ist: für $m = 0$ ist $x = 1 \in N$. Für $m > 0$ ist $x = (\tau_1 \cdot \ldots \cdot \tau_{2m-2})(\tau_{2m-1}\tau_{2m})$. Der erste Faktor ist per Induktion in N, der zweite ist dies, da $\tau_{2m-1}\tau_{2m}$ höchstens 4 Punkte bewegt, also (mindestens 2) Fixpunkte hat, da $n \geq 6$. Damit ist $N = A_n$.

(2): $\frac{1}{2}n! = |A_n| \geq |NA_{n-1}| = |N||A_{n-1}| = |N| \cdot \frac{1}{2}(n-1)!$, also $|N| \leq n$. Außerdem $N \cap A_{n-1}^g = N^g \cap A_{n-1}^g = (N \cap A_{n-1})^g = \{1\} \quad \forall g \in A_n$, d.h. eine gerade Permutation $\neq 1$, welche Fixpunkte hat (also in einem A_{n-1}^g liegt), ist nicht in N. Wir wollen zeigen, dass dann $N = \{1\}$. Dazu wähle $x \in N$. Sei m die kürzeste Länge in der Zyklenzerlegung von x. Dann hat $x^m \in N$ Fixpunkte, also ist $x^m = 1$. Daher haben alle Zyklen von x die Länge m. Wenn nun t deren Anzahl ist, dann ist $tm = n$ und mit $C := C_{S_n}(x)$ gilt $|C| = t! \cdot m^t$ nach (5.4). Außerdem ist $|x^{A_n}| = |A_n : C \cap A_n|$ nach (3.5). Wenn $C \leq A_n$, dann also $|x^{A_n}| = \frac{1}{2}n!/t!m^t$. Wenn $C \not\leq A_n$, dann $CA_n = S_n$, da $|S_n : A_n| = 2$, also $n!/t!m^t = |S_n : C| = |x^{S_n}| = |x^{CA_n}| = |x^{A_n}|$. In jedem Fall ist $|x^{A_n}| \geq n!/2t!m^t$. Da $x^{A_n} \subseteq N$ (weil $x \in N \lhd A_n$), folgt $n!/2t!m^t \leq |N| \leq n$, d.h. $(mt)! = n! \leq n \cdot 2t!m^t = 2t \cdot t! \cdot m^{t+1}$. Nach (5.3) geht dies nur, wenn $m = 1$ oder $(t,m) \in \{(1,2),(1,3),(1,4),(2,2)\}$. Im zweiten Fall ist $n = tm < 6$ entgegen der Voraussetzung. Also ist $m = 1$. Daher hat x nur Zyklen der Länge 1, also $x = \mathrm{id}$. Da $x \in N$ beliebig war, ist $N = \{1\}$.

5.6 Lemma: *Dedekind-Identität*

Seien $A, B, C \leq G$ mit $A \leq B$. Dann $AC \cap B = A(C \cap B)$.

Beweis: Klar.

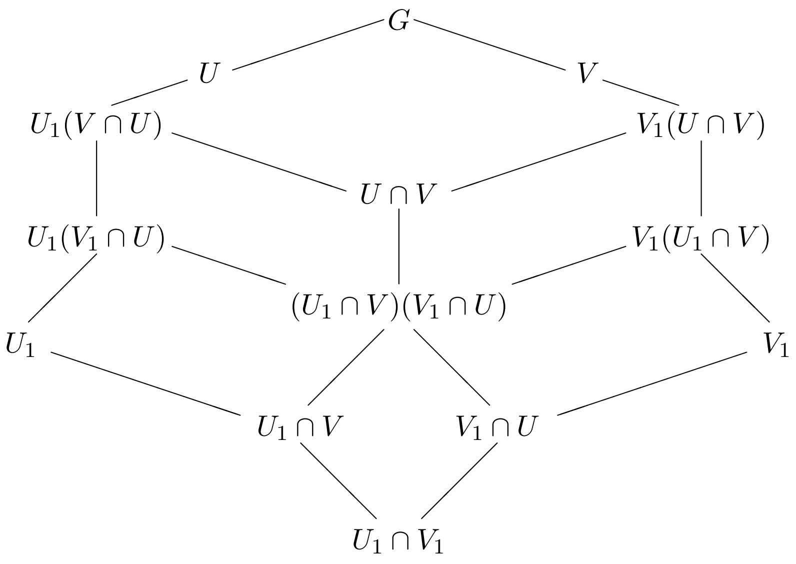
5.7 Lemma: *Schmetterlingslemma*

Seien U, V Untergruppen von G und $U_1 \lhd U, V_1 \lhd V$. Dann gilt:

(1) $U_1(V_1 \cap U) \lhd U_1(V \cap U)$

(2) $V_1(U_1 \cap V) \lhd V_1(U \cap V)$

(3) $U_1(V \cap U) / U_1(V_1 \cap U) \cong V_1(U \cap V) / V_1(U_1 \cap V)$



<u>*Beweis:*</u>

(1) Es ist $U_1 \lhd U$ und $V_1 \cap U \leq V \cap U \leq U$, also $U_1(V_1 \cap U) \leq U_1(V \cap U) \leq U$. Elemente aus $V \cap U$ normalisieren U_1, V_1 und U, also auch $U_1(V_1 \cap U)$. Daher gilt $V \cap U \leq N_G\left[U_1(V_1 \cap U)\right]$. Offenbar ist $U_1 \leq U_1(V_1 \cap U) \leq N_G\left[U_1(V_1 \cap U))\right]$. Demzufolge ist auch das Produkt $U_1(V \cap U) \leq N_G\left[U_1(V_1 \cap U))\right]$, d.h. $U_1(V_1 \cap U) \lhd U_1(V \cap U)$.

(2) Folgt aus (1), indem man U mit V und U_1 mit V_1 vertauscht.

(3) Betrachte $\phi : U \cap V \to {}^{U_1(V \cap U)}/_{U_1(V_1 \cap U)}$ definiert durch $\phi(x) = xU_1(V_1 \cap U)$. Dann ist ϕ offenbar ein Homomorphismus, sogar ein Epimorphismus, denn wenn $y \in U_1(V \cap U) = (U \cap V)U_1$, dann $y = xa$ mit $x \in U \cap V, a \in U_1$. Daher ist $yU_1(V_1 \cap U) = xaU_1(V_1 \cap U) = xU_1(U \cap V_1) = \phi(x)$. Es ist $x \in \mathrm{Ker}\,(\phi) \Leftrightarrow x \in (U \cap V) \cap U_1(V_1 \cap U) = (U \cap V \cap U_1)(V_1 \cap U)$, wobei die Gleichheit aus (5.6) folgt. Also $\mathrm{Ker}\,(\phi) = (U_1 \cap V)(V_1 \cap U)$. Nach dem 1.Isomorphiesatz (2.36) folgt: ${}^{U_1(V \cap U)}/_{U_1(V_1 \cap U)} \cong {}^{U \cap V}/_{(U_1 \cap V)(V_1 \cap U)}$. Vertausche wieder U, V und U_1, V_1. Dann ist auch ${}^{V_1(U \cap V)}/_{V_1(U_1 \cap V)} \cong {}^{V \cap U}/_{(V_1 \cap U)(U_1 \cap V)} = {}^{U \cap V}/_{(U_1 \cap V)(V_1 \cap U)}$ und die Behauptung folgt.

5.8 **Lemma:** *Gemeinsame Verfeinerung*

Seien $G = N_0 \rhd N_1 \rhd \ldots \rhd N_r = \{1\}$ und $G = K_0 \rhd K_1 \rhd \ldots \rhd K_s = \{1\}$ gegeben. Setze $N_{ij} = N_i(N_{i-1} \cap K_j)$ und $K_{ij} = K_j(K_{j-1} \cap N_i)$ für $i = 1, \ldots, r; j = 1, \ldots, s$. Dann gilt

$$\begin{aligned} N_{i-1} &= N_{i0} \rhd N_{i1} \rhd \ldots \rhd N_{is} = N_i \\ K_{j-1} &= K_{0j} \rhd K_{1j} \rhd \ldots \rhd K_{rj} = K_j \end{aligned}$$

und ${}^{N_{i,j-1}}/_{N_{i,j}} \cong {}^{K_{i-1,j}}/_{K_{i,j}}$.

<u>*Beweis:*</u> Verwende (für i und j fest) (5.7) mit $U = N_{i-1}, U_1 = N_i$ und $V = K_{j-1}, V_1 = K_j$. Dann $N_{ij} = N_i(N_{i-1} \cap K_j) \lhd N_i(N_{i-1} \cap K_{j-1}) = N_{i,j-1}$,
ebenso $K_{ij} = K_j(K_{j-1} \cap N_i) \lhd K_j(N_{i-1} \cap K_{j-1}) = K_{i-1,j}$ und ${}^{N_{i,j-1}}/_{N_{ij}} \cong {}^{K_{i-1,j}}/_{K_{ij}}$.
Es ist $N_{i0} = N_i(N_{i-1} \cap K_0) = N_i N_{i-1} = N_{i-1}$ und $N_{is} = N_i(N_{i-1} \cap K_s) = N_i \cdot 1 = N_i$.
Ebenso $K_{0j} = K_{j-1}$ und $K_{rj} = K_j$.

5.9 Definition: *Kompositionsreihe, -faktor und -länge*

Eine Reihe $G = N_0 \triangleright N_1 \triangleright \ldots \triangleright N_r = \{1\}$ heißt Kompositionsreihe von G, wenn ${}^{N_{i-1}}\!/_{N_i}$ eine einfache Gruppe ist für jedes $i = 1, \ldots, r$. Man nennt dann ${}^{N_{i-1}}\!/_{N_i}$ einen Kompositionsfaktor von G und r die Kompositionslänge.

5.10 Bemerkung: *Kompositionsreihen endlicher Gruppen*

Jede endliche Gruppe hat eine Kompositionsreihe . Aber z.B. $\mathbb{Z}$ hat keine.

5.11 Satz: *Jordan - Hölder*

Sei $G = N_0 \triangleright N_1 \triangleright \ldots \triangleright N_r = \{1\}$ eine Kompositionsreihe und sei
$(*)$ $\quad G = K_0 \triangleright K_1 \triangleright \ldots \triangleright K_s = \{1\}$ echt absteigend.

(1) $(*)$ läßt sich (durch Hinzufügen weiterer geeigneter Gruppen zwischen K_{i-1} und K_i) zu einer Kompositionsreihe von G verfeinern.

(2) Wenn $(*)$ ebenfalls eine Kompositionsreihe ist, dann ist $r = s$ und die Kompositionsfaktoren ${}^{N_{i-1}}\!/_{N_i}$ und ${}^{K_{i-1}}\!/_{K_i}$ sind bis auf Reihenfolge und Isomorphie dieselben.

Beweis: Weil ${}^{N_{i-1}}\!/_{N_i}$ einfach ist, gilt für ein festes i mit den Bezeichnungen von (5.8):

$$N_{i-1} = N_{i0} = \ldots = N_{i,t(i)-1} \underset{\neq}{\triangleright} N_{i,t(i)} = N_{i,t(i)+1} = \ldots = N_{is} = N_i.$$

Also hat man eine Abbildung $t : \{1, \ldots, r\} \to \{1, \ldots, s\}$ derart, dass $N_{ij-1} = N_{ij}$ außer für $j = t(i)$. Dann ist ${}^{N_{i,t(i)-1}}\!/_{N_{i,t(i)}} = {}^{N_{i-1}}\!/_{N_i}$ einfach. Aber dann $K_{i-1,j} = K_{i,j}$ für $j \neq t(i)$, und ${}^{K_{i-1,j}}\!/_{K_{i,j}} \cong {}^{N_{i-1}}\!/_{N_i}$ einfach für $j = t(i)$. Also bilden die K_{ij} nach Weglassen der Wiederholungen die gesuchte Verfeinerung. Das beweist (1).
Falls auch $(*)$ eine Kompositionsreihe ist, muß es für jedes j genau ein i geben mit ${}^{K_{i-1,j}}\!/_{K_{i,j}}$ einfach, d.h. $t(i) = j$. Also ist dann t eine Bijektion (insbesondere $r = s$) und ${}^{N_{i-1}}\!/_{N_i} \cong {}^{K_{t(i)-1}}\!/_{K_{t(i)}}$.

6 Auflösbare und nilpotente Gruppen

6.1 Definition: *Kommutator und Kommutatorgruppe*

Seien $x, y \in G$. Man nennt $[x, y] = x^{-1}y^{-1}xy$ den Kommutator von x und y. Die Gruppe $G' = \langle [x, y] \mid x, y \in G \rangle$ heißt die Kommutatorgruppe von G.

6.2 Bemerkung: *Kommutatoren*

(i) $yx\,[x, y] = xy$

(ii) $[x, y]^{-1} = [y, x]$

(iii) Die Kommutatorgruppe von G ist eine charakteristische Untergruppe von G, denn $\alpha\,[x, y] = [\alpha(x), \alpha(y)] \quad \forall \alpha \in Aut(G)$.
Insbesondere ist $G' \lhd G$. Wenn $N \lhd G$, dann ist $\left({}^{G}\!/_{N}\right)' = {}^{G'N}\!/_{N}$.
Insbesondere ist ${}^{G}\!/_{N}$ abelsch $\Leftrightarrow$ $\left({}^{G}\!/_{N}\right)' = \{1\}$ $\Leftrightarrow$ $G' \leq N$. Also ist G' der kleinste Normalteiler mit abelscher Faktorgruppe (vergleiche 2.39).

6.3 Definition: *höhere Kommutatorgruppe, auflösbare Gruppen*

(1) Für $n \in \mathbb{N}_0$ definiert man die höhere Kommutatorgruppe $G^{(n)}$ induktiv durch $G^{(0)} = G$ und $G^{(n)} = \left(G^{(n-1)}\right)'$ für $n > 0$.

(2) Man nennt G auflösbar, falls $G^{(n)} = \{1\}$ für ein $n \in \mathbb{N}_0$ gilt.

6.4 Bemerkung/Beispiel: *auflösbare Gruppen*

(i) Jede abelsche Gruppe G ist auflösbar, denn $G^{(1)} = G' = \{1\}$.

(ii) S_3 ist auflösbar, denn $S_3' = A_3$ ist abelsch, also $S_3'' = S_3^{(2)} = \{1\}$.

(iii) A_5 ist einfach und nicht abelsch. Also ist $A_5' = A_5$ und daher $A_5^{(n)} = A_5 \quad \forall n \in \mathbb{N}_0$.
Diese Gruppe ist nicht auflösbar. Ebenso ist die S_5 nicht auflösbar, weil $S_5^{(n)} = A_5 \quad \forall n \in \mathbb{N}$.

(iv) Die höheren Kommutatorgruppen sind alle charakteristische Untergruppen von G, wie man leicht induktiv beweist.

6.5 Lemma: *höhere Kommutatorgruppen von Untergruppen und Faktorgruppen*

(1) Für jede Untergruppe U von G und jedes $n \in \mathbb{N}_0$ gilt $U^{(n)} \leq G^{(n)}$.

(2) Wenn $N \lhd G$ und $n \in \mathbb{N}_0$, dann $\left({}^{G}\!/_{N}\right)^{(n)} = {}^{G^{(n)}N}\!/_{N}$.

Beweis: Induktion über n. Beide Behauptungen sind für $n = 0$ trivial. Sei nun $n > 0$.

(1) Weil per Induktion $U^{(n-1)} \leq G^{(n-1)}$, sind alle Kommutatoren von Elementen aus $U^{(n-1)}$ auch Kommutatoren von Elementen von $G^{(n-1)}$, also $U^{(n)} = \left(U^{(n-1)}\right)' \leq \left(G^{(n-1)}\right)' = G^{(n)}$.

(2) Wieder per Induktion ist $\left({}^{G}\!/_{N}\right)^{(n-1)} = {}^{G^{(n-1)}N}\!/_{N}$. Daher wird $\left({}^{G}\!/_{N}\right)^{(n)} = \left[\left({}^{G}\!/_{N}\right)^{(n-1)}\right]'$ von den Elementen $[xN, yN] = [x, y]\, N$ mit $x, y \in G^{(n-1)}$ erzeugt. Da $\{[x, y] \mid x, y \in G^{(n-1)}\}$ ein Erzeugendensystem von $G^{(n)}$ ist, folgt die Behauptung.

6.6 Satz: *Untergruppen auflösbarer Gruppen sind wieder auflösbar*

Wenn G auflösbar ist, dann gilt dies auch für jede Untergruppe und jede Faktorgruppe von G.

Beweis: Klar nach (6.5), weil $G^{(n)} = \{1\}$ für geeignetes n.

6.7 Satz: *Normalteiler in auflösbaren Gruppen*

Sei $N \triangleleft G$. äquivalent sind:

(1) G ist auflösbar.

(2) N und ${}^{G}\!/_{N}$ sind auflösbar.

Beweis:

(1)⇒(2) folgt aus (6.6).

(2)⇒(1) Weil ${}^{G}\!/_{N}$ auflösbar ist, gibt es ein n mit $\{1\} = \left({}^{G}\!/_{N}\right)^{(n)} = {}^{G^{(n)}N}\!/_{N}$ (vergleiche 6.5(2)), also $G^{(n)} \leq N$. Nach (6.5(1)) ist daher $G^{(n+m)} = \left(G^{(n)}\right)^{(m)} \leq N^{(m)} = \{1\}$ für geeignetes m, weil N auflösbar ist.

6.8 Satz: *Produkte und Schnitte von Normalteilern*

Seien $N_1, \ldots, N_s$ Normalteiler von G.

(1) Wenn ${}^{G}\!/_{N_i}$ auflösbar ist für alle i, dann ist ${}^{G}\!/_{\bigcap_i N_i}$ auflösbar.

(2) Wenn alle N_i auflösbar sind, dann ist auch $\prod_i N_i$ auflösbar.

Beweis:

(1) Endliche direkte Produkte von auflösbaren Gruppen sind auflösbar, da $(G_1 \times \ldots \times G_s)' = G_1' \times \ldots \times G_s'$. Weil ${}^{G}\!/_{\bigcap_i N_i}$ isomorph ist zu einer Untergruppe von ${}^{G}\!/_{N_i} \times \ldots \times {}^{G}\!/_{N_s}$ (vergleiche 2.39), folgt die Behauptung aus (6.6).

(2) Per Induktion kann man annehmen, dass $M = \prod_{i<s} N_i$ auflösbar ist. Dann ist $\prod_i N_i = MN_s$ auflösbar nach (6.7), denn N_s ist ein auflösbarer Normalteiler von MN_s und ${}^{MN_s}\!/_{N_s} \cong {}^{M}\!/_{M \cap N_s}$ ist auflösbar als Faktorgruppe von M (vergleiche 6.6 und den Zweiten Isomorphiesatz (2.37)).

6.9 **Satz:** *p-Gruppen sind auflösbar*

Jede p-Gruppe G ist auflösbar.

<u>*Beweis:*</u> Wenn $|G| = 1$, ist nichts zu zeigen. Andernfalls ist das Zentrum Z ein abelscher (also auflösbarer) Normalteiler von G. Da $Z \neq \{1\}$ nach (3.7), ist ${}^{G}/_{Z}$ eine p-Gruppe von kleinerer Ordnung. Diese ist auflösbar per Induktion über die Gruppenordnung. Nach (6.7) ist G auflösbar.

6.10 **Satz:** *$|G| = p^a q$ ist auflösbar*

Sei $|G| = p^a q$ mit Primzahlen p, q. Dann ist G auflösbar.

<u>*Beweis:*</u> Wenn $p = q$, dann folgt die Behauptung aus (6.9).
Sei also $p \neq q$. Wenn eine p-Sylow-Gruppe P normal ist, dann hat man nach (6.9) einen auflösbaren Normalteiler derart, dass auch die Faktorgruppe ${}^{G}/_{P}$ als q-Gruppe auflösbar ist, womit die Behauptung folgt.
Ebenso argumentiert man, wenn eine q-Sylowgruppe normal ist. Wir können also annehmen, dass es mehrere p-Sylow-Gruppen $P_1, P_2, \ldots$ und mehrere q-Sylowgruppen $Q_1, Q_2, \ldots$ gibt. Weil $|G : P| = q$ eine Primzahl ist, gibt es genau q p-Sylow-Gruppen. Außerdem gibt es mindestens p q-Sylowgruppen, also mindestens $p(q-1)$ Elemente der Ordnung q. Wäre $P_i \cap P_j = \{1\} \quad \forall i \neq j$, dann gäbe es $q(p^a - 1)$ Elemente $\neq 1$ mit einer p-Potenzordnung. Aber dann wäre $|G| \geq p(q-1) + q(p^a - 1) + 1 = p^a q + (p-1)(q-1) > |G|$, ein Widerspruch.
Wähle jetzt zwei verschiedene p-Sylow-Gruppen P_1 und P_2 mit $D = P_1 \cap P_2$ möglichst groß. Dann ist $D \neq \{1\}$, wie gerade gezeigt. Sei $H = N_G(D)$. Angenommen, H wäre eine p-Gruppe; dann gibt es eine p-Sylow-Gruppe P_3 von G mit $H \leq P_3$ nach (4.5(2)). Dann ist $P_1 \cap P_3 \geq P_1 \cap H = N_{P_1}(D) > D$ nach (3.9). Nach Wahl von D folgt $P_1 = P_3$ und ebenso $P_2 = P_3$, also $P_1 = P_2$, ein Widerspruch.
Also $q \mid |H|$ und dann offenbar $G = HP_1$. Daher ist $D^G = D^{HP_1} = D^{P_1}$, also liegen alle Konjugierten von D in P_1. Daher ist $\{1\} \neq K := \langle D^g \mid g \in G \rangle$ ein Normalteiler von G, welcher in P_1 liegt und daher auflösbar ist. Es ist $\left| {}^{G}/_{K} \right| = p^b q$ mit $b < a$. Per Induktion ist ${}^{G}/_{K}$ auflösbar und die Behauptung folgt wieder aus (6.7).

6.11 **Beispiel:** *zu (6.10), die S_4*

$|S_4| = 4! = 2^3 \cdot 3$; also ist die S_4 auflösbar.

6.12 **Satz:** *Burnside (1904)*

Sei $|G| = p^\alpha \cdot q^\beta$ mit Primzahlen p, q. Dann ist G auflösbar.
(Ohne Beweis!)

6.13 **Satz:** *Feit-Thompson (1963)*

Gruppen ungerader Ordnung sind auflösbar.
(Ohne Beweis!)

