Westfälische
Wilhelms-Universität
Münster

Fachbereich 10
Mathematik und
Informatik

Einführung in die Algebra

Aufarbeitung der Vorlesungsnotizen

Tobias Wedemeier

30. Januar 2015
gelesen von
Prof. Dr. Kramer

Hierbei handelt es sich um eine Aufarbeitung der Vorlesungsnotizenvon **Prof. Dr. Kramer**, WWU Münster, aus der Vorlesung **Einführung in die Algebra** im Wintersemester 2014/15. Dies ist kein Skript der Vorlesung und keine eigene Arbeit des Autors.

Für Fehler in der Aufarbeitung wird keine Haftung übernommen. Hinweise auf Fehler sind gerne gesehen, hierfür kann man mich in der Uni ansprechen oder alternativ eine e-Mail an:
tobias.wedemeier@gmx.de
Auch ist eine Mitarbeit über Github möglich.

Wenn Teile aus der Vorlesung selber fehlen, können diese gerne an meine e-Mail versandt werden. Ich werde diese dann einarbeiten.

Inhaltsverzeichnis

Prolog

Geplante Inhalte

- Gruppentheorie, Untergruppen, Normalteiler, Quotienten, Permutationsgruppen
- Kommutative Ringe, Ideale, Faktorisierbarkeit
- Körper, Galoistheorie, Konstruierbarkeit mit Zirkel und Lineal

Algebra: historisch

Algebra ist historisch gesehen das Auflösen von Gleichungen. Moderne Algebra untersucht sogenannte algebraische Strukturen wie Gruppe, Ringe, Körper, Varitäten,...

Literatur:

- Cohn Basic Algebra
- Jacobson Basic Algebra I
- Herstein Topics in Algebra
- Laug Algebra
- Bosch Algebra
- Lorenz Einführung in die Algebra

Zur Vorlesung

Regelmäßige Teilnahme + Mitschreiben. Meine eigenen Notizen gibt es dann immer im www eingescannt (kein Skript).
Übungen: Regelmäßige Teilnahme, vorrechnen. Zwei Namen auf Hausaufgaben, wenn beide alles vorrechnen können.
Regelmäßige Abgabe + mindestens eine Aufgabe erfolgreich vorrechnen + 50+x % richtig $\Rightarrow$ Klausurzulassung.

1 Elementare Gruppentheorie

Erinnerung: eine **Verknüpfung** auf einer nicht leeren Menge X ist eine Abbildung

$$X \times X \to X, (x, y) \mapsto m(x, y).$$

Häufig schreibt man $m(x, y) = x \cdot y$ oder $m(x, y) = x + y$, je nach Kontext. Die Schreibweise $m(x, y) = x + y$ wird eigentlich nur für kommutative Verknüpfungen benutzt, d.h. wenn $\forall x, y \in X$ gilt $m(x, y) = m(y, x)$.

1.1 Definition Gruppe

Eine **Gruppe** $(G, \cdot)$ besteht aus einer Verknüpfung $\cdot$ auf einer nicht leeren Menge G, mit folgenden Eigenschaften:

(G1) Die Verknüpfung ist assoziativ, d.h. $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ gilt $\forall x, y, z \in G$.
(Folglich darf man Klammern weglassen.)

(G2) Es gibt ein neutrales Element $e \in G$, d.h. es gilt $e \cdot x = x \cdot e = x \ \forall x \in G$

(G3) Zu jedem $x \in G$ gibt es ein Inverses $y \in G$, d.h. $xy = e = yx$.
man schreibt dann auch $y = x^{-1}$ für das Inverse zu x.

Fordert man von der Verknüpfung nur (G1) und (G2), so spricht man von einer Halbgruppe mit Eins oder einem **Monoid**. Fordert man nur (G1), so spricht man von einer **Halbgruppe**.

1.2 Beispiel 1

- $(\mathbb{Z}, +), (\mathbb{Q}, +)$ sind kommutative Gruppen.
- $(\mathbb{Z}, \cdot), (\mathbb{N}, \cdot), (\mathbb{N}, +)$ sind Monoide.

1.3 Beobachtungen

a) Das Neutraleelement (einer Verknüpfung) ist eindeutig bestimmt: sind e, e' beides Neutralelemente, so folgt:

$$e = ee' = e'$$

b) Das Inverse zu x ist eindeutig bestimmt:

$$xy = e = xy' = y'x \Rightarrow y' = y'e = y'xy = ey = y$$

1.4 Lemma 1 (Sparsame Definition von Gruppen)

Sei $G \times G \to G$ eine assoziative Verknüpfung. Dann ist G schon eine Gruppe, wenn gilt:

(i) es gibt $e \in G$ so, dass $ex = x \ \forall x \in G$ gilt.

(ii) zu jedem $x \in G$ gibt es ein $y \in G$ mit $yx = e$

Beweis
Sei $yx = e$, es folgt $yxy = y$. Wähle z mit $zy = e$, es folgt

$$z \underbrace{yx}_{=e} y = zy = e \Rightarrow xy = e$$

Weiter gilt

$$xe = xyx = ex = x.$$

□

1.5 Beispiel 2

Sei X eine nicht leere Menge, sei $X^X = \{f : X \to X\}$ die Menge aller Abbildungen von X nach X. Als Verknüpfung auf X nehmen wir die Komposition von Abbildungen. Dann gilt wegen

$$f = \mathrm{id}_X \circ f = f \circ \mathrm{id}_X,$$

dass id_X ein Neutralelement ist.
Damit haben wir ein Monoid $(X_X, \circ)$.
Sei $\mathrm{Sym}(X) = \{f : X \to X \mid f \text{ bijektiv}\}$. Zu jedem $f \in \mathrm{Sym}(X)$ gibt es also eine Umkehrabbildung $g : X \to X$ mit

$$f \circ g = g \circ f = \mathrm{id}_X\,.$$

Folglich ist $(\mathrm{Sym}(X), \circ)$ eine Gruppe, die **Symmetrische Gruppe**. Wenn X endlich ist mit n Elementen, so gibt es genau $n! = n(n-1)(n-2)\cdots 2\cdot 1$ Permutationen, also hat $\mathrm{Sym}(X)$ dann genau $n!$ Elemente. Für $X = \{1, 2, 3, \ldots, n\}$ schreibt man auch $\mathrm{Sym}(X) = \mathrm{Sym}(n)\big(= S_n\big)$.

1.6 Definition zentralisieren

Sei $G \times G \to G$ eine Verknüpfung. Wir sagen, $x, y \in G$ vertauschen oder kommutieren oder x **zentralisiert** y, wenn gilt

$$xy = yx.$$

Eine Gruppe, in der alle Elemente vertauschen heißt kommutativ oder **abelsch**.

1.7 Beispiel 3

(a) $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{Q}^*, \cdot)$ sind abelsche Gruppen.

(b) K Körper, $G = Gl_2(K) = \{X \in K^{2\times 2} \mid \det(X) \neq 0\}$ Gruppe der invertierbaren 2×2 Matrizen.

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

$\Rightarrow$ nicht abelsch, genauso $Gl_n(K)$ für $n \geq 2$.

(c) $\mathrm{Sym}(2)$ ist abelsch, aber $\mathrm{Sym}(3)$ nicht. Allgemein ist $\mathrm{Sym}(X)$ nicht abelsch, falls $\#X \geq 3$ gilt.

1.8 Definition Untergruppe

Sei G eine Gruppe, sei $H \subseteq G$. Wir nennen H **Untergruppe** von G, wenn gilt:

(UG1) $e \in H$

(UG2) $x, y \in H \Rightarrow xy \in H$

(UG3) $x \in H \Rightarrow x^{-1} \in H$

Offensichtlich ist eine Untergruppe dann wieder eine Gruppe, mit der von G vererbten Verknüpfung.

Beispiel

(a) $(\mathbb{Q}, +)$. $\mathbb{Z}$ ist Untergruppe, denn $0 \in \mathbb{Z}$; $m, n \in \mathbb{Z} \Rightarrow m + n \in \mathbb{Z}$ und $n \in \mathbb{Z} \Rightarrow -n \in \mathbb{Z}$

(b) $(\mathbb{Q}^*, \cdot)$. $\mathbb{Z}^*$ ist keine Untergruppe, kein Inverses.

1.9 Lemma 2

Sei G eine Gruppe und sei U eine nicht leere Menge von Untergruppen von G. Dann ist auch

$$\bigcap U = \{g \in G \mid \forall H \in U \text{ gilt } g \in H\}$$

eine Untergruppe von G.

Beweis:
Für alle $H \in U$ gilt $e \in H$, also $e \in \bigcap U$. Angenommen $x, y \in \bigcap U$. Dann gilt für alle $H \in U$, dass $xy \in H$ sowie $x^{-1} \in H$. Es folgt $xy \in \bigcap U$ sowie $x^{-1} \in \bigcap U$. □

1.10 Definition $\langle X \rangle$

Sei G eine Gruppe und $X \subseteq G$ eine Teilmenge. Wir setzen:

$$\langle X \rangle = \bigcap \{H \subseteq G \mid H \text{ Untergruppe und } X \subseteq H\}$$

Ist nicht leer, da mindestens G enthalten ist.

- Es gilt z.B. $\langle \emptyset \rangle = \{e\}$, denn $\{e\}$ ist Untergruppe.
- Ist $H \subseteq G$ Untergruppe mit $X \subseteq H$, so folgt $X \subseteq \langle X \rangle \subseteq H$, insb. also $\langle H \rangle = H$.

Satz

Sei $X \subseteq G$ und sei

$$W = \{x_1 \cdot x_2, \cdots x_s \mid s \geq 1, x_i \in X \text{ oder } x_i^{-1} \in X \ \forall i = 1, \ldots, s\}.$$

Dann gilt:

$$\langle X \rangle = \{e\} \cup W.$$

Beweis:
Wegen $X \subseteq \langle X \rangle$ und $e \in \langle X \rangle$ folgt $\{e\} \cup W \subseteq \langle X \rangle$. Ist $f, g \in W$, so folgt $fg \in W$ sowie $f^{-1} \in W$, also ist $H = \{e\} \cup W$ eine Untergruppe von G, mit $X \subseteq H$. Es folgt

$$\langle X \rangle \subseteq H = \{e\} \cup W.$$

□

1.11 Definition zyklische Gruppe

Sei G eine Gruppe und sei $g \in G$. Für $n \geq 1$ setze $g^n = \underbrace{g \cdots g}_{n-mal}$ sowie $g^{-n} = \underbrace{g^{-1} \cdots g^{-1}}_{n-mal}$ und $g^0 = e$.
Dann gilt $\forall k, l \in \mathbb{Z}$, dass $g^k \cdot g^l = g^{k+l}$.
Sei $\langle g \rangle = \langle \{g\} \rangle \overset{1.10}{=} \{g^n | n \in \mathbb{Z}\}$. Man nennt $\langle g \rangle$ die von g erzeugte **zyklische Gruppe**. Wenn für ein $n \geq 1$ gilt $g^n = e$, so heißt n ein **Exponent** von g. Die **Ordnung** von g ist der kleinste Exponent von g,

$$o(g) = \min\left(\{n \geq 1 | g^n = 1\} \cup \{\infty\}\right)$$

$o(g) = \infty$ bedeutet: $g^n \neq e \ \forall n \geq 1$
$o(g) = 1$ bedeutet: $g^n = g = e$

1.12 Zyklische Gruppen

Eine Gruppe G heißt **zyklisch**, wenn es ein $g \in G$ gibt mit $G = \langle g \rangle$. Wegen $g^k g^l = g^{k+l} = g^{l+k} = g^l g^k$ gilt: zyklische Gruppen sind abelsch.

Satz

Sei $G = \langle g \rangle$ zyklisch mit $o(g) = n < \infty$. Dann gilt $\#G = n$ und $G = \{g, g^2, g^3, \ldots, g^n\}$.

Beweis:
Jedes $m \in \mathbb{Z}$ lässt sich schreiben als $m = kn+l$ mit $0 \leq l < n$ (Teilen mit Rest), also $g^m = \underbrace{g^{kn}}_{=e}.g^l = g^l$.

Es folgt $G \subseteq \{g, g^2, \ldots, g^n\}, g^n = g^0$. Ist $g^k = g^l$ für $0 \leq k \leq l < n$, so gilt $e = g^0 = g^{l-k}$, also $l - k = 0$ (wegen $l < n$), also $\#\{g, g^2, \ldots, g^n = g^0\} = n$. □

Folgerung

Ist G endlich mit $\#G = n$ und ist $h \in G$ mit $o(h) = n$, so folgt $\langle h \rangle = G$. Insbesondere ist dann G eine zyklische Gruppe.

1.13 Nebenklassen

Sei G eine Gruppe und sei H eine Untergruppe. Sei $a \in G$. Wir definieren:

$$aH = \{ah | h \in H\} \subseteq G$$

$$Ha = \{ha | h \in H\} \subseteq G$$

Man nennt aH die **Linksnebenklassen** von a bzgl. H (und Ha die **Rechtsnebenklassen**). In nicht abelschen Gruppen gilt im allgemeinen $aH \neq Ha$.

Lemma

Sei $H \subseteq G$ Untergruppe der Gruppe G und $a, b \in G$.
Dann sind äquivalent:

(i) $b \in aH$

(ii) $bH = aH$

(iii) $bH \cap aH \neq \emptyset$

Beweis:

- $(i) \Rightarrow (ii)$: $b \in aH \Rightarrow b = ah$ für ein $h \in H \Rightarrow bH = \{ahh' | h' \in H\}$ $\overset{H \text{ Untergruppe}}{=} \{ah'' | h'' \in H\} = aH$
- $(ii) \Rightarrow (iii)$: klar
- $(iii) \Rightarrow (i)$: Sei $g \in bH \cap aH,\ g = bh = ah' \Rightarrow b = ah'h^{-1} \in aH$, da H Untergruppe

□

Folgerung

Jedes $g \in G$ liegt in genau einer Linksnebenklasse bzgl. H, nämlich $g \in gH$. Entsprechendes gilt natürlich für Rechtsnebenklassen. Man setzt:
$G/H = \{gH \mid g \in G\}$ Menge der Linksnebenklasse, Rechtsnebenklassen analog.

Lemma

Sei $H \subseteq G$ Untergruppe der Gruppe G, sei $g \in G$.
Dann ist die Abbildung $H \to gH, h \mapsto gH$ bijektiv.

Beweis:
'Surjektiv' ist klar nach Definition von gH. Angenommen, $gh = gh' \Rightarrow h = g^{-1}gh' = h'$ □

1.14 Satz 1, Satz von Lagrange

Sei G eine Gruppe und $H \subseteq G$ eine Untergruppe. Wenn zwei der drei Mengen $G, H, G/H$ endlich sind, dann ist die dritte ebenfalls endlich und es gilt:

$$\#G = \#H \cdot \#G/H$$

Insbesondere ist dann $\#H$ eine **Teiler** von $\#G$.

Beweis:
Wenn G endlich ist, dann sind auch H und G/H endlich.
Angenommen, G/H und H sind endlich. Dann ist auch $G = \bigcup G/H = \bigcup\{gH \mid gH \in G/H\}$ endlich, da $\#gH = \#H$ nach 1.13.
Jetzt zählen wir genauer: sei $\#G/H = m; \#H = n$ etwa $G/H = \{g_1H, g_2H, \ldots, g_mH\}$.
$\#g_iH \overset{1.13}{=} n \qquad g_iH \cap g_jH = \emptyset$ für $i \neq j$ nach 1.13.

$$G = g_1H \cap g_2H \cap \cdots \cap g_mH \Rightarrow \#G = m \cdot n$$

□

Bemerkung

(1) Eine entsprechende Aussage gilt für Rechtsnebenklassen.

(2) Die Abbildung $G \to G, \quad g \mapsto g^{-1}$ bildet die Linksnebenklassen bijektiv auf die Rechtsnebenklassen ab:

$$(gH)^{-1} = \{(gh)^{-1} \mid h \in H\} \overset{\text{Achtung!}}{=} \{h^{-1}g^{-1} \mid h \in H\} = \{hg^{-1} \mid h \in H\} = Hg^{-1} \qquad \text{(ÜA)}$$

Korollar A (Lagrange)

Sei G eine endliche Gruppe und sei $g \in G$. Dann teilt $o(g)$ die Zahl $\#G$.

Beweis:
Da G endlich ist, folgt $o(g) < \infty$. Nach dem Satz von Lagrange ist $\#\langle g\rangle = o(g)$ ein Teiler von $\#G$. □

Korollar B

Sei G eine endliche Gruppe, sei p eine **Primzahl** (d.h. die einzigen Teiler von p sind 1 und p) und $p > 1$. Wenn gilt $\#G = p$, dann ist G zyklisch. Für jedes $g \in G \backslash \{e\}$ gilt $\langle g \rangle = G$.

Beweis:
Sei $g \in G\backslash\{e\}$. Dann ist $o(g) > 1$ und $o(g)$ teilt p. Es folgt $o(g) = p$, also $G = \langle g \rangle$ vgl. 1.12. □

Für endliche Gruppen sind Teilbarkeitseigenschaften wichtig, wie wir sehen werden.
Die Zahl $\#^G/_H := [G : H]$ nennt man auch den **Index von H in G**.

Wichtige Rechenregeln in Gruppen

(a) Man darf kürzen

$$ax = ay \Rightarrow x = y$$
$$xa = ya \Rightarrow x = y$$

(multipliziere beide Seiten von links/rechts mit a^{-1})

(b) Es gilt $(x^{-1})^{-1} = x$ $(x^{-1}x = e = xx^{-1} \Rightarrow (x^{-1})^{-1} = x)$

(c) Beim Invertieren muss die Reihenfolge umgedreht werden:

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

(in abelschen Gruppen gilt natürlich damit $(ab)^{-1} = a^{-1}b^{-1}$)

1.15 Homomorphismen

Seien G, K Gruppen. Eine Abbildung $\varphi : G \to K$ heißt **(Gruppen-)Homomorphismus**, wenn $\forall x, y \in G$ gilt

$$\varphi \underbrace{(x \cdot y)}_{\text{Verküpfung in G}} = \underbrace{\varphi(x)\varphi(y)}_{\text{Verknüpfung in K}}$$

Beispiel

(a) $\mathrm{id}_G : G \to G$ ist Homomorphismus

(b) $H \subseteq G$ Untergruppe $i : H \hookrightarrow G, \quad h \mapsto h$ Inklusion, ist Homomorphismus.

(c) $(G, \cdot) = (\mathbb{Z}, +),\ m \in \mathbb{Z},\ \varphi : \mathbb{Z} \to \mathbb{Z},\ x \mapsto mx$ ist Homomorphismus, denn $\phi(x+y) = m(x+y) = mx + my = \varphi(x) + \varphi(y)$

(d) G Gruppe, $a \in G,\ a \neq e,\ \lambda_a(x) = ax$.
$\lambda : G \to G$ ist kein Homomorphismus, denn $\lambda_a(e) = a,\ \lambda(ee) = a$, aber $\lambda_a(e)\lambda_a(e) = aa \neq a$.

Lemma

Sei $\varphi : G \to K$ ein Homomorphismus von Gruppen. Dann gilt $\varphi(e_G) = e_K$ und $\varphi(x^{-1}) = \varphi(x)^{-1}\ \forall x \in G$. ($e_G$ Neutralelement in G und e_K Neutralelement in K)
Beweis:

$$\varphi(e_G) = \varphi(e_G \cdot e_G) = \varphi(e_G) \cdot \varphi(e_G) \overset{\text{kürzen}}{\Rightarrow} e_K = \varphi(e_G)$$

$$e_K = \varphi(e_G) = \varphi(x^{-1}x) = \varphi(x^{-1})\varphi(x) \Rightarrow \varphi(x)^{-1} = \varphi(x^{-1})$$

□

Achtung: $\varphi(x)^{-1}$ ist das Inverse in K von $\varphi(x)$ nicht die Umkehrabbildung!

Das **Bild** eines Homomorphismus $\varphi : G \to K$ ist $\varphi(G) \subseteq K$,
der **Kern** ist $\ker(\varphi) = \{x \in G \mid \varphi(x) = e_K\} \subseteq G$

1.16 Satz 2, Gruppenhomomorphismen

Bild und Kern von Gruppenhomomorphismen sind Untergruppen.

Beweis:
Setze $H = \varphi(G) \subseteq K$. Es folgt $e_K \in H$. Für $\varphi(x), \varphi(y) \in H$ gilt $\varphi(x)\varphi(y) = \varphi(xy) \in H$ sowie $\varphi(x)^{-1} = \varphi(x^{-1}) \in H$, also ist H Untergruppe. Betrachte jetzt $\ker(\varphi) \subseteq G$. Es gilt $\varphi(e_G) = e_K$, also $e_G \in \ker(\varphi)$. Ist $x, y \in \ker(\varphi)$, so folgt

$$\varphi(xy) = \varphi(x)\varphi(y) = e_K \cdot e_K = e_K \text{ , also } xy \in \ker(\varphi)$$

$$\varphi(x^{-1}) = \varphi(x)^{-1} = e_K^{-1} = e_K \text{ , also } x^{-1} \in \ker(\varphi)$$

□

Bemerkung

Jede Untergruppe von $H \subseteq G$ ist Bild eine geeigneten Homomorphismus (nämlich der Inklusion $H \hookrightarrow G$). Wir werden sehen, dass im allgemeinen nicht jede Untergruppe $H \subseteq G$ Kern eines Homomorphismus ist.

1.17 Normalteiler

Sei G eine Gruppe und $N \subseteq G$ eine Untergruppe. Wir nennen N **normal** in G oder **Normalteiler** in G, wenn eine der folgenden äquivalenten Bedingungen erfüllt ist:

(i) für alle $a \in G$ gilt $aN = Na$ (Rechtsnebenklassen sind Linksnebenklassen)

(ii) für alle $a \in G$ gilt $aNa^{-1} = N$, $(aNa^{-1} = \{ana^{-1} \mid n \in N\})$

(iii) für alle $a \in G$ gilt $aN \subseteq Na$

(iv) für alle $a \in G$ gilt $aNa^{-1} \subseteq N$

Beweis:
(i) und (ii) sind äquivalent: multipliziere von rechts mit a^{-1} bzw. a. Genauso sind (iii) und (iv) äquivalent.
Klar: (ii) $\Rightarrow$ (iv) (✓)
Zeige (iv) $\Rightarrow$ (ii): Setze $b = a^{-1}$, es folgt aus (iv), dass $bNb^{-1} \subseteq N \rightsquigarrow N \subseteq b^{-1}Nb = aNa^{-1}$. Also gilt für alle $a \in G$, dass $N \subseteq aNa^{-1}$ und $aNa^{-1} \subseteq N$, damit gilt (ii). □

Lemma

Ist $\varphi : G \to K$ ein Homomorphismus von Gruppen, dann ist $\ker(\varphi)$ ein Normalteiler in G.

Beweis:
Sei $N = \ker(\varphi) = \{n \in G \mid \varphi(n) = e\}$, sei $a \in G$. Dann gilt

$$\varphi(ana^{-1}) = \varphi(a)\underbrace{\varphi(n)}_{=e}\varphi(a^{-1}) = \varphi(a)\varphi(a^{-1}) = e$$

also gilt $aNa^{-1} \subseteq N \quad \forall a \in G$. □

Achtung:
Bilder von Homomorphismen sind nicht immer Normalteiler, nach Beispiel 1.15 (b) ist jede Untergruppe Bild eines Homomorphismus, aber nicht jede Untergruppe ist normal.

Beispiel

$G = \mathrm{Sym}(3)$, $g = (1,2)$ Transposition, die 1 und 2 vertauscht. $g^2 = id$, $\langle g \rangle = \{g, id\} \subseteq \mathrm{Sym}(3)$ ist Untergruppe, aber für $h = (2,3)$ gilt

$$h\langle g \rangle h^{-1} = \{hgh^{-1}, h\,\mathrm{id}\,h^{-1}\} = \{\underbrace{(2,3)(1,2)(2,3)}_{=(3,1)}, id\} \not\subseteq \langle g \rangle$$

also ist $\langle g \rangle$ kein Normalteiler in $\mathrm{Sym}(3)$.

Schreibweise: Ist $N \subseteq G$ ein Normalteiler, schreibt man kurz $N \trianglelefteq G$

Beachte: Ist G abelsch, dann sind alle Untergruppen $H \subseteq G$ automatisch normal.

1.18 Definition Teilmengen assoziativ

Für Teilmengen $X, Y, Z \subseteq G$ in einer Gruppe schreibe kurz:

$$XY = \{xy \mid x \in X,\ y \in Y\} \subseteq G$$
$$X^{-1} = \{x^{-1} \mid x \in X\} \subseteq G$$

Es gilt dann $(XY)Z = X(YZ)$, (weil die Verknüpfung assoziativ ist).

Satz

Sei $N \trianglelefteq G$ Normalteiler in der Gruppe G. Dann ist ${}^{G}/_{N} = \{gN \mid g \in G\}$ eine Gruppe mit der Verknüpfung $(gN) \cdot (hN) = ghN$
Das Neutralelement ist $eN = N$, das Inverse zu gN ist $g^{-1}N$.

Beweis:
Da N Normalteiler ist, gilt für $g, h \in G$

$$gNhN = g(Nh)N \overset{1.17}{=} g(hN)N = ghNN \overset{N \text{ Gruppe}}{=} ghN$$

Die Verknüpfung ist also einfach gegeben durch

$$gN \cdot hN = gNhN = ghN$$

und damit assoziativ nach obiger Bemerkung. Es gilt $NgN = gNN = gN = gNN$, also ist N ein Neutralelement. Weiter gilt:

$$gNg^{-1}N = gg^{-1}N = N = g^{-1}gN = g^{-1}NgN$$

□

1.19 Definition π_H

Ist G eine Gruppe und H eine Untergruppe, so definieren wir $\pi_H : G \to {}^{G}/_{H}$ durch $\pi_H(g) = gH$.

Satz

Ist $N \trianglelefteq G$ ein Normalteiler, dann ist $\pi_N : G \to {}^G\!/_N$ ein surjektiver Homomorphismus mit Kern

$$N = \ker(\pi_N)$$

Beweis:
π_N ist nach Definition surjektiv und

$$\pi_N(gh) = ghN = gNhN = \pi_N(g)\pi_N(h)$$

Weiter gilt

$$\pi_N(g) = N \iff gN = N \overset{1.13}{\iff} g \in N$$

□

Folgerung: Jeder Normalteiler ist auch ein Kern eines Homomorphismus.