6.14 **Definition:** *elementar-abelsche p-Gruppen, minimaler Normalteiler*

(1) Sei p eine Primzahl und G eine abelsche Gruppe.
Man nennt G eine <u>elementar-abelsche p-Gruppe</u>, wenn $x^p = 1 \quad \forall x \in G$.

(2) Ein Normalteiler $\{1\} \neq N \lhd G$ heißt <u>minimal</u>, falls $M \lhd G, M < N \Rightarrow M = \{1\}$.

6.15 **Satz:** *minimale Normalteiler in endlichen auflösbaren Gruppen*

Sei G eine endliche auflösbare Gruppe und N ein minimaler Normalteiler von G. Dann ist N eine elementar-abelsche p-Gruppe für eine geeignete Primzahl p.

Beweis: N ist auflösbar nach (6.6). Da $N \neq \{1\}$, ist $N' < N$. Weil N' char N nach (6.2), folgt $N' \lhd G$ nach (4.9). Die Minimalität von N erzwingt $N' = \{1\}$, also ist N abelsch. Sei p ein Primteiler von $|N|$. Dann ist $N_0 = \{x \in N \mid x^p = 1\}$ eine charakteristische Untergruppe von N, also wieder $N_0 \lhd G$. Da $N_0 \neq \{1\}$ nach (4.3), folgt $N = N_0$. Offenbar ist N_0 elementar-abelsch.

6.16 **Satz:** *minimale Normalteiler in auflösbaren Untergruppen der S_p*

Sei p ein Primzahl und G eine auflösbare transitive Untergruppe der symmetrischen Gruppe S_p. Dann ist die p-Sylow-Gruppe P von G der einzige minimale Normalteiler. Es ist ${}^{G}\!/_{P}$ abelsch. Wenn $p \geq 5$ ist, dann enthält G keine Transpositionen.

Beweis: Sei A ein minimaler Normalteiler von G. Nach (6.15) ist A eine elementar-abelsche q-Gruppe für eine Primzahl q. Wenn $q \neq p$, dann hat A einen Fixpunkt $\omega \in \{1, \ldots, p\}$, denn alle Bahnlängen von A sind Potenzen von q; sie können aber nicht alle durch q teilbar sein, weil $q \nmid p$. Aber dann $A \leq G_\omega$ und damit $A = A^g \leq (G_\omega)^g = G_{\omega g}$ (siehe 3.2) für jedes g. Da G transitiv operiert, läßt A alle Punkte fest, also $A = \{1\}$, und das ist ein Widerspruch.
Daher ist $q = p$, also $A = P$ (da $|P| = p$) der einzige minimale Normalteiler. Wenn $1 \neq x \in P$, $y, z \in G$, dann ist $x^y = x^i$ und $x^z = x^j$ für geeignete i, j, also ist $x^{yz} = x^{ij} = x^{zy}$. Daher ist $(yz)(zy)^{-1} \in C_G(x) = P$ (siehe 5.4), also $Pyz = Pzy$. Also ist ${}^{G}\!/_{P}$ abelsch.

Wenn $g \in G$ die Fixpunkte α und $\omega = \alpha x^i$ hat, dann ist $\alpha x^i = \omega = \omega g = \alpha x^i g = \alpha g (x^g)^i = \alpha (x^g)^i$. Es folgt $\alpha = \alpha (x^g)^i x^{-i} = \alpha (x^g x^{-1})^i$, weil $x^g \in P$ mit x vertauscht. Daher ist $(x^g x^{-1})^i = 1$; also ist $i \equiv 0 \pmod p$ und dann $\omega = \alpha x^i = \alpha$, oder es ist $x^g x^{-1} = 1$ und dann $g \in C_G(x) = P$. Im zweiten Fall muß $g = 1$ sein, da die anderen Elemente aus P keine Fixpunkte haben.
Wie haben gezeigt: Ein Element $1 \neq g \in G$ hat höchstens einen Fixpunkt. Da eine Transposition $p-2$ Fixpunkte hat, folgt die Behauptung.

6.17 **Bemerkung:** ${}^{G}\!/_{P}$ *ist zyklisch*

Wie werden später zeigen, dass ${}^{G}\!/_{P}$ unter den Voraussetzungen des Satzes nicht nur abelsch, sondern sogar zyklisch ist.

6.18 **Satz:** *endliche und auflösbare Gruppen*

Äquivalent sind:

(1) G ist endlich und auflösbar.

(2) G hat eine Reihe $G = G_0 > G_1 > \ldots > G_n = \{1\}$ mit $G_i \lhd G$ und ${}^{G_{i-1}}\!/_{G_i}$ abelsch und endlich.

(3) G hat eine Kompositionsreihe $G = N_0 > N_1 > \ldots > N_t = \{1\}$ mit ${}^{N_{i-1}}\!/_{N_i}$ zyklisch von Primzahlordnung.

Beweis:

(1)⇒(2) Sei $G_i = G^{(i)}$ die i-te Kommutatorgruppe. Dies ist eine charakteristische Untergruppe von G (6.4) und ${}^{G_{i-1}}\!/_{G_i} = {}^{G^{(i-1)}}\!/_{\left(G^{(i-1)}\right)'}$ ist abelsch nach (6.2).

(2)⇒(3) Verfeinere die in (2) gegebene Reihe zu einer Kompositionsreihe (vergleiche 5.11). Dann sind die Faktoren abelsch und einfach, also zyklisch von Primzahlordnung.

(3)⇒(1) Induktion über t.

$t = 0$ Dann ist $G = \{1\}$.

$t > 0$ Per Induktion ist N_1 endlich und auflösbar. Da auch ${}^{G}\!/_{N_1} = {}^{N_0}\!/_{N_1}$ endlich und auflösbar ist, folgt (1) aus (6.7).

6.19 Definition: *Zentralkette, nilpotent, auf- und absteigende Zentralreihe*

(1) Seien Normalteiler $N_0 \geq N_1 \geq \ldots$ $(*)$ von G gegeben. Man nennt $(*)$ eine Zentralkette von G, falls ${}^{N_i}\!/_{N_{i+1}} \leq Z\left({}^{G}\!/_{N_{i+1}}\right)$ für $i = 0, 1, \ldots$ gilt.

(2) Wenn eine Zentralkette $G = N_0 \geq \ldots \geq N_r = \{1\}$ existiert, dann heißt G nilpotent.

(3) Induktiv definiert man $Z_i = Z_i(G)$ durch $Z_0 = \{1\}$ und ${}^{Z_{i+1}}\!/_{Z_i} = Z\left({}^{G}\!/_{Z_i}\right)$. Dann heißt $Z_0 \leq Z_1 \leq \ldots$ die aufsteigende Zentralreihe von G.

(4) Induktiv definiert man G^i durch $G^0 = G$ und $G^{i+1} = \left[G^i, G\right] = \left\langle [a, g] \mid a \in G^i, g \in G \right\rangle$. Dann heißt $G^0 \geq G^1 \geq \ldots$ die absteigende Zentralreihe von G.

6.20 Bemerkung: *Z_i und G^i*

(i) Die Z_i und G^i sind charakteristische Untergruppen von G (leichte Induktion).

(ii) Die auf- und absteigenden Zentralreihen sind Zentralketten von G : für die aufsteigende Zentralreihe ist dies klar; für die absteigende Zentralreihe folgt aus $[G^i, G] \leq G^{i+1}$, dass $\left[{}^{G^i}\!/_{G^{i+1}}, {}^{G}\!/_{G^{i+1}}\right] = \{1\}$, also ${}^{G^i}\!/_{G^{i+1}} \leq Z\left({}^{G}\!/_{G^{i+1}}\right)$.

(iii) Wieder durch Induktion sieht man $G^{(n)} \leq G^n \quad \forall n$.

(iv) Wenn N und M Normalteiler von G sind, dann ist $[N, M] \leq N \cap M$. Insbesondere kommutieren zwei Normalteiler elementweise, wenn sie trivialen Schnitt haben.

6.21 Satz: *nilpotente Gruppen*

Sei G eine endliche Gruppe. Äquivalent sind:

(1) G ist nilpotent.

(2) Für genügend großes n gilt $G^n = \{1\}$. Die absteigende Zentralreihe endet also bei $\{1\}$.

(3) Ist $U \underset{\neq}{<} G$, so $N_G(U) > U$.

(4) Jede maximale Untergruppe ist Normalteiler.

(5) Alle Sylowgruppen von G sind Normalteiler.

(6) G ist das direkte Produkt seiner Sylowgruppen.

(7) Wenn $N \underset{\neq}{\triangleright} G$, dann ist $Z\left({}^{G}\!/_{N}\right) \neq \{1\}$.

(8) Für genügend großes m gilt $Z_m = G$.
Die aufsteigende Zentralreihe endet also bei G.

(9) Wenn $x, y \in G$ mit $o(x), o(y)$ teilerfremd, dann $xy = yx$.

<u>*Beweis:*</u>

(1)⇒(2) Sei $G = N_0 \geq \ldots \geq N_r = \{1\}$ eine Zentralkette.
Behauptung: $G^i \leq N_i \quad \forall i \leq r$ (insbesondere $G^r \leq N_r = \{1\}$).
Beweis durch Induktion über i. Der Fall $i = 0$ ist trivial. Wenn nun also die Behauptung für i gezeigt ist, dann ist $G^{i+1} = [G^i, G] \leq [N_i, G]$. Aber ${}^{N_i}\!/_{N_{i+1}} \leq Z\left({}^{G}\!/_{N_{i+1}}\right)$, also gilt $[N_i, G] \leq N_{i+1}$ und damit die Behauptung.

(2)⇒(3) Wähle i minimal mit $G^i \leq U$. Dann ist $i > 0$ und $G^{i-1} \not\leq U$. Aber $G^{i-1} \leq N_G(U)$, denn $\left[G^{i-1}, U\right] \leq \left[G^{i-1}, G\right] = G^i \leq U$, d.h. es ist $u^{-1}u^x = [u, x] = [x, u]^{-1} \in U \quad \forall x \in G^{i-1}, u \in U$, also auch $u^x \in U$. Daher ist $N_G(U) \neq U$, und die Behauptung folgt.

(3)⇒(4) Sei M eine maximale Untergruppe. Da $N_G(M) > M$, folgt $N_G(M) = G$, also $M \triangleleft G$.

(4)⇒(5) Sei P eine p-Sylow-Gruppe von G und $H = N_G(P)$. Wäre $H \neq G$, dann wäre $H \leq M$ für eine maximale Untergruppe M von G. Nach Voraussetzung ist $M \triangleleft G$. Dies widerspricht (4.10). Also ist $H = G$ und $P \triangleleft G$.

(5)⇒(6) Seien $P_1, \ldots, P_m$ die Sylowgruppen zu den verschiedenen Primteilern $p_1, \ldots, p_m$ von $|G| = \prod\limits_{i=1}^{m} p_i^{e_i}$.
Dann ist $\left|\prod\limits_{i \in I} P_i\right| = \prod\limits_{i \in I} p_i^{e_i}$ für jede Teilmenge I von $\{1, \ldots, m\}$. Insbesondere ist $P_i \cap \prod\limits_{j \neq i} P_j = \{1\}$ und $P_i \cap P_j = \{1\}$ für $i \neq j$. Daher kommutieren die verschiedenen Sylowgruppen elementweise.

(6)⇒(7) Wenn $G = P_1 \cdot P_2 \cdot \ldots \cdot P_m$ wie in (6), dann ist $Q_i = N \cap P_i$ eine p_i-Sylowgruppe von N (vergleiche 4.11), also $N = Q_1 \cdot Q_2 \cdot \ldots \cdot Q_m$. Daher ist
${}^{G}\!/_{N} \cong {}^{P_1}\!/_{Q_1} \cdot {}^{P_2}\!/_{Q_2} \cdot \ldots \cdot {}^{P_m}\!/_{Q_m}$ und
$Z\left({}^{G}\!/_{N}\right) \cong Z\left({}^{P_1}\!/_{Q_1}\right) \cdot Z\left({}^{P_2}\!/_{Q_2}\right) \cdot \ldots \cdot Z\left({}^{P_m}\!/_{Q_m}\right)$.
Weil $N \neq G$ ist, ist $Q_i \neq P_i$ für wenigstens ein i, d.h. ${}^{P_i}\!/_{Q_i} \neq \{1\}$. Nach (3.7) ist dann auch $Z\left({}^{P_i}\!/_{Q_i}\right) \neq \{1\}$, und die Behauptung folgt.

(7)⇒(8) Weil G endlich ist, muß $Z_{m+1} = Z_m$ für genügend großes m gelten. Es ist $Z_m \triangleleft G$. Wäre $Z_m \neq G$, dann $\{1\} \neq Z\left({}^{G}\!/_{Z_m}\right) = {}^{Z_{m+1}}\!/_{Z_m}$, also $Z_{m+1} > Z_m$, ein Widerspruch.

(8)⇒(1) Da $G = Z_m > Z_{m-1} > \ldots > Z_0 = \{1\}$ eine Zentralkette ist, ist G nilpotent.

(6)⇒(9) Seien wieder $p_1, \ldots, p_n$ die Primteiler von $|G|$ und $P_1, \ldots, P_m$ die zugehörige Sylowgruppe. Wenn $I = \{i \mid p_i \mid o(x)\}$ und $J = \{j \mid p_j \mid o(y)\}$, dann $I \cap J = \emptyset$, also $\prod\limits_{i \in I} P_i \cap \prod\limits_{j \in J} P_j = \{1\}$. Weil $x \in \prod\limits_{i \in I} P_i \triangleleft G$ und $y \in \prod\limits_{j \in J} P_j \triangleleft G$, folgt $[x, y] = 1$, also die Behauptung.

(9)⇒(5) Sei P eine p-Sylow-Gruppe von G und Q eine q-Sylowgruppe für ein $q \neq p$. Wenn $x \in P$ und $y \in Q$, dann sind $o(x), o(y)$ teilerfremd, also $xy = yx$, d.h. $y \in$

$C_G(x)$. Dies gilt für jedes $x \in P$, also $y \in C_G(P) \leq N_G(P)$. Daher ist $Q \leq N_G(P)$ für jede q-Sylowgruppe ($q \neq p$). Da auch $P \leq N_G(P)$, folgt $N_G(P) = G$, also $P \lhd G$.

6.22 Korollar: *Unter- und Faktorgruppen von nilpotenten Gruppen*

(1) Untergruppen und Faktorgruppe von nilpotenten endlichen Gruppen sind wieder nilpotent.

(2) Wenn N ein Normalteiler von G mit ${}^{G}/{}_{N}$ nilpotent ist und $N \leq Z_i(G)$ für ein i gilt, dann ist G nilpotent.

(3) Vorsicht: Eine Gruppe kann einen nilpotenten Normalteiler N mit nilpotenter Faktorgruppe ${}^{G}/{}_{N}$ haben, aber selbst nicht nilpotent sein.

Beweis:

(1) Die Eigenschaft (9) vererbt sich offenbar auf Untergruppen. Wenn $N \lhd G$ und P ein p-Sylow-Gruppe von G ist, dann ist ${}^{PN}/{}_{N}$ eine p-Sylow-Gruppe von ${}^{G}/{}_{N}$ nach (4.11). Daraus sieht man, dass sich die Eigenschaft (5) auf Faktorgruppen vererbt.

(2) Es ist ${}^{G}/{}_{Z_i(G)} \cong {}^{(G/N)}/{}_{(Z_i(G)/N)}$ nach dem 3.Isomorphiesatz (2.38), also nilpotent nach (1), weil ${}^{G}/{}_{N}$ nilpotent ist. Die aufsteigende Zentralreihe von ${}^{G}/{}_{Z_i(G)}$ endet also bei ${}^{G}/{}_{Z_i(G)}$. Weil ${}^{Z_{i+j}(G)}/{}_{Z_i(G)} = Z_j\left({}^{G}/{}_{Z_i(G)}\right)$ für $j = 0, 1, \ldots$ gilt, endet die aufsteigende Zentralreihe von G bei G.

(3) A_3 ist ein nilpotenter (da abelscher) Normalteiler der S_3. Auch die Faktorgruppe ist abelsch, aber die S_3 ist nicht nilpotent, da $Z(S_3) = \{1\}$.

6.23 Satz: *Zusammenhang zwischen auf- und absteigender Zentralreihe*

Sei G endlich und nilpotent und seien $G = G^0 > G^1 > \ldots > G^{n-1} > G^n = \{1\}$ und $\{1\} = Z_0 < Z_1 < \ldots < Z_{m-1} < Z_m = G$ die ab- bzw. aufsteigenden Zentralreihen. Dann ist $n = m$ und für jede Zentralkette $G = N_0 > N_1 > \ldots > N_{s-1} > N_s = \{1\}$ gilt $s \geq n$ und $G^i \leq N_i \leq Z_{s-i}$ für $i = 0, \ldots, s$ (dabei ist $G^i = \{1\}$ und $Z_i = G$ für $i \geq n$ gesetzt).

Beweis: Per Induktion ist $G^i \leq N_i$ (siehe Beweis (1)⇒(2) von 6.21); insbesondere ist $G^i \leq Z_{m-i}$. Als nächstes zeigen wir $N_i \leq Z_{s-i}$ durch Rückwärts-Induktion über i. Wenn $i = s$, dann ist die Behauptung trivial. Sei die Behauptung für ein $0 < i \leq s$ schon gezeigt. Weil ${}^{N_{i-1}}/{}_{N_i} \leq Z\left({}^{G}/{}_{N_i}\right)$, ist $[N_{i-1}, G] \leq N_i \leq Z_{s-i}$. Daher ist ${}^{N_{i-1}Z_{s-i}}/{}_{Z_{s-i}} \leq Z\left({}^{G}/{}_{Z_{s-i}}\right) = {}^{Z_{s-i+1}}/{}_{Z_{s-i}}$, d.h. $N_{i-1} \leq N_{i-1}Z_{s-i} \leq Z_{s-i+1} = Z_{s-(i-1)}$. Das ist die Behauptung für $i-1$.
Wäre $s < n$, dann $\{1\} < G^{n-1} \leq G^s \leq N_s = \{1\}$, ein Widerspruch. Insbesondere ist $m \geq n$.
Wäre $s < m$, dann $G = N_0 \leq Z_s \leq Z_{m-1} < Z_m = G$, ein Widerspruch. Insbesondere ist $n \geq m$.
Damit ist alles bewiesen.

6.24 Definition: *Klasse*

Man nennt n wie in (6.23) die Klasse der nilpotenten Gruppe G.

6.25 **Satz:** *Produkt von nilpotenten Normalteilern*

Sei G eine endliche Gruppe und seien N und M nilpotente Normalteiler von G. Dann ist auch NM ein nilpotenter Normalteiler von G.

Beweis: Sei p eine Primzahl und P_1 die p-Sylow-Gruppe von N und P_2 die p-Sylow-Gruppe von M. Dann sind P_1 und P_2 normal in G, da charakteristisch in N bzw. M. Daher ist $P_1P_2 \triangleleft NM$, und offenbar ist P_1P_2 eine p-Sylow-Gruppe von NM. Daher ist NM nilpotent nach (6.21).

Hinweis: Der Satz, aber nicht der Beweis, ist auch für unendliche Gruppen richtig.

6.26 **Bemerkung/Definition:** *Fitting-Gruppe*

Das Produkt aller nilpotenten Normalteiler einer endlichen Gruppe G ist nach (6.25) ein nilpotenter Normalteiler und offenbar der größte solche.
Man nennt ihn die Fitting-Gruppe $Fit(G)$ von G.

7 Polynom - Ringe

7.1 Bezeichnung/Bemerkung: *Einleitung*

Der ganze Paragraph ist eine knappe Wiederholung und Zusammenfassung von einfachen Aussagen über Polynom - Ringe, die schon in Paragraph 11 des Scripts zur *Linearen Algebra* stehen.
Ein Ring R ist eine Menge mit zwei Verknüpfungen, Addition „+“ und Multiplikation „·“, derart, dass $(R,+)$ eine abelsche Gruppe ist (neutrales Element heißt „Null“). Die Multiplikation ist assoziativ, und die beiden Distributivgesetze gelten. Die Ringe, die wir betrachten, sind kommutativ ($ab = ba \quad \forall a, b \in R$) und haben ein neutrales Element $1 \neq 0$ bezüglich der Multiplikation ($1a = a \quad \forall a \in R$). Elemente u, welche ein multiplikatives Inverses u^{-1} haben (also $uu^{-1} = 1$), heißen Einheiten. Ein kommutativer Ring mit 1, in welchem jedes Element $\neq 0$ eine Einheit ist, ist ein Körper. Ein Nullteiler ist eine Element $0 \neq a \in R$, zu welchem ein $0 \neq b \in R$ existiert mit $ab = 0$. Wenn es in R keine Nullteiler gibt, nennt man den Ring nullteilerfrei.
Ringhomomorphismen sind Abbildungen zwischen zwei Ringen R und S, die beide Verknüpfungen respektieren. Wir betrachten nur unitäre Homomorphismen, d.h. $1_R \mapsto 1_S$. Der Kern eines Homomorphismus $\phi : R \to S$ ist ein Ideal $I \triangleleft R$, d.h. eine additive Untergruppe in R, welche gegen Multiplikation mit Ringelementen von links und rechts abgeschlossen ist. Das Bild von ϕ ist ein Unterring von S. für jedes Ideal I ist $R/_I$ wieder ein Ring, der Faktorring von R nach I, und es gilt $\operatorname{Im}(\phi) \cong R/_{\operatorname{Ker}(\phi)}$ (isomorph als Ringe). Die letzte Aussage ist der Erste Isomorphiesatz für Ringe. Die beiden anderen gelten ebenfalls, wenn „Untergruppe“ durch „Unterring“ und „Normalteiler“ durch „Ideal“ ersetzt wird (vergleiche 2.37 - 2.38).
Summen, Schnitte und Produkte von Idealen sind wieder Ideale, wie man leicht sieht. Eine wichtige Klasse von Idealen sind die Hauptideale, das heißt die Ideale der Form $(a) = aR$ für $a \in R$.

Das neben $\mathbb{Z}$ wichtigste Beispiel für uns ist die Menge $R[x] = \left\{ \sum\limits_{i=0}^{n} r_i x^i \mid n \in \mathbb{N}, r_i \in R \right\}$ aller Polynome mit Koeffizienten aus einem Ring R, die mit der üblichen Addition und Multiplikation von Polynomen einen Ring bildet, genannt der Polynomring über R in einer Unbestimmten. Offenbar läßt sich diese Konstruktion verallgemeinern zu $R[X]$, wobei X eine Menge von Unbestimmten ist. Die konstanten Polynome bilden einen Unterring von $R[x]$, welcher in natürlicher Weise zu R isomorph ist. Man betrachtet daher R als Unterring von $R[x]$.