1.20 Der Homomorphiesatz

Sei $G \overset{\varphi}{\to} K$ ein Homomorphismus von Gruppen, sei $N \trianglelefteq G$ ein Normalteiler. Wenn gilt $N \subseteq \ker(\varphi)$, dann gibt es genau einen Homomorphismus $\overline{\varphi} : {}^G\!/_H \to K$ mit $\overline{\varphi} \circ \pi_H = \varphi$.

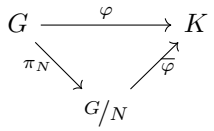


Abbildung 1: Homomorphiesatz

Beweis:
Existenz von $\overline{\varphi}$:
Für $g \in G$ setze $\overline{\varphi}(gN) = \varphi(g)$. Das ist eine wohldefinierte Abbildung, denn angenommen,

$$gN = g'N \Rightarrow g^{-1}g' \in N \subseteq \ker(\varphi) \Rightarrow \varphi(g^{-1}g') = e \Rightarrow \varphi(g) = \varphi(g')$$

Es gilt damit

$$\overline{\varphi}(gNhN) = \overline{\varphi}(ghN) = \varphi(gh) = \varphi(g)\varphi(h) = \overline{\varphi}(gN)\overline{\varphi}(hN)$$

also ist $\overline{\varphi}$ ein Homomorphismus.

Eindeutigkeit von $\overline{\varphi}$:
Sei $\psi : {}^G\!/_N \to K$ ein Homomorphismus mit $\psi \circ \pi_N = \varphi$.
Es folgt

$$\psi(gN) = \psi(\pi_N(g)) = \varphi(g) = \overline{\varphi}(gN) \quad \forall g \in G$$

Bemerkung

In der Situation vom Homomorphiesatz gilt:

(i) $\ker(\varphi) = \pi_N^{-1}\ \ker(\overline{\varphi})$

(ii) $\ker(\overline{\varphi}) = \pi_N\ \ker(\varphi)$

(iii) $\varphi(G) = \overline{\varphi}({}^G\!/_N)$

Beweis:
(iii) ist klar nach Konstruktion, $\overline{\varphi}(gN) = \varphi(g)$
(ii) $\overline{\varphi}(gN) = e = \varphi(g) \Leftrightarrow g \in \ker(\varphi)$, also $\ker(\overline{\varphi}) = \pi_N(\ker(\varphi))$
(i) $\varphi(g) = e \Rightarrow g \in \ker(\varphi) \Rightarrow \pi_N(g) \in \ker(\overline{\varphi}) \Rightarrow \varphi(g) = e$ □

1.21 Definition Isomorphismus

Ein Gruppenhomomorphismus $\varphi : G \to K$ heißt **Mono/Epi/Isomorphismus**, wenn φ injektiv/surjektiv/bijektiv ist.
(Klar: φ Epimorphismus $\Leftrightarrow \varphi(G) = K$)
Für einen Mono / Epi / Isomorphismus schreibt man auch:
$\overset{\varphi}{\rightarrowtail}$ $\overset{\varphi}{\twoheadrightarrow}$ und $\overset{\cong}{\to}$.

Lemma

Ein Gruppenhomomorphismus $G \overset{\varphi}{\to} K$ ist genau dann injektiv, wenn gilt $\ker(\varphi) = \{e_G\}$.

Beweis:
Wenn φ injektiv ist, dann ist $\ker(\varphi) = \{e_G\}$ (klar). Angenommen, $\ker(\varphi) = \{e_G\}$ und $a, b \in G$ mit $\varphi(a) = \varphi(b) \rightsquigarrow \varphi(a)\varphi(b)^{-1} = \varphi(ab^{-1}) = e_K \Rightarrow ab^{-1} = e_G \Rightarrow a = b$ □

1.22 Satz 3, Eigenschaften von Gruppenhomomorphismen

Sei $G \overset{\varphi}{\to} K$ ein Gruppenhomomorphismus. Dann gilt folgendes:

(i) Ist $H \subseteq G$ Untergruppe, so ist $\varphi(H) \subseteq K$ Untergruppe. Wenn $H \trianglelefteq G$, so gilt $\varphi(H) \trianglelefteq \varphi(G)$

(ii) Ist $L \subseteq K$ Untergruppe, so ist $\varphi^{-1}(L) \subseteq G$ Untergruppe. Ist $L \trianglelefteq K$, so gilt $\varphi^{-1}(L) \trianglelefteq G$. L Urbild unter φ

Beweis:

(i) Sei $a, b \in H$ und $g \in G$. Es gilt $\varphi(a)\varphi(b) = \varphi(ab) \in H$, $\varphi(a)^{-1} = \varphi(a^{-1}) \in \varphi(H)$. $\varphi(e_G) = e_K \in \varphi(H) \Rightarrow \varphi(H)$ Untergruppe.
Ist $H \trianglelefteq G$, so folgt $\varphi(g)\varphi(H)\varphi(g)^{-1} = \varphi(gHg^{-1}) \overset{H \trianglelefteq G}{=} \varphi(H)$ □

(ii) Sei $a, b \in \varphi^{-1}(L)$, $g \in G$ (also $\varphi(a), \varphi(b) \in L$). Es folgt $\varphi(ab) \in L$, $\varphi(a^{-1}) = \varphi(a)^{-1} \in L$ und $\varphi(e_G) = e_K \Rightarrow ab, a^{-1}, e_G \in \varphi^{-1}(L) \rightsquigarrow$ Untergruppe.
Angenommen, $L \trianglelefteq K$.
Es folgt $\varphi(gag^{-1}) = \varphi(g)\varphi(a)\varphi(g^{-1}) \in L$, also $g\varphi^{-1}(L)g^{-1} \subseteq \varphi^{-1}(L)$. □

Beispiele

Gruppe $(\mathbb{Z}, +)$, $\varphi : \mathbb{Z} \to \mathbb{Z}$ Homomorphismus, $\varphi(z) = m \cdot z$, $m \in \mathbb{Z}$ fest.
$\varphi(\mathbb{Z}) = m\mathbb{Z} = \{mz \mid z \in \mathbb{Z}\} = (-m)\mathbb{Z}$
z.B. $m = 2 \rightsquigarrow 2\mathbb{Z} = \{0, \pm 2, \pm 4, \pm 6, \dots\}$ gerade Zahlen
$\ker(\varphi) = \begin{cases} \{0\}, & \text{wenn } m \neq 0 \\ \mathbb{Z}, & \text{wenn } m = 0. \end{cases}$ φ surjektiv $\Leftrightarrow \quad m = \pm 1$
φ injektiv $\Leftrightarrow \quad m \neq 0$

Angenommen, $m > 0$, $a, b \in \mathbb{Z}$
$a + m\mathbb{Z} = b + m\mathbb{Z}$ Nebenklassen $\overset{1.13}{\Leftrightarrow} a \in b + m\mathbb{Z} \Leftrightarrow a - b \in m\mathbb{Z}$
Folglich $\mathbb{Z}/_{m\mathbb{Z}} = \{m\mathbb{Z}, 1 + m\mathbb{Z}, 2 + m\mathbb{Z}, \dots, (m-1) + m\mathbb{Z}\}$ insbesondere $\#\mathbb{Z}/_{m\mathbb{Z}} = m$.
Schreibe $\overline{k} = k + m\mathbb{Z}$ **Kongruenzklasse** von k **modulo** m.
$\mathbb{Z}/_{m\mathbb{Z}} = \{\overline{0}, \overline{1}, \dots, \overline{m-1}\}$ wird erzeugt von $\overline{1} \rightsquigarrow \mathbb{Z}/_{m\mathbb{Z}} = \langle\overline{1}\rangle$ zyklische Gruppe der Ordnung m. $o(\overline{1}) = m$.
Später mehr dazu.

1.23 Die Isomorphiesätze

Lemma

Sei G eine Gruppe, seien $H, N \subseteq G$ Untergruppen. Wenn $N \trianglelefteq G$ gilt, dann ist $HN = NH \subseteq G$ eine Untergruppe.

Beweis:
Es gilt $e = e \cdot e \in N \cdot H$. Weiter gilt für $h_1, h_2 \in H,\ n_1, n_2 \in N$, dass

$$h_1 n_1 h_2 n_2 = \underbrace{h_1 h_2}_{\in H} \underbrace{h_2^{-1} n_1 h_2}_{\in N} n_2 \in HN$$

$$(h_1 n_1)^{-1} = n_1^{-1} h_1^{-1} = h_1^{-1} \underbrace{h_1 n_1^{-1} h_1^{-1}}_{\in N} \in HN$$

$$(HN)^{-1} = N^{-1} H^{-1} = NH \subseteq HN \text{ genauso } HN \subseteq NH$$

□

Satz

Sei $G \xrightarrow{\varphi} K$ ein Epimorphismus von Gruppen. Sei $N = \ker(\varphi)$. Dann ist die Abbildung $\overline{\varphi} : {}^{G}\!/_{N} \to K$ aus dem Homomorphisatz 1.20 ein Isomorphismus.

Beweis:
$\overline{\varphi}({}^{G}\!/_{N}) = \varphi(G)$ und $\ker(\overline{\varphi}) = \{N\}$ nach dem Beweis von 1.20. Den Isomorphismus $\overline{\varphi} : {}^{G}\!/_{\ker(\varphi)} \xrightarrow{\cong} K$ nennt man **kanonisch** oder **natürlich**. □

Theorem: 1. Isomorphiesatz

Sei G eine Gruppe, seien $H, N \subseteq G$ Untergruppen mit $N \trianglelefteq G$. Dann gilt $H \cap N \trianglelefteq H$, $N \trianglelefteq NH$ und die Abbildung

$$\begin{aligned} {}^{H}\!/_{H \cap N} &\to {}^{NH}\!/_{N} \\ aH &\mapsto aNH \end{aligned}$$

ist ein Isomorphismus. ("Kürzungsregel")

Beweis:
Für alle $h \in H$ gilt $h(H \cap N)h^{-1} \subseteq N \cap H$, weil $N \trianglelefteq G$ und $hHh^{-1} = H$. $\Rightarrow N \cap H \trianglelefteq H$. Für alle $g \in NH$ gilt $gNg^{-1} \subseteq N \Rightarrow N \trianglelefteq NH$ □

Lemma

Sei $G \xrightarrow{\varphi} K$ ein Gruppenhomomorphismus. Dann sind äquivalent:

(i) φ ist bijektiv

(ii) es gibt ein Homomorphismus $\psi : K \to G$ mit $\varphi \circ \psi = \mathrm{id}_K$ und $\psi \circ \varphi = \mathrm{id}_G$.

Beweis:
(ii)⇒(i): klar, aus $\varphi \circ \psi = \mathrm{id}_K$ folgt, dass φ surjektiv ist und aus $\varphi \circ \psi = \mathrm{id}_G$ folgt, dass φ injektiv ist.

(i)⇒(ii): Sei $\psi : K \to G$ die eindeutig bestimmte Umkehrabbildung, also $\varphi \circ \psi = \mathrm{id}_K$ und $\psi \circ \varphi = \mathrm{id}_G$. Für $a, b \in K$ folgt

$$\psi(ab) = \psi(\varphi\psi(a)\varphi\psi(b)) \overset{\varphi \text{ Homo.}}{=} \underbrace{\psi(\varphi}_{\mathrm{id}}(\psi(a)\psi(b))) = \psi(a)\psi(b)$$

□

Betrachte die Abbildung $\varphi : H \to {}^{HN}/_{N} \subseteq {}^{G}/_{N},\ h \mapsto hN$ das ist ein Homomorphismus, weil $H \overset{i}{\to} G \overset{\pi_N}{\to} {}^{G}/_{N}$ ein Homomorphismus ist. Für $hn \in HN$ gilt

$$\varphi(h) = hN = hnN$$

also ist φ ein Epimorphismus. Der Kern ist $\ker(\varphi) = \{h \in H \mid hN = N\} = H \cap N$. Also gilt nach dem vorigem Satz

$${}^{H}/_{n\cap H} \underset{\cong}{\overset{\overline{\varphi}}{\to}} {}^{HN}/_{N}$$

□

Theorem: 2. Isomorphiesatz

Sei G Gruppe, seien $M, N \trianglelefteq G$ Normalteiler mit $M \subseteq N \subseteq G$. Dann gilt ${}^{N}/_{M} \trianglelefteq {}^{G}/_{M}$ und

$${}^{{}^{G}/_{M}}/_{{}^{N}/_{M}} \cong {}^{G}/_{N} \qquad \text{'Kürzungsregel'}$$

Beweis:
Es gilt ${}^{N}/_{M} = \{nM \mid n \in N\} = \pi_M(N) \subseteq {}^{G}/_{M}$
Nach 1.22(i) gilt ${}^{N}/_{M} \trianglelefteq {}^{G}/_{M}$.
Jetzt Homomorphiesatz 1.20

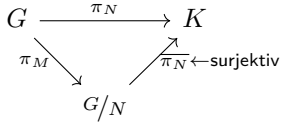


Abbildung 2: 2. Isomorphiesatz

Nach dem vorigen Satz gilt:

$${}^{{}^{G}/_{M}}/_{\ker(\overline{\pi_N})} \overset{\cong}{\to} {}^{G}/_{N}$$

$$\ker(\overline{\pi_N}) \overset{1.20}{=} \pi_M(N) = {}^{N}/_{M}$$

□

1.24 Produkte von Gruppen

Seien G, K zwei Gruppen. Dann ist das Produkt $G \times K$ wieder eine Gruppe, das **direkte Produkt**, mit Verknüpfung

$$(g_1, k_1) \cdot (g_2, k_2) = (g_1 g_2, k_1 k_2)$$

$$\text{Neutralelement } e = (e_G, e_K)$$

$$\text{Das Inverse zu } (g, k) \in G \times K \text{ ist } (g, k)^{-1} = (g^{-1}, k^{-1})$$

Den Beweis lassen wir weg, die Gruppenaxiome (G1)-(G3) sind leicht zu prüfen.
Wir haben kanonische Homomorphismen:

$$i_G : G \to G \times K \qquad i_K : K \to G \times K$$
$$g \mapsto (g, e_K) \qquad k \mapsto (e_G, k)$$

sowie

$$pr_G : G \times K \to G, \quad (g,k) \mapsto g$$
$$pr_K : G \times K \to K, \quad (g,k) \mapsto k$$

mit

$$pr_G \circ i_G = \mathrm{id}_G \qquad pr_K \circ i_K = \mathrm{id}_K$$
$$\ker(pr_G) = \{e_G\} \times K \cong K \qquad \ker(pr_K) = G \times \{e_K\} \cong G$$

Das geht auch mit Familien von (endliche vielen) Gruppen: ist $(G_i)_{i\in I}$ eine Familie von Gruppen, so ist $\prod_{i\in I} G_i$ wieder eine Gruppe, das **direkte Produkt** der G_i. Die Elemente sind Folgen $(g_i)_{i\in I},\ g_i \in G_i$ mit Verknüpfung $(g_i)_{i\in I} \cdot (g_i')_{i\in I} = (g_i g_i')_{i\in I}$ usw.

Satz

Sei G eine Gruppe mit Untergruppen $H, K \subseteq G$. Angenommen, es gilt folgendes

(i) $G = HK$

(ii) $H \cap K = \{e\}$

(iii) $hk = kh \quad \forall h \in H,\ k \in K$

Dann ist die Abbildung $H \times K \xrightarrow{\varphi} G$, $(h,k) \mapsto hk$ ein Isomorphismus, d.h. G 'ist' das direkte Produkt aus H und K.

Beweis:
Wegen (iii) gilt

$$\varphi((h_1,k_1)(h_2,k_2)) = \varphi(h_1h_2, k_1k_2) = h_1h_2k_1k_2$$
$$\varphi(h_1,k_1)\varphi(h_2,k_2) = h_1k_1h_2k_2 = h_1h_2k_1k_2$$

also ist φ ein Homomorphismus. Wegen (i) ist φ surjektiv.

$$(h,k) \in \ker(\varphi) \Leftrightarrow hk = e \Leftrightarrow \underbrace{h}_{\in H} = \underbrace{k^{-1}}_{\in K} \Leftrightarrow h = k = e \text{ wegen (ii)}$$

□

Beispiel

$G = \mathbb{Z}/6\mathbb{Z} = \{\overline{0}, \ldots, \overline{5}\}$ vgl. 1.22. Dann sind $H = \{\overline{0}, \overline{3}\}$ sowie $K = \{\overline{0}, \overline{2}, \overline{4}\}$ Untergruppen (nachrechnen!), $H \cong \mathbb{Z}/2\mathbb{Z},\ K \cong \mathbb{Z}/3\mathbb{Z}$ und (i),(ii),(iii) aus dem vorigen Satz sind erfüllt. Es folgt

$$\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

2 Gruppenwirkungen und Sylow-Sätze

2.1 Gruppenwirkungen

Sei G eine Gruppe und X eine nicht leere Menge. Eine **Wirkung** von G auf X (auch: G-**Wirkung**, 'G-**Aktion**') ist ein Homomorphismus $\alpha : G \to \mathrm{Sym}(X)$. Für $g \in G$ und $x \in X$ schreibe kurz

$$g(x) = \alpha(g)(x)$$

(wenn klar ist welches α gemeint ist). Die Abbildung $G \times X \to X,\ (g, x) \mapsto g(x)$ erfüllt folgende Eigenschaften:

(W1) $e(x) = x,\ \forall x \in X$ ($e \in G$ Neutralelement)

(W2) $(a \circ b)(x) = a(b(x)),\ \forall a, b \in G,\ x \in X$

Ist umgekehrt eine Abbildung $G \times X \to X$ gegeben die (W1) und (W2) erfüllt, so erhalten wir eine Wirkung $\alpha : G \to \mathrm{Sym}(X)$ durch

$$\alpha(g) = [x \mapsto g(x)]$$

denn aus (W2) folgt: $\alpha(g^{-1})$ ist Inverse zu $\alpha(g)$, also ist die Abbildung $\alpha(g) : X \to X$ bijektiv und $\alpha : G \to \mathrm{Sym}(X)$ ist ein Homomorphismus nach (W2).

2.2 Mehrere Definitionen

Gegeben sei eine G-Wirkung $G \times X \to X$. Für $x \in X$ ist der **Stabilisator** (die **Standgruppe**)

$$G_x = \{g \in G \mid g(x) = x\} \subseteq G$$

Die **Bahn** (der **Orbit**) von x ist

$$G(x) = \{g(x) \mid g \in G\} \subseteq X$$

Der Kern der Wirkung ist $\bigcap\limits_{x \in X} G_x \subseteq G$.

Satz

Der Stabilisator G_x ist eine Untergruppe und der Kern ist ein Normalteiler.

Beweis:
Es gilt $e(x) = x \rightsquigarrow e \in G_x$. Für $a, b \in G_x$ gilt

$$(ab)(x) = a(\underbrace{b(x)}_{=x}) = a(x) = x \rightsquigarrow ab \in G_x$$

$$a^{-1}(x) = a^{-1}(\underbrace{a(x)}_{=x}) = (a^{-1}a)(x) = e(x) = x \rightsquigarrow a^{-1} \in G_x$$

Also ist $G_x \subseteq G$ Untergruppe.
Es gilt:

$$\bigcap_{x \in X} G_x = \{g(x) = x \mid \forall x \in X\}$$

Das ist genau der Kern der zugehörigen Homomorphie $\alpha : G \to \mathrm{Sym}(X)$, also ein Normalteiler. □

2.3 Beispiel 4, Wirkungen

(a) Sei G eine Gruppe. Für $g \in G$ definiere eine Abbildung $\lambda_g : G \to G$ durch $\lambda_g(x) = gx$. Es folgt

$$\lambda_g \circ \lambda_h = \lambda_{gh} \quad \lambda_e = \mathrm{id}_G \rightsquigarrow \lambda_g \lambda_{g^{-1}} = \mathrm{id}_G = \lambda_{g^{-1}} \lambda_g$$

also $\lambda_g \in \mathrm{Sym}(G)$. Die Gruppe G wirkt also auf der Menge $G = X$. Es gilt für die Wirkung:

$$G_x = \{g \in G \mid \lambda_g(x) = x\} = \{g \in G \mid gx = x\} = \{e\}$$

Zu $x, y \in G$ gibt es genau ein $g \in G$ mit $\lambda_g(x) = y$, nämlich $g = yx^{-1}$.
Man nennt das die **Linksreguläre Wirkung** von G auf sich.

(b) Sei G eine Gruppe und $H \subseteq G$ Untergruppe. Sei $X = {}^G\!/_H = \{aH \mid a \in G\}$. Die Gruppe G wirkt auf X durch

$$\lambda_g : {}^G\!/_H \to {}^G\!/_H,\ aH \mapsto gaH$$

Es gilt wieder $\lambda_g \lambda_h = \lambda_{gh},\ \lambda_e = \mathrm{id}_{G/H}$.
Der Stabilisator von $x = H \in X$ ist

$$G_x = \{g \in G \mid gH = H\} = H$$

Zu $x = aH, y = bH \in X$ gibt es wieder $g \in G$ mit $g(x) = y$, nämlich $g = ba^{-1}$. Anders als im Bsp(a) ist g nicht eindeutig, falls $H \neq \{e\}$ gilt (für $H = \{e\}$ erhalten wir wieder Bsp(a)).

2.4 Satz 4, Satz von Cayley

Zu jeder Gruppe G gibt es eine Menge X und einen injektiven Homomorphismus $\alpha : G \to \mathrm{Sym}(X)$.

Beweis:
Setze $G = X$ und $\lambda : G \to \mathrm{Sym}(X)$ wie in Beispiel 2.3(a). □
Eine Untergruppe von $\mathrm{Sym}(X)$ nennt man auch eine **Permutationsgruppe**. Der Satz von Cayley wird auch so formuliert:
Jede Gruppe 'ist' (bis auf Isomorphie) eine Permutationsgruppe.

2.5 Definition transitiv

Eine G-Wirkung $G \times X \to X$ heißt **transitiv**, wenn es für alle $x, y \in X$ ein $g \in G$ gibt mit $g(x) = y$.
Die in Bsp. 2.3(a)(b) betrachteten Wirkungen sind also transitiv.

Satz

Gegeben sei ein transitive G-Wirkung $G \times X \to X$. Sei $x \in X$ und $H = G_x$. Dann ist die Abbildung ${}^G\!/_H \to X,\ gH \mapsto g(x)$ wohldefiniert und bijektiv. Für jedes $y \in X$ mit $y = g(x)$ gilt $G_y = gG_xg^{-1}$.

Beweis:
Betrachte die Abbildung $\epsilon : G \to X, \epsilon(g) = g(x)$. Es gilt

$$\epsilon(g) = \epsilon(g') \Leftrightarrow g(x) = g'(x) \Leftrightarrow g^{-1}g'(x) = x \Leftrightarrow g^{-1}g' \in G_x = H \overset{1.13}{\Leftrightarrow} g'H = gH$$

Damit ist die erste Behauptung gezeigt.
Für $y = g(x)$ gilt

$$a(y) = y \Leftrightarrow ag(x) = g(x) \Leftrightarrow g^{-1}ag(x) = x \Leftrightarrow g^{-1}ag \in G_x \Leftrightarrow a \in gG_xg^{-1}$$

□

2.6 Bahnen

Gegeben sei eine G-Wirkung $G \times X \to X$.

Lemma

Für **Bahnen** $G(x),\ G(y) \subseteq X$ gilt stets:

$$\text{Ist } G(x) \cap G(y) \neq \emptyset, \text{ so gilt } G(x) = G(y)$$

Bahnen sind entweder disjunkt oder gleich.

Beweis:
Angenommen, $z \in G(x) \cap G(y)$, also $z = a(x) = b(y)$ für $a, b \in G$. Es folgt $b^{-1}a(x) = y$, also $y \in G(x)$, also $G(y) \subseteq G(x)$. Genauso folgt auch $G(y) \supseteq G(x)$, also $G(x) = G(y)$. □

Bemerkung

Für jedes $x \in X$ wirkt G transitiv auf der Bahn $G(x) \subseteq X$. Denn für $y, z \in G(x),\ y = a(x)$ und $z = b(x)$ folgt

$$x = a^{-1}(y) \rightsquigarrow z = ba^{-1}(y)$$

Weiter gilt $g(y) = ga(x) \in G(x)$.

Definition Bahnenraum

Die Menge der Bahnen bezeichnen wir mit ${}_G\backslash^X = \{G(x) \mid x \in X\}$ 'Bahnenraum'.

Bemerkung

Das passt zur Notation für Nebenklassen: Gegeben sei eine Untergruppe $H \subseteq G$. Setze $X = G$, dann wirkt H auf $G = X$ durch $H \times X \to X,\ (h, x) \mapsto hx$
Die **Länge** einer Bahn $G(x)$ ist $\#G(x)$. Ist $\{x\} = \{G\}$ (Bahn der Länge 1), so sagt man, dass $x \in X$ ein **Fixpunkt** der G-Wirkung auf X ist. Für alle $g \in G$ gilt dann $g(x) = x$.
Die Bahnen der Wirkung von H auf G sind dann genau die Rechtsnebenklassen, $H(x) = Hx$ für $x \in X = G$, die Bahnenmenge ist also

$${}_H\backslash^G = \{Hx \mid x \in G\}$$

2.7 Satz 5, Die Bahnengleichung

Gegeben sei eine G-Wirkung $G \times X \to X$. Ein **Schnitt** (ein **Transversale**) ist eine Teilmenge $S \subseteq X$ mit folgender Eigenschaft: für jedes $x \in X$ gilt $\#(S \cap G(x)) = 1$, jede Bahn trifft S genau einmal. Es folgt $\#S = \#\left(G \backslash X\right)$. Mit Hilfe des Auswahlaxioms sieht man, dass Schnitte stets existieren.