$R[x]$ ist kommutativ, nullteilerfrei und hat eine 1, wenn dies für R gilt. Wenn $p = \sum\limits_{i=0}^{n} r_i x^i$ und $r_n \neq 0$, dann heißt $n = \deg p$ der Grad von p. Wenn sogar $r_n = 1$, spricht man von einem normierten Polynom. Polynome vom Grad Null sind also genau die konstanten Polynome $\neq 0$. Das Nullpolynom 0 hat $\deg 0 = -\infty$. Für das Produkt von Polynomen p und q gilt dann $\deg(pq) \leq \deg(p) + \deg(q)$. Wenn R nullteilerfrei ist, gilt die Gleichheit; man nennt dies die Gradformel . Die Einheiten in $R[x]$ sind dann die Einheiten in R.

7.2 Satz: *Homomorphismen und Ideale*

Sei $\alpha : R \to S$ ein surjektiver Ringhomomorphismus und seien I, J Ideale von R. Dann gilt:

(1) $I\alpha$ ist ein Ideal von S.

(2) Alle Ideale von S sind von dieser Form.

(3) $I\alpha \leq J\alpha \Leftrightarrow I + \mathrm{Ker}\,(\alpha) \leq J + \mathrm{Ker}\,(\alpha)$

(4) $I\alpha = J\alpha \Rightarrow I + \mathrm{Ker}\,(\alpha) = J + \mathrm{Ker}\,(\alpha)$

(5) $I \mapsto I\alpha$ ist eine Bijektion zwischen den Idealen von R, welche $\mathrm{Ker}\,(\alpha)$ enthalten, und den Idealen von S.

<u>*Beweis:*</u> Sei $K = \mathrm{Ker}\,(\alpha)$. Da $S = \mathrm{Im}\,(\alpha) \cong {}^{R}\!/_{K}$, darf man $S = {}^{R}\!/_{K}$ annehmen. Sei $r \mapsto \overline{r} = r + K$ der kanonische Epimorphismus von R auf S. Nach 2.28 ist dann $U \mapsto \overline{U} = {}^{U}\!/_{K}$ eine Bijektion zwischen den additiven Untergruppen $K \leq U \leq R$ und den additiven Untergruppen von S. Diese Bijektion erhält Ideale:
Für $s = \overline{r} \in S$ gilt $s\overline{U} = \overline{rU} \leq \overline{U}$ genau dann, wenn $rU + K \leq U$ (vergleiche 2.28(1)), das heißt genau dann, wenn $rU \leq U$. Da dies für jedes $s \in S$ gilt, ist U ein Ideal von R genau dann, wenn $\overline{U}$ ein Ideal von S ist. für beliebiges Ideal I von R ist $U = I + K$ ein Ideal mit $K \leq U$ und $\overline{U} = \overline{I}$. Die Behauptungen folgen jetzt alle aus 2.28.

7.3 Lemma: *Ringe und Körper*

Ein kommutativer Ring R mit $1 \neq 0$ ist genau dann ein Körper, wenn $\{0\}$ und R die einzigen Ideale von R sind.

<u>*Beweis:*</u> Für $0 \neq a \in R$ ist zu zeigen, dass a eine Einheit ist. Weil $0 \neq aR \triangleleft R$, ist $aR = R$, also gibt es ein $b \in R$ mit $ab = 1$.
Umgekehrt sei $0 \neq I \triangleleft R$ und R ein Körper. Dann gibt es $0 \neq a \in I$. Daher ist auch $b = (ba^{-1})a \in Ra \subseteq I$ für jedes $b \in R$, also $I = R$.

7.4 Korollar: *Körperhomomorphismen*

Ein Homomorphismus $0 \neq \mu : K \to R$ von einem Körper K in einen Ring R ist injektiv.
<u>*Beweis:*</u> $Ker(\mu)$ ist ein Ideal $\neq K$ von K, also $Ker(\mu) = 0$.

7.5 Bemerkung: *Allgemeines über Ringe*

(i) Wenn $M \neq R$ ein Ideal von R ist, dann ist nach (7.3) ${}^{R}\!/_{M}$ ein Körper genau dann, wenn ${}^{R}\!/_{M}$ keine echten Ideale hat. Nach (7.2(5)) ist dies genau dann der Fall, wenn M ein <u>maximales</u> Ideal ist.
Etwas allgemeiner folgt aus dem Ersten Isomorphiesatz: Wenn R ein kommutativer Ring und $\alpha : R \to S$ eine unitärer Ringhomomorphismus ist, dann gilt: $\mathrm{Im}\,(\alpha)$ ist ein Körper genau dann, wenn $\mathrm{Ker}\,(\alpha)$ ein maximales Ideal ist.

(ii) Zwei Elemente $a, b \in R$ heißen <u>assoziiert</u>, wenn es eine Einheit $u \in R$ gibt mit $b = ur$. Dies definiert eine Äquivalenzrelation auf R. Wenn a und b assoziiert sind, erzeugen sie das gleiche Ideal: $aR = bR$. Wenn R nullteilerfrei ist, gilt auch die Umkehrung.

(iii) Für Elemente $a, b \in R$ sagt man „a <u>teilt</u> b“ und schreibt $a \mid b$, wenn ein $c \in R$ existiert mit $ac = b$. Dies ist offenbar äquivalent zu $b \in (a) := aR$. In $R[x]$ gilt z.B.: $x - a \mid f \in R[x] \Leftrightarrow f(a) = 0$, d.h. a ist <u>Nullstelle</u> von f. Eine Einheit u teilt jedes b, weil $(u) = R$.

(iv) Ein <u>Primelement</u> ist ein $0 \neq p \in R$, welches keine Einheit ist, und ein Produkt ab mit $a, b \in R$ nur dann teilt, wenn es wenigstens einen der beiden Faktoren teilt.

(v) Ein Element $0 \neq q$ heißt irreduzibel, wenn aus $q = ab$ folgt, dass genau einer der Faktoren eine Einheit ist.

(vi) Ein Hauptidealring (kurz HIR) ist ein kommutativer, nullteilerfreier Ring R, in welchem jedes Ideal ein Hauptideal ist. Das wichtigste Beispiel für einen solchen Ring ist $\mathbb{Z}$.

(vii) In einem Hauptidealring ist jedes Primelement irreduzibel und umgekehrt. Es sind dies genau die Elemente, welche maximale Ideale $\neq \{0\}$ erzeugen. Nach (i) ist also $\mathbb{Z}/(p)$ ein Körper für jede Primzahl p.

(viii) Wie in $\mathbb{Z}$ hat man in jedem Hauptidealring eine Faktorisierung von Elementen $\neq 0$ als Produkt von Primelementen; diese ist eindeutig bis auf die Reihenfolge und Multiplikation mit Einheiten (d.h. Übergang zu assoziierte Primelementen).

(ix) Dies ist für uns wichtig, denn der Polynomring $K[x]$ ist ein Hauptidealring. Hier wie im Folgenden bezeichnet K einen Körper. Man sieht dies ähnlich wie für $\mathbb{Z}$ durch Division mit Rest.

(x) Wenn g ein gemeinsamer Teiler von $a, b \in R$ ist, d.h. $g \mid a$ und $g \mid b$, und jeder gemeinsame Teiler von a und b ein Teiler von g ist, dann heißt g ein größter gemeinsamer Teiler (kurz ggT) von a und b, geschrieben als $g = \operatorname{ggT}(a, b)$.

(xi) In jedem Hauptidealring existiert für alle a, b ein größter gemeinsamer Teiler $g = \operatorname{ggT}(a, b)$; dieser ist bis auf Assoziierte eindeutig, und in der Tat ist dann $(a) + (b) = (g)$. Man sieht hieraus, dass $g = ra + sb$ für geeignete $r, s \in R$.

(xii) In $K[x]$ kann man zu jedem Polynom die Ableitung bilden: Wenn $p(x) = \sum\limits_{i=0}^{n} a_i x^i$, dann ist $p'(x) := \sum\limits_{i=1}^{n} i a_i x^{i-1}$. Diese Konstruktion hat die üblichen formalen Eigenschaften der Ableitung (Ketten- und Produktregel).

(xiii) Eine Nullstelle $a \in K$ von $p \in K[x]$ heißt mehrfach, wenn $(x-a)^2 \mid p$.

7.6 Lemma: *mehrfache Nullstellen von Polynomen*

Sei $q = \operatorname{ggT}(p, p')$ für $0 \neq p \in K[x]$. Die Nullstellen von q sind genau die mehrfachen Nullstellen von p.

Beweis: Sei a eine mehrfache Nullstelle von p, etwa $p = (x-a)^2 r$.
Dann ist $p' = 2(x-a)r + (x-a)^2 r'$, also $x - a \mid p'$ und daher $x - a \mid q$, also $q(a) = 0$. Umgekehrt sei $q(a) = 0$. Dann ist auch $p(a) = 0$, weil $q \mid p$, also $x - a \mid p$, etwa $p = (x-a)s$; und ebenso $p'(a) = 0$. Aber $p' = (x-a)s' + s$ nach der Produktregel, also $0 = p'(a) = s(a)$. Daher $x - a \mid s$ und damit $(x-a)^2 \mid p$.

7.7 Bemerkung: *irreduzible Polynome*

Wenn $p \in K[x]$ irreduzibel ist und $q = \operatorname{ggT}(p, p')$, dann ist $q \mid p$. Wegen der Irreduzibilität von p ist also (bis auf Einheiten) $q = 1$ oder $q = p$. Wegen $q \mid p'$ und $\deg(p') < \deg(p)$ kann der zweite Fall nur eintreten, wenn $p' = 0$, also (mit den Bezeichnungen von 7.5(xi)) $i a_i = 0$ für $i = 1, \ldots, n$. Da K ein Körper ist, gilt also $0 = i \in K$, falls $a_i \neq 0$. Dabei ist $i = \underbrace{1 + \ldots + 1}_{i \times}$ ein Element von K (und nicht die natürlich Zahl). Dies kommt tatsächlich vor (siehe unten).

8 Irreduzibilitätskriterien

Ob ein gegebenes Polynom irreduzibel ist, kann man nicht immer leicht entscheiden. Einige Hilfe soll hier gegeben werden. Dabei werden wir uns auf Polynome in $\mathbb{Q}[x]$ konzentrieren. Manche der vorgestellten Methoden lassen sich verallgemeinern.

8.1 **Lemma:** *Irreduzibilität per Substitution*

Sei R ein kommutativer nullteilerfreier Ring und $p, f \in R[x]$, f nicht konstant.

(1) Wenn $p(f)$ irreduzibel ist, dann ist auch p irreduzibel.

(2) Wenn R ein Körper ist und $\deg f = 1$, dann gilt auch die Umkehrung: Wenn p irreduzibel ist, dann ist auch $p(f)$ irreduzibel.

Beweis:

(1) Wenn $p = rs$ eine Faktorisierung mit Nicht-Einheiten r und s ist, dann ist $p(f) = r(f)s(f)$ ebenfalls eine solche Faktorisierung, denn $\deg r(f) = (\deg r)(\deg f) \geq \deg r$, also ist $r(f)$ keine Einheit; denn wenn $\deg r = 0$, dann ist $r(f) = r$.

(2) Zu $f(x) = ax+b$ gibt es eine inverse lineare Substitution, nämlich $g(x) = a^{-1}(x-b)$, denn $f(g(x)) = g(f(x)) = x$. Die Behauptung folgt aus (1), wenn man g in $p(f)$ substituiert.

8.2 **Bemerkung/Beispiel:**

(i) Wenn K ein Körper ist, dann bilden die linearen Substitutionen ein Gruppe, wie man leicht sieht.

(ii) Wenn f konstant ist, kann (8.1 (1)) falsch sein: $p(x) = (2x-1)(x+1)$ ist reduzibel in $\mathbb{Z}[x]$, aber $p(1) = 2$ ist irreduzibel in $\mathbb{Z}[x]$.

(iii) Wenn $\deg f > 1$, dann kann durch Substitution von f die Irreduzibilität verloren gehen: Substituiert man etwa $f(x) = x^2$ in das irreduzible Polynom $p(x) = x$, so erhält man ein reduzibles Polynom.

(iv) Auch bei einer linearen Substitution kann die Irreduzibilität verloren gehen, wenn R kein Körper ist. Ein Beispiel ist $p(x) = x$ und $f(x) = 2x$ in $\mathbb{Z}[x]$.

(v) Sei $p(x) = x^2 - 4x + 5 \in \mathbb{R}[x]$. Substituiere $f(x) = x + 2$. Dann $p(f(x)) = (x+2)^2 - 4(x+2) + 5 = x^2 + 1$. Dies ist irreduzibel in $\mathbb{R}[x]$ (s.u.), also ist auch p irreduzibel.

8.3 **Lemma:** *Irreduzibilität in Körpern*

Sei K ein Körper.

(1) Jedes lineare Polynom in $K[x]$ ist irreduzibel.

(2) Wenn $\deg p = 2$ oder $\deg p = 3$, dann gilt: p ist reduzibel in $K[x]$ genau dann, wenn p eine Nullstelle in K hat.

Beweis:

(1) folgt aus der Gradformel (siehe 7.1), da Polynome vom Grad 0 Einheiten sind.

(2) Wenn $a \in K$ eine Nullstelle von p ist, dann ist $x - a$ ein Teiler von p (vergleiche 7.5), also ist p reduzibel.
Wenn umgekehrt p reduzibel ist, dann ist einer der Faktoren linear, etwa $ax - b$. Dann ist $a^{-1}b$ eine Nullstelle von p.

8.4 **Bemerkung:** *reduzible Polynome*

(i) In $\mathbb{Z}[x]$ ist (8.3 (1)) falsch, denn z.B. $2x$ ist linear, aber reduzibel, denn weder 2 noch x ist eine Einheit in $\mathbb{Z}[x]$.

(ii) Das Polynom $p = (2x-1)(3x-1) \in \mathbb{Z}[x]$ ist reduzibel und vom Grad 2, es hat aber keine Nullstelle in $\mathbb{Z}$. Also ist auch eine der Implikationen von (8.3 (2)) falsch in $\mathbb{Z}[x]$.

8.5 **Definition:** *primitives Polynom*

Ein Polynom $0 \neq f(x) = \sum\limits_{i=0}^{n} z_i x^i \in \mathbb{Z}[x]$ heißt <u>primitiv</u>, wenn 1 der größte gemeinsame Teiler der Koeffizienten $z_0, \ldots, z_n$ ist.

8.6 **Beispiel:** *primitive Polynome*

(i) $f(x) = 6x^2 + 10x + 15$ ist primitiv, $g(x) = 6x^2 + 10x + 14$ ist nicht primitiv.

(ii) Ein Polynom ist primitiv, wenn einer der Koeffizienten 1 ist (z.B. wenn das Polynom normiert ist).

8.7 **Satz:** *Faktorisierung in $\mathbb{Q}[x]$*

Sei $0 \neq f \in \mathbb{Q}[x]$. Dann gibt es $q \in \mathbb{Q}$ und ein primitives Polynom $g \in \mathbb{Z}[x]$ mit $f = qg$. Dies Darstellung ist eindeutig bis auf das Vorzeichen.

<u>*Beweis:*</u> Sei $f(x) = \sum\limits_{i=0}^{n} q_i x^i$ mit $q_i \in \mathbb{Q}$, etwa $q_i = {}^{a_i}/_{b_i}$ mit $a_i, b_i \in \mathbb{Z},\ b_i \neq 0$. Setzt man $b = \prod\limits_i b_i$, dann ist $z_i = bq_i \in \mathbb{Z}$ und $f(x) = {}^1/_b \sum\limits_{i=0}^{n} z_i x^i$.
Sei $t = \operatorname{ggT}(z_0, \ldots, z_n)$, etwa $z_i = tu_i,\ u_i \in \mathbb{Z}$. Dann ist $g(x) = \sum\limits_{i=0}^{n} u_i x^i \in \mathbb{Z}[x]$ primitiv und $f(x) = {}^t/_b \cdot g(x)$ eine Darstellung wie behauptet.
Wenn $0 \neq q_1 g_1 = q_2 g_2$ mit primitiven Polynomen $g_1, g_2 \in \mathbb{Z}[x]$ und $q_1, q_2 \in \mathbb{Q}$, etwa $q_i = {}^{r_i}/_{s_i}$ mit $r_i, s_i \in \mathbb{Z}$, dann ist $s_2 r_1 g_1 = s_1 r_2 g_2 \in \mathbb{Z}[x]$. Der größte gemeinsame Teiler der Koeffizienten dieses Polynoms ist $s_2 r_1$, da g_1 primitiv ist, aber ebenso ist er $s_1 r_2$. Da der größte gemeinsame Teiler bis auf Einheiten in $\mathbb{Z}$, also bis auf das Vorzeichen, bestimmt ist, folgt $s_2 r_1 = \pm s_1 r_2$, also $q_1 = \pm q_2$ und dann auch $g_1 = \pm g_2$.

8.8 **Bemerkung/Definition:** *Galoisfeld*

Sei $p \in \mathbb{Z}$ eine Primzahl.

(i) Man nennt ${}^{\mathbb{Z}}/_{(p)}$ das <u>Galoisfeld mit p Elementen</u> und schreibt dafür auch $\mathrm{GF}(p)$ oder $\mathcal{F}_p$.

(ii) Da (p) ein maximales Ideal von $\mathbb{Z}$ ist, ist $\mathcal{F}_p$ ein Körper und $|\mathcal{F}_p| = |\mathbb{Z} : (p)| = p$.

(iii) Man schreibt oft $\overline{z} := z + p\mathbb{Z}$, d.h. $^{-} : \mathbb{Z} \to \mathcal{F}_p$ ist der kanonische Epimorphismus.

(iv) Wenn $f(x) = \sum\limits_{i=0}^{n} z_i x^i \in \mathbb{Z}[x]$, dann ist $\overline{f}(x) = \sum\limits_{i=0}^{n} \overline{z_i} x^i \in \mathcal{F}_p[x]$.

(v) Die Abbildung $f \mapsto \overline{f}$ ist ein surjektiver Ringhomomorphismus von $\mathbb{Z}[x]$ auf $\mathcal{F}_p[x]$. Es gilt offenbar $\deg \overline{f} \leq \deg f$ mit Gleichheit genau dann, wenn der führende Koeffizient von f nicht durch p teilbar ist oder $f = 0$.

8.9 Lemma: *Gauß'sches Lemma*

Wenn $f, g \in \mathbb{Z}[x]$ primitive Polynome sind, dann ist auch fg primitiv.

Beweis: Andernfalls gibt es eine Primzahl p, welche alle Koeffizienten von fg teilt, also ist $0 = \overline{fg} = \overline{f}\,\overline{g}$. Aber $\overline{f}, \overline{g} \neq 0$, da f und g primitiv sind. Dies ist ein Widerspruch, da $\mathcal{F}_p[x]$ nullteilerfrei ist.

Der folgende Satz erlaubt es, Polynome in $\mathbb{Z}[x]$ statt solche in $\mathbb{Q}[x]$ zu betrachten, wenn man Irreduzibilität untersucht.

8.10 Satz: *Reduzibilität und primitive Polynome*

Sei $0 \neq f \in \mathbb{Q}[x]$ und sei $g \in \mathbb{Z}[x]$ primitiv mit $f = qg$ für ein $q \in \mathbb{Q}$ (vergleiche 8.7). Genau dann ist f reduzibel in $\mathbb{Q}[x]$, wenn g reduzibel in $\mathbb{Z}[x]$ ist.

Beweis: Sei $f = f_1 f_2$ eine echte Faktorisierung in $\mathbb{Q}[x]$, d.h. keiner der Faktoren ist eine Einheit. Nach (8.7) gibt es $q_1, q_2 \in \mathbb{Q}$ und primitive Polynome $g_1, g_2 \in \mathbb{Z}[x]$ mit $f_i = q_i g_i$. Daher ist $qg = f = f_1 f_2 = q_1 q_2 g_1 g_2$. Nach (8.9) ist $g_1 g_2$ primitiv. Wieder nach (8.7) folgt $g = \pm g_1 g_2$. Da $\deg(g_i) = \deg(f_i) \geq 1$, ist g_i keine Einheit, also ist g reduzibel.
Umgekehrt sei $g = g_1 g_2$ eine echte Faktorisierung in $\mathbb{Z}[x]$, dann ist g_i keine Einheit in $\mathbb{Z}[x]$, also $g_i \neq \pm 1$. Da g primitiv ist, kann g_i also kein konstantes Polynom sein; daher ist $f = (qg_1)g_2$ eine echte Faktorisierung, d.h. f ist reduzibel.

8.11 Satz: *Irreduzibilität durch Reduktion*

Sei $0 \neq f \in \mathbb{Z}[x]$ ein primitives Polynom und wieder $^- : \mathbb{Z}[x] \to \mathcal{F}_p[x]$ für eine Primzahl p. Wenn $\deg \overline{f} = \deg f$ und $\overline{f}$ irreduzibel, dann ist f irreduzibel.

Beweis: Sei $f = f_1 f_2$, also $\overline{f} = \overline{f_1}\ \overline{f_2}$. Weil $\deg f = \deg \overline{f} = \deg \overline{f_1} + \deg \overline{f_2} \leq \deg f_1 + \deg f_2 = \deg f$, ist $\deg f_i = \deg \overline{f_i}$. Da $\overline{f}$ irreduzibel ist, muss einer der Faktoren $\overline{f_i}$ eine Einheit sein, etwa $\overline{f_1}$, d.h. $\deg f_1 = \deg \overline{f_1} = 0$. Also ist f_1 ein konstantes Polynom. Weil f primitiv ist, muß $f_1 = \pm 1$ sein, also eine Einheit in $\mathbb{Z}[x]$. Daher ist f irreduzibel.

8.12 Beispiel: *Irreduzibilität durch Reduktion*

(i) $f(x) = 3x^3 + 4x^2 + 5x - 3 \in \mathbb{Z}[x]$ ist primitiv. für $p = 2$ ist $\overline{f} = x^3 + x + 1$, also $\deg \overline{f} = \deg f$. Da $\overline{f}$ keine Nullstellen in $\mathcal{F}_2$ hat (man setzt einfach 0 und 1 ein), ist $\overline{f}$ irreduzibel, also ist f irreduzibel.