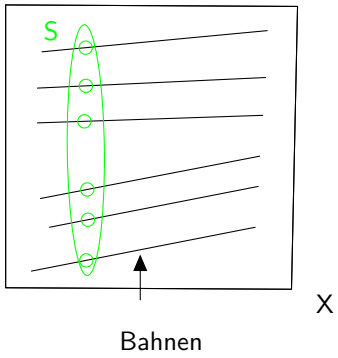


Abbildung 3: Die Bahnengleichung

Satz

Sei $S \subseteq X$ ein Schnitt der G-Wirkung $G \times X \to X$. Wenn X endlich ist, dann gilt

$$\#X = \sum_{s \in S} [G : G_s]$$

Beweis:
Sei $\#S = m$, $S = \{s_1, \ldots, s_m\} \rightsquigarrow X = G(s_1) \dot\cup G(s_2) \dot\cup \cdots \dot\cup G(s_m)$

$$\#G(s_i) \overset{2.5}{=} \#G/G_{s_i} \overset{1.14}{=} [G : G_{s_i}]$$

2.8 Automorphismen und Konjugationswirkungen

Sei G eine Gruppe. Ein bijektiver Homomorphismus $\alpha : G \to G$ heißt **Automorphismus** von G. Die Menge

$$\mathrm{Aut}(G) = \{\alpha : G \to G \mid \alpha \text{ Automorphismus}\}$$

ist eine Gruppe, mit der Komposition von Automorphismus als Verknüpfung und id_G als Neutralelement.

Beispiel

Sei $a \in G$. Dann ist die Abbildung $\gamma_a : G \to G,\ g \mapsto aga^{-1}$ ein Automorphismus. Denn:

$\gamma_a(gh) = agha^{-1} = aga^{-1}aha^{-1} = \gamma_a(g)\gamma_a(h)$
$\rightsquigarrow \gamma_a$ Homomorphismus
$\gamma_a(g) = e \Leftrightarrow aga^{-1} = e \Leftrightarrow g = a^{-1}ea = e$
$\rightsquigarrow \gamma_a$ Monomorphismus, $\ker(\gamma_a) = \{e\}$
Gegeben $g \in G$ folgt $\gamma_a(a^{-1}ga) = g$
$\rightsquigarrow \gamma_a$ Epimorphismus
$\Rightarrow \gamma_a$ Automorphismus

oder: $\gamma_a \circ \gamma_a = \mathrm{id}_G = \gamma_{a^{-1}} \circ \gamma_a$

Satz

Die Abbildung $G \xrightarrow{\gamma} \mathrm{Aut}(G),\ a \mapsto \gamma_a$ ist ein Homomorphismus.

Beweis:
Es gilt

$$\gamma_a \circ \gamma_b(g) = abgb^{-1}a^{-1} = abg(ab)^{-1} = \gamma_{ab}(g)$$

also $\gamma_a \circ \gamma_b = \gamma_{ab}$. □

Weil $\mathrm{Aut}(G) \subseteq \mathrm{Sym}(G)$ eine Untergruppe ist, ist $\gamma : G \to \mathrm{Aut}(G)$ eine Wirkung von G auf G, die **Konjugationswirkung**.
Beachte den Unterschied zu 2.3(a):

$$\lambda_a(g) = ag \qquad \gamma_a(g) = aga^{-1}$$

λ_a ist kein Homomorphismus (für $a \neq e$)

$$\lambda_a(gh) = agh \neq \lambda_a(g)\lambda_a(h) = agah$$

Der Kern von $\gamma : G \to \mathrm{Aut}(G)$ ist

$$\begin{aligned} Z(G) &= \{a \in G \mid \forall g \in G \text{ gilt } aga^{-1} = g\} \\ &= \{a \in G \mid \forall g \in G \text{ gilt } ag = ga\} \end{aligned}$$

Man nennt diesen Normalteiler das **Zentrum** von G. Das Zentrum von G ist also abelsch (und G ist genau dann abelsch, wenn $Z(G) = G$ gilt).

Bemerkung

Im Allgemeinen ist die Abbildung $\gamma : G \to \mathrm{Aut}(G)$ weder injektiv und surjektiv. Das Bild $\gamma(G) \subseteq \mathrm{Aut}(G)$ ist die Gruppe der **inneren Automorphismen**

$$\gamma(G) = \mathrm{Inn}(G) \subseteq \mathrm{Aut}(G)$$

Mit dem Homomorphiesatz also:

$$G/Z(G) \cong \mathrm{Inn}(G)$$

Wie sehen die Stabilisatoren in der Konjugationswirkung aus? Der Stabilisator von $g \in G$ ist der **Zentralisator** von g (vgl. 1.6)

$$\begin{aligned} Z_G(g) &= \{a \in G \mid aga^{-1} = g\} \\ &= \{a \in G \mid ag = ga\} \end{aligned}$$

Beachte: es gilt stets $\langle g \rangle \subseteq Z_G(g)$, denn

$$ggg^{-1} = g \rightsquigarrow g \in Z_G(g) \rightsquigarrow \langle g \rangle \subseteq Z_G(g)$$

Die Bahnen $G(g) = \{aga^{-1} \mid a \in G\}$ nennt man **Klassen** oder **Konjugiertenklassen** in G.

2.9 Satz 6, Die Klassengleichung

Sei G eine endliche Gruppe, sei $S \subseteq G$ ein Schnitt der Konjugationswirkung γ. Sei $\mathcal{K} = S \backslash Z(G)$. Dann gilt

$$\#G = \#Z(G) + \sum_{s \in \mathcal{K}} [G : Z_G(s)]$$

Beweis:
Nach der Bahnengleichung gilt

$$\#G = \sum_{s \in S} [G : Z_G(s)]$$

Für jedes $z \in Z(G)$ gilt $G(z) = \{aza^{-1} \mid a \in G\} = \{z\}$, also $Z(G) \subseteq S$ und $\#G(z) = 1\ \forall z \in Z$. □

2.10 Korollar über das Zentrum

Sei p eine Primzahl und G eine endliche Gruppe mit $\#G = p^m,\ m \geq 1$.
Dann gilt $Z(G) \neq \{e\}$.

Beweis:
Für $g \in G \backslash Z(G)$ ist $Z_G(g) \neq G$. Nach dem Satz von Lagrange 1.14 folgt $\#Z_G(g) = p^l,\ l < m$. Insbesondere ist dann p ein Teiler von $[G : Z_G(g)] = p^{m-l} \neq 1$. Folglich ist p ein Teiler von $\#Z(G)$, also $\#Z(G) \geq p$. □

Wenn G eine endliche Gruppe ist, dann nennt man ihre Kardinalität $\#G$ die **Ordnung** von G. Das passt zu 1.11: die Ordnung eines Elements $g \in G$ ist die Ordnung der von g erzeugten zyklischen Gruppe, $o(g) = \#\langle g \rangle$, vgl. 1.12.

Definition p-Gruppe

Eine endliche Gruppe G heißt **p-Gruppe**, für eine Primzahl p, wenn gilt $\#G = p^m$ für ein $m \geq 1$. Das vorige Korollar besagt also: jede p-Gruppe hat ein nicht-triviales Zentrum.

Beispiel

$G = \left\{ \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} \in K^{3\times 3} \right\}$ mit $K = \mathbb{F}_p$ (Körper mit p Elementen).

$\#G = p^3 \rightsquigarrow G$ ist p-Gruppe. Das Zentrum ist $\left\{ \begin{pmatrix} 1 & 0 & z \\ & 1 & 0 \\ & & 1 \end{pmatrix} \in K^{3\times 3} \right\}$.
Unser nächstes Ziel ist der Beweis der Sylow-Sätze. Das braucht etwas Vorbereitung.

2.11 Definition Normalisator

Sei G eine Gruppe und $H \subseteq G$ eine Untergruppe. Der **Normalisator** von H in G ist

$$N_G(H) = \{n \in G \mid nHn^{-1} = H\}$$

Satz

Der Normalisator $N_G(H)$ ist eine Untergruppe von G und es gilt

$$H \trianglelefteq N_G(H)$$

Insbesondere gilt $H \subseteq N_G(H)$.

Beweis:
Setze $X = \{aHa^{-1} \mid a \in G\}$. Dann wirkt G auf der Menge X durch Konjugation,

$$\begin{aligned} G \times X &\to X \\ (g, aHa^{-1}) &\mapsto gaHa^{-1}g^{-1} = (ga)H(ga)^{-1} \end{aligned}$$

Der Stabilisator von $H \in G$ ist genau $N_G(H)$, also eine Untergruppe.
Weiter gilt $H \subseteq N_G(H)$ (klar) und nach Definition gilt für alle $n \in N_G(H)$, dass $nHn^{-1} = H$, also $H \trianglelefteq N_G(H)$. □
Die Menge $X = \{aHa^{-1} \mid a \in G\}$ nennt man auch die **Konjugationsklasse** der Untergruppe H in G.
Folgerung aus dem Satz: Ist $K \subseteq N_G(H)$ eine Untergruppe, dann ist $KH \subseteq N_G(H)$ eine Untergruppe, denn $H \trianglelefteq N_G(H)$, das folgt aus 1.23 Lemma.

2.12 Satz 7, Cauchys Satz

Sei G eine endliche Gruppe und sei p eine Primzahl. Wenn p ein Teiler von $\#G$ ist , dann enthält G (mindestens) ein Element der Ordnung p.

Beweis:
Setze $X = \{(g_1, \ldots, g_p) \in G^p \mid g_1 \cdots g_p = e\}$. Da $g_1, \ldots, g_{p-1} \in G$ frei gewählt werden können und $g_p = (g_1, \cdots, g_{p-1})^{-1}$, gilt, $\#X = (\#G)^{p-1}$ und p teilt $\#X$. Gesucht ist ein Element $g \in G$ mit $g \neq e$ und $(g, \ldots, g) \in X$ (d.h. $g^p = e \neq g$).
Setze $K = \mathbb{Z}/p\mathbb{Z}$. Diese Gruppe K wirkt auf X wie folgt: sei $\overline{k} \in K$, setze $\overline{k}(g_{\overline{1}}, \ldots, g_{\overline{p}}) = (g_{\overline{1+k}}, \ldots, g_{\overline{p+k}})$.
Das ist wirklich eine K-Wirkung: $0 < k \leq p$ wirkt durch

$$\overline{k} : (g_{\overline{1}}, \ldots, g_{\overline{p}}) \mapsto (g_{\overline{1+k}}, \ldots, g_{\overline{p}}, g_{\overline{1}}, \ldots, g_{\overline{k}})$$

$g_{\overline{1}} \cdots g_{\overline{k}} = a, \quad g_{\overline{k+1}} \cdots g_{\overline{p}} = b \qquad ab = e$ nach Voraussetzung $\Rightarrow b = a^{-1}$

$$g_{\overline{1+k}} \cdots g_{\overline{p}} \cdot g_{\overline{1}} \cdots g_{\overline{k}} = ba = e \Rightarrow (g_{\overline{1+k}}, \ldots, g_{\overline{p}}) \in X$$

Die Fixpunkte dieser K-Wirkung sind genau die Tupel $(g, \ldots, g) \in X$. Also ist $(e, \ldots, e)$ ein Fixpunkt. Da $\#K = p$ hat jede K-Bahn $K(x)$ Länge $\#K(x) = [K : K_x] \in \{1, p\}$ und die der Länge 1 sind die Fixpunkte. Nach der Bahnengleichung gilt (für ein Schnitt $S \subseteq X$)

$$\#X = \#G^{p-1} = \sum_{s \in S} [K : K_s]$$

Die Primzahl p teilt beide Seiten, es gilt $[K : K_s] \in \{1, p\}$ und für $s = (e, \ldots, e)$ gilt $[K : K_s] = 1$. Also gibt es ein $s \neq (e, \ldots, e)$ mit $[K : K_s] = 1$. □

Wir brauchen noch das folgende technische Hilfsmittel.

2.13 Lemma 3

Sei $G \times X \to X$ eine Wirkung einer endlichen Gruppe G auf einer endlichen Menge X. Sei p eine Primzahl. Angenommen, es gilt folgendes:
(i) zu jedem $x \in X$ gibt es eine p-Gruppe $P \subseteq G$ mit $P(x) = \{x\}$.
Dann gilt $\#X = kp + 1$ für ein $k \geq 0$ und G wirkt transitiv auf X.

Beweis:
Sei $S \subseteq X$ ein Schnitt. Für jedes $s \in S$ wirkt G also transitiv auf $G(s)$. Sei $s \in S$. Sei $P \subseteq G$ p-Gruppe mit $P(s) = \{s\}$. Für jedes $x \in X \backslash \{s\}$ teilt p die Länge der Bahn $P(x)$ (weil P p-Gruppe ist und $P(x) \neq \{x\}$ nach (i)). Es folgt $\#G(s) = kp + 1$.
Angenommen, $S \neq \{s\}$. Für $t \in S \backslash \{s\}$ folgt $\#G(t) = lp$, weil P in $G(t)$ kein Fixpunkt hat. Anderseits zeigt das gleiche Argument, dass $G(t) = mp + 1$ ↯
Es folgt $S = \{s\}$ und $X = G(s)$ □

Jetzt beweisen wir Sylows Sätze. Peter Sylow war ein norwegischer Mathematiker und Lehrer. Seine Sätze sind in der endlichen Gruppentheorie ganz wesentlich.

2.14 Definition Sylow-Gruppe

Sei G eine endliche Gruppe, sei p eine Primzahl mit $\#G = p^m \cdot r$, wobei $m \geq 1$ sei und p kein Teiler von r ist. Eine Untergruppe $U \subseteq G$ heißt **Sylow-p-Gruppe** in G, wenn gilt $\#U = p^m$.
Die Menge aller Sylow-p-Gruppen in G wird mit $\mathrm{Syl}_p(G)$ bezeichnet.
(Im Moment ist nicht klar, dass $\mathrm{Syl}_p(G) \neq \emptyset$, aber das beweisen wir gleich.)

Sylows Sätze

Sei G eine endliche Gruppe, sei p eine Primzahl mit $\#G = p^m \cdot r,\ m \geq 1$, p kein Teiler von r. Dann gilt folgendes:

(1) $\mathrm{Syl}_p(G) \neq \emptyset$

(2) G wirkt transitiv auf $\mathrm{Syl}_p(G)$: zu $U, V \in \mathrm{Syl}_p(G)$ gibt es stets $g \in G$ mit $gUg^{-1} = V$

(3) $\#\,\mathrm{Syl}_p(G) = kp + 1$ für ein $k \geq 0$

(4) Ist $P \subseteq G$ ein p-Gruppe, so gibt es $U \in \mathrm{Syl}_p(G)$ mit $P \subseteq U$.

Beweis:
Sei Γ die Menge aller p-Gruppen in G. Nach Cauchys Satz ist $\Gamma \neq \emptyset$. Sei $\Omega \subseteq \Gamma$ die Menge aller maximalen p-Gruppen in Γ (weil G endlich ist, ist jede p-Gruppe $P \subseteq G$ ein einer maximalen p-Gruppe enthalten).
Die Gruppe G wirkt durch Konjugation auf der Menge Γ und Ω. Nach Definition gilt $\mathrm{Syl}_p(G) \subseteq \Omega$.

1. Schritt: G wirkt transitiv auf Ω und es gilt $\#\Omega = kp + 1$ für ein $k \geq 0$.
Beweis 1. Schritt: Wir benutzen das Lemma 2.13. Für $U \in \Omega$ ist U der einzige Fixpunkt der Wirkung von U auf der Menge Ω. Denn: wenn U das Element $V \in \Omega$ fixiert, so folgt $U \subseteq N_G(V) \overset{2.11}{=} UV \subseteq G$ Untergruppe, $V \trianglelefteq UV$. Es gilt

$$\#UV \overset{1.14}{=} \#V \cdot [UV : V] = \#V \cdot \#{}^{UV}/_{V}$$

sowie

$${}^{UV}/_{V} \overset{1.23}{\cong} {}^{U}/_{U\cap V} = \frac{\#U}{\#(U \cap V)} \text{ also ist } \#{}^{UV}/_{V} \text{ eine } p\text{-Potenz}$$

denn $\#U$ und $\#U \cap V$ sind p-Potenzen. Folglich ist $UV \subseteq G$ eine p-Gruppe. Da U und V maximale p-Gruppen sind und $U, V \subseteq UV$ folgt

$$U = UV = V$$

Mit Lemma 2.13 folgt nun: G wirkt transitiv auf Ω und $\#\Omega = kp + 1$. □
2. Schritt: Es gilt $\Omega = \mathrm{Syl}_p(G)$.
Beweis 2. Schritt: Sei $U \in \Omega,\ \#U = p^l$. Wir müssen zeigen, dass $p^l = p^m$ gilt.
Wegen Schritt 1 gilt jedenfalls

$$\#G = p^m \cdot r = \#N_G(U) \cdot \#\Omega = \#N_G(U)(kp + 1) \qquad (*)$$

und folglich

$$\#N_G(U) = p^m \cdot s \quad \text{für ein } s \geq 1 \qquad (**)$$

Angenommen, es gilt $l < m$. Betrachte

$$N_G(U) \overset{\pi_U}{\to} {}^{N_G(U)}/_{U} = K$$

Es folgt $\#N_G(U) = p^m \cdot s = \underbrace{\#U}_{=p^e}$, also ist p ein Teiler von $\#K$. Nach Cauchys Satz 2.12 gibt es eine p-Gruppe $P \subseteq K$. Setze $V = \pi_U^{-1}(P) \subseteq N_G(U)$. Es folgt mit $P = {}^{V}/_{U}$, dass

$$\#V = \#U \cdot \#P$$

also ist V eine p-Gruppe.
Da p ein Teiler von $\#P$ ist, folgt $V \not\supseteq U$, ein Widerspruch zur Maximalität von U.
Folglich gilt $\#U = p^m$ für alle $U \in \Omega$ und damit $\Omega = \mathrm{Syl}_p(G)$. □
Damit sind (1),(2) und (3) bewiesen. Wegen $\mathrm{Syl}_p(G) = \Omega$ folgt (4). □

Addendum zu Sylows Theorem

Es gilt (mit den Bezeichnungen von oben)

$$r = s \cdot (kp + 1)$$

Das folgt aus $(*)$ und $(**)$.

2.15 Beispiel 5, Anwendung

Lemma

Seien p, q Primzahlen mit $p < q$. Wenn G eine Gruppe ist mit $\#G = p \cdot q$ und wenn p kein Teiler von $q - 1$ ist, dann ist G abelsch.

Beweis:
Setze $\#\operatorname{Syl}_p(G) = kp + 1$ und $\#\operatorname{Syl}_q(G) = lq + 1$, dann folgt $q = s(kp + 1)$.
1.Fall: $s = 1 \rightsquigarrow q = kp + 1$ Widerspruch zur Annahme, dass p kein Teiler von $q - 1$ ist.
2.Fall: $kp + 1 = 1 \rightsquigarrow$ es gibt genau eine Sylow-p-Gruppe $U \subseteq G \rightsquigarrow G = N_G(U)$, d.h. $U \trianglelefteq G$.
Jetzt $p = s' \cdot (lq + 1)$ wegen $q > p$ folgt $s' = p$ und $lq + 1 = 1 \rightsquigarrow$ es gibt genau eine Sylow-q-Gruppe $Q \subseteq G \rightsquigarrow Q \trianglelefteq G$.
Weiter gilt:

$$\#P = p \text{ und } \#Q = q$$

Außerdem teilt $\#(P \cap Q)$ nach Lagrange p und $q \Rightarrow P \cap Q = \{e\}$. Weil $P \trianglelefteq G$ und $Q \trianglelefteq G$ gilt für $a \in P$ und $b \in Q$, dass

$$\underbrace{\underbrace{aba^{-1}}_{\in Q}\underbrace{b^{-1}}_{\in Q}}_{\in P} \in Q \cap P \text{ d.h. } ab = ba$$

Nach 1.23 haben wir ein Monomorphismus $P \times Q \xrightarrow{\varphi} G,\ (a, b) \mapsto ab$. Wegen $\#(P \times Q) = p \cdot q = \#G$ ist φ surjektiv, also ein Isomorphismus.
Wegen $\#P = p$ und $\#Q = q$ sind P und Q abelsch: ist $a \in P,\ a \neq e$, so gilt $o(a) > 1$ und $o(a)$ teilt p

$$\Rightarrow o(a) = p \Rightarrow \langle a \rangle = P \Rightarrow P \text{ zyklisch } \Rightarrow P \text{ abelsch, vgl. 1.12.}$$

Gleiches gilt für Q (mit ÜA 4.3 einfügen folgt jetzt sogar: G ist zyklisch) □

Beispiel

Die Gruppe $\operatorname{Sym}(3)$ ist nicht abelsch, vgl 1.7. Es gilt $\#\operatorname{Sym}(3) = 2 \cdot 3$ (aber 2 teilt 3-1 !). Was sind die Sylowgruppen in $\operatorname{Sym}(3)$? (ÜA)

Bemerkung

Im Beweis vom obigen Lemma haben wir einige nützliche Fakten bewiesen, die auch sonst hilfreich sein können:

(1) Jede endliche Gruppe, deren Ordnung eine Primzahl ist, ist ablesch.

(2) Wenn $\varphi : K \to G$ ein Monomorphismus von endlichen Gruppen ist und wenn gilt $\#K = \#G$, dann ist φ ein Isomorphismus.

(3) Wenn $N, M \subseteq G$ Normalteiler sind und wenn gilt $N \cap M = \{e\}$, dann ist die Abbildung $N \times M \to G,\ (n, m) \mapsto n \cdot m$ ein Monomorphismus.

(4) Wenn G endlich ist und p eine Primzahl und wenn p ein Teiler von $\#G$ ist mit $\operatorname{Syl}_p(G) = 1$, dann ist die (eindeutige) Sylow-p-Gruppe $U \in \operatorname{Syl}_p(G)$ ein Normalteiler in G, $U \trianglelefteq G$.

2.16 Satz 8

Sei G eine endliche Gruppe mit $\#G = pq,\ p \neq q$ Primzahlen. Dann gilt es gibt einen Normalteiler $N \trianglelefteq G,\ \{e\} \neq N \neq G$.

Beweis:
OE $p < q,\ \#\mathrm{Syl}_q(G) = lq + 1$

$$\overset{2.14}{\Rightarrow} p = s(lq+1) \Rightarrow lq + 1 = 1 \text{ wegen } p < q$$
$$\Rightarrow \text{ es gibt genau eine Sylow-}q\text{-Gruppe } U \subseteq G$$
$$\Rightarrow U \trianglelefteq G \text{ und } \#U = p$$

□

Wir betrachten als nächstes p-Gruppen genauer.

2.17 Lemma 4

Sei G eine Gruppe. Dann ist jede Untergruppe $H \subseteq Z(G)$ Normalteiler in G.

Beweis:
Sei $g \in G$ und $h \in H \subseteq Z(G)$. Es folgt $ghg^{-1} = h$, also $gHg^{-1} = H$. □

Satz

Sei p Primzahl und G eine p-Gruppe, $\#G = p^m,\ m \geq 1$. Dann gibt es Normalteiler $G_k \trianglelefteq G$ mit $\#G_k = p^k$ für $0 \leq k \leq m$ und mit

$$G_m \trianglelefteq G_{m-1} \trianglelefteq \ldots \trianglelefteq G_1 \trianglelefteq G_0 = \{e\}$$

Beweis:
Induktion nach m. Für $m = 1$ ist nichts zu zeigen. Sei jetzt $\#G = p^m$, $m \geq 1$.
Nach 2.10 ist $Z(G) \neq \{e\}$, also $Z(G) = p^s$ für ein $s > 1$ (Lagrange). Nach Cauchys Satz 2.12 gibt es $g \in Z(G)$ mit $o(g) = p$. Setze $G_1 = \langle g \rangle$ und $G \xrightarrow{\pi} \tilde{G} = {}^{G}/_{G_1}$ (nach dem Lemma gilt $G_1 \trianglelefteq G$).
Es folgt $\#\tilde{G} = p^{m-1}$ nach Induktionannahme gibt es $\tilde{G}_k \trianglelefteq \tilde{G}$ mit $\#\tilde{G}_k = p^k,\ \tilde{G} \supseteq \tilde{G}_{m-2} \supseteq \cdots \supseteq \tilde{G}_0$.
Setze $G_{k+1} = \pi^{-1}(G_k)$, es folgt nach 1.22, dass $G_{k+1} \trianglelefteq G$, sowie $G_m \supseteq G_{m-1} \supseteq \cdots \supseteq G_0 = \{e\}$.
Wegen $G_1 \subseteq G_{k+1}$ folgt $\tilde{G}_k \cong {}^{G_{k+1}}/_{G_1}$, also

$$\#G_{k+1} = p \cdot \#\tilde{G}_k = p^{k+1}$$

□

Folgerung

Ist G eine endliche Gruppe, p eine Primzahl und ist p^k ein Teiler von $\#G$, dann hat G eine Untergruppe der Ordnung p^k.

Beweis:
Sei $U \in \mathrm{Syl}_p(G),\ \#U = p^m$.
Dann gilt $k \leq m$ und nach dem vorigen Satz gibt es eine Untergruppe $H \subseteq U$ mit $\#H = p^k$ □

2.18 Definition Normalreihe

Sei G eine Gruppe, sei $G = G_m \supseteq G_{m-1} \supseteq \cdots \supseteq G_0 = \{e\}$ Untergruppen. Wenn gilt

$$G_{k-1} \trianglelefteq \mathcal{G}_k,$$

dann heißt $G_m \supseteq \cdots \supseteq G_0$ **Normalreihe** in G. Die Quotienten ${}^{G_k}/_{G_{k+1}}$ heißen **Faktoren** der Normalreihe.
Eine Gruppe, die eine Normalreihe mit ableschen Faktoren hat, heißt **auflösbare Gruppe**.

Beispiele

(a) G abelsch $\Rightarrow G$ auflösbar, setze $G_1 = G \supseteq G_0 = \{e\}$

(b) $G = \mathrm{Sym}(3),\ \#G = 6,\ \tau : \{1,2,3\} \to \{1,2,3\}\ \tau : \begin{matrix} 1 \mapsto 2 \\ 2 \mapsto 3 \\ 3 \mapsto 1 \end{matrix}$
$o(\tau) = 3,\ G_1 = \langle \tau \rangle \trianglelefteq G$ (weil $[G : G_1] = 2$, ÜA 3.2 oder 2.16)
$\#{}^{G}/_{G_1} = 2 \rightsquigarrow$ abelsch, also ist $\mathrm{Sym}(3)$ auflösbar.

(c) Nach Satz 2.17 ist jede p-Gruppe auflösbar.

Wir betrachten jetzt abelsche p-Gruppen.