(ii) Sei $g(x) = (2x-1)(x+1)$. Nach dem Gauß'schen Lemma (8.9) ist g primitiv. Wählt man wieder $p = 2$, so ist $\overline{g} = x + 1$, also irreduzibel; dagegen ist aber g offenbar reduzibel. Die Bedingung $\deg f = \deg \overline{f}$ in (8.11) ist also wesentlich.

(iii) Ein nicht primitives Polynom in $\mathbb{Z}[x]$ ist sicher reduzibel, kann aber die sonstigen Voraussetzungen des Satzes erfüllen: sei etwa $h(x) = 3x$ und wieder $p = 2$, dann ist $\deg \overline{h} = \deg h$ und $\overline{h} = x$, also irreduzibel.

8.13 Satz: *Eisenstein Kriterium*

Sei $f(x) = \sum_{i=0}^{n} z_i x^i \in \mathbb{Z}[x]$ ein primitives Polynom. Wenn eine Primzahl p existiert mit $p \mid z_i$ für alle $i < n$ und $p^2 \nmid z_0$, dann ist f irreduzibel.

Beweis: Wegen der Primitivität von f gilt $p \nmid z_n$. Sei $f = f_1 f_2$ eine Faktorisierung. Reduktion modulo p ergibt $\overline{f_1}\ \overline{f_2} = \overline{f} = \overline{z_n} x^n \neq 0$, weil $\overline{z_i} = 0$ für $i < n$. Also ist $\overline{f_1} = ax^m$, $\overline{f_2} = bx^{n-m}$ mit $ab = \overline{z_n}$.
Wenn $m \geq 1$ und $n - m \geq 1$, dann haben f_1 und f_2 durch p teilbare absolute Terme; das Produkt dieser Terme ist aber z_0 und nach Voraussetzung nicht durch p^2 teilbar, ein Widerspruch.
Also o.B.d.A. $\deg \overline{f_1} = 0$. Wegen $\deg \overline{f} = \deg f$ folgt $\deg f_1 = 0$, also ist f_1 konstant. Da f primitiv ist, muß f_1 eine Einheit sein.

8.14 Beispiel:

Sei $f(x) = x^{p-1} + x^{p-2} + \ldots + x + 1$ für eine Primzahl p. Dann ist offenbar $(x-1)f(x) = x^p - 1$. Substitution von $x + 1$ liefert $xf(x+1) = (x+1)^p - 1 = \sum_{k=1}^{p} \binom{p}{k} x^k$, also $f(x+1) = \sum_{k=1}^{p} \binom{p}{k} x^{k-1}$.
Dies ist ein normiertes, insbesondere also ein primitives Polynom. Alle Koeffizienten $\binom{p}{k}$ mit $1 \leq k < p$ sind durch p teilbar. Der absolute Term ist $\binom{p}{1} = p$, also nicht durch p^2 teilbar. Nach (8.13) ist $f(x+1)$ irreduzibel, nach (8.1) also auch $f(x)$.

9 Quotientenkörper

9.1 **Satz:** *Konstruktion des Quotientenkörpers*

Sei R ein kommutativer nullteilerfreier Ring mit 1. Dann gibt es einen Körper $Q = \mathrm{Q}(R)$ und einen Ringmonomorphismus $\mu : R \to Q$ mit folgender Eigenschaft:
Zu jedem Ringmomomorphismus $\sigma : R \to K$ in einen beliebigen Körper K existiert genau ein Körperhomomorphismus $\phi : Q \to K$ derart, dass

$$\begin{tikzcd} R \arrow[rr, "\mu"] \arrow[dr, "\sigma"'] & & Q \arrow[dl, "\phi"] \\ & K & \end{tikzcd}$$

kommutativ ist.
Das Paar (Q, μ) ist dadurch bis auf Isomorphie bestimmt; außerdem ist μ injektiv. Man nennt $\mathrm{Q}(R)$ den Quotientenkörper von R.

Beweis:

(i) Konstruktion von Q
Auf der Menge $\{(a, b) \mid a, b \in R, b \neq 0\}$ definiert man eine Relation $\sim$ durch $(a, b) \sim (x, y) \Leftrightarrow ay = xb$. Diese Relation ist offenbar reflexiv und symmetrisch. Sie ist auch transitiv:
Wenn $(a, b) \sim (x, y)$ und $(x, y) \sim (u, v)$, also $ay = xb$ und $xv = uy$, dann ist $ayv = xbv = uyb$, also $av = ub$, da $y \neq 0$ und R nullteilerfrei; d.h. $(a, b) \sim (u, v)$.
Die Äquivalenzklasse von (a, b) wird mit a/b bezeichnet. Auf der Menge Q dieser „Brüche" wird nun auf die übliche Weise Addition und Multiplikation erklärt, d.h. $a/b + x/y = ay + xb/by$ und $a/b \cdot x/y = ax/by$. Man überzeugt sich, dass diese Verknüpfungen wohldefiniert sind, d.h. unabhängig von der Wahl der Vertreter in den Äquivalenzklassen. Mit diesen Verknüpfungen ist Q ein Körper, wie man leicht kontrolliert. $1/1$ ist das Einzelement von Q, $0/1$ das Nullelement.

(ii) Definition von μ
Man setzt $\mu(a) = a/1$ für $a \in R$. Dann ist μ ein Homomorphismus; wenn $a \in \mathrm{Ker}(\mu)$, also $a/1 = \mu(a) = 0 = 0/1$, dann ist $a = a \cdot 1 = 0 \cdot 1 = 0$, also ist μ injektiv.

(iii) Zu jedem σ existiert ϕ.
Man definiert $\phi : Q \to K$ durch $\phi\left(a/b\right) = \sigma(a)\sigma(b)^{-1}$; dies ist sinnvoll,denn $b \neq 0$ nach Voraussetzung, daher $\sigma(b) \neq 0$ (weil σ injektiv), also hat $\sigma(b)$ ein Inverses in K. Wieder kontrolliert man leicht, dass ϕ wohldefiniert und ein Homomorphismus ist. Für $a \in R$ gilt $\phi\mu(a) = \phi\left(a/1\right) = \sigma(a)\sigma(1)^{-1} = \sigma(a)$, also kommutiert das Diagramm.

(iv) Dieses ϕ ist eindeutig.
Sei auch $\psi : Q \to K$ mit $\psi\mu = \sigma$ und sei $x = a/b \in Q$. Dann ist $\mu(b)x = \mu(a)$, also $\sigma(a) = \psi\mu(a) = \psi(\mu(b)x) = \psi\mu(b)\psi(x) = \sigma(b)\psi(x)$, und daher $\psi(x) = \sigma(a)\sigma(b)^{-1} = \phi(x)$.

(v) (Q, μ) ist bis auf Isomorphie bestimmt.
Sei auch (Q', μ') mit den Eigenschaften von (Q, μ) gegeben. Mit $K = Q$ und $\sigma = \mu$ folgt dann, dass ein Homomorphismus $\phi : Q' \to Q$ existiert, der das Diagramm

$$\begin{tikzcd} R \arrow[rr, "\mu'"] \arrow[dr, "\mu"'] & & Q' \arrow[dl, "\phi"] \\ & Q & \end{tikzcd}$$

kommutativ macht. Da μ injektiv ist, ist auch μ' injektiv. Mit dem gleichen Argument gibt es dann einen Homomorphismus $\psi : Q \to Q'$, welcher

$$\begin{tikzcd} R \arrow[rr, "\mu"] \arrow[dr, "\mu'"'] & & Q \arrow[dl, "\psi"] \\ & Q' & \end{tikzcd}$$

kommutativ macht. Dann ist auch das Diagramm

$$\begin{tikzcd} R \arrow[rr, "\mu"] \arrow[dr, "\mu"'] & & Q \arrow[dl, "\phi\psi"] \\ & Q & \end{tikzcd}$$

kommutativ. Da auch

$$\begin{tikzcd} R \arrow[rr, "\mu"] \arrow[dr, "\mu"'] & & Q \arrow[dl, "\mathrm{id}"] \\ & Q & \end{tikzcd}$$

kommutativ ist, und da wir in (iv) die Eindeutigkeit der Abbildung bewiesen haben, folgt $\phi\psi = \mathrm{id}_Q$.
Insbesondere ist ϕ surjektiv; als Körperhomomorphismus ist ϕ injektiv (siehe 7.4). Daher ist ϕ ein Isomorphismus, also $Q' \cong Q$ und $\mu' = \phi^{-1}\mu$.

9.2 Korollar: *Quotientenkörper eines Körpers*

Sei R wie oben. Genau dann ist R ein Körper, wenn $\mathrm{Q}(R) \cong R$.

Beweis: Wenn $\mathrm{Q}(R) \cong R$, dann ist R isomorph zu einem Körper, also selbst ein Körper.
Wenn R ein Körper ist, dann ist μ surjektiv (also ein Isomorphismus $R \to \mathrm{Q}(R)$), denn für ${}^a/_b \in Q$ ist $\mu(ab^{-1}) = {}^{ab^{-1}}/_1 = {}^a/_b$, weil $(ab^{-1})b = a \cdot 1$.

10 Algebraische Körpererweiterungen

10.1 Definition: *Grad einer Erweiterung*

Sei K ein Körper enthalten in einem Ring R. Dann kann man R als K-Vektorraum betrachten. Man nennt $\dim_K R$ den Grad von R über K und schreibt auch $|R:K| = \dim_K R$.

10.2 Beispiel: *Körpererweiterungen*

(i) $|L:K| = 1 \Leftrightarrow K = L$

(ii) $|\mathbb{C}:\mathbb{R}| = 2$ (Basis $\{1, i\}$)

(iii) K sei ein beliebiger Körper und $L = K(x)$ der Quotientenkörper von $K[x]$. Dann ist $|L:K| = \infty$ und sogar schon $|K[x]:K| = \infty$.

10.3 Bemerkung: *Gradsatz*

Wenn $K \leq L \leq F$, dann $|F:K| = |F:L||L:K|$.
Beweis: Wenn $\{f_i \mid i \in I\}$ eine L-Basis von F ist und $\{l_j \mid j \in J\}$ eine K-Basis von L, dann ist $\{f_i l_j \mid i \in I,\ j \in J\}$ eine K-Basis von F, wie man leicht sieht.

10.4 Satz: *einfache Erweiterungen*

Sei K ein Körper und $p \in K[x]$ ein irreduzibles Polynom. Sei $L = {}^{K[x]}/_{(p)}$. Dann gilt:

(1) L ist ein Körper, und es gibt eine (kanonische) Einbettung von K in L. Man kann also K als Unterkörper von L betrachten.

(2) $\{1+(p), x+(p), x^2+(p), \ldots, x^{n-1}+(p)\}$ ist eine $K-$Basis von L, wenn $n = \deg p$. Insbesondere ist $|L:K| = \deg p$.

(3) p hat eine Nullstelle in L.

Beweis:

(1) Nach (7.5 (i),(vi),(vii)) ist L ein Körper. Die Abbildung $a \mapsto a + (p), a \in K$ ist ein Homomorphismus, also sogar ein Monomorphismus (vergleiche 7.4).

(2) Linear unabhängig: $0 = \sum\limits_{i=0}^{n-1} k_i[x^i + (p)] = \left(\sum\limits_{i=0}^{n-1} k_i x^i\right) + (p) \Rightarrow r = \sum\limits_{i=0}^{n-1} k_i x^i \in (p)$, etwa $r = pq$. Wenn $q \neq 0$, dann $n = \deg p \leq \deg p + \deg q = \deg r \leq n-1$; das ist ein Widerspruch, also $q = 0, r = 0$. Daher müssen alle $k_i = 0$ sein.
Erzeugenden-System: Sei $q \in K[x]$ beliebig. Gesucht sind k_i mit $q + (p)$ $= \sum\limits_{i=0}^{n-1} k_i[x^i + (p)]$. Es existieren Polynome s und r mit $q = sp + r$ und $\deg r < n$ $(= \deg p)$ (Division mit Rest), etwa $r = \sum\limits_{i=0}^{n-1} k_i x^i$. Es ist $q - r = sp \in (p)$, also $q + (p) = r + (p) = \sum\limits_{i=0}^{n-1} k_i[x^i + (p)]$.

(3) Betrachte p als Polynom über L (sinnvoll, da $K \leq L$). Es ist $x + (p) \in L$ und $p[x + (p)] = p(x) + (p) = 0$, weil $p(x) \in (p)$.

10.5 Definition: *algebraisch, transzendent*

Sei $K \leq L$ ein Unterkörper und sei $a \in L$. Man nennt a algebraisch über K, wenn ein Polynom $0 \neq f \in K[x]$ existiert mit $f(a) = 0$. Andernfalls heißt a transzendent über K. Man nennt L eine algebraische Erweiterung von K, wenn alle Elemente von L algebraisch über K sind.

10.6 Beispiel: *algebraische Erweiterungen*

(i) Wenn $a \in K$, dann ist $0 \neq p = x - a \in K[x]$ und $p(a) = 0$; also ist jedes Element aus K algebraisch über K.

(ii) $i \in \mathbb{C}$ ist algebraisch über $\mathbb{R}$, sogar schon über $\mathbb{Q}$, denn i ist eine Nullstelle von $x^2 + 1$.

(iii) K ist Unterkörper von $K(x)$, dem Quotientenkörper von $K[x]$. Jedes Element aus $K(x)$, welches nicht zu K gehört, ist transzendent über K.

Beweis: Sei ${}^{p}/_{q} \in K(x)$, d.h. $p, q \in K[x], q \neq 0$. O.B.d.A seien p und q teilerfremd (nach Kürzen) und nicht beide konstant (sonst ${}^{p}/_{q} \in K$). Angenommen, es gibt ein Polynom $0 \neq f \in K[x]$ mit $f\left({}^{p}/_{q}\right) = 0$ etwa $f(x) = a_0 + a_1 x + \ldots + a_n x^n$ mit $a_n \neq 0$. Dann ist $0 = q^n f\left({}^{p}/_{q}\right) = q^n a_0 + q^{n-1} a_1 p + \ldots + a_n p^n$, also $-a_n p^n = qb$ für ein b. Insbesondere gilt $q \mid p^n$. Aber q und p sind teilerfremd, daher sind auch q und p^n teilerfremd. Daher ist q eine Einheit. Also kann p kein konstantes Polynom sein, d.h. $\deg p \geq 1$. Daher ist $-\infty = \deg(q^n a_0 + q^{n-1} a_1 p + \ldots + a_n p^n) = n \deg p \geq 0$, ein Widerspruch.

10.7 Definition: *Körper- und Ringerzeugnis*

Sei $K \leq L$ ein Unterkörper und $T \subseteq L$ (beliebige Teilmenge).
Man nennt $K(T) = \bigcap\limits_{K,T \subseteq F} F$, wobei F ein Unterkörper von L ist, den von T (über K) erzeugten Unterkörper von L.
Man nennt $K[T] = \bigcap\limits_{K,T \subseteq R} R$, wobei R ein Unterring von L ist, den von T (über K) erzeugten Unterring von L.

10.8 Bemerkung/Definition: *Primkörper, Charakteristik*

(i) Ein Durchschnitt von Unterkörpern ist wieder ein Unterkörper. Ebenso ist ein Durchschnitt von Unterringen ein Unterring.

(ii) Insbesondere ist der Schnitt aller Unterkörper eines Körpers K der kleinste in K enthaltene Körper. Man nennt ihn den Primkörper von K. Er enthält $1 \in K$ und daher auch $Im(\mu)$, wobei $\mu : \mathbb{Z} \to K$ der natürliche Homomorphismus ist, welcher definiert wird durch $\mu(n) = 1 + \cdots + 1$ (n Summanden) für $n \in \mathbb{N}_0$ und $\mu(-n) = -\mu(n)$. Da K als Körper nullteilerfrei ist, ist $\text{Ker}\,(\mu) = 0$ oder $\text{Ker}\,(\mu) = (p)$ für eine Primzahl p. Entsprechend sagt man, dass die Charakteristik von R gleich 0 oder p ist (Schreibweise: $char(R)$). Im ersten Fall ist der Primkörper isomorph zum Quotientenkörper von $\mathbb{Z}$, also zu $\mathbb{Q}$, im zweiten ist $Im(\mu)$ nach 7.5(vii) selbst schon ein Körper, also der Primkörper.

(iii) $K(T)$ ist der kleinste Unterkörper von L, welcher K und T enthält. $K[T]$ ist der kleinste Unterring von L, welcher K und T enthält. $K[T] \subseteq K(T)$ und sogar $K(T) \cong \mathrm{Q}\,(K[T])$.

Beweis: Die drei ersten Aussagen sind klar. Bleibt zu zeigen: $K(T) \cong \mathrm{Q}(K[T])$. Dazu betrachten wir

$$\begin{tikzcd} K(T) & \\ K[T] \arrow[u, "\sigma"] \arrow[r, "\mu"'] & \mathrm{Q}(K[T]) \arrow[ul, "\exists\phi"'] \end{tikzcd}$$

(Vergleiche (9.1))

ϕ ist ein Monomorphismus, weil $\phi \neq 0$ und $\mathrm{Q}(K[T])$ ein Körper ist. ϕ ist ein Epimorphismus, weil $\mathrm{Im}(\phi)$ ein Unterkörper von $K(T)$, also von L ist, welcher K und T enthält, also $\mathrm{Im}(\phi) \geq K(T)$.

10.9 Satz: *Körpererweiterungen*

Sei $K \leq L$ ein Unterkörper und $a \in L$. Sei $\phi : K[x] \to L$ die Abbildung $q(x) \mapsto q(a)$. Die folgenden Aussagen sind äquivalent:

(1) a ist algebraisch über K.

(2) ϕ ist nicht injektiv.

(3) $\mathrm{Ker}(\phi) = (p)$ für ein eindeutig bestimmtes, normiertes, irreduzibles Polynom $p \in K[x]$. (Man nennt p das Minimalpolynom von a.)

(4) Es gibt ein Polynom $p \neq 0$ in $K[x]$ und einen Isomorphismus $\sigma : K[x]/(p) \to K[a]$ so, dass das Diagramm

$$\begin{tikzcd} K[x]/(p) \arrow[rr, "\sigma"] & & K[a] \\ & K \arrow[ul, "\mu"] \arrow[ur] & \end{tikzcd}$$

kommutativ ist und $[x+(p)]\sigma = a$, wobei μ die kanonische Einbettung $k \mapsto k+(p)$ von K in $K[x]/(p)$ ist.

(5) $K[x]/(p) \cong K[a]$ für ein $0 \neq p \in K[x]$

(6) $K[a]$ ist ein Körper.

(7) $K(a) = K[a]$

(8) $|K(a) : K| < \infty$

(9) $|K[a] : K| < \infty$

Beweis:

(1)⇒(2) Nach Voraussetzung existiert ein Polynom $0 \neq f \in K[x]$ mit $f(a) = 0$, d.h. $f \in \mathrm{Ker}(\phi)$.

(2)⇒(3) Da $K[x]$ ein Hauptidealring ist und ϕ ein Homomorphismus, gilt $\mathrm{Ker}(\phi) = (p)$ für ein eindeutig bestimmtes, normiertes Polynom $p \neq 0$. Wäre p nicht irreduzibel, dann hätte $K[a] = \mathrm{Im}(\phi) \cong K[x]/\mathrm{Ker}(\phi) = K[x]/(p)$ Nullteiler; das ist ein Widerspruch, da $K[a] \subseteq L$.

(3)⇒(4) Man kann für σ die kanonische Abbildung $q(x) + (p) \mapsto q(a)$ nehmen.

(4)⇒(5) Trivial

(5)⇒(6) Da $K[a]$ nullteilerfrei ist und $p \neq 0$, muß p irreduzibel sein, also ist (p) maximal, daher ist $K[x]/(p)$ ein Körper (vergleiche 7.5). Also ist auch $K[a]$ ein Körper.

(6)⇒(7) Nach (10.8) ist $K(a)$ der Quotientenkörper von $K[a]$. Da $K[a]$ ein Körper ist, gilt Gleichheit nach (9.2).

(7)⇒(8) Klar, falls $a = 0$, denn dann $K(a) = K$. Sei $a \neq 0$. Da $a^{-1} \in K(a) = K[a]$, existiert ein Polynom $f \in K[x]$ mit $a^{-1} = f(a)$; daher $0 = af(a) - 1$. Also existiert ein Polynom $h \neq 0$ in $K[x]$ mit $h(a) = 0$, d.h. a ist algebraisch. Wie wir schon gesehen haben, folgt $K(a) = K[a] \cong K[x]/(p)$ für ein $0 \neq p \in K[x]$.

Da $|K[x]/(p) : K| = \deg p < \infty$ (siehe 10.4), folgt daraus die Behauptung.

(8)⇒(9) Trivial, da $K[a] \leq K(a)$.

(9)⇒(1) Es können nicht $1, a, a^2, \ldots$ alle linear unabhängig über K sein. Also gibt es Elemente $k_i \in K, i = 0, \ldots, n$, so dass nicht alle $k_i = 0$ sind und $\sum_{i=0}^{n} k_i a^i = 0$. Sei $f(x) := \sum_{i=0}^{n} k_i x^i \in K[x]$. Es ist dann $f \neq 0 \in K[x]$ und $f(a) = 0$, woraus die Behauptung folgt.

10.10 Korollar: *Erweiterungsgrad*

Sei $a \in L$ algebraisch über K und p das Minimalpolynom von a. Dann ist $|K(a) : K| = \deg p$.

<u>*Beweis:*</u> Folgt aus (10.9) und (10.4)

10.11 Korollar: *Fortsetzung von Homomorphismen auf einfache Erweiterungen*

Sei $\tau : K \to F$ ein Körperhomomorphismus, $K \leq L$ und $F \leq E$. Sei $a \in L$ algebraisch über K mit Minimalpolynom $p \in K[x]$ und $b \in E$ algebraisch über F mit Minimalpolynom $q \in F[x]$. Wenn $p\tau = q$ ist, dann existiert ein Körperhomomorphismus $\sigma : K[a] \to F[b]$ mit $\sigma_{|K} = \tau$ und $a\sigma = b$.

<u>*Beweis:*</u> Nach (10.9) existieren Isomorphismen α und β, welche die beiden Diagramme

$$\begin{tikzcd} K[x]/(p) & & K[a] \arrow[ll, "\alpha"'] \\ & K \arrow[ul, "\mu"] \arrow[ur] & \end{tikzcd} \quad \text{und} \quad \begin{tikzcd} F[x]/(q) \arrow[rr, "\beta"] & & F[b] \\ & F \arrow[ul, "\mu'"] \arrow[ur] & \end{tikzcd}$$

kommmutativ machen und so, dass $a\alpha = x + (p)$ und $[x + (q)]\beta = b$. Außerdem ist durch $\left[\sum k_i x^i + (p)\right] \overline{\tau} = \sum (k_i\tau)x^i + (q)$ ein Homomorphismus $\overline{\tau} : K[x]/(p) \to F[x]/(q)$ wohldefiniert mit

$$\begin{tikzcd} K[x]/(p) \arrow[r, "\overline{\tau}"] & F[x]/(q) \\ K \arrow[u, "\mu"] \arrow[r, "\tau"'] & F \arrow[u, "\mu'"'] \end{tikzcd}$$

kommmutativ und $a\alpha\overline{\tau}\beta = b$. Also ist $\sigma = \alpha\overline{\tau}\beta$ der gesuchte Homomorphismus.

10.12 **Bemerkung:** *Spezialfälle*

Der wichtigste Spezialfall von (10.11) ist $K = F$ und $\tau = \mathrm{id}$. In diesem Fall sind also $K[a]$ und $K[b]$ isomorph, wenn $p = q$. Das heißt **nicht**, dass $K[a] = K[b]$ ist; auch wenn $K[a] = K[b]$, ist $\sigma \neq \mathrm{id}$ (außer $a = b$).

10.13 **Beispiel:**

$x^2 - 2$ und $x^3 - 2$ sind beide irreduzibel über $\mathbb{Q}$ (Eisenstein und (8.10)). Das erste Polynom hat zwei Nullstellen, beide in $\mathbb{R}$, nämlich $\pm\sqrt{2}$. Offenbar ist $L = \mathbb{Q}[\sqrt{2}] = \mathbb{Q}[-\sqrt{2}]$. Die Aussage von (10.11) ist dann, dass ein Automorphismus σ von L existiert mit $\sigma_{|\mathbb{Q}} = \mathrm{id}$ und $(\sqrt{2})\sigma = -\sqrt{2}$.
Für das zweite Polynom ist die Situation anders: eine Nullstelle ist $\sqrt[3]{2} \in \mathbb{R}$. Es gibt aber in $\mathbb{C}$ noch andere Nullstellen: Sei $\omega = -\frac{1}{2}(1 + i\sqrt{3})$. Dann ist

$$\begin{aligned} \omega^3 &= -\frac{1}{8}\left(1 + 3i\sqrt{3} + 3(i\sqrt{3})^2 + (i\sqrt{3})^3\right) \\ &= -\frac{1}{8}\left(1 + 3i\sqrt{3} - 9 - 3i\sqrt{3}\right) = 1. \end{aligned}$$

Daher ist $[\omega\sqrt[3]{2}]^3 - 2 = 0$, also auch $\alpha = \omega\sqrt[3]{2}$ eine Nullstelle von $x^3 - 2$. Aber $\alpha \notin \mathbb{R}$, also ist $\mathbb{Q}[\alpha] \neq \mathbb{Q}[\sqrt[3]{2}]$. Die Aussage von (10.11) ist hier, dass diese beiden Körper isomorph sind, genauer dass es einen sehr speziellen Isomorphismus σ gibt, nämlich $\sigma_{|\mathbb{Q}} = \mathrm{id}$, $\sigma(\sqrt[3]{2}) = \alpha$.

10.14 **Korollar:** *„algebraisch“ ist transitiv*

Sei $F \leq K \leq L$ mit K algebraisch über F und L algebraisch über K. Dann ist L algebraisch über F.

Beweis: Nach (10.9) g.z.z. $|F(a) : F| < \infty \quad \forall a \in L$. Da a algebraisch über K ist, existiert ein Polynom $0 \neq f(x) = \sum_{i=0}^{n} k_i x^i \in K[x]$ mit $f(a) = 0$. Sei $E = F(k_1, \ldots, k_n)$. Dann ist $f \in E[x]$, also ist a algebraisch über E, d.h. $|E(a) : E| < \infty$. Da K algebraisch über F, sind $k_1, \ldots, k_n$ algebraisch über F. Daher ist $|E : F| < \infty$. Beweis dazu per Induktion über n:

$n = 0$: trivial

$n - 1 \to n$: Dazu sei $E_0 := F(k_1, \ldots, k_{n-1})$. Dann ist also $|E_0 : F| < \infty$; außerdem ist $E = E_0(k_n)$, und k_n ist algebraisch über E_0 (sogar über F), also $|E : E_0| < \infty$. Daher $|E : F| = |E : E_0||E_0 : F| < \infty$.

Also ist $|E(a) : F| = |E(a) : E||E : F| < \infty$, und erst recht $|F(a) : F| < \infty$.

10.15 **Korollar:** *endliche Erweiterungen sind algebraisch*

Sei $|L : K| = n < \infty$. Dann ist L eine algebraische Erweiterung von K. Wenn $a \in L$ das Minimalpolynom p hat, dann gilt $\deg p \mid n$, insbesondere $\deg p \leq n$.

Beweis: $K \leq K[a] \leq L$, also $|K[a] : K| \mid |L : K| = n < \infty$ nach dem Gradsatz. Daher ist a algebraisch und außerdem $|K[a] : K| = \deg p$ (siehe 10.10.

10.16 **Korollar:** *algebraisches Erzeugnis*

Sei $K \leq L$ ein Körpererweiterung und sei $L = K[A]$, wobei A eine Menge von über K algebraischen Elementen ist. Dann ist L algebraisch über K.

Beweis: Für jedes $b \in L$ gibt es endlich viele Elemente $a_i \in A,\ i = 1, \ldots, s$ mit $b \in L_0 = K[a_1, \ldots, a_s]$. Wie im Beweis von 10.14 sieht man, dass $|L_0 : K|$ endlich ist. Nach 10.15 ist b algebraisch.

10.17 **Korollar:** *relativer algebraischer Abschluss*

Sei $K \leq L$ ein Körpererweiterung und sei $E = \{a \in L \mid a \text{ algebraisch über } K\}$. Dann gilt:

(1) E ist ein Körper mit $K \leq E \leq L$. Außerdem ist E algebraisch über K.

(2) Wenn $a \in L$ algebraisch über E ist, dann ist $a \in E$.

Man nennt E den algebraischen Abschluss von K in L.

Beweis:

(1) Sei $a, b \in E$. Es ist zu zeigen, dass $a + b, a - b, ab$ und ab^{-1} (wenn definiert) alle wieder zu E gehören. Alle diese Elemente liegen in $K(a, b)$. Da b algebraisch über K ist, ist erst recht b algebraisch über $K(a)$. Außerdem ist a algebraisch über K. Also ist $|K(a, b) : K| = |K(a)(b) : K(a)||K(a) : K| < \infty$. Nach (10.15) folgt die Behauptung. Offenbar ist $E \subseteq L$. Jedes Element von K ist algebraisch über K, also $K \subseteq E$.

(2) Sei a algebraisch über E. Weil E algebraisch über K ist, folgt aus 10.14, dass a auch algebraisch über K ist, also $a \in E$ (nach Definition von E).

10.18 **Definition:** *algebraisch abgeschlossen*

Ein Körper K heißt algebraisch abgeschlossen, wenn jedes irreduzible Polynom aus $K[x]$ linear ist.

10.19 **Lemma:** *Eigenschaften des algebraischen Abschlusses*

Sei K ein Körper. äquivalent sind:

(1) K ist algebraisch abgeschlossen.

(2) Jedes nicht konstante Polynom aus $K[x]$ läßt sich als Produkt von linearen Polynomen schreiben.

(3) Jedes nicht konstante Polynom aus $K[x]$ hat eine Nullstelle in K.

(4) Wenn L eine algebraische Erweiterung von K ist, dann ist $L = K$.

Beweis:

(1)$\Rightarrow$(2) Jedes Polynom aus $K[x]$ läßt sich als Produkt irreduzibler Polynome schreiben nach (7.5). Diese sind alle linear nach Voraussetzung.

(2)$\Rightarrow$(3) Sei f nicht konstant, p ein Linearfaktor von f, etwa $p = x - a$. Dann ist a eine Nullstelle von p, also auch von f.

(3)⇒(4) Sei $L \geq K$ eine algebraische Erweiterung und $a \in L$. Sei p das Minimalpolynom von a in $K[x]$. Dann ist p nicht konstant, hat also eine Nullstelle in K und daher einen Linearfaktor in $K[x]$. Aber als Minimalpolynom ist p irreduzibel nach (10.9), also ist p linear; daher ist $a \in K$.

(4)⇒(1) Sei $p \in K[x]$ irreduzibel. Dann ist $L = {}^{K[x]}\!/_{(p)}$ eine Körpererweiterung mit $|L : K| = \deg p$ (10.4). Nach (10.15) ist L algebraisch über K. Nach Voraussetzung ist daher $L = K$, d.h. $\deg p = |L : K| = 1$, also ist p linear.

10.20 **Lemma:** *Nullstellen zu endlich vielen Polynomen*

Sei K ein Körper und $f_1, \ldots, f_n \in K[x]$, alle nicht konstant. Dann existiert eine Körpererweiterung $K \leq L$ derart, dass jedes f_i eine Nullstelle in L hat.

Beweis: Induktion über n

$n = 0$ $K = L$ tut es.

$n-1 \to n$ Sei (per Induktion) eine Körpererweiterung $L_0 \geq K$ so gewählt, dass $f_1, \ldots, f_{n-1}$ Nullstellen in L_0 besitzen. Betrachte f_n als Polynom in $L_0[x]$ (geht, da $K \leq L_0$). Sei $p \in L_0[x]$ ein irreduzibler Faktor von f_n und $L = {}^{L_0[x]}\!/_{(p)}$. Dann ist L eine Körpererweiterung von L_0, also von K, und p (und damit erst recht f_n) hat eine Nullstelle in L nach (10.4).

10.21 **Satz:** *algebraisch abgeschlossene Erweiterung*

Sei K ein Körper. Dann existiert eine Körpererweiterung $L \geq K$ mit algebraisch abgeschlossenem L.

Beweis: Sei $\mathcal{P}$ die Menge der irreduziblen Polynome in $K[x]$. Sei $Y = \{y_p \mid p \in \mathcal{P}\}$, d.h. Y ist eine Menge von ebenso vielen Unbestimmten wie es Polynome in $\mathcal{P}$ gibt. Wir können dann den Polynomring $K[Y]$ bilden. Das ist ein Polynomring in vielen Unbestimmten; in jedem einzelnen Polynom treten aber nur endlich viele Unbestimmte auf. In $K[Y]$ betrachten wir jetzt die Polynome $p(y_p)$ für alle $p \in \mathcal{P}$. Sei $I = \sum\limits_{p \in \mathcal{P}} K[Y]p(y_p)$. Dann ist I ein Ideal von $K[Y]$. Es ist sogar $I \neq K[Y]$, denn sonst gibt es eine endlich Teilmenge $T \subseteq \mathcal{P}$ mit $1 = \sum\limits_{p \in T} g_p p(y_p)$. Nun sei L eine Körpererweiterung von K, in welcher alle $p \in T$ eine Nullstelle haben (existiert nach (10.20), sei etwa $a_p \in L$ eine Nullstelle von p. Sei $\phi : K[Y] \to L$ der Homomorphismus, welcher durch

$$\begin{aligned} k\phi &= k & &\forall k \in K \\ y_p\phi &= a_p & &p \in T \\ y_q\phi &= 0 & &q \in \mathcal{P} \setminus T \end{aligned}$$

definiert ist. Dann folgt $1 = 1\phi = \sum\limits_{p \in T} (g_p\phi)p(a_p) = 0$, ein Widerspruch.

Also ist I ein echtes Ideal von $K[Y]$. Nach dem Zorn'schen Lemma existiert ein maximales Ideal $J \geq I$ in $K[Y]$. Daher ist $K_1 = {}^{K[Y]}\!/_{J}$ eine Körpererweiterung von K. Wenn $p \in \mathcal{P}$, dann ist $y_p + J \in K_1$ und $p(y_p + J) = p(y_p) + J = J = 0$, denn sogar $p(y_p) \in I \subseteq J$. Also hat p eine Nullstelle in K_1.

Was wir bisher geschafft haben: Ausgehend von einem beliebigen Körper K, haben wir eine Körpererweiterung K_1 konstruiert, in welcher jedes irreduzible Polynom aus $K[x]$ eine Nullstelle hat. Jetzt kann man dies wieder tun mit K_1 statt mit K und so weiter.

Man erhält so eine Folge von Körpererweiterungen:$K = K_0 \leq K_1 \leq K_2 \leq \ldots$, derart, dass jedes irreduzible Polynom von K_i eine Nullstelle in K_{i+1} hat. Sei nun $L = \bigcup\limits_{i \in \mathbb{N}} K_i$. Dann ist L ein Körper. Wenn $p \in L[x]$ irreduzibel ist, dann ist $p \in K_s[x]$ für ein $s \in \mathbb{N}$, da ja nur endlich viele Koeffizienten in p auftreten. Natürlich ist p in $K_s[x]$ irreduzibel; also hat p eine Nullstelle in K_{s+1}. Erst recht hat p eine Nullstelle in E und daher einen Linearfaktor in $L[x]$. Da p irreduzibel ist, muss es also linear sein. Daher ist L algebraisch abgeschlossen.

10.22 **Definition:** *algebraischer Abschluss*

Sei $K \leq E$ eine Körpererweiterung. Man nennt E einen <u>algebraischen Abschluss</u> von K, wenn

(1) E algebraisch abgeschlossen ist und

(2) E algebraisch über K ist.

10.23 **Satz:** *Existenz des algebraischen Abschlusses*

Zu jedem Körper K existiert ein algebraischer Abschluss.

<u>*Beweis:*</u> Nach (10.21) können wir K in einen algebraisch abgeschlossenen Körper L einbetten. Sei E der algebraische Abschluss von K in L. Nach (10.17(1)) ist E eine algebraische Erweiterung von K. Bleibt zu zeigen: E ist algebraisch abgeschlossen. Sei $0 \neq p \in E[x]$ nicht konstant. Dann ist p ein nicht-konstantes Polynom in $L[x]$. Nach (10.19) hat p eine Nullstelle a in L; diese ist algebraisch über E. Nach (10.17(2)) folgt $a \in E$. Also hat jedes nicht-konstante Polynom aus $E[x]$ eine Nullstelle in E. Nach (10.19) ist E algebraisch abgeschlossen.

11 Zerfällungskörper und normale Erweiterungen

11.1 **Definition:** *Zerfällungskörper*

Sei K ein Körper und $\mathcal{P}$ eine Menge von Polynomen aus $K[x]$. Eine Körpererweiterung E von K heißt Zerfällungskörper von $\mathcal{P}$, falls

(1) jedes nicht-konstante Polynom aus $\mathcal{P}$ über $E[x]$ in Linearfaktoren zerfällt

und

(2) $E = K(\mathcal{N})$, wobei $\mathcal{N}$ die Menge aller Nullstellen von Polynomen $\neq 0$ aus $\mathcal{P}$ ist.

11.2 **Satz:** *Fortsetzungen von Homomorphismen auf algebraische Erweiterungen*

Sei E eine algebraische Erweiterung von K, und sei $\alpha : K \to L$ mit algebraisch abgeschlossenem Körper L. Dann existiert ein Homomorphismus $\tau : E \to L$ mit $\tau_{|K} = \alpha$.

Beweis: Betrachte die Menge $\mathcal{M} = \{(F, \sigma) \mid K \leq F \leq E,\ \sigma : F \to L$ Körperhomomorphismus mit $\sigma_{|K} = \alpha\}$. Es ist $\mathcal{M} \neq \emptyset$, denn $(K, \alpha) \in \mathcal{M}$. Definiere eine Ordnung auf $\mathcal{M}$ durch $(F, \sigma) \leq (F', \sigma')$, falls $F \leq F'$ und $\sigma'_{|F} = \sigma$. Die Ketten in $\mathcal{M}$ haben obere Schranken, also existiert ein maximales Element in $\mathcal{M}$, etwa (F, σ). Es genügt zu zeigen, dass $F = E$ ist.
Sei $a \in E$, dann ist a algebraisch über F (sogar über K). Sei p das Minimalpolynom von a in $F[x]$. Sei $q = \sigma(p) \in \sigma(F)[x]$. Es ist $\sigma(F) \leq L$, und dieser Körper ist algebraisch abgeschlossen; also hat q eine Nullstelle b in L. Nach (10.10) existiert ein Körperhomomorphismus $\tau : F[a] \to \sigma(F)[b] \subseteq L$ mit $\tau_{|F} = \sigma$ und $a\tau = b$.
Also ist $(F[a], \tau) \geq (F, \sigma)$. Wegen der Maximalität ist $F[a] = F$, d.h. $a \in F$ und daher $F = E$.

11.3 **Satz:** *Existenz des Zerfällungskörpers*

Sei K ein Körper und $\mathcal{P} \subseteq K[x]$.

(1) Es gibt einen Zerfällungskörper E von $\mathcal{P}$.

(2) Sei $K \leq L$, L algebraisch abgeschlossen, und sei E ein Zerfällungskörper von $\mathcal{P}$. Dann existiert ein Körperhomomorphismus $\tau : E \to L$ mit $\tau_{|K} = \mathrm{id}$.

(3) Wenn $\tau : E \to L$ wie in (2) ist, dann ist $\mathrm{Im}\,(\tau) = K(\mathcal{N})$, wobei $\mathcal{N}$ die Menge aller Nullstellen von Polynomen $\neq 0$ aus $\mathcal{P}$ in L ist.

(4) Wenn auch E' ein Zerfällungskörper von $\mathcal{P}$ ist, dann existiert ein Isomorphismus $\sigma : E \to E'$ mit $\sigma_{|K} = \mathrm{id}$.

Beweis:

(1) Sei $K \leq L$ und L algebraisch abgeschlossen (existiert nach (10.21) und sei $\mathcal{N}$ die Menge der Nullstellen von $\mathcal{P}$ in L.
Setze $E = K(\mathcal{N})$. Dann ist E ein Zerfällungskörper von $\mathcal{P}$: Bedingung (2) ist offenbar erfüllt. Über L zerfällt jedes Polynom f aus $\mathcal{P}$ in Linearfaktoren: $f(x) = c\prod(x - \alpha_i)$; die α_i sind die Nullstellen, also alle in $\mathcal{N}$, daher in E und $c \in K$. Daher zerfällt f schon über E in Linearfaktoren.

(2) Sei $\mathcal{N}_1$ die Menge der Nullstellen von $\mathcal{P}$ in E. Da $E = K(\mathcal{N}_1)$ und alle Elemente in $\mathcal{N}_1$ algebraisch sind, ist E nach (10.16) eine algebraische Erweiterung von K. Wegen (11.2) folgt die Behauptung.

(3) Sei f ein Polynom aus $\mathcal{P}$. Dann ist $f(x) = c\prod_{i=1}^{n}(x - a_i)$ mit geeigneten $a_i \in E$, $c \in K$. Es ist $f\tau = f$, weil die Koeffizienten von f in K liegen, und $\tau_{|K} = \text{id}$. Daher $f(x) = (f\tau)(x) = c\tau\prod(x - a_i\tau) = c\prod(x - a_i\tau)$. Daher sind die $a_i\tau$ alle in $\mathcal{N}$. Daher ist $\mathcal{N}_1\tau \subseteq \mathcal{N}$ und $E\tau \leq K(\mathcal{N})$.
Außerdem zerfällt über $E\tau$ jedes Polynom aus $\mathcal{P}$ in Linearfaktoren, d.h. $\mathcal{N} \subseteq E\tau$ und daher $K(\mathcal{N}) \leq E\tau$. Also ist $K(\mathcal{N}) = E\tau$.

(4) Nach (2) und (3) für E und E' existieren Homomorphismen $\tau : E \to L$ und $\tau' : E' \to L$ mit $\tau_{|K} = \tau'_{|K} = \text{id}$ und $\text{Im}\,(\tau) = K(\mathcal{N}) = \text{Im}\,(\tau')$. Daher ist $\sigma = \tau(\tau')^{-1}$ wie gewünscht.

11.4 **Korollar:** *Eindeutigkeit des Zerfällungskörpers*

(1) Ein Zerfällungskörper von $\mathcal{P} \subseteq K[x]$ ist bis auf Isomorphie durch $\mathcal{P}$ bestimmt. Wir reden daher von dem Zerfällungskörper von $\mathcal{P}$.

(2) Der algebraische Abschluss von K ist bis auf Isomorphie durch K bestimmt. Wir reden daher von dem algebraischen Abschluss von K (oft bezeichnet mit $\overline{K}$).

Beweis:

(1) ist eine Wiederholung von (11.3(4))

(2) ist eine Spezialfall von (1), nämlich $\mathcal{P} = K[x] =$ alle Polynome.

11.5 **Satz:** *normale Erweiterungen*

Sei $K \leq E \leq \overline{K}$. Die folgenden Aussagen sind äquivalent:

(1) E ist der Zerfällungskörper einer geeigneten Menge von Polynomen.

(2) Wenn ein irreduzibles Polynom $p \in K[x]$ eine Nullstelle in E hat, dann liegen alle Nullstellen von p in E.

(3) Wenn $\sigma : E \to \overline{K}$ ein Homomorphismus ist mit $\sigma_{|K} = \text{id}$, dann ist $E\sigma = E$ (also ist σ ein Automorphismus von E).

Beweis:

(3)⇒(2) Sei $a \in E$ eine Nullstelle des irreduziblen Polynoms $p \in K[x]$ und sei auch b eine Nullstelle von p. Zu zeigen: $b \in E$. Nach (10.10) existiert ein Homomorphismus $\alpha : K[a] \to K[b]$ mit $\alpha_{|K} = \text{id}$ und $a\alpha = b$. Nach (11.2) existiert ein Fortsetzung $\sigma : E \to \overline{K}$ von α, da E eine algebraische Erweiterung von $K[a]$ und $\overline{K}$ algebraisch abgeschlossen ist. Dann ist $\sigma_{|K} = \text{id}$ (weil $\alpha_{|K} = \text{id}$). Nach Voraussetzung (3) ist $E\sigma = E$. Insbesondere ist $b = a\sigma \in E\sigma = E$.

(2)⇒(1) Sei $\mathcal{P} =$ alle Minimalpolynome in $K[x]$ von Elementen aus E. Dann zerfällt jedes Polynom aus $\mathcal{P}$ in $E[x]$ in Linearfaktoren, weil eine Nullstelle, also alle Nullstellen in E liegen. Außerdem wird $E = K(\mathcal{N})$ von den Nullstellen $\mathcal{N}$ von $\mathcal{P}$ erzeugt. Also ist E der Zerfällungskörper von $\mathcal{P}$.