2.19 Lemmata 5,6,7

Lemma A

Sei G abelsche p-Gruppe. Wenn G genau eine Untergruppe $H \subseteq G$ der Ordnung p hat, dann ist G zyklisch.

Beweis:
Setze $\#G = p^m,\ m \geq 1$. Induktion nach m. Für $m = 1$ ist nichts zu zeigen. Sei jetzt $m > 1$. Betrachte den Homomorphismus $\varphi : G \to G,\ g \mapsto g^p$ (das ist ein Homomorphismus, weil G abelsch ist: $(gh)^p = g^p h^p$).
Es gilt $\ker(\varphi) = \{g \in G \mid g^p = e\} = \{g \in G \mid o(g) \in \{1, p\}\}$. Ist $o(g) = p$, so folgt aus der Annahme $g \in H$, also $H = \ker(\varphi)$, denn $h \in H \rightsquigarrow o(h) \in \{1, p\}$.
Setze $K = \varphi(G)$. Nach dem Homomorphiesatz 1.20 gilt $K \cong {}^{G}/_{H}$, also $\#K = p^{m-1}$. Wegen $m > 1$ folgt aus Cauchys Satz 2.12, dass K ein Element der Ordnung p enthält. Folglich gilt $H \subseteq K$. Also hat K genau eine Untergruppe der Ordnung p und ist deswegen nach Induktionsannahme zyklisch, $K = \langle k \rangle$ für ein $k \in K = \varphi(G)$. Wähle $g \in G$ mit $\varphi(g) = g^p = k$. Wegen $o(g) = p \cdot r$ folgt $o(g^r) = p \rightsquigarrow H \subseteq \langle g \rangle$ (wegen der Eindeutigkeit von H), also

$${}^{\langle g \rangle}/_{H} \cong K \Rightarrow \#\langle g \rangle = \#K \cdot \#H = \#G \Rightarrow G = \langle g \rangle$$

□

Lemma B

Sei G zyklisch mit $\#G = k \cdot l$. Dann hat G genau eine Untergruppe $H \subseteq G$ mit $\#H = k$ (ÜA 4.1).

Beweis:
Betrachte $\varphi : G \to G,\ g \mapsto g^k$, das ist ein Homomorphismus. Der Kern ist $K = \{g \in G \mid g^k = e\}$. Ist $H \subseteq G$ Untergruppe mit $\#H = k$, so folgt $H \subseteq K$. Sei $u \in G$ Erzeuger, $G = \langle u \rangle$. Das Bild von φ ist dann $\varphi(G) = \langle u^k \rangle$ und $o(u^k) = l$. Also folgt

$$l = \#\varphi(G) = \frac{\#G}{\#K} \Rightarrow \#K = k \Rightarrow H = K.$$

□

Lemma C

Sei G eine abelsche p-Gruppe, sei $u \in G$ eine Element maximaler Ordnung in G und sei $U = \langle u \rangle$. Dann gibt es eine Untergruppe $H \subseteq G$ mit

$$H \cap U = \{e\} \text{ und } G = HU, \text{ d.h. } H \times U \cong G.$$

Beweis:
Setze $\#G = p^m$. Für $m = 1$ ist G zyklisch, setze $U = G$ und $H = \{e\} \rightsquigarrow$ fertig.
Sei jetzt $m > 1$, Induktion nach m.
1. Fall: G zyklisch, $G = U,\ H = \{e\} \rightsquigarrow$ fertig.
2. Fall: G nicht zyklisch. Da U genau eine Untergruppe der Ordnung p hat (Lemma B) gibt es nach Lemma A und Cauchys Satz 2.12 ein Element $w \in G \backslash U$ mit $o(w) = p$. Setze $W = \langle w \rangle$.
Es folgt $U \cap W = \{e\}$, weil $w \notin U$ ($\#U \cap W$ ist p-Potenz). Betrachte $\pi : G \to {}^G\!/_W$. Wegen $\ker(\pi) = W$ ist die Einschränkung von π auf U injektiv, d.h. $o(\pi(u)) = o(u)$. Folglich ist $\pi(u)$ ein Element maximaler Ordnung in $L = {}^G\!/_H$, und $\#{}^G\!/_W = p^{m-1}$.

Nach Induktionsannahme gibt es eine Untergruppe $H' \subseteq L$ mit $H' \cap \pi(U) = \{e_L\}$ und $L = \pi(U)H' \cong \pi(U) \times H'$.
Setze $H = \pi^{-1}(H')$. Es folgt $H \cap U = \{e\}$, denn:

$$h \in H,\ \pi(h) \in \pi(U) \rightsquigarrow \pi(h) = e_L \rightsquigarrow h \in W.$$

Weiter gilt für $g \in G$, dass

$$\begin{aligned} &\pi(g) = \pi(u^k)\pi(h) && \text{für ein } k \geq 0,\ h \in H \\ &\rightsquigarrow g = u^k(h \cdot w^l) && \text{für ein } l \geq 0, \text{ aber } w \in H \\ &\Rightarrow G = UH \end{aligned}$$

□

Korollar

Sei G eine abelsche p-Gruppe, $\#G = p^m$ mit $m \geq 1$. Dann gibt es Zahlen $n_1 \geq \cdots \geq n_r \geq 1$ mit $m = n_1 + \cdots + n_r$ und

$$G \cong {}^{\mathbb{Z}}\!/_{p^{n_1}\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{p^{n_2}\mathbb{Z}} \times \cdots \times {}^{\mathbb{Z}}\!/_{p^{n_r}\mathbb{Z}}$$

Beweis:
Wähle $u_1 \in G$ mit maximaler Ordnung $o(u_1) = p^{n_1}$, $U_1 = \langle u_1 \rangle \cong {}^{\mathbb{Z}}\!/_{p^{n_1}\mathbb{Z}}$ und eine Untergruppe $G_1 \subseteq G$ wie in Lemma C mit $U_1 \cap G_1 = \{e\},\ G = U_1G_1 \cong U_1 \times G_1$. Wähle $u_2 \in G_1$ mit maximaler Ordung $o(u_2) = p^{n_2},\ U_2 = \langle u_2 \rangle \cong {}^{\mathbb{Z}}\!/_{p^{n_2}\mathbb{Z}},\ G_1 = U_2G_2$ usw. Nach endlich vielen Schritten

$$G = U_1U_2 \cdots U_r \cong U_1 \times \cdots \times U_r$$

Zur Eindeutigkeit der Zahlen $n_1, \dots, n_r$:
Für $l \geq 1$ sei $\varphi_l : G \to G,\ g \mapsto g^{p^l}$.
Da G abelsch ist, ist φ_l ein Homomorphismus mit

$$\ker(\varphi_l) = \{g \in G \mid o(g) \text{ teilt } p^l\},$$

insbesondere

$$\left.\begin{array}{ll} \varphi_l(u_i) = e & \text{für } l \geq n_i \\ \varphi_l(u_i) \neq & \text{sonst} \end{array}\right\} \Rightarrow \#\varphi_l(U_i) = \begin{cases} \{1\} & l \geq n_i \\ \mathbb{Z}/p^{n_i - l}\mathbb{Z} & l < n_i \end{cases}$$

$\Rightarrow \#\varphi_l(G) = \prod_{n_i > l} p^{n_i - l} = p^{N_l}$, aus den Zahlen $N_1, N_2, \dots$ lassen sich die n_i berechnen, $N_l = \sum_{n_i > l}(n_i - l)$. □

2.20 Satz 9

Sei G eine endliche abelsche Gruppe, $\#G = p_1^{l_1} \cdots p_s^{l_s},\ 2 \leq p_1 < p_2 < \cdots < p_s$ Primzahlen, $l_1, \dots, l_s \geq 1$. Dann gilt

$$G \cong P_1 \times \cdots \times P_s$$

wobei P_j eine abelsche p_j-Gruppe der Ordnung $p_j^{l_j}$ ist wie im vorigen Korollar.
Insbesondere ist jede endliche abelsche Gruppe ein Produkt von zyklischen Gruppen.

Beweis:
Da G abelsch ist,ist jede Sylow-p_j-gruppe in G normal, also gibt es (wegen 2.14(2)) genau eine Sylow-p_j-Gruppe $P_j \subseteq G$, und P_j enthält alle Elemente $g \in G$, deren Ordnung eine p_j-Potenz ist.
Betrachte

$$\varphi : P_1 \times \cdots \times P_s \to G$$
$$(g_1, \dots, g_s) \mapsto g_1 g_2 \cdots g_s$$

Weil G abelsch ist, ist φ ein Homomorphismus (oder: weil für alle $i < j$ gilt $P_i \cap P_j = \{e\} \rightsquigarrow$ B6 A($*$)).
Es genügt zu zeigen, dass φ injektiv ist, dann folgt aus Kardinalitätsgründen, dass φ bijektiv ist.
$\mathbb{Z}\!\!\mathbb{Z} \ker(\varphi) = \{e\}$.
Angenommen, $g_1 \cdots g_s = e,\ g_i \in P_i$.
Setze $r_i = \frac{\#G}{p_i^{l_i}}$. Für $i \neq j$ folgt $g_j^{r_i} = e$, weil $\#P_j$ ein Teiler von r_i ist. Also gilt

$$(g_1 \cdot g_s)^{r_i} = g_1^{r_i} \cdot g_s^{r_i} = g_i^{r_i} = e^{r_i} = e$$

Also ist $o(g_i)$ ein Teiler von r_i. Weil $o(g_i)$ eine p_i-Potenz ist, folgt $o(g_i) = 1$, d.h. $g_i = 1$.
Es folgt $\ker(\varphi) = \{(e, \dots, e)\}$. □

2.21 Satz 10

Sei G eine endliche auflösbare Gruppe mit einer Normalreihe $G = G_m \trianglelefteq \dots \trianglelefteq G_0$ mit abelschen Faktoren. Dann gibt es für jedes $1 \leq k \leq m$ Untergruppe H_j mit

$$G_k \trianglelefteq H_l \trianglelefteq \dots \trianglelefteq H_0 = \mathcal{G}_{k-1}$$

mit $H_j/H_{j-1} \cong \mathbb{Z}/p_j\mathbb{Z}$, p_j Primzahl.
Insbesondere hat jede endliche auflösbare Gruppe eine Normalreihe, in der alle Faktoren zyklisch von Primzahlordnung sind.

Beweis:
Betrachte die abelsche Gruppe $A = G_k/G_{k-1}$.
Nach Satz 2.20 und 2.17, angewandt auf die Sylowgruppen von A, gibt es Untergruppen

$$A = A_l \supseteq \cdots \supseteq A_0 = \{e\} \text{ mit } A_j/A_{j-1} \cong \mathbb{Z}/p_j\mathbb{Z},\ p_j \text{ Primzahl}$$

Setze $\pi : \mathcal{G}_k \to {}^{G_k}/_{G_{k-1}} = A$ kanonischee Epimorphismus und $H_j = \pi^{-1}(A_j) \rightsquigarrow H_j \trianglelefteq G_k$ und

$$G_k \trianglelefteq H_l \trianglelefteq \dots H_0 = G_{k-1}$$

$${}^{H_j}/_{H_{j-1}} \overset{\text{2.Iso-Satz}}{\cong} {}^{A_j}/_{A_{j-1}} \cong {}^{\mathbb{Z}}/_{p_j\mathbb{Z}}$$

□

2.22 Komutatoren

Sei G eine Gruppe, $a, b \in G$. Der **Komutator** von a und b ist

$$[a,b] = aba^{-1}b^{-1} = ab(ba)^{-1} \rightsquigarrow ab = [a,b]ba$$

Offensichtlich gilt $[a,b]^{-1} = [b,a]$ und

$$[a,b] = e \Leftrightarrow a \text{ zentralisiert } b \Leftrightarrow b \text{ zentralisiert } a \Leftrightarrow a \text{ und } b \text{ vertauschen}$$

Die **Kommutatorengruppe** von G ist

$$\mathcal{D}G = \langle\, [a,b] \,|\, a,b \in G \rangle\,,$$

die von allen Komutatoren erzeugte Gruppe.

Satz

Sei G eine Gruppe. Dann gilt

(i) $\mathcal{D}G \trianglelefteq G$

(ii) ${}^{G}/_{\mathcal{D}G}$ ist abelsch

(iii) Ist A abelsche Gruppe und $\varphi : G \to A$ ein Homomorphismus, so gilt $\mathcal{D}G \subseteq \ker(\varphi)$.

Beweis:

(i) Für $g, a, b \in G$ gilt $g[a,b]g^{-1} = [gag^{-1}, gbg^{-1}]$ (nachrechnen), also gilt für alle $g \in G,\ a_1, \dots, a_s, b_1, \dots, b_s \in G$, dass

$$g[a_1,b_1]\cdots[a_s,b_s]g^{-1} \in \mathcal{D}G$$

also $g\mathcal{D}Gg^{-1} \subseteq \mathcal{D}G$ für alle $g \in G \Rightarrow \mathcal{D}G \trianglelefteq G$.

(ii) Sei $g, h \in G$. Es folgt wegen $gh = [g,h]hg$, dass

$$gh\mathcal{D}G = \underbrace{[g,h]}_{\in \mathcal{D}G} hg\mathcal{D}G = hg\mathcal{D}G$$

und damit, dass ${}^{G}/_{\mathcal{D}G}$ abelsch ist.

(iii) Für alle $g, h \in G$ gilt

$$\varphi([g,h]) = [\varphi(g), \varphi(h)] = e_A, \text{ weil } A \text{ abelsch ist,}$$

also

$$\{[g,h] \mid g,h \in G\} \subseteq \ker(\varphi) \Rightarrow \mathcal{D}G \subseteq \ker(\varphi)$$

□

Man definiert rekursiv

$$\mathcal{D}^0G = G,\ \mathcal{D}^1G = G,\ \mathcal{D}^{k+1}G = \mathcal{D}(\mathcal{D}^kG)$$

Es folgt $D^{k+1}G \trianglelefteq G$.
Genauer: $D^{k+1}G \trianglelefteq G$ mit Induktion

$$a, b \in \mathcal{D}^kG \Rightarrow g[a,b]g^{-1} = [\underbrace{gag^{-1}}_{\in \mathcal{D}^kG}, \underbrace{gbg^{-1}}_{\in \mathcal{D}^kG}] \in D^{k+1}G$$

also $g(D^kG)g^{-1} \subseteq D^{k+1}G$.

2.23 Satz 11

Eine Gruppe G ist auflösbar genau dann, wenn gilt $D^mG = \{e\}$ für ein $m \geq 0$.

Beweis:
Angenommmen, $D^mG = \{e\}$ für ein $m \geq 0$. Dann ist $\mathcal{D}^0G \supseteq \mathcal{D}^1G \supseteq \cdots \supseteq \mathcal{D}^mG = \{e\}$ eine Normalreihe und ${}^{\mathcal{D}^kG}/_{\mathcal{D}^{k+1}G} = {}^{\mathcal{D}^kG}/_{\mathcal{D}(\mathcal{D}^kG)}$ ist abelsch nach 2.22(ii), also ist G auflösbar.
Ist umgekehrt G auflösbar und $G = G_m \trianglelefteq \ldots \trianglelefteq G_0 = \{e\}$ eine Normalreihe mit abelschen Faktoren, so folgt aus 2.22(iii), dass $\mathcal{D}G_k \subseteq G_{k-1}$, also iteriert auch

$$D^{l+1}G_k \subseteq D^lG_{k-1}$$

$$\Rightarrow \mathcal{D}^mG = \mathcal{D}^mG_m \subseteq \mathcal{D}^{m-1}G_{m-1} \subseteq \cdots \subseteq \mathcal{D}^0G_0 = \{e\}$$

□

Korollar

Bilder und Untergruppen von auflösbaren Gruppen sind wieder auflösbar.

Beweis:
Sei $\varphi : G \to K$ Homomorphismus und G auflösbar, $D^mG = \{e\}$. Wegen

$$\varphi([a,b]) = \varphi(aba^{-1}b^{-1}) = [\varphi(a), \varphi(b)]$$

folgt

$$\mathcal{D}^m(\varphi(G)) = \varphi(\mathcal{D}^mG) = \varphi(e_G) = \{e_K\}$$

Bilder von Komutatoren sind Komutatoren

Ist $H \subseteq G$, so folgt $\mathcal{D}^kH \subseteq \mathcal{D}^kG$ für alle $k \geq 0$, also

$$\mathcal{D}^mG = \{e_g\} \Rightarrow D^mH = \{e_G\}$$

Also folgt mit dem Satz von oben, dass H auflösbar ist. □

2.24 Definition perfekt

Eine Gruppe G heißt **perfekt**, wenn gilt $\mathcal{D}G = G$.
Eine Gruppe, die gleichzeitig perfekt und auflösbar ist, ist trivial.

2.25 Die symmetrischen und alternierenden Gruppen

Sei $\mathrm{Sym}(n)$ die Gruppe aller Permutationen der Menge $\{1,\dots,n\}$. Es gilt $\#\mathrm{Sym}(n) = n! = n(n-1)(n-2)\cdots 2\cdot 1$, denn $\mathrm{Sym}(n)$ wirkt transitiv auf der n-elementigen Menge $\{1,\dots,n\}$.
Der Stabilisator von n ist isomorph zu $\mathrm{Sym}(n-1)$.

$$\overset{\text{Bahnengl.}}{\Rightarrow} \#\mathrm{Sym}(n) = n\cdot\mathrm{Sym}(n-1) \text{ und } \#\mathrm{Sym}(1) = 1$$

Erinnerung an LA II, Kapitel über Determinanten, 4.6.
Für $\pi \in \mathrm{Sym}(n)$ setze

abelsche Gruppe der Ordnung 2 bzgl. Multiplikation

$$\mathrm{sign}(\pi) = \prod_{i<j} \frac{\pi(i)-\pi(j)}{i-j} \in \{\pm 1\} = C_2.$$

$\mathrm{sign} : \mathrm{Sym}(n) \to C_2$ ist ein Homomorphismus.
Der Kern von sign ist die alternierende Gruppe

$$\mathrm{Alt}(n) = \{\pi \in \mathrm{Sym}(n) \mid \mathrm{sign}(\pi) = 1\}$$

Aus 2.22 folgt $\mathcal{D}\,\mathrm{Sym}(n) \subseteq \mathrm{Alt}(n)$, weil C_2 abelsch ist.

Satz

Es gilt $\mathcal{D}\,\mathrm{Sym}(n) = \mathrm{Alt}(n)$. Für $n \geq 5$ ist $\mathrm{Alt}(n)$ perfekt.

Beweis:
Seien $i_1,\dots,i_k$ k paarweise verschiedene Zahlen in $\{1,\dots,n\}$. Die Permutation $i_1 \overset{\pi}{\to} i_2 \overset{\pi}{\to} i_3 \overset{\pi}{\to} \cdots \overset{\pi}{\to} i_k \overset{\pi}{\to} i_1$, also $\pi(i_l) = i_{l+1}$ für $l = 1,\dots,k$, $\pi(i_k) = i_1$ und $\pi(j) = j$ sonst. Diese Permutation nennt man ein **k-Zykel** und schreibt sich kurz mit $\pi = (i_1,\dots,i_k)$.
Die 2-Zykel vertauschen zwei Zahlen i_1, i_2, man nennt sie **Transpositionen**. Nach LA II Übungsaufgabe 4.3 ist jede Permutation ein Produkt von 2-Zykeln. Weiter gilt $\mathrm{sign}((i_1,i_2)) = -1$. Also besteht $\mathrm{Alt}(n)$ aus allen Permutationen, die sich schreiben lassen als Produkt einer geraden Anzahl von 2-Zykeln.

Behauptung: $\mathrm{Alt}(n)$ wird von den 3-Zykeln erzeugt.
Beweis: Seien $a,b,c,d \in \{1,\dots,n\}$ paarweise verschieden. Es gilt

$$(a,c)\circ(a,b) = (a,b,c) \text{ sowie } (a,b)\circ(c,d) = (a,d,c)\circ(a,b,c)$$

□

Zum Satz:

$$[(a,b,c),(b,c)] = (b,a,c) \in \mathcal{D}\,\mathrm{Sym}(n) \Rightarrow \mathcal{D}\,\mathrm{Sym}(n) = \mathrm{Alt}(n)$$

Seien a,b,c,d,e paarweise verschieden

$$[(a,b,c),(c,d,e)] = (d,c,a) \Rightarrow \mathcal{D}\,\mathrm{Alt}(n) = \mathrm{Alt}(n) \text{ für } n \geq 5$$

□

Folgerung

Für $n \geq 5$ ist $\mathrm{Sym}(n)$ nicht auflösbar.
Für $n = 1,2,3,4$ ist $\mathrm{Sym}(n)$ auflösbar. (ÜA)

Ausblick

(1) Jede endliche Gruppe G mit ungerader Ordnung ist auflösbar. (Feit-Thompson-Theorem, viele hundert Seiten langer Beweis)

(2) Eine Gruppe G heißt **einfach**, wenn $G \neq \{e\}$ und wenn $G, \{e\}$ die einzigen Normalteiler in G sind.

Theorem (Klassifikation der endlichen einfachen Gruppen)

Sei G eine endliche einfache Gruppe. Dann kommt G in folgender Liste vor:

- abelsche einfache Gruppe $\mathbb{Z}/p\mathbb{Z},\ p$ Primzahl
- $\mathrm{Alt}(n),\ n \geq 5$
- Matrizengruppen wie $\mathrm{Sl}_n(F),\ F$ endlicher Körper, "Gruppen vom Lie-Typ"
- 26 sogenannte sporadische einfache endliche Gruppen.
  Der Beweis ist ca. 10000 Seiten in vielen Arbeiten lang, ca. 1980er Jahre.

Die größte sporadische Gruppe, das "Monster", hat mehr Elemente als es Elementarteilchen gibt.

3 Kommutative Ringe

3.1 Erinnerung / Definiton

Sei $(R, +)$ eine abelsche Gruppe mit Neutralelement $0 \in R$. Angenommen, es gibt eine weitere assoziative Verknüpfung auf R, die Multiplikation $R \times R \to R,\ (a, b) \mapsto a \cdot b = ab$.
Weiter gilt:

(R1) es gelten die Distributivgesetze,

$$a(x + y) = ax + ay$$
$$(x + y)a = xa + ya$$

(R2) Es gibt ein Einselement $1 \in R$, d.h.

$$1 \cdot x = x = x \cdot 1\ \forall x \in R$$

(R3) $ab = ba$ für alle $a, b \in R$

dann heißt $(R, +, \cdot)$ ein **kommutativer Ring**. Verlangt man nur (R1) & (R2), spricht man von einem nicht kommutativem Ring. Wenn man nur (R1) fordert, spricht man von einem Ring ohne Eins oder **Rng** (Jacobsen).

Beispiele

(a) Jeder Körper ist ein Ring, z.B. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$

(b) $\mathbb{Z}$ ist ein Ring (kommutativ).

(c) V ein K-Vektorraum, $\mathrm{End}(V) = \{\varphi : V \to V \mid \varphi \text{ linear}\}$

$$\varphi, \psi \in \mathrm{End}(V) : (\varphi + \psi)(v) = \varphi(v) + \psi(v),\ v \in V$$
$$(\varphi \circ \psi)(v) = \varphi(\psi(v))$$

$\Rightarrow \mathrm{End}(V)$ Ring, nicht kommutativ, falls $\dim(V) \geq 2$.

(d) $m\mathbb{Z} = \{mk \mid k \in \mathbb{Z}\}$ für ein $m \geq 1$
Rng, wenn $m \geq 2$.

(e) $R = \{0\}$ mit $0 \cdot 0 = 0 = 0 + 0$ der Nullring. Im Nullring gilt $0 = 1$.

3.2 Rechenregeln in Ringen

(a) Additiv darf man kürzen:

$$a + x = a + y \Rightarrow x = y$$

(addieren von $-a$ auf beiden Seiten)

(b) Es gilt stets

$$0 \cdot a = a \cdot 0 = 0$$

(c) Es gilt

$$a(-b) = -(ab) = (-a)b,\ (-a)(-b) = ab \text{ und } (-1)a = -a = a(-1)$$

Beweis:
(b):

$$0 \cdot a = (0+0)a \overset{\text{R1}}{=} 0a + 0a \overset{\text{Kürzen}}{\Rightarrow} 0a = 0$$

genauso $a \cdot 0 = 0$.
(c):

$$a(-b) + ab \overset{\text{R1}}{=} a(b-b) = a0 = 0 \Rightarrow a(-b) = -(ab)$$

genauso

$$(-a)b + ab = (-a+a)b = 0b = 0 \Rightarrow (-a)b = -(ab)$$

$$(-a)(-b) = -(a(-b)) = -(-(ab)) = ab$$

sowie

$$(-1)a = -(1a) = -a = a(-1)$$

□

Vorsicht! Beim Multiplizieren darf man nicht immer einfach kürzen. Beispiel:

$$a = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix},\ x = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix},\ y = \begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix}$$

$a, x, y \in \mathbb{R}^{2\times 2},\ ax = ay$, aber $x \neq y$.

3.3 Definition Einheiten

Sei R ein Ring. Ein Element $a \in R$ heißt **Einheit**, wenn es $b \in R$ gibt mit

$$ab = 1 = ba$$

Die Menge aller Einheiten ist die **Einheitengruppe**

$$R^* = \{a \in R \mid a \text{ Einheit}\}$$

Offensichtlich ist $(R^*, \cdot)$ eine Gruppe, mit 1 als Neutralelement.

Beispiel:

(a) K Körper, $K^* = K \backslash \{0\}$

(b) $\mathbb{Z}^* = \{\pm 1\}$

(c) $\mathrm{End}(V)^* = \mathrm{Gl}(V) = \{\varphi : V \to V \mid \varphi \text{ linear + bijektiv}\}$

(d) $R = \{0\},\ R^* = R$

3.4 Homomorphismen und Ideale

Seien R und S Ringe. Eine Abbildung $\varphi : R \to S$ heißt **Ringhomomorphismus**, wenn für alle $x, y \in R$ gilt:

(H1) $\varphi(x+y) = \varphi(x) + \varphi(y)$

(H2) $\varphi(xy) = \varphi(x)\varphi(y)$

(H3) $\varphi(1_R) = 1_S$

(H1) sagt, dass φ ein Homomorphismus der additven Gruppe $(R,+)$ und $(S,+)$ ist.
Der Kern eines Ringhomomorphismus φ ist

$$\ker(\varphi) = \{x \in R \mid \varphi(x) = 0\}$$

Ist R ein Ring und $S \subseteq R$ eine Teilmenge mit folgenden Eigenschaften, so heißt S **Teilring** oder **Unterring**

(TR1) $0 \in S$ und $x \pm y \in S$ für alle $x, y \in S$

(TR2) $x \cdot y \in S$ für alle $x, y \in S$

(TR3) $1 \in S$

Wenn nur (TR1) und (TR2) verlangt wird, spricht man von einem "Teilrng".
Sei R ein Ring. Ein Teilrng $I \in R$ heißt **Ideal**, wenn für alle $r \in R$ und $i \in I$ gilt

$$ir \in I \text{ und } ri \in I$$

Man schreibt $I \trianglelefteq R$. Für ein Ideal $I \trianglelefteq R$ gilt offensichtlich

$$I = R \Leftrightarrow 1 \in I$$

(denn: $1 \in I \Rightarrow r = r \cdot 1 \in I$ für alle $r \in R$.)