(1)⇒(3) Nach (11.3(3)) ist $E\sigma = \text{Im}\,(\sigma) = K(\mathcal{N}) = E$.

11.6 **Definition:** *normale Erweiterung*

Eine Erweiterung E von K,welche die Bedingungen von (11.5) erfüllt, heißt <u>normal</u> über K.

12 Separable Erweiterungen

12.1 Definition: *separabel*

Ein Polynom $p \in K[x]$ heißt separabel, wenn es keine mehrfachen Nullstellen im algebraischen Abschluss $\overline{K}$ hat.
Ein Element $a \in E \geq K$ heißt separabel (über K), wenn es algebraisch ist und das Minimalpolynom von a in $K[x]$ separabel ist.
Eine algebraische Erweiterung E von K heißt separabel (über K), wenn alle Elemente aus E separabel über K sind.

12.2 Lemma: *separable Polynome*

Sei $p \in K[x]$ irreduzibel. Genau dann ist p separabel, wenn $p' \neq 0$.

Beweis: Nach (7.6) ist p separabel genau dann, wenn $\operatorname{ggT}(p, p') = 1$. Insbesondere ist dann $p' \neq 0$, denn sonst wäre $\operatorname{ggT}(p, p') = p$. Sei umgekehrt $p' \neq 0$ und $f \mid p, p'$. Da $\deg f \leq \deg p' < \deg p$ und p irreduzibel ist, folgt $\deg f = 0$, also ist f eine Einheit, d.h. $\operatorname{ggT}(p, p') = 1$.

12.3 Korollar: *Körper mit der Charakteristik 0*

Sei K ein Körper mit der Charakteristik 0. Dann ist jede algebraische Erweiterung E von K separabel (über K).

Beweis: Sei $a \in E$ und p das Minimalpolynom von a, etwa $p(x) = x^n + k_{n-1}x^{n-1} + \ldots + k_0 \quad (n \geq 1)$. Dann ist $p'(x) = nx^{n-1} + \ldots \neq 0$.

12.4 Bemerkung: *Körper mit der Charakteristik p*

(i) Sei K ein Körper der Charakteristik p. Die Abbildung $\sigma : K \to K$ definiert durch $a\sigma = a^p$ ist ein Körperhomomorphismus.

Beweis: $(ab)\sigma = (ab)^p = a^p b^p = (a\sigma)(b\sigma)$

$(a+b)\sigma = (a+b)^p = \sum\limits_{\mu=0}^{p} \begin{pmatrix} p \\ \mu \end{pmatrix} a^\mu b^{p-\mu}$.

Für $1 \leq \mu \leq p-1$ ist $p \mid \begin{pmatrix} p \\ \mu \end{pmatrix} = \frac{p(p-1)\cdots(p-\mu+1)}{1\cdot 2\cdots \mu}$; da $p \cdot 1 = 0$, sind alle Terme der Summe $= 0$, bis auf $\begin{pmatrix} p \\ 0 \end{pmatrix} a^0 b^{p-0} = b^p$ und $\begin{pmatrix} p \\ p \end{pmatrix} a^p b^{p-p} = a^p$. Also ist $(a+b)^p = a^p + b^p = a\sigma + b\sigma$.

(ii) σ ist injektiv (als Körperhomomorphismus), muß aber nicht surjektiv sein. Wenn K endlich ist, dann ist σ natürlich auch surjektiv.

12.5 Korollar: *endliche Körper*

Sei K ein endlicher Körper. Dann ist jede algebraische Erweiterung von K separabel über K.

Beweis: Sei $q \in K[x]$ irreduzibel; g.z.z. $q' \neq 0$. Sei $q(x) = \sum\limits_{i=0}^{n} k_i x^i$. Wenn $0 = q'(x) = \sum\limits_{i=1}^{n} i k_i x^{i-1}$, dann $ik_i = 0$ für $i = 1, \ldots, n$, aber $i \neq 0$ in K für $p \nmid i$. Also $k_i = 0$, falls

$p \nmid i$ und daher $q(x) = \sum_{i=0}^{n/p} k_{ip} x^{ip}$. Da $k_{ip} = l_i^p$ für geeignete $l_i \in K$ nach (12.4), folgt $q(x) = \sum_{i=0}^{n/p} (l_i x^i)^p = \left(\sum_{i=0}^{n/p} l_i x^i \right)^p$, also reduzibel, ein Widerspruch.

12.6 Lemma: *Schranke für die möglichen Fortsetzungen eines Homomorphismus*

Sei $|E : K| = n < \infty$ und $\sigma : K \to L$ ein Homomorphismus. Dann existieren höchstens n verschiedene Homomorphismen $\tau_i : E \to L$ mit $\tau_{i|K} = \sigma$.

Beweis: Sei $E = K[a_1, \ldots, a_t]$. Der Beweis erfolgt per Induktion über t.

$t = 0$ Dann ist $E = K$, $n = 1$ und $\tau = \sigma$ der einzige Homomorphismus.

$t - 1 \to t$ Setze $F = K[a_1, \ldots, a_{t-1}]$. Dann $K \leq F \leq E$ und $E = F[a_t]$. Sei p das Minimalpolynom von a_t in $F[x]$ und $d = \deg p$. Dann ist $|E : F| = d$ nach (10.10) und daher $|F : K| = n/d = m$. Per Induktion gibt es höchstens m Homomorphismen $\sigma_i : F \to L$ mit $\sigma_{i|K} = \sigma$, etwa $i = 1, \ldots, l \leq m$. Sei nun $\tau : E \to L$ mit $\tau_{|K} = \sigma$, dann ist $\tau_{|F}$ eines der σ_i.
Auf wie viele verschiedene Weisen läßt sich eine festes σ_i zu einem τ fortsetzen? Wenn τ eine Fortsetzung von σ_i ist, dann ist $a_t \tau$ eine Nullstelle (in L) von $p\tau$ ($= p\sigma_i$, weil die Koeffizienten von p in F liegen). Aber $p\sigma_i$ ist ein Polynom vom Grad d in $L[x]$, hat also höchstens d Nullstellen; daher gibt es nur höchstens d mögliche Werte für $a_t\tau$. Wenn $\tau_{|F} = \tau'_{|F} = \sigma_i$ und $a_t\tau = a_t\tau'$, dann ist $\tau = \tau'$, also gibt es höchstens d Fortsetzungen von σ_i zu E. Da dies für jedes $i = 1, \ldots, l$ gilt, ist die Anzahl der verschiedenen τ's höchstens gleich $ld \leq md = n$.

12.7 Satz: *separable Erweiterungen*

Sei $|E : K| = n < \infty$. Äquivalent sind:

(1) E ist separabel über K.

(2) Es gibt endlich viele Elemente $a_1, \ldots, a_t \in E$, alle separabel über K, mit $E = K[a_1, \ldots, a_t]$.

(3) Es gibt genau n verschiedene Homomorphismen $\tau_1, \ldots, \tau_n : E \to \overline{K}$ mit $\tau_{i|K} = \text{id}$.

Beweis:

(1)⇒(2) Da $|E : K| < \infty$, gibt es endlich viele Elemente $a_i \in E$, $i = 1, \ldots, t$, so dass $E = K[a_1, \ldots, a_t]$. Diese sind separabel, da alle Elemente aus E separabel sind.

(2)⇒(3) Induktion über t:

$t = 0$ Dann ist $E = K$, $n = 1$ und $\tau_1 = \text{id}$ ist der einzige Homomorphismus mit den gewünschten Eigenschaften.

$t - 1 \to t$ Sei wieder $F = K[a_1, \ldots, a_{t-1}]$, p das Minimalpolynom von a_t in $F[x]$ vom Grad d und $|F : K| = m$, also $md = n$. Per Induktion gibt es genau m verschiedene Homomorphismen $\sigma_1, \ldots, \sigma_m : F \to \overline{K}$ mit $\sigma_{i|K} = \text{id}$.
g.z.z.: Jedes σ_i läßt sich auf genau d verschiedene Weisen zu E fortsetzen. Es ist p ein separables Polynom, denn wenn q das Minimalpolynom von a_t in $K[x]$ ist, dann ist $q \in F[x]$ und $q(a_t) = 0$, also $p \mid q$ in $F[x]$. Hätte p mehrfache Nullstellen, dann auch q. Aber dann wäre a_t nicht separabel über K entgegen der Voraussetzung.
Also ist auch $p\sigma_i \in \overline{K}[x]$ separabel, hat also genau d verschiedene Nullstellen

in $\overline{K}$, etwa $b_1, \ldots, b_d$. Nach 10.11 existieren Homomorphismen $\tau_1^i, \ldots, \tau_d^i : E \to \overline{K}$ mit $\tau^i_{j|F} = \sigma_i$ und $a_t \tau_j^i = b_j$. Die τ_j^i's sind also alle verschieden für $j = 1, \ldots, d$ und $i = 1, \ldots, m$. Daher gibt es $dm = n$ solche Homomorphismen.

(3)⇒(1) Sei $a \in E$ und p das Minimalpolynom von a in $K[x]$, $d = \deg p$. Sei $F = K[a]$. Dann ist $|F : K| = d$, also $|E : F| = {}^{n}/_{d} = m$.
Seien $\sigma_1, \ldots, \sigma_r$ die verschiedenen Homomorphismen $F \to \overline{K}$ mit $\sigma_{i|K} = \text{id}$. Dann sind die $a\sigma_i$'s verschiedene Nullstellen von $p\sigma_i = p$ in $\overline{K}$, und daher ist $r \leq d$. Nach (12.6) hat jedes σ_i höchstens m verschiedene Fortsetzungen auf E. Also hat id_K höchstens rm viele Fortsetzungen auf E, d.h. $rm \geq n = dm$. Folglich ist $r \geq d$, also $r = d$. Daher hat p genau d verschiedene Nullstellen, ist also separabel; damit ist auch a separabel.

12.8 Satz: *Satz vom primitiven Element*

Sei L eine endliche Erweiterung von K. Genau dann existiert ein $a \in L$ mit $L = K[a]$ (ein sogenanntes primitives Element), wenn es nur endlich viele Körper zwischen L und K gibt.
Wenn L eine separable Erweiterung ist, ist dies stets der Fall.

Beweis: Unter der zusätzlichen Voraussetzung, dass K ein unendlicher Körper ist.

Wir setzen zunächst voraus, dass es nur endlich viele Zwischenkörper $K \leq E \leq L$ gibt. Seien $a, b \in L$. Betrachte alle Elemente der Form $a + kb \in L$ mit $k \in K$. Für jedes der unendlich vielen $k \in K$ ist $K[a + kb]$ ein Zwischenkörper. Also gibt es $k_1 \neq k_2$ in K mit $K[a + k_1 b] = K[a + k_2 b] =: E$. Dann sind $a + k_1 b,\ a + k_2 b \in E$, also auch $(a + k_1 b) - (a + k_2 b) = (k_1 - k_2) b \in E$. Da $0 \neq k_1 - k_2 \in K \leq E$, folgt $b \in E,\ k_1 b \in E$ und damit auch $a = (a + k_1 b) - k_1 b \in E$, d.h. $a, b \in E$, also $K[a, b] = K[a + k_1 b]$. Damit ist gezeigt, dass jede von zwei Elementen erzeugte Erweiterung mit einem Element erzeugbar ist. Per Induktion folgt leicht, dass jede endlich erzeugte Erweiterung von einem Element erzeugt wird; also ist $L = K[a]$.
Umgekehrt sei $L = K[a]$. Zu zeigen: Es gibt nur endlich viele Zwischenkörper. Sei p das Minimalpolynom von a über K und sei E ein Zwischenkörper. Dann ist auch $L = E[a]$; sei q das Minimalpolynom von a über E. Dann gilt $q \mid p$ in $E[x]$. Wenn $a_1, \ldots, a_n$ die Nullstellen von p in $\overline{K}$ sind, dann ist $p(x) = \prod_{i=1}^{n} (x - a_i)$ und $q(x) = \prod_{j \in J} (x - a_j)$ für eine Teilmenge $J \subseteq \{1, \ldots, n\}$. Da es nur endlich viele Teilmengen von $\{1, \ldots, n\}$ gibt, gibt es auch nur endlich viele normierte Polynome $q \mid p$. Also hat man eine Abbildung $E \mapsto q_E(x)$ von der Menge der Zwischenkörper in eine endliche Menge von Polynomen. Diese Abbildung ist injektiv: sei $E_0 \leq E$ der Unterkörper von E, welcher von K und allen Koeffizienten von q_E erzeugt wird (so dass also $q_E \in E_0[x]$). Dann ist q_E irreduzibel in $E_0[x]$, daher das Minimalpolynom von a über E_0. Natürlich ist $K[a] \leq E_0[a] \leq L = K[a]$, also ist $L = E_0[a]$, daher $|L : E_0| = \deg q_E = |L : E|$. Weil $E_0 \leq E$, folgt $E_0 = E$ aus dem Gradsatz. Daher ist die Abbildung injektiv; es gibt also nur endlich viele Zwischenkörper.
Sei schließlich L eine separable Erweiterung von K. Wir wollen zeigen, dass L von einem Element erzeugt wird. Per Induktion braucht man nur den Fall zu betrachten, in dem $L = K[a, b]$. Sei etwa $|L : K| = n$, und seien $\sigma_1, \ldots, \sigma_n$ die verschiedenen Homomorphismen von L in $\overline{K}$ mit $\sigma_{i|K} = \text{id}$. Setze $p(x) = \prod_{i \neq j} (a\sigma_i + xb\sigma_i - a\sigma_j - xb\sigma_j)$.
Dann ist $p(x) \neq 0$, denn sonst wäre $a\sigma_i + xb\sigma_i - a\sigma_j - xb\sigma_j = 0$ für ein Paar $i \neq j$; aber dann $a\sigma_i = a\sigma_j$ und $b\sigma_i = b\sigma_j$; wegen $L = K[a, b]$ wäre dann $\sigma_i = \sigma_j$, ein Widerspruch. Also hat $p(x) \neq 0$ nur endlich viele Nullstellen. Sei $k \in K$ mit $p(k) \neq 0$. Dann sind

alle $(a+kb)\sigma_i$ verschieden, daher gibt es mindestens n verschiedene Homomorphismen $K[a+kb] \to \overline{K}$. Nach (12.6) ist $|K[a+kb]:K| \geq n$, also $K[a+kb] = L$.

12.9 **Bemerkung:** *zur zusätzlichen Voraussetzung*

Teile von (12.8) wurden bewiesen unter der zusätzlichen Annahme, dass K unendlich ist. Der Satz ist vollständig bewiesen, wenn wir zeigen können:

12.10 **Satz:** *Erweiterung eines endlichen Körpers*

Sei K ein endlicher Körper und K_0 der Primkörper von K. Dann existiert ein $a \in K$ mit $K = K_0[a]$.

Beweis: Später!

12.11 **Korollar:** *Zwischenkörper von primitiven Erweiterungen*

Sei $K \leq E \leq K[a]$. Dann gibt es $b \in E$ mit $E = K[b]$.

Beweis: Es gibt offenbar nur endlich viele Körper zeischen K und E.

13 Galois-Theorie

13.1 Bemerkung: *Vorsicht*

In diesem Paragraphen wird 12.8 verwendet. Dies ist aber bisher nicht vollständig bewiesen.

13.2 Definition: *Fixkörper*

Sei K ein Körper, $A = \mathrm{Aut}\,(K)$ die Automorphismengruppe von K und sei G ein Untergruppe von A. Man nennt $\mathrm{Fix}\,(G) = \{a \in K \mid a^\alpha = a \quad \forall \alpha \in G\}$ den Fixkörper von G.

13.3 Lemma: *Der Fixkörper ist Unterkörper*

$\mathrm{Fix}\,(G)$ ist ein Unterkörper von K.

Beweis: Trivial.

13.4 Beispiel: *Fixkörper*

(i) K beliebig und $G = \{1\}$. Dann ist $\mathrm{Fix}\,(G) = K$.

(ii) $K = \mathbb{C}$ und $G = \{id,\ c \mapsto \bar{c}\}$. Dann ist $\mathrm{Fix}\,(G) = \mathbb{R}$.

13.5 Lemma: *Untergruppen und Fixkörper*

Wenn K ein Körper und $H \leq G \leq \mathrm{Aut}\,(K)$, dann ist $\mathrm{Fix}\,(H) \geq \mathrm{Fix}\,(G)$.

Beweis: Trivial.

13.6 Definition: *Automorphismengruppe über einem Körper*

Sei K ein Unterkörper von E. Man nennt $\Gamma\,(E/K) = \{\alpha \in \mathrm{Aut}\,(E) \mid a^\alpha = a \quad \forall a \in K\}$ die Automorphismengruppe von E über K.

13.7 Lemma: *Automorphismengruppe*

Sei E eine Körpererweiterung von K.

(1) $\Gamma\,(E/K) \leq \mathrm{Aut}\,(E)$

(2) $\mathrm{Fix}\,(\Gamma\,(E/K)) \geq K$

(3) Wenn $G \leq \mathrm{Aut}\,(E)$, dann ist $\Gamma = \Gamma\,(E/\mathrm{Fix}\,(G)) \geq G$ und $\mathrm{Fix}\,(\Gamma) = \mathrm{Fix}\,(G)$.

Beweis: Trivial.

13.8 Definition: *Galois-Erweiterung, Galois-Gruppe*

Sei E eine Erweiterung von K. Man nennt E eine Galois-Erweiterung von K, wenn $K = \mathrm{Fix}\,(\Gamma\,(E/K))$. Dann heißt $\Gamma\,(E/K)$ die Galois-Gruppe von E über K.

13.9 **Lemma:** *Minimalpolynome und Erweiterungsgrad*

Sei E eine separable Erweiterung von K. Wenn alle Elemente von E über K ein Minimalpolynom vom Grad $\leq n$ haben, dann ist $|E : K| \leq n$.

<u>*Beweis:*</u> Sei $a \in E$ mit Minimalpolynom maximalen Grades, etwa m $(\leq n)$. Wäre $K[a] < E$, dann existiert $b \in E \setminus K[a]$; also ist dann $K[a,b] > K[a]$. Aber nach dem Satz vom primitiven Element (12.8) existiert ein $c \in E$ mit $K[a,b] = K[c]$ (12.8 ist anwendbar, da $K[a,b]$ eine endliche separable Erweiterung von K ist). Wenn t der Grad des Minimalpolynoms von c über K ist, dann $t = |K[c] : K| > |K[a] : K| = m$, ein Widerspruch zur Wahl von m.

13.10 **Satz:** *endliche Untergruppen erzeugen normale und separable Erweiterungen*

Sei E ein Körper und G eine endliche Untergruppe von $\mathrm{Aut}\,(E)$. Sei $K = \mathrm{Fix}\,(G)$. Dann gilt: E ist normale und separable Erweiterung von K und $|E : K| \leq |G|$ (es gilt sogar Gleichheit, wie wir zeigen werden).

<u>*Beweis:*</u> Sei $a \in E$. Betrachte die Menge $B = \{a^\gamma \mid \gamma \in G\}$. Diese Menge ist endlich mit höchstens $|G|$ Elementen, und es gilt $B^G = B$. Sei $p(x) = \prod\limits_{b \in B} (x - b)$. Dieses Polynom ist invariant unter G, hat also Koeffizienten in K. Außerdem ist a eine Nullstelle von p. Daher ist a algebraisch über K. Da alle Nullstellen von p verschieden sind, ist a separabel über K. Da p in $E[x]$ in Linearfaktoren zerfällt, ist E eine normale Erweiterung von K. Da jedes $a \in E$ ein Minimalpolynom vom Grad $\leq |G|$ hat, ist $|E : K| \leq |G|$ nach (13.9).

13.11 **Satz:** *normal und separabel ist Galois'sch*

Sei E eine endliche Erweiterung von K und sei $\Gamma = \Gamma\,(E/K)$. Dann gilt:

(1) $|\Gamma| \leq |E : K|$

(2) Äquivalent sind:

  (i) $|\Gamma| = |E : K|$

  (ii) E ist normale und separable Erweiterung von K.

  (iii) E ist Galois-Erweiterung von K.

<u>*Beweis:*</u> Betrachte:

$$\begin{tikzcd}
K \arrow[rr, "\mu"] \arrow[dr, "\mu"'] & & E \arrow[r, "\nu"] & \overline{K} \\
& E \arrow[ur, "\alpha \in \Gamma"'] & &
\end{tikzcd}$$

wobei $\overline{K}$ der algebraische Abschluss von K ist und μ und ν die Einbettungen.
Sei $\Phi = \{\phi : E \to \overline{K} \mid \phi$ ist Homomorphismus mit $\phi_{|K} = \mathrm{id}\}$ und $\Phi_0 = \{\phi \in \Phi \mid E\phi = E\}$. Dann ist $\Phi_0 \subseteq \Phi$ und nach (11.5) gilt $\Phi_0 = \Phi$ genau dann, wenn E normale Erweiterung von K ist. Außerdem ist $|\Phi| \leq |E : K|$, nach (12.6), und nach (12.7) ist $|\Phi| = |E : K|$ genau dann, wenn E separabel über K ist.
Die Abbildung $\Gamma \ni \alpha \mapsto \alpha\nu \in \Phi_0$ ist eine Bijektion. Also gilt $|\Gamma| = |\Phi_0| \leq |\Phi| \leq |E : K|$ mit „$=$“ $\Leftrightarrow$ E ist normal und separabel über K.
Dies zeigt (1) und die Äquivalenz von (i) und (ii) in (2).

(iii)⇒(ii) Nach Voraussetzung ist $K = \mathrm{Fix}(\Gamma)$. Da Γ endlich ist nach (1), ist E normal und separabel über K nach (13.10).

(i)⇒(iii) Sei $L = \mathrm{Fix}(\Gamma)$; zu zeigen ist $L = K$. Nach (13.7(2)) ist $L \geq K$, also $|E : L| \leq |E : K|$. Nach (1) ist $|\Gamma(E/L)| \leq |E : L|$. Aber $\Gamma \leq \Gamma(E/\mathrm{Fix}(\Gamma)) = \Gamma(E/L)$ nach (13.7(3)), also $|E : K| = |\Gamma| \leq |\Gamma(E/L)| \leq |E : L|$. Es folgt $|E : L| = |E : K|$ und damit $L = K$.

13.12 Korollar: *endliche Untergruppen erzeugen Galois-Erweiterungen*

Sei G eine endliche Untergruppe von $\mathrm{Aut}(E)$ und $K = \mathrm{Fix}(G)$. Dann ist E eine Galois-Erweiterung von K mit Galois-Gruppe G und $|G| = |E : K|$.