Konstruktion

Sei R ein Ring und $I \trianglelefteq R$ Ideal. Dann ist

$$R/I = \{x + I \mid x \in R\}$$

ein Ring mit Multiplikation

$$(x + I)(y + I) = xy + I$$

Denn: Das ist eine wohldefinierte Verknüpfung,

$$\begin{array}{l} x + I = x' + I \\ y + I = y' + I \end{array} \Rightarrow \begin{array}{l} x' = x + i \\ y' = y + j \end{array} \text{ für } i, j \in I \Rightarrow x'y' + I = (x + i)(y + j) + I$$
$$= xy + \underbrace{iy + xj + ij}_{\in I} + I = xy + I$$

Es gilt weiter

$$(1 + I)(x + I) = (x + I) = (x + I)(1 + I)$$

□

Satz

Sei R ein Ring und $I \subseteq R$. Dann sind äquivalent:

(i) $I \trianglelefteq R$

(ii) Es gibt ein Ring S und einen Homomorphismus $R \xrightarrow{\varphi} S$ mit $\ker(\varphi) = I$.

Beweis:
(i)⇒(ii): Setze $S = {}^{R}/_{I},\ \pi_I : R \to S,\ x \mapsto x + I$
Nach obiger Konstruktion ist ${}^{R}/_{I}$ ein Ring. Es gilt

$$\ker(\pi_I) = \{x \in R \mid x + I = I\} = I$$

(ii)⇒(i): Sei $\varphi : R \to S$ ein Ringhomomorphismus mit $I = \ker(\varphi)$. Dann ist $(I, +)$ Untergruppe von $(R, +)$. Für alle $i \in I,\ r \in R$ gilt

$$\left.\begin{array}{c}\varphi(ir) = \varphi(i)\varphi(r) = 0_S \cdot \varphi(r) = 0_S \\ \text{und } \varphi(ri) = \cdots = 0_S\end{array}\right\} \Rightarrow ir, ri \in I$$

□

3.5 Homomorphiesatz für Ringe, Isomorphiesätze

Satz (Homomorphiesatz)

Sei $R \overset{\varphi}{\to} S$ ein Ringhomomorphismus, sei $I \trianglelefteq R$ Ideal mit $I \subseteq \ker(\varphi)$. Dann gibt es genau ein Ringhomomorphismus $\overline{\varphi} : {}^{R}/_{I} \to S$ mit $\overline{\varphi} \circ \pi_I = \varphi$

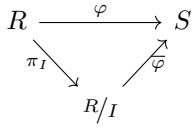


Abbildung 4: Homomorphiesatz für Ringe

Beweis:
Aus dem Isomorphiesatz für Gruppen 1.20 angewandt auf den Gruppenhomomorphismus $(R, +) \overset{\varphi}{\to} (S, +)$ erhalten wir die Existenz und Eindeutigkeit des Gruppenhomomorphismus $\overline{\varphi}$. Zu zeigen bleibt, dass $\overline{\varphi}$ ein Ringhomomorphismus ist. Für $x \in R$ gilt

$$\overline{\varphi}(x + I) = \varphi(x) \qquad \text{vgl. 1.20}$$

$$\overline{\varphi}(xy + I) = \varphi(xy) \overset{\varphi \text{ Ringhom.}}{=} \varphi(x)\varphi(y) = \overline{\varphi}(x + I)\overline{\varphi}(y + I)$$

sowie

$$\overline{\varphi}(1_R + I) = \varphi(1_R) = 1_S$$

□

Satz (1. Isomorphiesatz für Ringe)

Sei R ein Ring, $S \subseteq R$ Teilring und $I \trianglelefteq R$ ein Ideal. Dann ist $S + I = \{s + i \mid s \in S,\ i \in I\} \subseteq R$ Teilring und $S \cap I \trianglelefteq S$ Ideal. Die Abbildung

$${}^{s}/_{s\cap I} \overset{\varphi}{\to} {}^{S+I}/_{I},\ s + S \cap I \mapsto s + I$$

ist ein Ringisomorphismus (bijektiver Ringhomomorphismus).

Beweis:
Klar: $S + I$ und $S \cap I$ sind Untergruppen in $(R, +)$. Für $s, s' \in S,\ i, i' \in I$ gilt

$$(s + i)(s' + i') = ss' + \underbrace{is' + si + ii'}_{\in I} \in S + I$$

sowie $1 \in S \subseteq S+I \Rightarrow S+I \subseteq R$ ist Teilring. Für $s \in S,\ i \in I \cap S$ gilt $\left.\begin{matrix} is \in I \cap S \\ si \in I \cap S \end{matrix}\right\} \Rightarrow I \cap S \trianglelefteq S.$
Die Abbildung $\varphi : s+S\cap I \mapsto s+I$ ist nach 1.23 ein Gruppenisomorphismus bzgl. der Addition. Es gilt $\varphi(1+S\cap I) = 1+I$ sowie für $s,t \in S$

$$\varphi(st+I\cap S) = st+I = (s+I)(t+I) = \varphi(s+I\cap S)\varphi(t+I\cap s)$$

□

Satz (2. Isomorphiesatz für Ringe)

Sei R ein Ring, $I, J \trianglelefteq R$ Ideale mit $I \subseteq J$. Dann ist

$$J/I = \{j+I \mid j \in J\} \subseteq R/I$$

ein Ideal und es gibt

$$\frac{R/I}{J/I} \xrightarrow{\cong} R/J$$

einen Ringisomorphismus.

Beweis:
Genau wie in 1.23. Betrachte $\psi : R \to R/J,\ x \mapsto x+J \rightsquigarrow$ Homomorphismus $\overline{\psi} : R/I \to R/J$ (Homomorphiesatz). $\ker(\overline{\psi} = J/I)$, also existiert der Ringisomorphismus. □

Bemerkung

Ein **Ringisomorphismus** ist also ein bijektiver Ringhomomorphismus $\varphi : R \to S$. Die Umkehrabbildung ψ von φ, $\psi : S \to R$ ist dann ebenfalls ein Ringhomomorphismus (Ringisomorphismus).

3.6 Rechnen mit Idealen

Sei R ein Ring mit Idealen $I, J \trianglelefteq R$. Dann sind auch die folgenden Mengen Ideale:

(a) $I+J = \{i+j \mid i \in I,\ j \in J\}$

(b) $I \cap J$

(c) $IJ = \{i_1j_1 + i_2j_2 + \cdots + i_lj_l \mid l \geq 1,\ i_1,\ldots,i_l \in I,\ j_1,\ldots,j_l \in J\}$

Es gilt

$$IJ \subseteq I\cap J \subseteq I, J \subseteq I+J$$

Beweis:
Klar: $I+J,\ I\cap J$ und IJ sind additive Gruppen. Sei $r \in R,\ i \in I,\ j \in J$. Es folgt

$$r(i+j) = \underbrace{ri+rj}_{\in I+J}$$

$$(i+j)r = \underbrace{ir+jr}_{\in I+J} \Rightarrow I+J \trianglelefteq R$$

$$i \in I\cap J \Rightarrow ri \in I\cap J \Rightarrow I\cap J \trianglelefteq R$$

$$r(ij) = \underbrace{ri}_{\in I}\cdot j \in J \text{ genauso } r(ij) \in I$$

also $IJ \trianglelefteq R$ und $IJ \subseteq I\cap J$. □

3.7 Beispiel 6, Ideale

(a) K ein Körper. Ist $I \trianglelefteq K$ Ideal und $I \neq \{0\}$, so folgt $1 \in I$, denn:

$$i \in I \backslash \{0\} \Rightarrow i^{-1}i = 1 \in I \Rightarrow I = K.$$

Also sind $\{0\}$ und K die einzigen Ideale in K.

(b) $V \neq \{0\}$ ein K-Vektorraum, $R = \mathrm{End}(V)$. Die einzigen Ideale in R sind $\{0\}, R$ ($\rightsquigarrow$ Höhere Algebra?)

(c) R kommutativer Ring, $a \in R$. Setze $(a) := Ra = \{ra \mid r \in R\}$. Dann gilt $(a) \trianglelefteq R$.
Denn

$$0 = 0a \in Ra,\ ra, sa \in Ra \Rightarrow ra \pm sa = (r \pm s)a \in Ra$$

Für $r, s \in R$ gilt

$$r \underbrace{sa}_{\in Ra} = (rs)a \in Ra \rightsquigarrow \text{Ideal}$$

(d) $R = \mathbb{Z}$. Wir zeigen gleich: jedes Ideal $I \trianglelefteq \mathbb{Z}$ ist von der Form $I = m\mathbb{Z} = \{mk \mid k \in \mathbb{Z}\}$ für ein $m \in \mathbb{N}$. Als Quotient erhält man für $m \geq 1$

$$\mathbb{Z}/_m := \mathbb{Z}/_{m\mathbb{Z}} = \{\overline{0}, \ldots, \overline{m-1}, \overline{m} = \overline{0}\}$$

$\overline{k} = k + m\mathbb{Z}$ **Kongruenzklasse** von k **modulo** m (die Bedeutung des Querstrichs hängt also vom m ab!)
Addition: $\overline{k} \pm \overline{l} = \overline{k \pm l}$, Multiplikation: $\overline{k} \cdot \overline{l} = \overline{kl}$ nach 3.4. Also ist für $m \geq 1$ $\mathbb{Z}/_m$ ein kommutativer Ring mit m Elementen. Für $m = 0$ gilt $\mathbb{Z}/_0 \cong \mathbb{Z}$.

3.8 Satz 12

Sei $I \subseteq \mathbb{Z}$ eine Teilmenge. Dann sind äquivalent:

(i) $I = m\mathbb{Z} = \{mk \mid k \in \mathbb{Z}\}$ für ein $m \in \mathbb{N}$

(ii) $I \subseteq \mathbb{Z}$ ist eine Untergruppe (bzgl. Addition)

(iii) $I \subseteq \mathbb{Z}$ ist ein Rng (Ring ohne Eins)

(iv) $I \trianglelefteq \mathbb{Z}$ ist ein Ideal

Beweis:
(iv)⇒(iii)⇒(ii) nach Definition. Wir haben eben überlegt, dass $m\mathbb{Z} \trianglelefteq \mathbb{Z}$, also (i)⇒(iv). Fehlt noch (ii)⇒(i): Sei $I \subseteq \mathbb{Z}$ Untergruppe bzgl. "+".

Fall 1: $I = \{0\} = 0\mathbb{Z}$ fertig.
Fall 2: Es gibt $x \in I,\ x \neq 0$. Es folgt $\pm x \in I$, also gibt es $x \in I$ mit $x > 0$. Setze $m = \min\{x \in I \mid x > 0\}$. Es folgt $m \in I$ und damit $m\mathbb{Z} \subseteq I$, weil I Untergruppe ist.
Behauptung: $I = m\mathbb{Z}$. Denn angenommen, $y \in I \backslash m\mathbb{Z}$. Teilen durch m mit Rest liefert

$$y = \underbrace{m \cdot k}_{\in m\mathbb{Z}} + l \text{ mit } 0 \leq l < m$$

und $l \neq 0$ wegen $y \notin m\mathbb{Z}$. Es folgt

$$y - mk = l \in I, \text{ aber } 0 < l < m \quad \lightning \text{ zur Minimalität von } m$$

Also gibt es solch ein y nicht, $I = m\mathbb{Z}$. □

3.9 Definition Nullteiler

Sei R ein Ring. Ein Element $a \in R$ heißt **Nullteiler**, wenn es ein $0 \neq b \in R$ gibt mit

$$ab = 0 \text{ (oder } ba = 0)$$

Beispiele

(a) $R = \mathbb{Z}$. Der einzige Nullteiler ist 0.

(b) $R = \mathbb{Z}/6$. Es gilt $\overline{2} \neq \overline{0} \neq \overline{3}$, aber $\overline{2} \cdot \overline{3} = \overline{6} = \overline{0}$, also sind $\overline{0}, \overline{2}, \overline{3}$ Nullteiler in $\mathbb{Z}/6$.

Ist R ein Ring und $a \in R$ kein Nullteiler in R, dann darf man beim Multiplizieren mit a kürzen, d.h.

$$ax = ay \Rightarrow x = y$$

Denn

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

□

3.10 Definition Integritätsbereich

Ein kommutativer Ring $R \neq \{0\}$ heißt **Integritätsbereich** (engl.: integral domain oder domain), wenn 0 der einzige Nullteiler in R ist.

Beispiele

(a) $\mathbb{Z}$ ist ein Integritätsbereich.

(b) Jeder Körper ist ein Integritätsbereich.

(c) $\mathbb{Z}/6$ ist kein Integritätsbereich.

Lemma

Jeder endliche Integritätsbereich ist ein Körper.

Beweis:
Sei R ein endlicher Integritätsbereich. Also gilt $R \neq \{0\}$. Sei $a \in R \backslash \{0\}$, zeige, dass a eine Einheit ist, d.h. es gibt $b \in R$ mit $ab = 1$.
Betrachte die Abbildung $\lambda_a : R \to R,\ x \mapsto ax$. Diese Abbildung λ_a ist injektiv, denn

$$\lambda_a(x) = \lambda_a(y) \Rightarrow ax = ay \overset{a \neq 0}{\Rightarrow} x = y$$

Weil R endlich ist, ist λ_a auch surjektiv, insbesondere gibt es $b \in R$ mit

$$\lambda_a(b) = ab = 1$$

□

Bemerkung

$\mathbb{Z}$ ist ein (unendlicher) Integritätsbereich, aber kein Körper.

3.11 Der Quotientenkörper eines Integritätsbereiches

Ziel: R Integritätsbereich, konstruiere aus R ein Körper Q, der R als Teilring enthält. Idee: Kopiere die Konstruktion von $\mathbb{Q}$ aus $\mathbb{Z}$.

Sei R ein Integritätsbereich, z.B. $R = \mathbb{Z}$. Setze $M = \{(x, y) \mid x, y \in R,\ y \neq 0\}$. Definiere Verknüpfungen $+$ und $\cdot$ auf M durch

$$(x, y) + (u, v) := (xv + yu, \underbrace{yv}_{\neq 0})$$

$$(x, y) \cdot (u, v) := (xu, \underbrace{yv}_{\neq 0})$$

Es gilt $(x, y) + (0, 1) = (x, y) = (0, 1) + (x, y)$, ebenso $(x, y) \cdot (1, 1) = (x, y) = (1, 1) \cdot (x, y)$.
Beide Verknüpfungen sind assoziativ (nachzurechnen...), aber es fehlen Kürzungs- und Erweiterungsregeln für Brüche. Inverse funktionieren so nicht.
Wir definieren eine Relation $\sim$ auf M durch:

$$(x, y) \sim (x', y') \overset{\text{DEF}}{\Leftrightarrow} \qquad \left(\frac{x}{y} = \frac{x'}{y'} \Leftrightarrow xy' = x'y\right)$$

Behauptung: Das ist $\sim$ eine Äquivalenzrelation auf M.
Denn:

$$(x, y) \sim (x, y)\ (\checkmark)$$

$$(x, y) \sim (x', y') \Rightarrow (x', y') \sim (x, y)\ (\checkmark)$$

$$(x, y) \sim (x', y') \sim (x'', y'') \overset{!}{\Rightarrow} (x, y) \sim (x'', y'')$$

Folgt aus: $xy' = x'y$ und $x'y'' = x''y'$

$$\Rightarrow xx'y'' = xx''y',\ xx'y'' = x'x''y \overset{x' \neq 0}{\Rightarrow} xy'' = x''y$$

Wenn $x' = 0$, dann $x = x'' = 0$. $(\checkmark)$

Wir bezeichnen die Äquivalenzklassen von $(x, y) \in M$ mit

$$\frac{x}{y} = \{(x', y') \in M \mid (x, y) \sim (x', y')\}$$

Setze $\mathrm{Quot}(R) := \left\{\frac{a}{b} \mid (a, b) \in Q\right\}$.
Behauptung:

$$\left.\begin{array}{l}(x, y) \sim (x', y') \\ (u, v) \sim (u', v')\end{array}\right\} \Rightarrow \begin{array}{c}(x, y) + (u, v) \sim (x', y') \sim (u', v') \\ \text{und } (x, y) \cdot (u, v) \sim (x', y') \cdot (u', v')\end{array}$$

Denn:

$$(xxv + yu, yv) \sim (x'v' + u'y', y'v')$$

$$\Leftrightarrow \underbrace{xy'}_{} vv' + \underbrace{uv'}_{} yy' = \underbrace{x'y}_{} vv' + \underbrace{u'v}_{} yy'$$

und $xy' = x'y$ sowie $uv' = u'v$, Rest genauso.

Folgerung: Wir erhalten wohldefinierte Verknüpfungen

$$\frac{x}{y} + \frac{u}{v} = \frac{xv + yu}{yv},\ \frac{x}{y} \cdot \frac{u}{v} = \frac{xu}{yv}$$

Eine Routine-Rechnung zeigt: $(\mathrm{Quot}(R), +, \cdot)$ ist ein Ring mit Nullelement $\frac{0}{1}$ und Einselement $\frac{1}{1} \neq \frac{0}{1}$. Ist $a, b \neq 0$ so gilt $\frac{a}{b} \cdot \frac{b}{a} = \frac{1}{1}$, also ist $\mathrm{Quot}(R)$ sogar ein Körper.
Wir definieren $\iota : R \to \mathrm{Quot}(R),\ r \mapsto \frac{r}{1}$, das ist ein Ringhomomorphismus und injektiv, $\ker(\iota) = \{e\}$. Für $R = \mathbb{Z}$ erhalten wir genau $\mathrm{Quot}(\mathbb{Z}) = \mathbb{Q}$.

Satz

Der **Quotientenkörper** $\mathrm{Quot}(R)$ hat folgende universelle Eigenschaft:
Ist K ein Körper und R ein Integritätsbereich und ist $\varphi : R \to K$ ein injektiver Ringhomomorphismus, so gibt es genau einen Ringhomomorphismus $\tilde{\varphi}$ mit

$$\tilde{\varphi} \circ \iota = \varphi$$

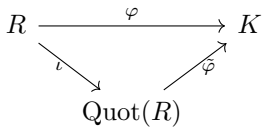


Abbildung 5: Quotientenkörper

Beweis:
Definiere $\tilde{\varphi}\left(\frac{a}{b}\right) = \frac{\varphi(a)}{\varphi(b)}$. Das ist wohldefiniert:

$$\frac{a}{b} = \frac{a'}{b'} \Rightarrow ab' = a'b \Rightarrow \varphi(a)\underbrace{\varphi(b')}_{\neq 0} = \varphi(a')\underbrace{\varphi(b)}_{\neq 0} \text{ da } \varphi \text{ injektiv}$$

$$\Rightarrow \frac{\varphi(a)}{\varphi(b)} = \frac{\varphi(a')}{\varphi(b')}$$

Es folgt (nachrechnen), dass $\tilde{\varphi}$ ein Homomorphismus ist

$$\tilde{\varphi}\left(\frac{a}{b} + \frac{u}{v}\right) = \tilde{\varphi}\left(\frac{a}{b}\right) + \tilde{\varphi}\left(\frac{u}{v}\right),\ \tilde{\varphi}\left(\frac{a}{b} \cdot \frac{u}{v}\right) = \tilde{\varphi}\left(\frac{a}{b}\right) \cdot \tilde{\varphi}\left(\frac{u}{v}\right),\ \tilde{\varphi}\left(\frac{1}{1}\right) = \mathbb{1}_K$$

Zur Eindeutigkeit von $\tilde{\varphi}$: Angenommen, $\psi : \mathrm{Quot}(R) \to K$ ist ein Homomorphismus mit $\psi \circ \iota = \varphi$. Für $a, b \in R,\ b \neq 0$ folgt

$$\varphi(a) = \psi\left(\frac{a}{1}\right),\ \varphi(b) = \psi\left(\frac{b}{1}\right) \neq 0 \Rightarrow \psi\left(\frac{1}{b}\right) = \frac{1}{\varphi(b)} \Rightarrow \psi\left(\frac{a}{b}\right) = \psi\left(\frac{a}{1} \cdot \frac{1}{b}\right) = \frac{\varphi(a)}{\varphi(b)}$$

□

3.12 Satz 13

Sei $\varphi : R \to S$ ein Homomorphismus von (kommutativen oder nicht kommutativen) Ringen. Wenn $I \trianglelefteq R$ ein Ideal ist, so ist $\varphi(I) \trianglelefteq \varphi(R)$ ein Ideal (und $\varphi(R) \subseteq S$ ist Teilring). Wenn $J \trianglelefteq S$ ein Ideal ist, so ist $\varphi^{-1}(J) = \{r \in R \mid \varphi(r) \in J\} \trianglelefteq R$ ein Ideal.

Beweis:
Übungsaufgabe! □

3.13 Definition verschiedener Ideale

Sei R ein kommutativer Ring und $I \trianglelefteq R$ ein Ideal.

(a) I heißt **maximales Ideal**, wenn $I \neq R$ und wenn es kein Ideal $J \trianglelefteq R$ gibt mit

$$I \subsetneq J \subsetneq R$$

(b) I heißt **Primideal**, wenn gilt: $I \neq R$ und für $a, b \in R$ und $ab \in I$, so folgt

$$a \in I \text{ oder } b \in I$$

Satz

Sei R ein kommutativer Ring, sei $I \trianglelefteq R$ ein Ideal.

(i) I ist Primideal genau dann, wenn R/I ein Integritätsbereich ist.

(ii) I ist maximales Ideal genau dann, wenn R/I ein Körper ist.

Beweis:
(i): Ist I Primideal, so ist $I \neq R \rightsquigarrow R/I \neq \{0\}$. Ist $x = r + I,\ y = s + I$ und $xy = I$, so folgt $rs \in I \rightsquigarrow r \in I$ oder $s \in I \rightsquigarrow x = I$ oder $y = I \Rightarrow R/I$ Integritätsbereich.
Ist R/I ein Integritätsbereich, so ist $I \neq R$. Für $r, s \in R$ gilt

$$\pi_I(rs) = 0 + I \Leftrightarrow rs \in I \Leftrightarrow \pi_I(r) = r + I = I \text{ oder } \pi_I(s) = s + I = I \Leftrightarrow r \in I \text{ oder } s \in I$$

□

(ii): Sei $I \trianglelefteq R$ ein maximales Ideal, sei $a + I \in R/I$ mit $a \notin I$. Da $(a) + I = aR + I$ ein Ideal ist und $I \subsetneq (a) + I$, folgt $R = (a) + I$, d.h. es gibt $b \in R$ und $i \in I$ mit $ab + i = 1$. Es folgt

$$(a + I)(b + I) = ab + i + I = ab + I = 1 + I,$$

also $a + I \in (R/I)^*$ Einheit $\Rightarrow R/I$ ist Körper.
Ist R/I ein Körper, so ist $I \neq R$. Angenommen, $J \trianglelefteq R$ ist ein Ideal mit $I \subsetneq J$. Es folgt aus 3.12, dass $\pi_I(J) \subseteq R/I$ ein Ideal ist und $\pi_I(J) \neq \{0_{R/I}\}$. Da R/I ein Körper ist, folgt mit 3.7(a),dass $\pi_I(J) = R/I$. Wegen $I \supseteq J$ folgt

$$J = \pi_I^{-1}(\pi_I(J)) = R$$

□

Korollar

Jedes maximale Ideal ist ein Primideal.

Beweis:
Jeder Körper ist ein Integritätsbereich. □

3.14 Satz 14

Sei R ein kommutativer Ring, sei $R \neq I \trianglelefteq R$ ein Ideal. Dann existiert ein maximales Ideal $J \trianglelefteq R$ mit

$$I \subseteq J \subsetneq R.$$

Beweis:
Sei $P = \{J \trianglelefteq R \mid 1 \notin J \text{ und } I \subseteq J\}$. Dann ist P bzgl. $\subseteq$ partiell geordnet. Wir benutzen Zorns Lemma, vgl. LA II §7. Sei $C \subseteq P$ eine Kette (d.h. für alle $J, K \in C$ gilt $J \subseteq K$ oder $K \subseteq J$). Setze $J = \bigcup C$. Es folgt $1 \notin J$ (weil $1 \notin \bigcup P$).
Behauptung: J ist ein Ideal.
Denn: $a, b \in J,\ r \in R \rightsquigarrow$ es gibt $K, L \in C$ mit $a \in K,\ b \in L$.
ŒK $\subseteq L$: $\Rightarrow a, b \in L \rightsquigarrow a \pm b \in L,\ a \cdot b \in L,\ ra \in L$. Wegen $L \subseteq J$ folgt

$$a \cdot b,\ a \pm b,\ ra \in J.$$

Also $J \trianglelefteq R$. Wegen $1 \notin J$ ist $R \neq J$, also (wegen $I \subseteq J$) $J \in P$.
Nach Zorns Lemma gibt es maximale Elemente in P. Nach Konstruktion und 3.4 besteht P genau aus allen Idealen $J \trianglelefteq R$ mit

$$I \subseteq J \subsetneq R.$$

□

Korollar

Ist R ein kommutativer Ring, $R \neq \{0\}$, so existiert ein Körper K und ein surjektiver Ringhomomorphismus $R \overset{\varphi}{\to} K$. □

3.15 Beispiel 7

$R = \mathbb{Z}$ wir wissen bereits: alle Ideale sind von der Form $I = m\mathbb{Z},\ m \in \mathbb{N}$.

- $I = \{0\} = 0\mathbb{Z}$ ist ein Primideal, denn $\mathbb{Z}/0 \cong \mathbb{Z}$ ist Integritätsbereich. Oder direkt: $a, b \in \mathbb{Z},\ ab \in \{0\} \Rightarrow a = 0$ oder $b = 0$.
- p Primzahl $\rightsquigarrow p\mathbb{Z}$ Primideal, denn: $a, b \in \mathbb{Z}$:

  $$ab = k \cdot p \rightsquigarrow p \text{ teilt } a \text{ oder } p \text{ teilt } b \overset{\text{Euklids Lemma}}{\rightsquigarrow} a \in p\mathbb{Z} \text{ oder } b \in p\mathbb{Z}.$$

  Da jeder endliche Integritätsbereich ein Körper ist, vgl.3.10, ist $p\mathbb{Z}$ auch ein maximales Ideal in $\mathbb{Z}$.
- $m = k \cdot l$ mit $k, l \geq 2$. Dann gilt

  $$\overline{k} \cdot \overline{l} = \overline{m} = \overline{0}, \text{ aber } \overline{k} \neq \overline{0} \neq \overline{l}.$$

  Da $\mathbb{Z}/m$ kein Integritätsbereich ist, ist $m\mathbb{Z}$ kein Primideal.

Fazit: Die Primideale in $\mathbb{Z}$ sind die Ideale $0\mathbb{Z},\ p\mathbb{Z}$ mit p ist Primzahl. Die maximalen Ideale in $\mathbb{Z}$ sind die Ideale $p\mathbb{Z}$ mit p ist Primzahl.
Wenn $m > 1$ und m keine Primzahl ist, dann ist $m\mathbb{Z}$ kein Primideal/maximales Ideal (und $1 \cdot \mathbb{Z} = \mathbb{Z}$ ist kein echtes Ideal!)

3.16 Erinnerung

Zwei Zahlen $k, l \in \mathbb{Z}$ heißen **teilerfremd** oder **koprim**, wenn ± 1 die einzigen gemeinsamen Teiler von k und l sind.

Beispiel:

- $1, l$ sind für alle $l \in \mathbb{Z}$ koprim.
- $|0, 1|$ sind koprim, 2,6 sind nicht koprim.
- $0, l$ sind für $l \neq \pm 1$ koprim.

Lemma

Sei $k, l \in \mathbb{Z}$. Dann sind äquivalent:

(i) k und l sind koprim.

(ii) $1 \in k\mathbb{Z} + l\mathbb{Z}$ (äquivalent: $\mathbb{Z} = k\mathbb{Z} + l\mathbb{Z}$, vgl. 3.4 und 3.6).

(iii) $\overline{k}$ ist Einheit in $\mathbb{Z}/l\mathbb{Z}$.

Beweis:
(iii)⇒(ii): $\overline{k}$ Einheit $\rightsquigarrow \overline{k}\overline{u} = \overline{1}$ für ein $u \in \mathbb{Z} \rightsquigarrow ku = 1 + lv$ für $u, v \in \mathbb{Z} \Rightarrow 1 = ku - vl$.

(ii)⇒(i): Ist t ein Teiler von k und l, so ist t auch Teiler von $ku + lv = 1$, fertig.

(i)⇒(iii): Angenommen, $\overline{k}$ ist keine Einheit in $\mathbb{Z}/l\mathbb{Z}$.
1. Fall: $l = 0 \rightsquigarrow k$ keine Einheit in $\mathbb{Z} \rightsquigarrow k \neq \pm 1$ (dann $\mathbb{Z}^* = \{\pm 1\}$) $\rightsquigarrow k, l$ koprim (✓)
2. Fall: $l \neq 0$. Dann gibt es $w \in \mathbb{Z}$ mit $0 < w < |l|$ mit $\overline{kw} = \overline{0}$ (ÜA 8.3), d.h.

$$o(\overline{k}) \leq w < |l| = \#\mathbb{Z}/l\mathbb{Z}.$$

Setze $u = o(\overline{k})$, dann gibt es $l' \neq \pm 1$ mit $l'u = l$, denn u teilt $|l|$ nach Lagrange.
Es folgt

$$u\overline{k} = \overline{0} \rightsquigarrow uk = vl = vul' \Rightarrow k = vl'$$

also ist $l' \neq \pm 1$ ein gemeinsamer Teiler von k und l.

3.17 Produkt von Ringen

Sei $(R_i)_{i \in I}$ eine (endliche oder unendliche) Familie von Ringen. Dann ist auch

$$R = \prod_{i \in I} R_i$$

ein Ring, mit

$$(x_i)_{i \in I} + (y_i)_{i \in I} = (x_i + y_i)_{i \in I},\ (x_i)_{i \in I} \cdot (y_i)_{i \in I} = (x_i \cdot y_i)_{i \in I}$$

Nullelement $(0_i)_{i \in I}$, Einselement $(1_i)_{i \in I}$. Solche Produkte haben im allgemeinen viele Nullteiler, $\mathbb{Z} \times \mathbb{Z}$ hat $(l, 0)$ sowie $(0, l)$ als Nullteiler.

Koprime Ideale

Sei R ein kommutativer Ring. Zwei Ideale $I, J \trianglelefteq R$ heißen koprim, wenn gilt

$$R = I + J \qquad (\text{äquivalent: } 1 \in I + J)$$

3.18 Der chinesische Restsatz

Theorem (Chinesischer Restsatz, algebraische Version)

Sei R ein kommutativer Ring und seien $I_1, \ldots, I_n \trianglelefteq R$ Ideale. Wenn für alle $1 \leq s < t \leq n$ gilt $R = I_s + I_t$ (d.h. wenn die Ideale $I_1, \ldots, I_n$ paarweise koprim sind), dann ist der Ringhomomorphismus

$$R \xrightarrow{\pi} R/I_1 \times \cdots \times R/I_n,\ r \mapsto (r + I_1, \ldots, r + I_n)$$

surjektiv. Der Kern von π ist $I_1 \cap \cdots \cap I_n$.

Beweis:
Induktion nach n. Für $n = 1$ ist nichts zu zeigen. Wir nehmen jetzt an, die Aussage gilt für n paarweise koprime Ideale.
Seien $I_1, \ldots, I_{n+1} \trianglelefteq R$ paarweise koprim. Sei $(x_1, \ldots, x_{n+1}) \in R^{n+1}$ gegeben. Wir suchen ein $x \in R$ mit $x + I_s = x_s + I_s$ für $s = 1, \ldots, n$ mit

$$y_s + z_s = 1\ (I_s + I_{n+1} = R).$$

Es folgt

$$1 = (y_1 + z_1) \cdots (y_n + z_n) \in \underbrace{I_1 \cdot I_2 \cdots I_n}_{= K \subseteq I_n \cap \cdots \cap I_n} + I_{n+1}$$

also sind $K = I_1 I_2 \cdots I_n \subseteq I_1 \cap \cdots \cap I_n$ und I_{n+1} koprim. Wähle $j \in I_{n+1}$ und $k \in K$ mit $j + k = 1$. Wähle jetzt $x' \in R^n$ so, dass gilt

$$\begin{aligned} x_s + I_s &= x' + I_s \text{ für } s = 1, \ldots, n \text{ (Induktionsannahme)} \\ 1 + I_s &= (j + k) + I_s \overset{k \in I_s \subseteq K}{=} j + I_s \text{ für } 1 \leq s \leq n \\ 1 + I_{n+1} &= (j + k) + I_{n+1} = k + I_{n+1} \end{aligned}$$

Setze $x = \underbrace{x' \cdot j}_{\in I_{n+1}} + \underbrace{x_{n+1} \cdot k}_{\in K}$, es folgt

$$x + I_s = x' \cdot j + I_s = x'(j + k) + I_s = x' + I_s,\ 1 \leq s \leq n$$

$$x + I_{n+1} = x_{n+1} \cdot k + I_{n+1} = x_{n+1}(j + k) + I_{n+1} = x_{n+1} + I_{n+1}$$

Der Kern von π ist

$$\{x \in R \mid x + I_1 = I_1, \ldots, x + I_n = I_n\} = \{x \in R \mid x \in I_1, \ldots, x \in I_n\} = I_1 \cap \cdots \cap I_n$$

□

Korollar A (Chinesischer Restsatz, Sun Zi)

Seien $l_1, \ldots, l_n \in \mathbb{Z}$ n verschiedene paarweise koprime ganze Zahlen. Dann gibt es zu jedem n-Tupel $(x_1, \ldots, x_n) \in \mathbb{Z}^n$ eine ganze Zahl $y \in \mathbb{Z}$ mit

$$y + l_i\mathbb{Z} = x_i + l_i\mathbb{Z},\ i = 1, \ldots, n$$

□

Korollar B

Seien $l_1, \ldots, l_n \in \mathbb{Z}$ n paarweise koprime ganze Zahlen. Dann existiert ein Ringisomorphismus

$$\mathbb{Z}/_{l_1 \cdots l_n \mathbb{Z}} \overset{\cong}{\to} \mathbb{Z}/_{l_1\mathbb{Z}} \times \cdots \times \mathbb{Z}/_{l_n\mathbb{Z}}$$

Beweis:
Betrachte $\pi : \mathbb{Z} \to \mathbb{Z}/_{l_1\mathbb{Z}} \times \cdots \times \mathbb{Z}/_{l_n\mathbb{Z}}$ Epimorphismus wie im Theorem. Es gilt

$$\ker(\pi) = l_1\mathbb{Z} \cap \cdots \cap l_n\mathbb{Z}.$$

Für $n = 2$ erhalten wir $l_1\mathbb{Z} \cap l_n\mathbb{Z} = l_1 l_2 \mathbb{Z}$ (denn $l_1 l_2$ ist das kleinste gemeinsame Vielfache von l_1, l_2 vgl. ÜA 8.2) und damit sofort

$$l_1\mathbb{Z} \cap \cdots \cap l_n\mathbb{Z} = l_1 \cdots l_n \mathbb{Z}$$

per Induktion. Jetzt Homomorphiesatz 3.5. □

3.19 Polynomringe

Sei R ein kommutativer Ring. Sei $R^{(\mathbb{N})} = \{(r_i)_{i \in \mathbb{N}} \mid r_i = 0 \text{ für fast alle } i \in \mathbb{N}\}$ ('für **fast alle**' heißt: nur endlich viele Ausnahmen). Dann ist $R^{(\mathbb{N})}$ eine abelsche Gruppe bzgl. komponentenweiser Addition

$$(r_i)_{i \in \mathbb{N}} + (s_i)_{i \in \mathbb{N}} = (r_i + s_i)_{i \in \mathbb{N}}.$$

Wir definieren eine Multiplikation auf $\mathbb{R}^{(\mathbb{N})}$ wie folgt:

$$(r_i)_{i \in \mathbb{N}} \cdot (s_i)_{i \in \mathbb{N}} = (t_i)_{i \in \mathbb{N}},\ t_j = \sum_{i=0}^{j} r_i s_{j-i}$$

Eine einfache Rechnung zeigt: $\mathbb{R}^{(\mathbb{N})}$ wird mit diesen beiden Verknüpfungen ein kommutativer Ring.
Sei T ein nicht in R enthaltenes Element. Ist $(r_i)_{i\in\mathbb{N}} \in R^{(\mathbb{N})}$, so gibt es ein $n \in \mathbb{N}$ mit $r_i = 0$ für alle $i > n$ (weil nur endlich viele $r_i \neq 0$).
Schreibe formal

$$(r_i)_{i\in\mathbb{N}} = r_0 + r_1T + r_2T^2 + \cdots + r_nT^n$$

Die Terme r_iT^i mit $r_i = 0$ lässt man auch weg. Die beiden Verknüpfungen $+$ und $\cdot$ schreiben sich dann intuitiv als

$$(r_0 + r_1T + \cdots + r_nT^n) + (s_0 + s_1T + \cdots + s_nT^n) = (r_0 + s_0) + (r_1 + s_1)T + \cdots + (r_n + s_n)T^n$$

wobei $n \gg 1$ so gewählt wird, dass $r_i = 0 = s_i$ für alle $i > n$ gilt.

$$(r_0 + \cdots + r_nT^n) \cdot (s_0 + \cdots + s_nT^n) = \sum_{j=0}^{n}\sum_{i=0}^{j} r_is_{j-i}T^j$$

Man nennt $R[T] = \mathbb{R}^{(\mathbb{N})}$ den **Polynomring** über $\mathbb{R}$ (in der Unbekannten T). Die Elemente von $R[T]$ heißen **Polynome** in R (in der Unbekannten T).

Bemerkung

- $T, T^2, T^3, \ldots, T^n$ sind Terme, die man symbolisch hinschreibt. Statt T nennt man die Unbekannten oft auch X und schreibt $R[X]$ usw.
- Der Polynomring $R[T]$ enthält R als Teilring via $R \to R[T],\ t \mapsto r = r + 0T$. Das Nullelement in $R[T]$ ist 0 (das **Nullpolynom**), das Einselement ist $1 = 1 + 0T$. Die Polynome der Form $r,\ r \in R$ nennt man auch konstant oder Skalare.
- Warum haben wir $R[T]$ nicht definiert als Menge der Abbildungen der Form

  $$f(x) = r_0 + xr_1 + x^2r_2 + \cdots + x^nr_n\ ?$$

  Beispiel: $R = \mathbb{F}_2 = \{0, 1\}$. Die beiden Abbildungen

  $$f(x) = 0,\ g(x) = x + x^2$$

  stimmen überein. Dagegen sind die Polynome $0,\ T + T^2 \in \mathbb{F}_2[T]$ so, wie wir das definiert haben, von einander verschieden. In der Algebra ist der Unterschied wichtig!

Der **Grad** eines Polynoms $f = r_0 + r_1T + \cdots + r_nT^n \neq 0$ ist

$$\deg(f) = \max\{k \geq 0 \mid r_k \neq 0\}.$$

Für das Nullpolynom setzt man $\deg(0) = -\infty$. Ist $f = r_0 + r_1T + \cdots + r_nT^n$ mit Grad $\deg(f) = n$, so heißt r_n der **Leitkoeffizient** von f und r_0 heißt der **konstante Term** von f.

3.20 Lemma 8

Seien $f = r_0 + \cdots + r_nT^n,\ g = s_0 + \cdots + s_mT^m$ Polynome in $R[T]$, R ein kommutativer Ring, mit $\deg(f) = n$ und $\deg(g) = m,\ n, m \geq 0$.
Dann gilt

$$\deg(f + g) \leq \max\{\deg(f), \deg(g)\}$$

$$\deg(f \cdot g) \leq \deg(f) \cdot \deg(g)$$

Wenn die Leitkoeffizienten r_n und s_m keine Nullteiler sind, gilt

$$\deg(f \cdot g) = \deg(f) + \deg(g)$$

Beweis:
Die beiden Formeln folgen direkt aus den Additions- und Multiplikationsregeln für Polynome. Es gilt

$$f \cdot g = r_0 s_0 + \cdots + r_n s_m T^{n+m}$$

Wenn also r_n, s_m keine Nullteiler sind, so folgt, dass $r_n s_m$ der Leitkoeffizient von $f \cdot g$ ist.

Korollar

Sei R ein kommutativer Ring. Dann sind äquivalent:

(i) R ist Integritätsbereich

(ii) $R[T]$ ist Integritätsbereich

Beweis:
(i)⇒(ii): Ist $f, g \neq 0$, so ist $\deg(f \cdot g) \neq -\infty$, also $f \cdot g \neq 0$.
(ii)⇒(i): R ist ein Teilring von $R[T]$ □

4 Teilbarkeit in Integritätsbereichen

4.1 Definition Teiler

Sei R ein kommutativer Ring, sei $a, b \in R$. Wir nennen a einen **Teiler** von b, wenn es ein $x \in R$ gibt mit $ax = b$. Schreibe dafür kurz

$$a \mid b \qquad (\text{'}a \text{ teilt } b\text{'})$$

Wenn a kein Teiler von b ist, schreibe $a \nmid b$.
Klar: $1 \mid a$ und $a \mid 0$ gilt für alle $a \in R$. Weiter gilt

$$a \mid 1 \Leftrightarrow a \text{ Einheit}$$

$$a \mid b \text{ und } b \mid c \Rightarrow a \mid c$$

Wenn a kein Nullteiler ist und wenn gilt

$$a \mid b \text{ und } b \mid a,$$

so folgt: es gibt eine Einheit $u \in R^*$ mit $au = b$.
Denn:

$$b = ax,\ a = by \Rightarrow a = axy \overset{a \text{ kein Nullteiler}}{\Rightarrow} 1 = xy$$

Ist $u \in R^*$, so gilt stets $ua \mid a$. Sind $b_1, \ldots, b_n \in R$ und gilt

$$a \mid b_1, \ldots, a \mid b_n, \text{ so folgt } a \mid b_1 + \cdots + b_n.$$

Definition ggT

Sei R ein Integritätsbereich, sei $b_1, \ldots, b_n \in R$. Wir nennen a einen **größten gemeinsamen Teiler** von $b_1, \ldots, b_n$, wenn gilt:

(1) $a \mid b_1, \ldots, a \mid b_n$

(2) Ist $c \in R$ mit $c \mid b_1, \ldots, c \mid b_n$, so folgt $c \mid a$.

Schreibe kurz $a \in \mathrm{ggT}(b_1, \ldots, b_n)$. (Der ggT ist im allgemeinen nicht eindeutig bestimmt: ist $u \in R^*$ und $a \in \mathrm{ggT}(b_1, \ldots, b_n)$, so folgt $au \in \mathrm{ggT}(b_1, \ldots, b_n)$. Über die Existenz einen ggT wird hier nichts behauptet.)

4.2 Definition Hauptideal

Sei R ein kommutativer Ring, sei $a_1, \ldots, a_n \in R$. Wir setzen $(a_1, \ldots, a_n) = a_1R + \cdots + a_nR$ (übliche, aber etwas problematische Schreibweise - links steht kein n-Tupel...).
Ist speziell $n = 1$, so heißt $(a_1) = a_1R$ das von a_1 erzeugte **Hauptideal**.
Ein Integritätsbereich R heißt **Hauptidealbereich** (**Hauptidealring**, engl. principal ideal domain PID), wenn alle Ideal in R Hauptideale sind.

Beispiele

(a) Jeder Körper K ist ein Hauptidealbereich, denn $\{0\} = (0)$ und $K = (1)$ sind die einzigen Ideale.

(b) $R = \mathbb{Z}$, jedes Ideal ist von der Form $m\mathbb{Z} = (m)$ nach 3.8.

4.3 Lemma 9

Sei R ein Integritätsbereich, $d, b_1, \ldots, b_n \in R$. Wenn gilt

$$(d) = (b_1, \ldots, b_n),$$

dann ist $d \in \mathrm{ggT}(b_1, \ldots, b_n)$.

Beweis:
Aus $b_j \in (d)$ folgt $d \mid b_j,\ j = 1, \ldots, n$. Weiter gibt es $r_1, \ldots, r_n \in R$ mit

$$d = b_1 r_1 + \cdots + b_n r_n,$$

weil $d \in (b_1, \ldots, b_n)$. Wenn also $c \in R$ ein gemeinsamer Teiler der b_j ist, so gilt $c \mid d$. □
In Hauptidealbereichen existieren also immer ggT's.

Korollar (Lemma von Bézout)

Ist $b_1, \ldots, b_n \in \mathbb{Z}$ und ist d ein ggT von $b_1, \ldots, b_n$, so gibt es $r_1, \ldots, r_n \in \mathbb{Z}$ mit

$$d = b_1 r_1 + \cdots + b_n r_n$$

□

4.4 Definition irreduzibel und prim

Sei R ein Integritätsbereich, sei $r \in R,\ r \neq 0,\ r \notin R^*$.

(a) r heißt **irreduzibel**, wenn aus $r = xy,\ x, y \in R$ folgt, dass $x \in R^*$ oder $y \in R^*$.

(b) r heißt **prim**, wenn aus $r \mid xy,\ x, y \in R$ folgt, dass $r \mid x$ oder $r \mid y$.

Beispiel

In $\mathbb{Z}$ gilt: $r \in \mathbb{Z}$ ist irreduzibel $\Leftrightarrow \pm r$ Primzahl $\overset{\text{Euklids Lemma}}{\Leftrightarrow}$ r ist prim

Lemma

Sei R ein Integritätsbereich, sei $r \in R,\ r \neq 0,\ r \notin R^*$. Dann gilt folgendes:

(i) r prim $\Rightarrow r$ irreduzibel

(ii) r prim $\Leftrightarrow (r)$ Primideal

Beweis:
(i): Sei $r \in R$ prim und $r = xy$ für $x, y \in R$ dann gilt

$$r \mid xy \overset{r \text{ prim}}{\rightsquigarrow} r \mid x \text{ oder } r \mid y.$$

Wenn $r \mid x$, dann

$$x = sr \text{ für ein } s \in R \rightsquigarrow r = sry \overset{\text{kürzen}}{\rightsquigarrow} 1 = sy \rightsquigarrow s \in R^* \text{ und } y \in R^*.$$

Genauso, wenn $r \mid y \rightsquigarrow r$ irreduzibel. □

(ii): Sei r prim, sei

$$xy \in (r) \rightsquigarrow r \mid xy \rightsquigarrow r \mid x \text{ oder } r \mid y \rightsquigarrow x \in (r) \text{ oder } y \in (r) \Rightarrow (r) \text{ Primideal}$$

Sei (r) Primideal und gelte

$$r \mid xy \rightsquigarrow xy \in (r) \rightsquigarrow x \in (r) \text{ oder } y \in (r) \rightsquigarrow r \mid x \text{ oder } r \mid y.$$

□

4.5 Satz 15

Sei R ein Hauptidealbereich, sei $r \in R,\ r \neq 0,\ r \notin R^*$. Dann sind äquivalent:

(i) r ist prim

(ii) r ist irreduzibel

(iii) (r) ist maximales Ideal

(iv) (r) ist Primideal

Beweis:
Wir wissen schon: (iii)$\overset{3.13}{\Rightarrow}(iv)\Leftrightarrow$(i)$\Rightarrow$(ii).
$\mathbb{Z}\!\!\!/$ (ii)$\Rightarrow$(iii). Angenommen, es gibt $J \trianglelefteq R$ mit $(r) \subseteq J \subseteq R$. Schreibe $J = (a)$ für ein $a \in R$, $(r) \subseteq (a) \subseteq R$. Es folgt $a \mid r \rightsquigarrow r = ab$ für ein $b \in R$. Es folgt $a \in R^*$ oder $b \in R^*$, da r irreduzibel ist. Wenn $a \in R^*$, dann ist $(a) = R$. Wenn $b \in R^*$, dann ist $a \in (r)$ also $(a) = (r)$. Also ist (r) maximal. $(r) \neq R$ weil $r \notin R^*$. □

Beim Faktorisieren ganzer Zahlen ist die **Primfaktorzerlegung** ganz wichtig. Wir suchen eine Analogie dazu in Integritätsbereichen.

4.6 Definition faktoriell

Ein Integritätsbereich R heißt **faktoriell** (Faktorieller Ring, Gauß'scher Ring, ZPE-Ring ('zerlegbar in prim Elemente'), engl. UFD (unique factorization domain)), wenn jedes $r \in R,\ r \neq 0,\ r \notin R^*$ ein Produkt von Primelementen (=Elemente, die prim sind) ist.

Satz

Jeder Hauptidealbereich ist faktoriell.

Beweis:
Vorüberlegung: Ist $a_n \in R$, für alle $n \in \mathbb{N}$ mit

$$(a_0) \subseteq (a_1) \subseteq (a_2) \subseteq \ldots$$

so gibt es ein $m \in \mathbb{N}$ so, dass

$$(a_m) = (a_{m+1}) = \cdots = (a_{m+k}) \text{ für alle } k \geq 0,$$

jede aufsteigende Kette von Idealen wird stationär (ÜA 9.4). Wenn dies für alle Ketten von Idealen in R gilt, heißt R **noethersch**.
Sei $S = \{s \in R \mid s \neq 0,\ s \notin R^*,\ s \text{ kein Produkt von Primelementen}\}$. Zeige: $S = \emptyset$. Angenommen,

wähle t solange größer bis dies gilt

$S \neq \emptyset$. Dann gibt es $s \in S$ mit folgender Eigenschaft: ist $(t) \not\supseteq (s)$, so ist $t \notin S$. Das geht nach der Vorüberlegung. Weiter ist s nicht prim, also gibt es $x, y \in R$ mit

$$s = xy,\ x, y \notin R^*.$$

Es folgt

$$(s) \subsetneq (x) \text{ und } (s) \subsetneq (y) \Rightarrow x, y \notin S.$$

Also sind x, y beide Produkte von Primelementen. Aber dann ist $s = xy$ auch ein Produkt von Primelementen, $s \notin S$↯ □

4.7 Satz 16

Sei R ein Integritätsbereich. Dann sind folgende Bedingungen äquivalent:

(i) R ist faktoriell

(ii) Jedes Element $r \in R,\ r \neq 0,\ r \notin R^*$ ist ein Produkt irreduzibler Elemente, $r = p_1 \cdots p_m,\ p_j$ irreduzibel, wobei die p_j bis auf Reihenfolge und Multiplikation mit Einheiten eindeutig sind.

Beweis:
(i)⇒(ii): Weil Primelemente irreduzibel sind, ist nur die Eindeutigkeit der Faktorisierung zu zeigen.
Sei also $r \in R,\ r \neq 0,\ r \notin R^*$, dann

$$r = p_1 \cdots p_m = q_1 \cdots q_n,\ q_i \text{ prim},\ p_i \text{ irreduzibel}$$

Also $q_1 \mid r \overset{q_1 \text{ prim}}{\rightsquigarrow}$ es gibt ein j mit $q_1 \mid p_j$ Œ$j = 1$ (Umnummerieren).

Teiler von Einheiten sind wieder Einheiten

Daher $q_1 \mid p_1 \rightsquigarrow p_1 = u_1 q_1 \overset{p_1 \text{ irreduzibel}}{\rightsquigarrow} u_1 \in R^*$. Also $p_2 \cdots p_m u_1 = q_2 \cdots q_n$.
Iteriere das, dann folgt $n = m$ und wir haben $p_j = u_j q_j$ für $u_j \in R^* \rightsquigarrow$ fertig.