Beweis: Nach (13.10) ist E normal, separabel und endlich über K. Nach (13.11) ist E Galois'sch über K und $|\Gamma(E/K)| = |E : K|$. Da $G \leq \Gamma(E/K)$ nach (13.7(3)) und $|E : K| \leq |G|$ wieder nach (13.10), folgt $|G| \leq |\Gamma(E/K)| = |E : K| \leq |G|$, also $|\Gamma(E/K)| = |G|$ und $G = \Gamma(E/K)$.

13.13 Korollar: *Galois'sch bleibt Galois'sch über Zwischenkörpern*

Sei E eine endliche Galois-Erweiterung von K und sei L ein Zwischenkörper. Dann ist E eine endliche Galois-Erweiterung von L.

Beweis: „Endlich“ ist klar. Nach (13.11) g.z.z. E ist normal und separabel über L. Sei $a \in E$ und $p \in L[x]$ das Minimalpolynom von a über L; g.z.z. p hat keine mehrfachen Nullstellen (separabel), und p zerfällt in $E[x]$ in Linearfaktoren (normal). Aber wenn $q \in K[x]$ das Minimalpolynom von a über K ist, dann hat q diese Eigenschaften, weil E normal und separabel über K ist. Da $p \mid q$ in $L[x]$ (wegen $q(a) = 0$), folgt die Behauptung.

13.14 Bemerkung: *Zwischenkörper sind separabel aber nicht unbedingt normal*

Wenn E normal und separabel über K und L ein Zwischenkörper ist, dann ist auch L separabel über K (trivialerweise); hingegen muß L nicht unbedingt normal über K sein. (Betrachte den Zerfällungskörper von $p(x) = x^3 - 2$!)

13.15 Satz: *Hauptsatz der Galois-Theorie*

Sei E eine endliche Galois-Erweiterung von K mit Galois-Gruppe $\Gamma = \Gamma(E/K)$. Dann:

(1) Die Abbildung $H \mapsto \mathrm{Fix}(H)$ ist eine inklusionsumkehrende Bijektion von der Menge der Untergruppen von Γ auf die Menge der Zwischenkörper. Die Umkehrabbildung ist $L \mapsto \Gamma(E/L)$.

(2) Sei $H \leq \Gamma$. Genau dann ist $\mathrm{Fix}(H)$ eine normale Erweiterung von K, wenn $H \lhd \Gamma$. In diesem Fall ist $\mathrm{Fix}(H)$ eine Galois-Erweiterung von K, und es gilt $\Gamma(\mathrm{Fix}(H)/K) \cong {}^{\Gamma}/_{H}$.

Beweis:

(1) Dass die Abbildung Inklusionen umkehrt, ist klar. Es ist zu zeigen, dass $H = \Gamma(E/\mathrm{Fix}(H))$ für alle Untergruppen $H \leq \Gamma$ und dass $L = \mathrm{Fix}(\Gamma(E/L))$ für alle Zwischenkörper L.
Die erste Behauptung ist klar nach (13.12).
Nach (13.13) ist E Galois'sch über L. Nach Definition folgt die zweite Behauptung.

(2) Sei $L = \mathrm{Fix}\,(H)$ eine normale Erweiterung von K. Für jeden Automorphismus $\alpha \in \Gamma$ folgt nach (11.5), dass $L\alpha = L$, also ist $\alpha_{|L} \in \Gamma\,(L/K)$. Die Einschränkung von α auf L gibt also einen Homomorphismus von Γ in $\Gamma\,(L/K)$. Der Kern dieser Abbildung ist genau H; insbesondere ist $H \lhd \Gamma$ und ${}^{\Gamma}/_{H}$ isomorph zu einer Untergruppe von $\Gamma\,(L/K)$.
Da $|H||\Gamma : H| = |\Gamma| = |E : K| = |E : L||L : K| = |H|\,|\Gamma\,(L/K)|$, ist diese Abbildung auch surjektiv, also ${}^{\Gamma}/_{H} \cong \Gamma\,(L/K)$.
Sei umgekehrt $H \lhd \Gamma$ und sei $L = \mathrm{Fix}\,(H)$, dann ist z.z.: L ist normal über K. Sei $a \in L$ und $B = \{a^\gamma \mid \gamma \in \Gamma\}$. Dann ist $p(x) = \prod_{b \in B} (x - b)$ invariant unter Γ, also $p \in K[x]$, daher ist das Minimalpolynom q von a über K ein Teiler von p. Die Nullstellen von q bilden also eine Teilmenge von B. G.z.z. $B \subseteq L$. Sei $b = a^\gamma \in B$ und sei $\beta \in H$ beliebig. Dann ist auch $\beta' = \gamma\beta\gamma^{-1} \in H$, weil $H \lhd \Gamma$, also $b^\beta = a^{\gamma\beta\gamma^{-1}\gamma} = a^{\beta'\gamma} = a^\gamma = b$, weil $a \in L = \mathrm{Fix}\,(H)$. Da dies für jedes $\beta \in H$ gilt, ist $b \in \mathrm{Fix}\,(H) = L$.

13.16 **Definition:** *Kompositum, Erzeugnis*

(1) Sei E ein Körper und L_1 und L_2 Unterkörper. Das Kompositum L_1L_2 ist der kleinste Unterkörper von E, welcher L_1 und L_2 enthält.

(2) Sei G eine Gruppe und H_1 und H_2 Untergruppen. Das Erzeugnis $\langle H_1, H_2\rangle$ ist die kleinster Untergruppe von G, welche H_1 und H_2 enthält.

13.17 **Korollar:** *Schnitt und Erzeugnis*

Sei E eine endliche Galois-Erweiterung von K mit der Galois-Gruppe Γ.
Seien $H_i \leq \Gamma,\ i = 1, 2$. Dann gilt:

(1) $\mathrm{Fix}\,(H_1 \cap H_2) = \mathrm{Fix}\,(H_1)\,\mathrm{Fix}\,(H_2)$

(2) $\mathrm{Fix}\,(\langle H_1, H_2\rangle) = \mathrm{Fix}\,(H_1) \cap \mathrm{Fix}\,(H_2)$

Beweis: Sei $L_i = \mathrm{Fix}\,(H_i)\,, i = 1, 2$.

(1) Da $H_1 \cap H_2 \leq H_1, H_2$, ist $\mathrm{Fix}\,(H_1 \cap H_2) \geq \mathrm{Fix}\,(H_1)\,, \mathrm{Fix}\,(H_2) = L_1, L_2$, also $\mathrm{Fix}\,(H_1 \cap H_2) \geq L_1L_2$.
Sei $H \leq \Gamma$ derart, dass $\mathrm{Fix}\,(H) = L_1L_2$ (ein solches H existiert nach (13.15(1))). Dann $H \leq H_i$, denn $L_1L_2 \geq L_i$ für $i = 1, 2$, also $H \leq H_1 \cap H_2$ und daher $L_1L_2 = \mathrm{Fix}\,(H) \geq \mathrm{Fix}\,(H_1 \cap H_2)$. Zusammen ist also $\mathrm{Fix}\,(H_1 \cap H_2) = L_1L_2$.

(2) Da $H_i \leq \langle H_1, H_2\rangle$, ist $L_i \geq \mathrm{Fix}\,(\langle H_1, H_2\rangle)$ für $i = 1, 2$; also $L_1 \cap L_2 \geq \mathrm{Fix}\,(\langle H_1, H_2\rangle)$.
Sei H definiert durch $\mathrm{Fix}\,(H) = L_1 \cap L_2$. Dann $\mathrm{Fix}\,(H) \leq \mathrm{Fix}\,(H_i)$, also $H \geq H_i$ für $i = 1, 2$, d.h. $H \geq \langle H_1, H_2\rangle$ und daher $L_1 \cap L_2 = \mathrm{Fix}\,(H) \leq \mathrm{Fix}\,(\langle H_1, H_2\rangle)$. Zusammen ist also $\mathrm{Fix}\,(\langle H_1, H_2\rangle) = L_1 \cap L_2$.

13.18 **Satz:** *Kompositum ist Galois'sch.*

Sei E eine endliche Galois-Erweiterung von K, sei F eine beliebige Erweiterung von K, beide enthalten in einem Körper L. Also hat man folgende Situation:

$$\begin{tikzcd} & L \arrow[d, dash] & \\ & EF \arrow[dl, dash] \arrow[dr, dash] & \\ E \arrow[dr, dash] & & F \arrow[dl, dash] \\ & E \cap F \arrow[d, dash] & \\ & K & \end{tikzcd}$$

Dann ist EF Galois'sch über F und $\Gamma\,(EF/F) \cong \Gamma\,(E/E \cap F)$.

<u>*Bemerkung:*</u>

- Nach (13.13) ist E eine Galois-Erweiterung von $E \cap F$.
- Offenbar ist $\Gamma\,(E/E \cap F) \leq \Gamma\,(E/K)$.

<u>*Beweis:*</u> Nach dem Satz vom primitiven Element (12.8) gibt es ein $a \in E$ mit $E = (E \cap F)[a]$. Sei p das Minimalpolynom von a in $(E \cap F)[x]$. Dann ist E der Zerfällungskörper von p, da E normal über $E \cap F$ ist; außerdem ist p separabel.
Es ist $p \in F[x]$ und $EF = F[a]$ der Zerfällungskörper von p über F. Daher ist EF über F endlich, normal und separabel nach (11.5) und (12.7(2)); nach (13.11) ist EF eine Galois-Erweiterung von F. Sei $\alpha \in \Gamma\,(EF/F)$, dann $\alpha_{|K} = \mathrm{id}$, also ist $\alpha_{|E} \in \Gamma\,(E/K)$. Die Abbildung $\varrho : \alpha \mapsto \alpha_{|E}$ ist offenbar ein Homomorphismus $\Gamma\,(EF/F) \to \Gamma\,(E/K)$. Außerdem ist ϱ injektiv, denn wenn $\alpha_{|E} = \mathrm{id}$, dann ist $a^\alpha = a$, also $\alpha = id$, weil $EF = F[a]$.
Sei $H = \mathrm{Im}\,(\varrho)$; dann also $\Gamma\,(EF/F) \cong H \leq \Gamma\,(E/K)$. Es ist $b \in \mathrm{Fix}\,(H) \Leftrightarrow b \in E \cap \mathrm{Fix}\,(\Gamma\,(EF/F)) = E \cap F$. Nach dem Hauptsatz ist $H = \Gamma\,(E/E \cap F)$.

13.19 Korollar: *Grad des Kompositums*

Unter den Voraussetzungen von (13.18) gilt:

$$|EF : F| \,\big|\, |E : K|.$$

<u>*Beweis:*</u> $|EF : F| = |E : E \cap F|$ nach (13.18 und 13.11). Nach dem Gradsatz ist $|E : E \cap F| \,\big|\, |E : K|$.

13.20 Bemerkung/Definition: *Galois-Gruppe eines Polynoms*

Sei $p \in K[x]$ ein separables Polynom. Sei E der Zerfällungskörper von p. Dann ist E eine Galois-Erweiterung von K (normal ist klar, separabel nach (12.7)). Die <u>Galois-Gruppe</u> von p ist $\Gamma\,(E/K) = \Gamma_p$.

13.21 Satz: *Galois-Gruppe operiert transitiv auf den Nullstellen*

Sei $p \in K[x]$ ein irreduzibles und separables Polynom vom Grad n mit Galois-Gruppe Γ und $A = \{a_1, \ldots, a_n\}$ die Menge der Nullstellen von p. Dann ist A eine transitive Γ-Menge. Wenn $\gamma \in \Gamma$ und $a_i^\gamma = a_i \;\forall i$, dann $\gamma = \mathrm{id}$.

<u>*Beweis:*</u> Sei $\gamma \in \Gamma,\; a_i \in A$. Dann ist a_i eine Nullstelle von p, also a_i^γ eine Nullstelle von $p^\gamma = p$, weil $p \in K[x]$ und $K = \mathrm{Fix}\,(\Gamma)$. Daher ist $a_i^\gamma \in A$. Sei $a_1 \in B \subseteq A$ eine Γ-Bahn.

Dann ist $q(x) = \prod_{b \in B} (x - b)$ invariant unter Γ, also $q \in K[x]$. Da $q(a_1) = 0$ und p das Minimalpolynom von a_1 ist, folgt $p \mid q$, also $n = \deg p \leq \deg q = |B| \leq |A| = n$, daher $A = B$, d.h. A ist transitive Γ-Menge.
Wenn $\gamma \in \Gamma$ mit $a_i^\gamma = a_i \ \forall i$, dann läßt γ alle Elemente aus $K[a_1, \ldots, a_n]$ fest, weil $\gamma_{|K} = \text{id}$. Aber $K[a_1, \ldots, a_n] = (\text{Zerfällungskörper von } p) = E$, also $\gamma = \text{id}$.

13.22 Korollar: *Galois-Gruppe ist Untergruppe der S_n*

Seien die Voraussetzungen wie in (13.21) und E der Zerfällungskörper von p. Dann ist $\Gamma \overset{\sim}{\leq} S_n$ und $n \,\big|\, |\Gamma| = |E : K| \,\big|\, n!$.

Beweis: Da A eine Γ-Menge mit n Elementen ist, haben wir einen Homomorphismus $\mu : \Gamma \to S_A \cong S_n$. Dieser ist injektiv: $\gamma \in \operatorname{Ker}(\mu) \Leftrightarrow a_i^\gamma = a_i \ \forall i \Leftrightarrow \gamma = id_E$. Daher ist $\Gamma \cong \mu(\Gamma) \leq S_n$. Insbesondere $|\Gamma| \,\big|\, |S_n| = n!$. Da Γ transitiv auf A operiert, folgt $n = |A| = |\Gamma : \operatorname{Stab}_\Gamma(a_1)| \,\big|\, |\Gamma|$. Schließlich ist $|\Gamma| = |E : K|$ nach (13.11).

14 Auflösbarkeit durch Radikale

In diesem Paragraphen ist $\operatorname{char}(K) = 0$ vorausgesetzt.

14.1 Definition: *einfache Radikal-Erweiterung*

(1) Eine Körper-Erweiterung E von K heißt einfache Radikal-Erweiterung, falls $E = K[a]$, wobei $a^n \in K$ für ein $n \in \mathbb{N}$.

(2) Eine Körper-Erweiterung E von K heißt Radikal-Erweiterung von K, falls es Zwischenkörper $K = E_0 \leq E_1 \leq \ldots \leq E_t = E$ gibt derart, dass E_i eine einfache Radikal-Erweiterung von E_{i-1} ist für jedes $i = 1, \ldots, t$.

14.2 Lemma: *Eigenschaften der Radikal-Erweiterung*

Sei E eine Radikal-Erweiterung von K.

(1) Sei F eine Radikal-Erweiterung von E. Dann ist F eine Radikal-Erweiterung von K.

(2) Sei L beliebige Erweiterung von K und seien E und L in Ω enthalten. Dann ist EL eine Radikal-Erweiterung von L.

(3) Sei L ein Zwischenkörper ($K \leq L \leq E$). Dann ist E Radikal-Erweiterung von L.

(4) Sei F Radikal-Erweiterung von K und $E, F \subseteq \Omega$. Dann ist EF eine Radikal-Erweiterung von K.

(5) Sei $\tau : E \to F$ eine Körperhomomorphismus.
Dann ist $E\tau$ eine Radikal-Erweiterung von $K\tau$.

Beweis: Klar.

14.3 Satz: *Einbettung einer Radikal-Erweiterung in eine normale Erweiterung*

Sei E eine Radikal-Erweiterung von K. Dann existiert eine Radikal-Erweiterung F von K mit $F \geq E$ und F normal über K.
(Jede Radikal-Erweiterung kann in eine normale Radikal-Erweiterung eingebettet werden.)

Beweis: Das Kompositum F der sämtlichen Körper $E\tau$, wobei $\tau : E \to \overline{K}$, $\tau_{|K} = \mathrm{id}$, ist normal nach (11.5) und eine Radikal-Erweiterung (14.2(5)) und (14.2(4)).

14.4 Definition: *auflösbar durch Radikale*

Sei $\operatorname{char} K = 0$ und sei $f \in K[x]$. Man nennt f auflösbar durch Radikale, falls es eine Radikal-Erweiterung E von K gibt derart, dass E alle Nullstellen von f enthält.

14.5 Bemerkung: *Eigenschaften der durch Radikale auflösbaren Polynome*

(i) Das heißt gerade, dass die Nullstellen von f sich als iterierte Radikale schreiben lassen.

(ii) Äquivalent: Der Zerfällungskörper von f ist in einer Radikal-Erweiterung von K enthalten.

(iii) Falls f irreduzibel ist, genügt es anzunehmen, dass eine Nullstelle in einer Radikal-Erweiterung liegt: Wenn E eine Radikal-Erweiterung von K ist, welche eine Nullstelle von f enthält, sei $F \geq E$ eine normale Radikal-Erweiterung von K (existiert nach 14.3). Dann enthält F den Zerfällungskörper von f; also liegen alle Nullstellen von f in der Radikal-Erweiterung F.

14.6 Lemma: *p-te Einheitswurzel als Eigenwert*

Sei V ein endlich-dimensionaler K-Vektorraum und $\alpha \in \mathrm{Aut}\,(V)$ mit $\alpha^p = \mathrm{id}$, p eine Primzahl. Wenn $\alpha \neq \mathrm{id}$, dann gibt es einen Eigenwert $\omega \in \overline{K}$ von α mit $\omega^p = 1 \neq \omega$ (d.h. ω ist eine primitive p-te Einheitswurzel).

Beweis: Das Minimalpolynom f von α ist ein Teiler von $x^p - 1$, aber $f \neq x - 1$, da $\alpha \neq \mathrm{id}$. Jede Nullstelle $\neq 1$ von f hat die gewünschte Eigenschaft.

14.7 Lemma: *Erweiterungen durch p-te Wurzel*

Sei p eine Primzahl, $0 \neq a \in K$ und E der Zerfällungskörper von $f(x) = x^p - a \in K[x]$. Dann ist $\Gamma(E/K)$ auflösbar.

Beweis: Wenn b ein Nullstelle von f ist, dann erhält man die anderen Nullstellen als $b\omega$, wobei ω die sämtlichen p-ten Einheitswurzeln durchläuft. Daher ist $E = K[\omega, b]$ für eine primitive p-te Einheitswurzel. Sei $E_0 = K[\omega]$; dann ist E_0 eine Galois'sche Erweiterung von K und $K \leq E_0 \leq E$. Wenn $E_0 = Fix(N)$, dann ist $N \triangleleft \Gamma(E/K)$. Außerdem sind $N = \Gamma(E/E_0)$ und ${}^{\Gamma(E/K)}/_{N} \cong \Gamma(E_0/K)$ beide abelsch, denn ein Automorphismus von E_0 muss ω auf eine Potenz abbilden, ein Automorphismus von E, welcher auf E_0 die Identität ist, muss b auf ein $b\omega^i$ abbilden. Nach (6.7) ist $\Gamma(E/K)$ auflösbar.

14.8 Satz: Galois

Sei E eine endliche, normale Erweiterung von K mit der Galois-Gruppe Γ. Genau dann ist E in einer Radikal-Erweiterung von K enthalten, wenn Γ auflösbar ist.

Beweis: Sei zunächst Γ auflösbar.
Induktion über $|\Gamma|$:
Wenn $|\Gamma| = 1$, dann ist $E = K$; fertig. Sei $1 < N \underset{\neq}{\triangleleft} \Gamma$ und sei $E_0 = \mathrm{Fix}\,(N)$. Dann $K < E_0 < E$, und E ist normal über E_0 mit der Galois-Gruppe N, und E_0 ist normal über K mit der Galois-Gruppe ${}^{\Gamma}/_{N}$. Nach (6.7) sind N und ${}^{\Gamma}/_{N}$ auflösbar. Da $|N|, \left|{}^{\Gamma}/_{N}\right| < |\Gamma|$, gilt per Induktion: E_0 ist enthalten in einer Radikal-Erweiterung F_0 von K, und E ist enthalten in einer Radikal-Erweiterung F von E_0. Nach (14.2(2)) ist FF_0 eine Radikal-Erweiterung von F_0. Da F_0 eine Radikal-Erweiterung von K, ist nach (14.2(1)) FF_0 eine Radikal-Erweiterung von K, welche F, also E, enthält. Fertig.

Es bleibt der Fall, dass Γ keine echten Normalteiler enthält, also einfach ist. Offenbar ist dann $|\Gamma| = p$ eine Primzahl. Sei K_1 der Zerfällungskörper von $x^p - 1$. Dies ist eine Radikal-Erweiterung von K, nämlich $K_1 = K[\omega]$, wobei ω eine primitive p-te Einheitswurzel ist. Nach (13.18) ist $E_1 = EK_1$ eine Galois-Erweiterung von K_1 mit einer Galois-Gruppe $\overset{\sim}{\leq} \Gamma$. Aber Γ hat nur zwei Untergruppen, nämlich 1 und Γ.
Falls $\Gamma\,(EK_1/K_1) = 1$, dann $EK_1 = K_1$, $E \leq K_1$; fertig.
Falls $\Gamma_1 := \Gamma\,(E_1/K_1) \cong \Gamma$, sei $1 \neq \alpha \in \Gamma_1$. Die Abbildung $e \mapsto e^\alpha$ ist ein K_1-Automorphismus von E_1. Daher existiert nach 14.6 ein Eigenwert $\omega \neq 1 = \omega^p$ von α. Sei $0 \neq e \in E_1$ ein Eigenvektor zu ω, dann $e^\alpha = \omega e$ (insbesondere $e \notin K_1$) und $(e^p)^\alpha = (e^\alpha)^p = (\omega e)^p = e^p$. Daher ist e^p ein Fixpunkt unter α, daher unter Γ_1, d.h.

$a = e^p \in K_1$. Also ist e Nullstelle von $x^p - a \in K_1[x]$ und $K_1[e] = E_1$, da $e \notin K_1$ und $|E_1 : K_1| = p$. Daher ist E_1 eine einfache Radikal-Erweiterung von K_1, also eine Radikal-Erweiterung von K und $E \subseteq E_1$; fertig.