(ii)⇒(i): Zeige: wenn (ii) gilt, ist jedes irreduzible Element prim.
Sei $r \in R$ irreduzibel und gelte $r \mid xy$. Ist $x \in R^*$ so folgt $r \mid y$ und wenn $y \in R^*$ folgt $r \mid x$. ist weder x noch y eine Einheit, so folgt

$$x = x_1 \cdots x_k,\ y = y_1 \cdots y_l,\ x_i, y_i \text{ irreduzibel und eindeutig}$$

Wenn $r \mid x_1 \cdots x_k \cdot y_1 \cdots y_l \rightsquigarrow$ es gibt x_j mit $r \mid x_j$ oder y_j mit $r \mid y_j$, daraus folgt $r \mid x$ oder $r \mid y$. □

Bemerkung

In faktoriellen Integritätsbereichen gilt also: 'prim'='irreduzibel'.

4.8 Beobachtung

Ist R faktoriell, $r \in R,\ r \neq 0,\ r \notin R^*$, schreibe

$$r = p_1^{l_1} \cdots p_n^{l_n} \text{ wobei für } i \neq j \text{ gelte: } p_i \nmid p_j,\ p_j \text{ prim}$$

Dann ist jeder Teiler von r von der Form

$$s = p_1^{k_1} \cdots p_n^{k_n} \cdot u \text{ mit } u \in R^*,\ k_i \leq l_i\ (p_j^0 = 1)$$

Folglich existieren in faktoriellen Ringen ggT's.

4.9 Definition euklidischer Bereich

Sei R ein Integritätsbereich. Eine Abbildung $\delta : R \to \mathbb{N}$ heißt **Gradfunktion**, wenn gilt: Für alle $a, b \in R$ mit $b \neq 0$ gibt es $q, r \in R$ mit

$$a = bq + r \text{ und } \delta(r) < \delta(b).$$

Ein Integritätsbereich mit Gradfunktion heißt **euklidischer Bereich** (euklidischer Ring).

Beispiel

(a) $R = \mathbb{Z},\ \delta(x) = |x|$ Absolutbetrag. Dann liefert teilen mit Rest: ist $a, b \in \mathbb{Z},\ b \neq 0$, so gibt es $q, r \in \mathbb{Z}$ mit

$$a = bq + r,\ 0 \leq r < |b|$$

(b) K Körper, $\delta(x) \begin{cases} 1 & x \neq 0 \\ 0 & x = 0 \end{cases}$ ist Gradfunktion:

$$a = bq \text{ mit } q = ab^{-1} \text{ (Teilen ohne Rest)}$$

4.10 Satz 17

Jeder euklidischer Bereich ist ein Hauptidealbereich.

Beweis:
Sei δ eine Gradfunktion auf R, sei $I \trianglelefteq R$. Für $I = \{0\} = (0)$ ist I ein Hauptideal. Für $I \neq \{0\}$ wähle $b \in I \backslash \{0\}$ so, dass $\delta(b)$ minimal ist. Ist $a \in I$ schreibe $a = bq + r$ mit $\delta(r) < \delta(b)$. Es folgt

$$r = a - bq \in I, \text{ also } r = 0 \rightsquigarrow a \in (b) \rightsquigarrow I = (b)$$

□

Gezeigt ist damit:
R Körper $\Rightarrow$ R euklidischer Bereich $\Rightarrow$ R Hauptidealbereich $\Rightarrow$ R faktoriell
(keiner der Pfeile ist umkehrbar!).

4.11 Lemma 10 (Polynomdivision)

Sei R ein Integritätsbereich, sei $g = a_0 + a_1 T + \cdots + a_m T^m \in R[T]$ mit $\deg(g) = m \geq 0$ und Leitkoeffizient $a_m \in R^*$. Sei $f \in R[T]$. Dann gibt es eindeutig bestimmte Polynome $q, r \in R[T]$ mit

$$f = q \cdot g + r \text{ und } \deg(r) < m.$$

Beweis:
Eindeutigkeit: $f = gq + r = g\tilde{q} + \tilde{r}$ und $\deg(\tilde{r}) < m \rightsquigarrow g(q - \tilde{q}) = \tilde{r} - r$. Da $a_m \in R^*$ folgt

$$\deg(g(q - \tilde{q})) = \underbrace{\deg(g)}_{=m} + \deg(q - \tilde{q}) = \underbrace{\deg(\tilde{r} - r)}_{<m}$$

also

$$\deg(q - \tilde{q}) = -\infty \text{ d.h. } q = \tilde{q} \rightsquigarrow r = \tilde{r}$$

Existenz: Induktion nach $\deg(f) = n$. Für $n < m$ setze $q = 0$ und $r = f \rightsquigarrow$ fertig. Sei jetzt $n \geq m \geq 0,\ f = b_o + \cdots + b_n T^n$. Setze $h = f - b_n a_m^{-1} T^{n-m} \cdot g$, es folgt $\deg(h) < n$. Also gibt es $\tilde{q}, r \in R[T]$ mit

$$h = g \cdot \tilde{q} + r,\ \deg(r) < m.$$

Es folgt

$$f = h + b_n a_m^{-1} T^{n-m} g = g(\tilde{q} + b_n a_m^{-1} T^{n-m}) + r$$

□

4.12 Korollar 1

Sei K ein Körper. Dann ist der Polynomring $K[T]$ ein euklidischer Bereich und insbesondere faktoriell.

Beweis:
Setze $\delta(f) = 2 - \deg(f),\ 2 - \infty = 0 \rightsquigarrow \delta$ ist Gradfunktion nach 4.11. □

Unser nächstes Ziel ist der Satz von Gauß: wenn R faktoriell ist, so ist auch $R[T]$ faktoriell.
Die Idee: betrachte $\underbrace{R \subseteq R[T] \subseteq Q[T]}_{\text{faktoriell}},\ Q = \mathrm{Quot}(R)$.

4.13 Vorbereitung für den Satz von Gauß

Sei R ein faktorieller Integritätsbereich.

(A) Es gilt $R[T]^* = R^*$. Ist $r \in R$ irreduzibel in R, so ist r auch irreduzibel in $R[T]$ (ÜA).

(B) Sei $f \in R[T]$ mit $\deg(f) = m \geq 1,\ f = a_0 + \cdots + a_m T^m$. Sei $d \in \mathrm{ggT}(a_0, \ldots, a_m)$, es folgt mit $a_i = d \cdot b_i$, dass
$$f = d(b_0 + \cdots + b_m T^m) \text{ und } 1 \in \mathrm{ggT}(b_0, \ldots, b_m).$$
Man nennt ein Polynom $g \in R[T]$ mit $\deg(g) = m \geq 1$ **primitiv**, wenn
$$g = b_0 + \cdots + b_m T^m \text{ und } 1 \in \mathrm{ggT}(b_0, \ldots, b_m).$$
Jedes Polynom $f \in R[T]$ mit $\deg(f) \geq 1$ lässt sich also schreiben als $f = d \cdot \tilde{f}$, mit $d \in R$ und $\tilde{f} \in R[T]$ primitiv. Diese Zerlegung ist eindeutig bis auf Multiplikation mit Einheiten, weil ggT bis auf Einheiten eindeutig ist. Außerdem sind irreduzible Polynome von $\deg(.) \geq 1$ primitiv.

(C) Sei $m = \deg(f) \geq 1,\ f = \frac{a_0}{b_0} + \cdots + \frac{a_m}{b_m} T^m,\ b = b_0 \cdot b_m,\ a_i, b_i \in R$. Es folgt $b \cdot f \in R[T] \rightsquigarrow b \cdot f = d \cdot \tilde{f}$ mit $\tilde{f} \in R[T]$ primitiv, $d \in R \rightsquigarrow f = \frac{d}{b} \cdot \tilde{f}$. Ist $f = \frac{x}{y} \tilde{\tilde{f}}$ mit $\tilde{\tilde{f}} \in R[T]$ primitiv, $x, y \in R$, so folgt
$$y \cdot d \cdot \tilde{f} = x \cdot b \cdot \tilde{\tilde{f}} \overset{(B)}{\Rightarrow} \tilde{\tilde{f}} = u \cdot \tilde{f} \text{ für } u \in R^*$$

4.14 Lemma 11 (Gauß Lemma)

Sei R faktoriell, seien $f, g \in R[T]$ primitiv, $\deg(f), \deg(g) \geq 1$.
Dann ist $h = f \cdot g$ primitiv.

Beweis:
Angenommen, das ist falsch. Dann existiert ein Element $p \in R$, p prim, mit $h = p \cdot \tilde{h},\ \tilde{h} \in R[T]$.
Integritätsbereich weil (p) Primideal
Betrachte $\varphi : R \to R/(p)$ und $\varphi : R[T] \to R/(p)[T],\ a_0 + \cdots + a_n T^n \mapsto \varphi(a_0) + \cdots + \varphi(a_n) T^n$. Es folgt $\varphi(h) = 0$, aber $\varphi(f) \neq 0 \neq \varphi(g)$, weil p nicht alle Koeffizienten von f und g teilt. ↯ □

4.15 Satz 18

Sei R faktoriell und $f \in R[T]$ mit $\deg(f) \geq 1$. Wenn f irreduzibel in $R[T]$ ist, so ist f auch irreduzibel in $Q[T],\ Q = \mathrm{Quot}(R)$.

Beweis:
Angenommen, es gibt $g, h \in Q[T]$ mit $\deg(g), \deg(h) \geq 1$ und $f = g \cdot h$ (Skalare sind Einheiten in $Q[T]$). Schreibe $g = a\tilde{g},\ h = b \cdot \tilde{h}$ mit $\tilde{g}, \tilde{h} \in R[T]$ primitiv $\rightsquigarrow f = a \cdot b \cdot \underbrace{(\tilde{g}\tilde{h})}_{\text{primitiv}}$. Andererseits $f = d \cdot \tilde{f}$ mit $\tilde{f}$ primitiv. Schriebe $ab = \frac{x}{y}$ mit $x, y \in R$:

$$y \cdot d \cdot \tilde{f} = x \cdot (\tilde{g} \cdot \tilde{h}) \rightsquigarrow \tilde{f} = u \cdot \tilde{g} \cdot \tilde{h}$$

für ien $u \in R^*$ und 4.13 (B)$\lightning$ □

4.16 Theorem (Satz von Gauß)

Wenn R ein faktorieller Integritätsbereich ist, os ist auch $R[T]$ faktoriell.

Beweis:
Wir wenden Theorem 4.7 an. Sei zuerst $f \in R[T]$ mit $\deg(f) \geq 1$ primitiv. Wenn f nicht irreduzibel ist, gibt es $g, h \in R[T]$ mit $f = g \cdot h,\ g, h \notin R[T]^* = R^*$. Weil f primitiv ist, folgt $\deg(g), \deg(h) \geq 1$ und g, h sind ebenfalls primitiv. Induktiv folgt

$$f = q_1 \cdots q_m,\ q_i \in R[T] \text{ primitiv, irreduzibel, } \deg(q_i) \geq 1.$$

Angenommen, $\tilde{q}_1, \ldots, \tilde{q}_n \in R[T]$ sind ebenfalls irreduzibel mit $f = ildeq_1 \cdots \tilde{q}_n$. Das folgt (weil f primitiv) $\deg(\tilde{q}_j) \geq 1$ und $\tilde{q}_j$ primitiv. Nach Satz 4.15 sind die $\tilde{q}_j, q_i$ irreduzibel in $Q[T]$. Da $Q[T]$ faktoriell ist, folgt $n = m$ und nach Umsortieren

$$\tilde{q}_i = a_i q_i,\ a_i = \frac{x_i}{y_i} \in Q,\ x_i, y_i \in R$$

Wegen $y_i \tilde{q}_i = x_i q_i$ folgt $a_i \in R^*$ (wie vorher) $\Rightarrow$ die Zerlegung $f = q_1 \cdots q_n$ ist eindeutig bis auf Einheiten in R^*.
Sei jetzt $f \in R[T],\ f \neq 0,\ f \notin R[T]^* = R^*$. Wenn $\deg(f) = 0$, so ist $f \in R$ und hat eine eindeutige Zerlegung in R (weil R faktoriell ist), also auch in $R[T]$ nach 4.13 (A). Ist $\deg(f) \leq 1$ schreibe $f = D \cdot \tilde{f}$ mit $\tilde{f} \in R[T]$ primitiv, dann folgt

$$f = c_1 \cdots c_k \cdot g_1 \cdots g_l,\ c_i \in R \text{ irreduzibel, } g_j \in R[T] \text{ prmitiv und irreduzibel, } \deg(g_i) \geq 1$$

Ist $f = \tilde{c}_1 \cdots \tilde{c}_{\tilde{k}} \cdot \tilde{g}_1 \cdots \tilde{g}_{\tilde{l}}$ eine zweite Zerlegung in primitive Elemente, mit $\tilde{c}_i \in R,\ \deg(\tilde{g}_i) \geq 1$, so sind die $\tilde{g}_j$ primitiv (weil irreduzibel). Es folgt

$$\tilde{c}_1 \cdots \tilde{c}_{\tilde{k}} = c_1 \cdots c_k \cdot u,\ u \in R^* \qquad \tilde{g}_1 \cdots \tilde{g}_{\tilde{l}} = g_1 \cdots g_k \cdot u^{-1}$$

und damit $k = \tilde{k},\ l = \tilde{l}$ und (nach Umsortieren)

$$\tilde{c}_i = u_i c_i,\ u_i \in R^* \qquad \tilde{g}_j = v_j g_j,\ v_j \in R^*$$

□

5 Körper, Körpererweiterungen und Konstruierbarkeit

5.1 Definition Charakteristik

Sei K ein Körper, sei $c : \mathbb{Z} \to K$ der Ringhomomorphismus $c(n) = n \cdot 1_K = \underbrace{1_K + 1_K + \cdots + 1_K}_{n-\text{mal}}$. Es gilt $\ker(c) = l\mathbb{Z}$ für ein $l \in \mathbb{N}$ nach 3.8 ($I \subseteq \mathbb{Z} \Leftrightarrow I = l\mathbb{Z}$ für ein $l \in \mathbb{N}$). Die Zahl l nennt man die **Charakteristik** von K, $l = \mathrm{char}(K)$. Da $c(\mathbb{Z}) \subseteq K$ ein Integritätsbereich ist, folgt $l = 0$ oder l ist Primzahl, vgl. 3.13 und 3.15.

denn:

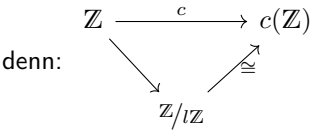


Abbildung 6: Charakteristik von K

5.2 Beobachtungen über Körper

(a) Sind K, L Körper und ist $\varphi : K \to L$ ein Ringhomomorphismus, so ist φ injektiv, weil $\{0\}, K$ die einzigen Ideale in K sind und weil $\varphi(1_K) = 1_L$. Es folgt $\mathrm{char}(K) = \mathrm{char}(L)$ (denn: $\mathbb{Z} \xrightarrow{c} K \xhookrightarrow{\varphi} L$), also $\ker(c : \mathbb{Z} \to K) = \ker(\varphi \circ c = c' : \mathbb{Z} \to L)$).

(b) Ist K ein Körper, $X \subseteq K$ eine Teilmenge, so ist

$$\bigcap \{L \subseteq K \mid L \text{ Teilkörper, } X \subseteq L\} \subseteq K \text{ ein Teilkörper}$$

der von X erzeugte **Teilkörper**.

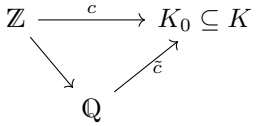
5.3 Satz 19

Jeder Körper K besitzt einen eindeutig bestimmten minimalen Teilkörper $K_0 \subseteq K$, den **Primkörper**. Wenn $\mathrm{char}(K) = 0$, gilt $K_0 \cong \mathbb{Q}$ und wenn $\mathrm{char}(K) = l > 0$ gilt, ist $K_0 = c(\mathbb{Z}) \cong \mathbb{Z}/l\mathbb{Z}$.

Beweis:
Sei $K_0 = \bigcap \{L \subseteq K \mid L \text{ Teilkörper}\}$, dann ist $K_0 \subseteq K$ ein Teilkörper nach 5.2. Wegen $1_K \in K_0$ folgt $c(\mathbb{Z}) \subseteq K_0$. Wenn $l > 0$ ist, $c(\mathbb{Z}) \cong \mathbb{Z}/l\mathbb{Z}$ ein Teilkörper, also $K_0 \subseteq c(\mathbb{Z})$, also

$$c(\mathbb{Z}) = K_0$$

Ist $\mathrm{char}(K) = 0$, so ist $c : \mathbb{Z} \to K$, so ist c injektiv, nach 3.11 existiert ein (eindeutiger) Homomorphismus:



$$\Rightarrow \underbrace{\tilde{c}(\mathbb{Q})}_{\cong \mathbb{Q}} = K_0$$

□

5.4 Erinnerung an LA II, der verbesserte Einsetzungshomomorphismus

Seien R, S kommutative Ringe, $\varphi : R \to S$ ein Ringhomomorphismus. Sei $a \in S$. Definiere

$$\Phi_a : R[T] \to S, +\Phi_a(r_0 + \cdots + r_n T^n) = \varphi(r_0) + \cdots + \varphi(r_n)a^n$$

Das ist ein Ringhomomorphismus, der **Einsetzungshomomorphismus**.
Für $R = S$ und $\varphi = \mathrm{id}_R$ schreibe $\Phi_a(f) = f(a)$.

5.5 Definition Körpererweiterung

Sei $K \subseteq L$ ein Teilkörper des Körpers L. Dann nennt man L eine **Körpererweiterung** von K.
Beispiele: $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ sind Körpererweiterungen.

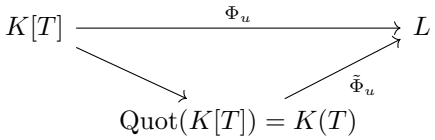
Sei nun $u \in L$, betrachte $\Phi_u : K[T] \to L,\ r_0 + \cdots + r_n T^n \mapsto r_0 + \cdots + r_n u^n$.
1. Möglichkeit: Φ_u ist injektiv: Dann heißt u **transzendent** über K, das heißt es gibt kein Polynom $f \neq 0$ in $K[T]$ mit

$$\Phi_u(f) = f(u) = 0,$$

also erfüllt u keine algebraische Gleichung über K.
Beispiele: $e = 2.71828.. = \exp(1)$ und $\pi = 3.14159..$ sind transzendent über $\mathbb{Q}$ (!)
Der kleinste Teilkörper von L, der $K \cup \{u\}$ enthält, ist dann isomorph zu

$$K(T) = \mathrm{Quot}(K[T]) = \left\{ \frac{f}{g} \mid f, g \in K[T],\ g \neq 0 \right\}$$

dem Körper der rationalen Funktionen auf K, denn wir haben nach 3.11:



Man schreibt $K(u) = \left\{ \frac{f(u)}{g(u)} \in L \mid f, g \in K[T],\ g \neq 0 \right\} \cong K(T)$.

2. Möglichkeit: $\Phi_u K[T] \to L$ ist nicht injektiv, also gibt es $f \neq 0,\ f \in K[T]$ mit

$$\Phi_u(f) = f(u) = 0.$$

Nach 4.12 ist $K[T]$ ein Hauptidealbereich, alos gibt es ein Polynom $\mu \in K[T]$ mit

$$\ker(\Phi_u) = (\mu) \subseteq K[T].$$

Es gilt $\deg(\mu) \geq 1$ (denn fpr $f \in K[T]$ mit $\deg(f) = 0$ gilt $\Phi_u(f) \neq 0$). Bis auf Multiplikation mit Skalaren $a \in K^*$ ist μ eindeutig bestimmt (4.1), wir dürfen annehmen, dass

$$\mu = \mu_u = r_0 + \cdots + r_{n-1}T^{n-1} + T^n \text{ und } \deg(\mu) = n \geq 1.$$

Man nennt $\mu = r_0 + \cdots + T^n$ das **Minimalpolynom** von u üder K und nennt u **algebraisch** über K. Da L ein Integritätsbereich ist, ist (μ) ein Primideal in $K[T]$, und da $\deg(\mu) \geq 1$ ist $(\mu) \neq K[T]$. Also ist (μ) nach 4.5 ein maximales Ideal und damit ist $\Phi_u(K[T]) \cong {}^{K[T]}/_{(\mu)}$ ein Körper, der kleinste Teilkörpervon L, der $K \cup \{u\}$ enthält. Man schreibt dann kurz

$$K[u] = \{f(u) \mid f \in K[T]\} \subseteq L$$

und nennt u einen **primitiven Erzeuger** von $K[u]$.

Beispiel: $K = \mathbb{Q},\ l = \mathbb{R},\ u = \sqrt{2} \notin \mathbb{Q}$. Es gilt $f(u) = 0$ für $f = T^2 - 2$ und $u = f$ das Minimalpolynom von u. Es folgt, dass $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{2}] \subseteq \mathbb{R}$ ein Teilkörper ist.

In beiden Fällen 1. und 2. schreibt man

$$K(u) \bigcap \{M \subseteq L \text{ Teilkörper} \mid K \cup \{u\} \subseteq M\}$$

u algebraisch $\Rightarrow K(u) = K[u]$,
u transzendent $\Rightarrow K(u) = \left\{ \frac{f(u)}{g(u)} \mid f, g \in K[T],\ g \neq 0 \right\}$.

5.6 Definition

Sei $K \subseteq L$ eine Körpererweiterung. Dann ist L ein K-Vektorraum: $(L, +)$ ist abelsche Gruppe, für $v \in L,\ a \in K$ ist $va \in L$ und die Vektorraumaxiome gelten alle. Man nennt die Dimension von L als K-Vektorraum den **Grad der Körpererweiterung** und schreibt:

Teilkörper $K \subseteq L$ mit angeben!

$$[L : K] = \dim_K L$$

Satz

Sei $K \subseteq L$ eine Körpererweiterung, sei $u \in L,\ n \in \mathbb{N}$. Dann sind äquivalent:

(i) u ist algebraisch über K mit Minimalpolynom μ und $\deg(\mu) = n$.

(ii) $[K(u) : K] = n < \infty$.

Beweis:
(i)⇒(ii): Sei $g \in K[T]$ beliebig, dann $g = q \cdot \mu + r$ mit $q, r \in K[T],\ \deg(r) < n = \deg(\mu)$, vgl. 4.11. Es folgt:

$$g(u) = \underbrace{q(u) \cdot \underbrace{\mu(u)}_{=0} + r(u)}_{=0} = r(u),$$

also

$$K[u] = \left\{ r_0 + \cdots + r_{n-1} u^{n-1} \mid r_0, \ldots, r_{n-1} \in K \right\}$$

daraus folgt: $\dim_K K[u] \leq n$, denn $\{1, u, \ldots, u^{n-1}\}$ ist ein lineares Erzeugendensystem von $K[u]$. Dieses ERZ ist linear unabhängig:

$$r_0 \cdot 1 + \cdots + r_{n-1} u^{n-1} = 0 \rightsquigarrow f = r_0 + \cdots + r_{n-1} T^{n-1} \rightsquigarrow f \in (\mu),$$

aber $\deg(f) < \deg(\mu) \Rightarrow f = 0$.
ALso ist $\{1, u, u^{n-1} \ldots, u^{n-1}\}$ eine Basis von $K[u]$ als K-Vektorraum.
(ii)⇒(i): Angenommen, u ist transzendent über K. Dann gilt $g(u) \neq 0$ für alle $g \in K[T], +g \neq 0$. Folglich ist die unendliche Menge $\{1, u, u^2, ...\}$ linear unabhängig über K, daraus folgt $\dim_K K(u)$ ist nicht endlich. □

5.7 Satz 20

Seien $K \subseteq L \subseteq M$ Körpererweiterungen. Dann gilt $[M : K] = n < \infty$ genau dann, wenn $[M : L] = l < \infty$ und $[L : K] = k < \infty$, mit $n = k \cdot l$,

$$[M : K] = [M : L] \cdot [L : K]$$

Beweis:
Ist $\dim_K(M) = n$, so folgt $\dim_K(L) = l < \infty$, da $L \subseteq M$ ein Unterraum ist. Sei $u_1, \dots, u_n \in M$ eine Basis für M über K, so ist $u_1, \dots, u_n$ ein Erzeugendensystem für M über L, also

$$\dim_L(M) \leq n.$$

Sei nun $v_1, \dots, v_l \in M$ eine Basis für M über L und $w_1, \dots, w_k \in L$ eine Basis für L über K.
Sei $x \in M,\ x = \sum_{j=1}^{l} v_j x_j$ mit $x_j \in L$. Schreibe $x_j = \sum_{i=1}^{k} w_i \xi_{ij}$ mit $\xi_{ij} \in K \rightsquigarrow x = \sum_{i,j} = v_j w_i \xi_{ij}$, also ist die Menge

$$\{v_j w_i \mid 1 \leq j \leq l,\ 1 \leq i \leq k\}$$

ein Erzeugendensystem für M über K und

$$[M : K] \leq \underbrace{[M : L]}_{=l} \cdot \underbrace{[L : K]}_{=k}$$

Behauptung: diese Menge $\{v_j w_i \mid i, j, \dots\}$ ist linear unabhängig über K. Denn angenommen, $\xi_{ij} \in K$ mit

$$\sum_{i,j} v_j \underbrace{w_i \xi_{ij}}_{\in L} = 0 \overset{\{v_j\} \text{ Basis}}{\Rightarrow} \sum_i w_i \xi_{ij} = 0 \overset{\{w_i\} \text{ Basis}}{\Rightarrow} \xi_{ij} = 0$$

Also $u = k \cdot l$. □

5.8 Konstruierbarkeit mit Zirkel und Lineal

Gegeben sei eine endliche Menge von Punkten $S = \{P_1, \dots, P_n\} \subseteq \mathbb{R}^2$ in der Ebene. Ein Punkt $q \in \mathbb{R}^2$ heißt **elemntar konstruierbar** aus S, wenn q von den folgenden Typen ist

(a) q ist Schnittpunkt zweier geraden k, l, wobei k und l jeweils durch zwei Punkte in S gehen

(b) q ist Schnittpunkt einer Geraden l, die durch zwei Punkte in S geht mit einem Kreis k, dessen Mittelpunkt in S ist und dessen Radius der Abstand zweier Punkte in S ist $\Big($Abstand heißt: euklidischer Abstand, $p = (x, y),\ p' = (x', y'),\ d(p, p') = \big((x - x')^2 + (y - y')^2\big)^{\frac{1}{2}}\Big)$

(c) q ist Schnittpunkt zweier Kreise k, l, deren Mittelpunkte in S sind und deren Radien Abstände von Punkten in S sind.