Umgekehrt sei E in einer Radikal-Erweiterung enthalten. Nach (14.4) ist es dann in einer normalen Radikal-Erweiterung F enthalten. Wenn $\Gamma(F/K)$ auflösbar ist, dann auch $\Gamma(E/K)$, denn $\Gamma(E/K)$ ist (nach dem Hauptsatz der Galois-Theorie 13.15) isomorph zu einer Faktorgruppe von $\Gamma(F/K)$ und die Behauptung folgt aus (6.7). Also dürfen wir annehmen, dass E eine normale Radikal-Erweiterung von K ist. Außerdem o.B.d.A. $E > K$. Dann existiert eine einfache Radikal-Erweiterung $E \geq E_1 > K$, etwa $E_1 = K[a]$ mit $a^n \in K$ für ein $n \in \mathbb{N}$. Sei n_0 minimal mit $a^{n_0} \in K$, dann $n_0 > 1$ (sonst $a \in K$ und $E_1 = K$, Widerspruch); sei p ein Primteiler von n_0, etwa $n_0 = mp$. Setze $b = a^m$. Dann $b^p \in K$, aber $b \notin K$, weil $m < n_0$. Sei E_0 der Zerfällungskörper von $x^p - b^p \in K[x]$. Dann $E \geq E_0 > K$ und E_0 normal über K. Außerdem $E_0 = \mathrm{Fix}(N)$ für ein $N \triangleleft \Gamma(E/K)$ und E ist eine normale Radikal-Erweiterung (14.2(3)) von E_0. Per Induktion ist $N = \Gamma(E/E_0)$ auflösbar. Außerdem ist ${}^{\Gamma(E/K)}/_{N} \cong \Gamma(E_0/K)$. Aber $\Gamma(E_0/K)$ ist auflösbar nach 14.7. Nach (6.7) ist dann $\Gamma(E/K)$ auflösbar.

14.9 Korollar: *auflösbare Polynome und deren Galois-Gruppe*

Sei $f \in K[x]$ irreduzibel. Äquivalent sind:

(1) f ist durch Radikale auflösbar.

(2) Γ_f ist auflösbar.

14.10 Lemma: *Transposition und langer Zykel erzeugen die S_p*

Sei p eine Primzahl und H eine Untergruppe der S_p, welche eine Transposition und ein Element der Ordnung p enthält. Dann ist $H = S_p$.

<u>*Beweis:*</u> Seien o.B.d.A. $\tau = (1,2)$, $\alpha = (12\dots p) \in H$. Dann ist $\tau^{\alpha^i} = (i+1, i+2)$ für $i = 0, \dots, p-1$.
Beweis dazu:

$$\begin{aligned}
j\alpha^i &\equiv j + i \pmod p \\
j\alpha^{-i} &= j - i \\
j\alpha^{-i}\tau\alpha^i &= j \quad \forall (j-i) \notin \{1,2\} \\
(i+1)\alpha^{-i}\tau\alpha^i &= 1\tau\alpha^i = 2\alpha^i = i+2 \\
(i+2)\alpha^{-i}\tau\alpha^i &= 2\tau\alpha^i = 1\alpha^i = i+1
\end{aligned}$$

Für $k > j$ ist
$(jk) = (k-1,k)(k-2,k-1)\cdots(j+2,j+1)(j+1,j)(j+2,j+1)\cdots(k-1,k)$.
Also enthält die Gruppe H mit τ und α auch alle Transpositionen (jk). Aber jede Permutation ist Produkt von Transpositionen, daher $H = S_p$.

14.11 Beispiel: $f(x) = x^5 - 5x + 1$

Sei $f(x) = x^5 - 5x + 1$. Dann ist f ein irreduzibles Polynom in $\mathbb{Q}[x]$ und $\Gamma_f \cong S_5$. Insbesondere ist f nicht durch Radikale auflösbar.

<u>*Beweis:*</u> Setze $x = y - 1$. Dann ist $x^5 - 5x + 1 = (y-1)^5 - 5(y-1) + 1 = y^5 - 5y^4 + 10y^3 - 10y^2 + 5y - 1 - 5y + 5 + 1 = y^5 - 5y^4 + 10y^3 - 10y^2 + 5$ irreduzibel nach Eisenstein (8.13).

Es ist $f'(x) = 5x^4 - 5 = 5(x^2+1)(x^2-1)$. Also hat f' zwei Nullstellen in $\mathbb{Q}$, nämlich ± 1. Es ist aber auch:

$$\begin{aligned} f(-1) &= (-1)^5 + 5 + 1 = 5 \\ f(1) &= 1 - 5 + 1 = -3 \end{aligned}$$

D.h. f hat drei reelle Nullstellen und zwei konjugiert komplexe.
Da Γ_f transitiv auf den 5 Nullstellen von f operiert, gilt $5 \,\big|\, |\Gamma_f|$, also enthält Γ_f Elemente der Ordnung 5, d.h. einen Zyklus der Länge 5. Die komplexe Konjugation ist eine Transposition. Nach Lemma (14.10) ist $\Gamma_f \cong S_5$.

15 Konstruktion mit Zirkel und Lineal

15.1 Bemerkung: *Was ist eine Konstruktion?*

(i) Gegeben seien (endlich oder unendlich viele) Punkte in der Ebene. Welche weiteren Punkte lassen sich mit „mit Zirkel und Lineal" konstruieren? Erlaubt ist dabei:

(1) „mit dem Lineal" eine Gerade $\overline{PQ}$ durch zwei verschiedene schon vorhandene Punkte P und Q zu ziehen.

(2) „mit dem Zirkel" einen Kreis mit schon vorhandenem Mittelpunkt und vorhandenem Radius (d.h. Abstand zweier vorhandener Punkte) zu ziehen.

Neue Punkte entstehen als Schnittpunkte von zwei Geraden, zwei Kreisen oder einer Geraden und einem Kreis.
Die Schritte dürfen iteriert werden. Die so entstehenden Punkte heißen konstruierbar.
Nicht erlaubt ist, einen Punkt, eine Gerade oder einen Kreis zufällig auszuwählen (z.B. einen „Zufalls"-Punkt auf einer Geraden, eine „Zufalls"-Gerade durch einen Punkt oder einen Kreis mit „zufälligem" Radius.)

(iii) Wenn die gegeben Punktmenge leer ist, oder nur aus einem Punkt besteht, lassen sich daraus keine weiteren Punkte konstruieren. Wir nehmen daher an, dass mindestens zwei Punkte O und E gegeben sind.

(iv) Die Gerade durch O und E nennen wir Abszisse. Die Punkte identifizieren wir mit 0 und 1. Durch wiederholtes Abtragen der Strecke zwischen 0 und 1 auf $\overline{OE}$ können wir dann alle Punkte $z \in \mathbb{Z}$ auf der Abszisse konstruieren.

(v) Auf bekannte Weise läßt sich eine Senkrechte zur Abszisse in O errichten (die Ordinate) und auch auf dieser alle Punkte mit dem Abstand z vom Nullpunkt.
Verwendet wird: Wenn P ein Punkt auf einer Geraden g ist, dann ist die Gerade durch P senkrecht zu g konstruierbar („Senkrechte errichten").

(vi) Die Konstruktion in (v) ist auch ausführbar, wenn P nicht auf g liegt („Lot fällen").

(vii) Seien ein Punkt P und eine Gerade g gegeben, dann ist die zu g parallele Gerade durch P konstruierbar („Parallelverschiebung").

(viii) Seien drei Punkte P, Q und R gegeben, die nicht auf einer Geraden liegen. Dann ist ein Punkt $S \neq P$ so konstruierbar, dass die Winkel zwischen $\overline{PS}$ und $\overline{PQ}$ einerseits und zwischen $\overline{PS}$ und $\overline{PR}$ andererseits gleich sind („Winkelhalbierende").

(ix) Die Punkte auf der Abszisse identifizieren wir mit den reellen Zahlen. Entsprechend reden wir auch von „konstruierbaren Zahlen". Allgemeiner kann man jeden Punkt der Ebene mit einem Paar von Koordinaten $(a, b) \in \mathbb{R}^2$ identifizieren. Offenbar ist ein Punkt genau dann konstruierbar, wenn seine Koordinaten konstruierbar sind.

15.2 Bezeichnung/Bemerkung: *der Körper der konstruierbaren Zahlen*

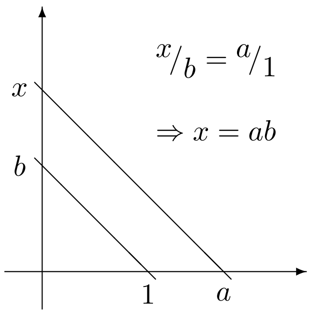
Sei im folgenden K_0 der Körper, den man erhält, indem man zu $\mathbb{Q}$ die Koordinaten der sämtlichen gegebenen Punkte adjungiert. Es ist also $\mathbb{Q} \leq K_0 \leq \mathbb{R}$.
Wenn nur die Punkte O und E gegeben sind (oder allgemeiner nur Punkte aus $\mathbb{Q}$),

ist $K_0 = \mathbb{Q}$. Mit K bezeichnen wir die Menge der konstruierbaren Zahlen, also der konstruierbaren Punkte auf der Abszisse. Nach (15.1) ist $K_0 \subseteq K$, und per Definition ist $K \subseteq \mathbb{R}$. Die Bezeichnung wird gerechtfertigt durch:

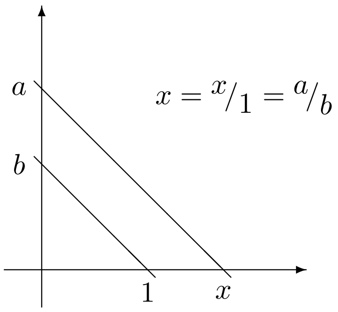
15.3 **Satz:** *die konstruierbaren Zahlen bilden einen Körper*

K ist ein Körper.

Beweis: $0, 1 \in K$ nach Definition.
Addition: Wenn $a, b \in K$, dann offenbar auch $a \pm b \in K$.
Multiplikation:



Division:



Daher ist K ein Körper.

15.4 **Bemerkung:**

Ebenso bilden die konstruierbaren komplexen Zahlen einen Unterkörper von $\mathbb{C}$, nämlich offenbar gerade $K[i]$.

15.5 **Lemma:** *Erweiterungsgrad bei einem Schritt ist höchstens 2*

Sei S Schnittpunkt zweier verschiedener Geraden oder einer Geraden und eines Kreises oder zweier verschiedener Kreise. Sei L ein Körper, der für jede beteiligte Gerade die Koordinaten zweier Punkte auf dieser Geraden und für jeden beteiligten Kreis das Quadrat des Radius' und die Koordinaten des Mittelpunktes enthält. Sei L' der Körper, der aus L durch Adjunktion der Koordinaten von S entsteht. Dann ist $|L' : L| \leq 2$.

Beweis: Sei $S = (x, y)$, also $L' = L[x, y]$.

1. Fall S ist Schnittpunkt zweier Geraden g, h. Nach Voraussetzung gibt es $P_1 = (a_1, b_1)$, $P_2 = (a_2, b_2)$ auf g und $Q_1 = (u_1, v_1)$, $Q_2 = (u_2, v_2)$ auf h mit $a_i, b_i, u_i, v_i \in L$ für $i = 1, 2$. Es ist

$$\begin{aligned} x &= a_1 + (a_2 - a_1)\lambda \\ x &= u_1 + (u_2 - u_1)\mu \\ y &= b_1 + (b_2 - b_1)\lambda \\ y &= v_1 + (v_2 - v_1)\mu \end{aligned}$$

Dieses lineare Gleichungssystem mit Koeffizienten in L und den Unbestimmten x, y, λ, μ hat eine eindeutige Lösung $(x, y, \lambda, \mu) \in L$ (es gibt genau einen Schnittpunkt). Insbesondere $x, y \in L$, also $L' = L$.

2. Fall S ist Schnittpunkt zweier Kreise um $P = (a, b)$ mit Radius r und um $Q = (u, v)$ mit Radius s, wobei $a, b, u, v, r, s \in L$. Es ist dann

$$\begin{aligned} (x-a)^2 + (y-b)^2 &= r^2 & (1)\\ (x-u)^2 + (y-v)^2 &= s^2 & (2) \end{aligned}$$

und es folgt $2(u-a)x + a^2 - u^2 + 2(v-b)y + b^2 - v^2 = r^2 - s^2$.
Wenn $u = a$, dann $v \neq b$, da sonst die Kreise gleich oder disjunkt wären. Es ist dann $y \in L$, und x erfüllt die quadratische Gleichung (1) mit Koeffizienten in L. Also hat $L' = L[x, y] = L[x]$ einen Grad ≤ 2 über L.
Wenn $u \neq a$, dann kann nach x aufgelöst werden, etwa $x = l_1 y + l_2$. Daher $L' = L[x, y] = L[y]$. Nach Einsetzen von x in (1) erfüllt y eine quadratische Gleichung mit Koeffizienten in L, also $|L[y] : L| \leq 2$.

3. Fall S ist Schnittpunkt einer Geraden und eines Kreises, also mit Bezeichnungen wie oben:

$$\begin{aligned} x - a_1 &= (a_2 - a_1)\lambda \\ y - b_1 &= (b_2 - b_1)\lambda \\ s^2 &= (x-u)^2 + (y-v)^2, \end{aligned}$$

wobei $a_i, b_i, u, v, s \in L$ und o.B.d.A. $a_1 \neq a_2$. Dann ist also $\lambda = \frac{(x-a_1)}{(a_2-a_1)}$ und damit

$$y = b_1 + \frac{(x-a_1)(b_2-b_1)}{a_2-a_1} \in L[x] \ .$$

Daher ist $L' = L[x]$, und man erhält wieder eine quadratische Gleichung für x mit Koeffizienten in L, also $|L[x] : L| \leq 2$.

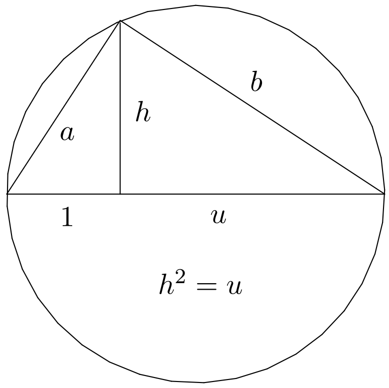
15.6 **Satz:** *konstruierbare Zahlen*

Sei $r \in \mathbb{R}$. Genau dann ist r konstruierbar, wenn es $n \in \mathbb{N}_0$ und Körper $K_0 \leq K_1 \leq \ldots \leq K_n$ gibt mit $|K_i : K_{i-1}| \leq 2$ und $r \in K_n$.

Beweis: Wenn r konstruierbar ist, dann gibt es eine endliche Folge $S_1, \ldots, S_n = (r, 0)$ von Punkten $S_i = (x_i, y_i)$, die jeweils als Schnittpunkte wie in (15.5) entstehen. Setzt man $K_i = K_{i-1}[x_i, y_i]$, so folgt die Behauptung aus (15.5).
Umgekehrt: Wenn E ein reeller Körper mit $|E : L| = 2$ ist und $L \leq K$, dann auch $E \leq K$, denn wenn $E = L[e]$ und $x^2 + ax + b \in L[x]$ das Minimalpolynom von e ist, dann ist

$$e = -\frac{a}{2} \pm \sqrt{\frac{a^2}{4} - b}$$

konstruierbar wie folgt: Es ist $0 \leq u := {}^{a^2}\!/_4 - b \in L$. Also genügt es, eine Wurzel aus u zu konstruieren.



Aus den Sätzen des Thales und des Pythagoras folgt:

$$\begin{aligned} 1 + 2u + u^2 = (1+u)^2 &= a^2 + b^2 \\ &= 1 + h^2 + h^2 + u^2 \\ &= 1 + 2h^2 + u^2 \end{aligned}$$

Also ist $h^2 = u$. Daher ist jedes Element aus E konstruierbar und damit per Induktion auch jedes Element aus K_n.

15.7 **Korollar:** *alles Konstruierbare ist auch algebraisch*

Wenn r konstruierbar ist, dann ist r algebraisch über K_0, und der Grad des Minimalpolynoms ist eine Potenz von 2.

<u>*Beweis:*</u> Wenn $r \in K_n$ wie in (15.6), dann ist $K_0 \leq K_0[r] \leq K_n$, also $|K_0[r] : K_0| \,\big|\, |K_n : K_0| = 2^t$. Daher die Behauptung.

Im folgenden besteht die gegebene Punktmenge nur aus 2 Punkten, also $K_0 = \mathbb{Q}$.

15.8 **Korollar:** *Verdopplung des Würfels*

Es ist unmöglich, mit Zirkel und Lineal die Kantenlänge eines Würfels mit Volumen 2 zu konstruieren.

<u>*Beweis:*</u> Sonst hat man ein a konstruiert mit $a^3 = 2$. Das Minimalpolynom von a über $\mathbb{Q}$ ist $x^3 - 2$ und hat den Grad 3, also keine 2-Potenz.

15.9 **Korollar:** *Dreiteilung des Winkels*

Ein Winkel von $20°$ $(= \frac{1}{3}60°)$ ist nicht konstruierbar.

<u>*Beweis:*</u> Sonst kann man auch $a = \cos 20°$ konstruieren. Wegen $\cos 3\alpha = 4\cos^3\alpha - 3\cos\alpha$ und $\cos 60° = \frac{1}{2}$ folgt: $4a^3 - 3a = \frac{1}{2}$, d.h. a ist Nullstelle von

$$p(x) = 8x^3 - 6x - 1.$$

Durch die Substitution $2x = y + 1$ ist $p(x) = y^3 + 3y^2 - 3$, und dies ist nach Eisenstein (8.13) irreduzibel. Also ist p bis auf Normierung das Minimalpolynom von a. Es ist $\deg p = 3$, und damit a nicht konstruierbar.

15.10 **Korollar:** *Quadratur des Kreises*

Es ist unmöglich, ein Quadrat zu konstruieren, das den Flächeninhalt des Einheitskreises hat.

<u>*Beweis:*</u> Dieser Flächeninhalt ist $\pi r^2 = \pi$. Also müsste die Kantenlänge des Quadrats $\sqrt{\pi}$ sein. Dies ist nicht konstruierbar, da π transzendent ist (ohne Beweis).

15.11 **Bemerkung:** *Konstruktion eines regelmäßigen n-Ecks*

Die Konstruktion des regelmäßigen n-Ecks läuft auf die Konstruktion einer primitiven n-ten Einheitswurzel hinaus, da ja zwei komplexe Zahlen multipliziert werden, indem die Winkel addiert und die Längen multipliziert werden.
Wenn eine primitive n-te Einheitswurzel konstruierbar ist, dann auch eine primitive m-te Einheitswurzel für jeden Teiler m von n. Wenn umgekehrt ω eine primitive n-te und α eine primitive m-te Einheitswurzel ist und $\operatorname{ggT}(n, m) = 1$, dann ist $\alpha\omega$ eine primitive (nm)-te Einheitswurzel. Also genügt es, den Spezialfall zu betrachten , dass n eine Primzahlpotenz ist.

15.12 **Lemma:** *Minimalpolynom einer primitiven p^r-ten Einheitswurzel*

Sei ω eine primitive p^r-te Einheitswurzel für eine Primzahl p. Dann ist
$f(x) = x^{(p-1)p^{r-1}} + x^{(p-2)p^{r-1}} + \ldots + x^{p^{r-1}} + 1$ das Minimalpolynom von ω in $\mathbb{Q}[x]$.

Beweis: Offenbar ist $(x^{p^{r-1}} - 1)f(x) = x^{p^r} - 1$. Daher ist $f(\omega) = 0$. Substituiert man $x = y + 1$ und beachtet $(y+1)^p \equiv y^p + 1 \pmod p$, so ergibt sich

$$y^{p^{r-1}} f(y+1) \equiv y^{p^r} \pmod p \ ,$$

also $f(y+1) \equiv y^{(p-1)p^{r-1}} \pmod p$.
Offenbar hat $f(y+1)$ als Absolutglied genau p. Nach Eisenstein ist f irreduzibel.

15.13 Definition: *Fermat'sche Primzahl*

Eine ungerade Primzahl p der Form $p = 2^n + 1$ heißt Fermat'sche Primzahl.

15.14 Satz: *konstruierbare p^r-Ecke*

Sei $n = p^r$ mit einer Primzahl p. Genau dann ist das regelmäßige n-Eck mit Zirkel und Lineal konstruierbar, wenn $p = 2$ oder $r = 1$ und p eine Fermat'sche Primzahl ist.

Beweis: Sei ω eine konstruierbare primitive n-te Einheitswurzel und L der Körper, den man aus $\mathbb{Q}$ durch Adjunktion der Koordinaten von ω erhält. Dann ist $|L : Q|$ eine 2-Potenz nach (15.6). Da $\mathbb{Q}[\omega] \leq L[i]$, ist auch $|\mathbb{Q}[\omega] : \mathbb{Q}|$ eine 2-Potenz; nach (15.12) ist also $p^{r-1}(p-1)$ eine 2-Potenz. Wenn p ungerade ist, muß also $r = 1$ und p Fermat'sch sein.

Umgekehrt sei dies vorausgesetzt. Wir wollen zeigen, dass dann ω konstruierbar ist. Dies ist klar für $p = 2$, denn dann braucht man nur Winkelhalbierungen vorzunehmen. Sei also p Fermat'sch. Da $\mathbb{Q}[\omega]$ der Zerfällungskörper von $x^{p-1} + \ldots + x + 1$ ist, ist $\mathbb{Q}[\omega]$ Galois'sch über $\mathbb{Q}$. Die Galois-Gruppe Γ hat die Ordnung $p - 1$, also eine 2-Potenz. Daher gibt es nach 4.2 eine Kette von Untergruppen $1 = U_0 < U_1 < \ldots < U_t = \Gamma$ mit $|U_i : U_{i-1}| = 2$.
Entsprechend gibt es eine Kette von Zwischenkörpern $K_i = \mathrm{Fix}\,(U_i)$ mit $\mathbb{Q}[\omega] = K_0 > K_1 > \ldots > K_t = \mathbb{Q}$ und $|K_i : K_{i+1}| = 2$. Also entsteht K_i aus K_{i+1} durch Adjunktion einer komplexen Quadratwurzel. Geometrisch bedeutet dies, einen Winkel zu halbieren und die Wurzel aus der Länge zu ziehen. Beides ist mit Zirkel und Lineal möglich (vergleiche den Beweis von (15.6)). Per Induktion ist ω konstruierbar.

15.15 Korollar: *konstruierbare n-Ecke*

Genau dann ist das regelmäßige n-Eck konstruierbar, wenn $n = 2^a \cdot p_1 \cdot \ldots \cdot p_s$, wobei $a \in \mathbb{N}_0$ und $p_1, \ldots, p_s$ verschiedene Fermat'sche Primzahlen sind.

Beweis: folgt nach (15.11) aus (15.14).