Setze nun $S = S_0$ und

$$S_{j+1} = S_j \cup \big\{q \in \mathbb{R}^2 \mid q \text{ aus } S_j \text{ elemntar konstruierbar}\big\}$$

sowie $\mathcal{K}(S) = \bigcup_{j \geq 0} S_j$. Die Punkte in $\mathcal{K}(S)$ ist die Menge aller aus S in endlich vielen Schritten mit Zirkel und Lineal konstruierbaren Punkte.
Ist $S = \emptyset$, so ist $S_j = \emptyset\ \forall j \rightsquigarrow \mathcal{K}(S) = \emptyset$. Ist $S = \{p\}$, so ist $S_J = \{p\}\ \forall j \rightsquigarrow \mathcal{K}(S) = \{p\}$, diese beiden Fälle sind interessant.

Beobachtung

Verschiebungen, Drehungen und zentrische Streckungen von $\mathbb{R}^2$ überführen Kreise in Kreise und Geraden in Geraden. Wenn also $\#S \geq 2$ gilt, dann dürfen wir annehmen, dass die Punkte $(0, 0)$ und $(1, 0)$ in S liegen, indem wir S geeignet verschieben, drehen und strecken; die ganze Menge $\mathcal{K}(S)$ wird dann auch verschoben, gedreht und gestreckt.

5.9 Erinnerung: Die komplexen Zahlen

$\mathbb{C} = \mathbb{R}^2$, setze $1 = (1,0)$ und $i = (0,1)$. Jede komplexe Zahl $z \in \mathbb{C}$ ist von der Form

$$z = (u,v) = u \cdot 1 + v \cdot i,\ u,v \in \mathbb{R}.$$

Die Addition ist die Addition im $\mathbb{R}$-Vektorraum $\mathbb{R}^2$, die Multiplikation ist erklärt durch

$$z = (u,v) = u + v \cdot i,\ u,v \in \mathbb{R}$$

$$w = (x,y) = x + y \cdot i,\ x,y \in \mathbb{R}$$

$$z \cdot w = (u+vi)(x+yi) = (ux - vy) + (uy + vx)i$$

Damit ist $\mathbb{C}$ ein Körper, der $\mathbb{R}$ als Teilkörper enthält via $r \mapsto r \cdot 1 + 0 \cdot i,\ r \in \mathbb{R}$. Es gilt $i^2 = -1$, vgl. LA II 3.18. Ist $z = u + vi \in \mathbb{C},\ u,v \in \mathbb{R}$, so setzt man $\mathrm{Re}(z) = u$ **Realteil** von z, $\mathrm{Im}(z) = v$ **Imaginärteil** von z:

$$\overline{z} = u - vi \text{ **komplexe Konjugierte** von } z.$$

Nachrechnen zeigt:

$$\overline{z \cdot w} = \overline{z} \cdot \overline{w},\ \overline{z + w} = \overline{z} + \overline{w},\ \overline{\overline{z}} = z,\ \overline{1} = 1$$

also ist die Abbildung $\mathbb{C} \to \mathbb{C},\ z \mapsto \overline{z}$ ist ein Automorphismus des Körpers $\mathbb{C}$.
Beachte auch: $z \cdot \overline{z} = (u^2 + v^2) \cdot 1 \in \mathbb{R} \subseteq \mathbb{C}$. Der Absolutbetrag von z wird definiert als

$$|z| = \sqrt{z\overline{z}} \in \mathbb{R}_{\geq 0}$$

5.10 Satz 21

Sei nun $S \subseteq \mathbb{R}^2$ endlich. Wir identifizieren $\mathbb{R}^2$ mit $\mathbb{C}$ und betrachten S als Teilmenge des Körpers $\mathbb{C}$.
Sei $S \subseteq \mathbb{C}$ endlich mit $0, 1 \in S$. Dann ist $\mathcal{K}(S) \subseteq \mathbb{C}$ ein Teilkörper. Für alle $z \in \mathbb{C}$ gilt folgendes:

(i) $z \in \mathcal{K}(S) \Leftrightarrow \overline{z} \in \mathcal{K}(S)$

(ii) $z^2 \in \mathcal{K}(S) \Leftrightarrow z \in \mathcal{K}(S)$

Beweis:

(i) $\mathcal{K}(S)$ ist Gruppe bzgl. $+$.

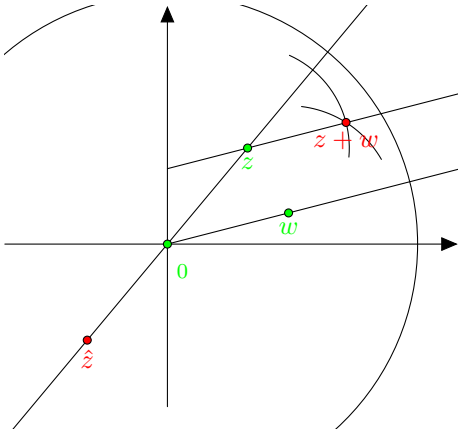


Abbildung 7: Konstruierbarkeit (i)

(ii) Es gilt $i \in \mathcal{K}(S)$

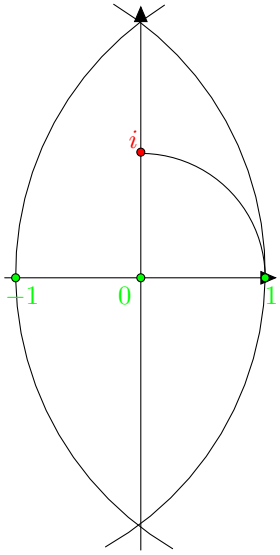


Abbildung 8: Konstruierbarkeit (ii)

(iii) $z \in \mathcal{K}(S) \Rightarrow \mathrm{Re}(z),\ \mathrm{Im}(z), \overline{z} \in \mathcal{K}(S)$ also $i \cdot \mathrm{Im}(z) = z - \mathrm{Re}(z) \in \mathcal{K}(S)$.

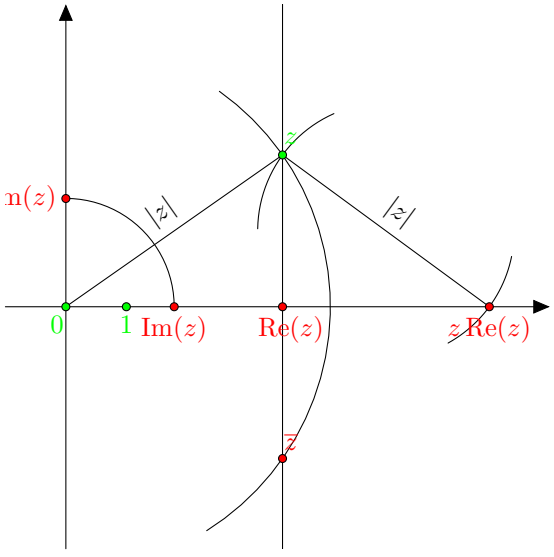


Abbildung 9: Konstruierbarkeit (iii)

(iv) $z \in \mathcal{K}(S),\ z \neq 0 \Rightarrow \hat{z} = \frac{z}{|z|} \in \mathcal{K}(S)$.

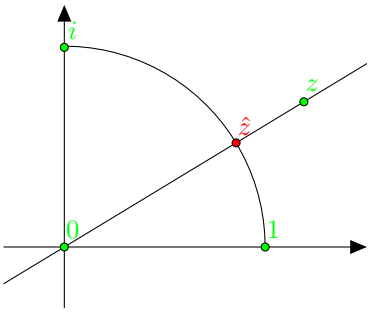


Abbildung 10: Konstruierbarkeit (iv)

(v) $z, w \in \mathcal{K}(S),\ z, w \neq v \Rightarrow \hat{z} \cdot \hat{w} \in \mathcal{K}(S)$.

$\hat{z}, \hat{w}$ sind Drehungen um den Ursprung um Winkel $\alpha, \beta \rightsquigarrow \hat{z} \cdot \hat{w}$ Drehung um Winkel $\alpha + \beta$.

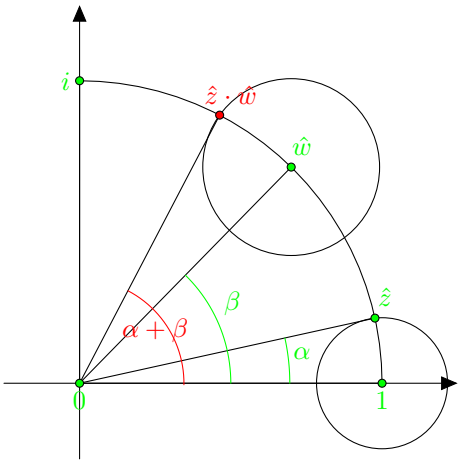


Abbildung 11: Konstruierbarkeit (v)

(vi) $r, s \in \mathcal{K}(S),\ r, s \neq 0 \Rightarrow \frac{s}{r} \in \mathcal{K}(S)$ und $\Rightarrow r, s \in \mathcal{K}(S) \wedge \mathbb{R} \Rightarrow r \cdot s \in \mathcal{K}(S)$

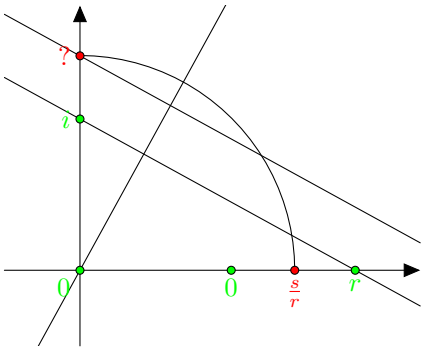


Abbildung 12: Konstruierbarkeit (vi)

(vii) $z \in \mathcal{K}(S),\ z \neq 0 \Rightarrow |z| \in \mathcal{K}(S)$

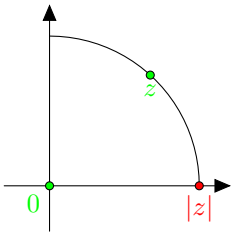


Abbildung 13: Konstruierbarkeit (vii)

(viii) $z \neq 0$ mit $\hat{z}, |z| \in \mathcal{K}(S) \Rightarrow z \in \mathcal{K}(S)$
Es folgt $z, w \in \mathcal{K}(S),\ z, w \neq 0$

$$z \cdot w = \hat{z}\,|z| \cdot \hat{w}\,|w| = \hat{z}\hat{w} \cdot |z|\,|w| = z\hat{w}\,|zw|$$

sowie

$$\frac{1}{z} = \frac{\hat{z}^{-1}}{|z|} = \frac{\overline{\hat{z}}}{|z|} \in \mathcal{K}(S)$$

Weil

$$\hat{z}\overline{\hat{z}} = |\hat{z}|^2 = 1$$

$$z = |z|\,\hat{z} \Rightarrow \frac{1}{z}\frac{1}{|z|\,\hat{z}} = \frac{\hat{z}^{-1}}{|z|}$$

Also ist $\mathcal{K}(S)$ ein Körper und $z \in \mathcal{K}(S) \Rightarrow \overline{z} \in \mathcal{K}(S)$.

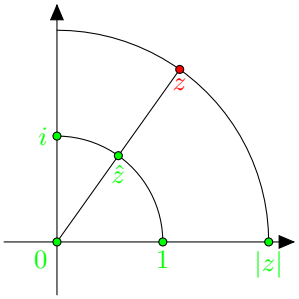


Abbildung 14: Konstruierbarkeit (viii)

(ix) $r \in \mathcal{K}(S) \cap \mathbb{R},\ r > 0 \Rightarrow \sqrt{r} \in \mathcal{K}(S)$

$$\begin{aligned} 1^2 + s^2 &= \beta^2 \\ r^2 + s^2 &= \alpha^2 \\ \alpha^2 + \beta^2 &= (1+r)^2 \\ 1 + s^2 + r^2 + s^2 &= 1 + 2r + r^2 \\ s^2 &= r \Rightarrow s = \sqrt{r} \end{aligned}$$

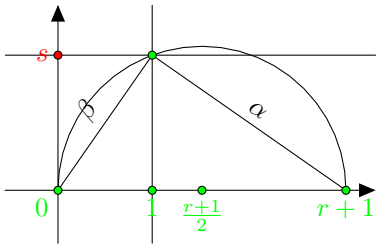


Abbildung 15: Konstruierbarkeit (ix)

(x) $z \in \mathcal{K}(S),\ w \in \mathbb{C},\ w^2 = z \Rightarrow w \in \mathcal{K}(S)$.

$$\hat{w}^2 = \hat{z},\ w = \pm\hat{w}\sqrt{|z|}$$

sind die beiden Quadratwurzeln aus z mit

$$w^2 = z,\ w = \hat{w}\,|w|$$

$$w^2 = \hat{w}\hat{w}\,|w|\,|w| = w\hat{w}\,|ww| = \hat{z}\,|z|$$

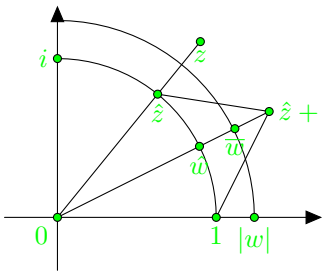


Abbildung 16: Konstruierbarkeit (x)

□

5.11 Lemma 12

Lemma A

Sei $K \subseteq L$ eine Körpererweiterung, sei $u \in L$ mit $u^2 \in K$. Dann gilt

$$[K(u) : K] \leq 2$$

Beweis:
u ist Nullstelle von $T^2 - u^2 \in K[T]$, also algebraisch über K. Für das Minimalpolynom μ_u von u über K gilt

$$\mu_u \mid T^2 - u^2 \Rightarrow \deg(\mu_u) \leq 2$$

und

$$\deg(\mu_u) = [K(u) : K]$$

nach 5.6. □

Lemma B

Sei $K \subseteq \mathbb{C}$ eine Teilkörper mit folgender Eigenschaft:

$$x \in K \Rightarrow \overline{x} \in K$$

Ist dann $z \in \mathbb{C}$ aus einer Teilmenge $S \subseteq K$ mit einem der drei Verfahren aus 5.8 konstruierbar, so gibt es $w \in \mathbb{C}$ mit $w^2 \in K$ mit $z \in K(w)$.

Beweis:

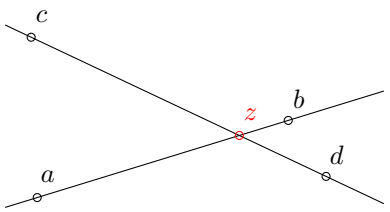
(a) Betrachte die Abbildung $x \mapsto x' = \frac{x-a}{b-a} \in K$. Dann ist $z' = c' + t(d' - c'),\ t \in \mathbb{R}$ also

$$z' \in \mathbb{R} \Leftrightarrow \operatorname{Im}(z') = 0 \Leftrightarrow \operatorname{Im}(c') + t \cdot \operatorname{Im}(d' - c') = 0$$

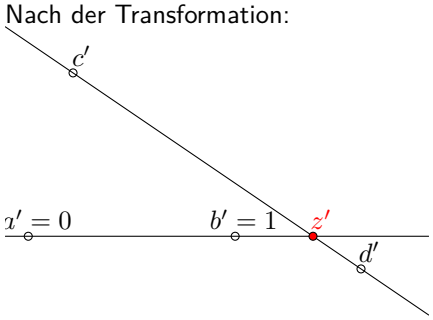
dann kann t berechnet werden, $t = \frac{-\operatorname{Im}(c')}{\operatorname{Im}(d'-c')} = \frac{-i\operatorname{Im}(c')}{i\operatorname{Im}(d'-c')}$.
Ist $x \in K$, so ist auch $\overline{x} \in K$. Wegen $\operatorname{Re}(x) = \frac{1}{2}(x + \overline{x})$ gilt dann

$$\operatorname{Re}(x) \in K \Rightarrow \operatorname{Im}(x) \cdot i = x - \operatorname{Re}(x) \in K$$

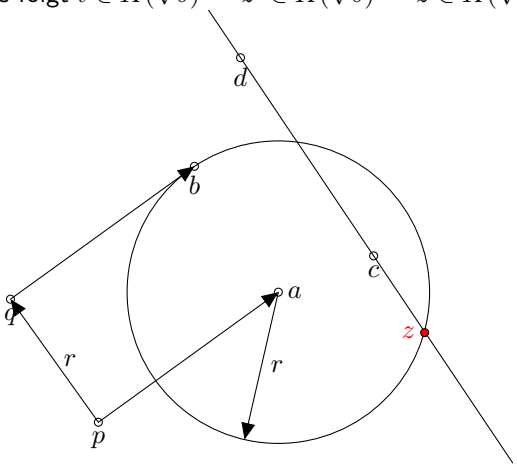
Es folgt $t \in K$, also $z' \in K$, also auch $z \in K$. Also $z \in K = K(1)$.



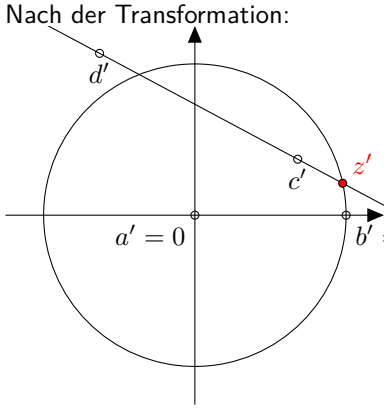
Nach der Transformation:



(b) Betrachte Transformation $x \mapsto x' = \frac{x-a}{b-a} \in K$.
Ansatz $z' = d' + t(d' - c')$ mit $|z'|^2 = 1$ führt auf quadratische Gleichung $t = \alpha + \sqrt{\delta},\ \alpha \in K,\ \delta \cap \mathbb{R}_{\geq 0}$.
Es folgt $t \in K(\sqrt{\delta}) \rightsquigarrow z' \in K(\sqrt{\delta}) \rightsquigarrow z \in K(\sqrt{\delta})$.



Nach der Transformation:



(c) Schnitt zweier Kreise führt auf genauso eine Formel.

□

5.12 Notation

Sei $K \subseteq L$ eine Körpererweiterung, sei $u \in L$. Dann bezeichnet $K(u)$ den kleinsten Teilkörper von L, der $K \cup \{u\}$ enthält. Die Elemente von $K(u)$ sind von der Form

$$x = x_k u^k + x_{k+1} u^{k+1} + \cdots + x_{k+l} u^{k+l},\ x_k \in K,\ k \in \mathbb{Z},\ l \geq 0$$

Sind $u_1, \ldots, u_m \in L$, so schreibe

$$K(u_1, \ldots, u_m) = K(u_1)K(u_2)\ldots K(u_m),$$

das ist der kleinste Teilkörper von L, der $K \cup \{u_1, \ldots, u_m\}$ enthält.

5.13 Satz 22

Sei $S = \{0, 1, p_1, \ldots, p_m\} \subseteq \mathbb{C}$, sei $K = \mathbb{Q}(p_1, \bar{p_1}, \ldots, p_m, \bar{p_m}) \subseteq \mathcal{K}(S) \subseteq \mathbb{C}$. Sei $q \in \mathcal{K}(S)$. Dann gibt es Teilkörper

$$K_0 = K \subseteq K_1 \subseteq \cdots \subseteq K_n \subseteq \mathcal{K}(S) \text{ mit } q \in K_n$$

und $[K_{j+1} : K_j] = 2$. Es folgt

$$[K_n : K] = 2^n.$$

Beweis:
Die Elemente von K sind Linearkombinationen von Potenzen der $p_j, \bar{p}_j$, also gilt für alle $x \in K$, dass $\bar{x} \in K$.
Wir benutzen die Notation aus 5.5: S_{j+1} entsteht aus S_j durch Hinzunahme aller Punkte, die durch die Verfahren (a),(b),(c) aus S_j mit Zirkel und Lineal konstruierbar sind, mit $S_0 = S$. Sei $q \in S_1$. Dann gibt es nach 5.11 ein $w \in \mathbb{C}$ mit $w^2 \in K$ und $q \in K(w)$. Weiter ist $[K(w) : K] \leq 2$ und $\bar{w}^2 \in K \subseteq K(w)$

$$\Rightarrow [K(w, \bar{w}) : K] = \underbrace{[K(w, \bar{w}) : K(w)]}_{\leq 2} \cdot \underbrace{[K(w) : K]}_{\leq 2} \in \{1, 2, 4\}$$

Ist also $S_1 = S_0 \cup \{q_1, \ldots, q_r\}$ so gibt es $w_1, \ldots, w_r \in \mathbb{C}$ mit $w_j^2 \in K$:

$$S_1 \subseteq K(w_1, \bar{w_1}, \ldots, w_r \bar{w}_r) = K' \subseteq \mathcal{K}(S)$$

$$K \subseteq K(w_1) \subseteq K(w_1, \bar{w_1}) \subseteq K(w_1, \bar{w}_1, w_2) \subseteq \cdots \subseteq K'$$

und $[K' : K]$ ist Zweierpotenz und $S_1 \subseteq K'$. Jetzt weiter mit S_2 und $K' \rightsquigarrow$ Behauptung □

5.14 Satz 23

Ausgehend von der Menge $S = \{0, 1\}$ ist die Dreiteilung des Winkels $60° = \frac{\pi}{3}$ nicht mit Zirkel und Lineal möglich.

Beweis:

$$w = \frac{1}{2} + i\frac{\sqrt{3}}{2}$$
$$q^3 = w$$
$$q = \cos(20°) + i \cdot \sin(20°) = u + iv,\ u^2 + v^2 = 1 \Leftrightarrow v^2 = 1 - u^2$$

Wenn q konstruierbar ist, so auch $u = \mathrm{Re}(q)$. Für das Minimalpolynom von $2u$ über $\mathbb{Q}$ gilt, wegen $(2u)^3 - 3(2u) - 1 = 0$, dass

$$q^3 = (u + iv)^3$$
$$\mathrm{Re}(q^3) = \frac{1}{2} = \mathrm{Re}\left((u + iv)(u^2 - v^2 + 2iuv)\right) = u^3 - uv^2 - 2uv^2$$
$$= u^3 - u(1 - u^2) - 2u(1 - u^2) = u^3 - u + u^3 - 2u + 2u^3$$
$$= 4u^3 - 3u$$

$$\mu_{2u} \mid T^3 - 3T - 1$$

Behauptung: $T^3 - 3T - 1 \in \mathbb{Z}[T]$ ist irreduzibel in $\mathbb{Z}[T]$, also auch in $\mathbb{Q}[T]$.
Beweis:

$$T^3 - 3T - 1 = (\alpha T + \beta)(\gamma T^2 + \delta T + \epsilon) \text{ mit } \alpha, \beta, \gamma, \delta, \epsilon \in \mathbb{Z},\ 1 = \alpha \cdot \gamma \text{»} \alpha = 1$$

daraus folgt

$$-1 = \beta \cdot \epsilon \Rightarrow \beta = \pm 1$$

ist Nullstelle von f, aber

$$f(1) \neq 0 \neq f(-1) \lightning$$

□

Es folgt $\mu_{2u} = T^3 - 3 - 1$, also $[\mathbb{Q}(2u) : \mathbb{Q}] = 3$. Wäre$u \in \mathcal{K}(\{0,1\})$, so wäre $2u \in L$ mit

$$[L : \mathbb{Q}] = 2^l, \text{ aber } [L : \mathbb{Q}] = [L : \mathbb{Q}(2u)] \cdot \underbrace{[\mathbb{Q}(2u) : \mathbb{Q}]}_{=3} \lightning$$

□

5.15 Bemerkung

Wir haben im vorigen Beweis folgende nützliche Hilfsmittel benutzt:

(A) Ist R faktoriell und $f \in R[T]$ irreduzibel, so ist f irreduzbel in $Q[T]$ für $Q = \mathrm{Quot}(R)$ (vgl. 4.15).

(B) Sei $f = aT^3 + bT^2 + cT + d \in R[T]$ und $a = 1$ und sei R faktoriell. Wenn f reduzibel ist, is gibt es ein Teiler von d, der Nullstelle von f ist.
Denn: $f = (\alpha T + \beta)(\gamma T^2 + \delta T + \epsilon)$ (f primitiv!)

$$\Rightarrow \alpha\gamma = 1 \text{ » } \alpha = 1 \rightsquigarrow f(-\beta) = 0 \text{ und } d = \beta \cdot \epsilon$$

(C) Ist $K \subseteq L$ eine Körpererweiterung mit $m = [L : K]$, ist $u \in L$ mit Minimalpolynom μ_u über K, so gilt

$$\deg(\mu_u) \mid m.$$

Denn

$$m = [L : K] = [L : K(u)] \cdot \underbrace{[K(u) : K]}_{\deg \mu_u}$$

5.16 Das Delische Problem

Das **Delische Problem** ist mit Zirkel und Lineal nicht lösbar.
Die Pest wütete in Delos... Aufgabe: einen Würfel zu konstruieren, dessen Volumen 2 ist.

Satz

$\sqrt[3]{2} \notin \mathcal{K}(\{0,1\})$, die Zahl $\sqrt[3]{2}$ ist nicht mit Zirkel und Lineal aus $\{0,1\}$ konstruierbar.

Beweis:
$u = \sqrt[3]{2}$ ist Nullstelle von $T^3 - 2 = f$. Da $\pm 1, \pm 2$ keine Nullstellen von f sind und f primitiv in $\mathbb{Z}[T]$ ist, ist f irreduzibel, also

$$\mu_u = T^3 - 2 \rightsquigarrow \left[\mathbb{Q}\left(\sqrt[3]{2}\right) : \mathbb{Q}\right] = 3$$
$$\Rightarrow \sqrt[3]{2} \notin \mathcal{K}(\{0,1\})$$

□

Wie kann man Irreduzibilität von Polynomen in $\mathbb{Z}[T]$ prüfen?
Vorsicht: Kriterium 5.15 (B) greift nur bei Polynomen von Grad ≤ 3!!

Beispiel

$f = (T^2+1)^2$ ist primitiv in $\mathbb{Z}[T]$, hat keine Nullstelle in $\mathbb{Z}, \mathbb{Q}$ oder $\mathbb{R}$, ist aber reduzibel!

5.17 Satz 24 (Eisensteins Kriterium)

Sei R faktoriell, sei $p \in R$ prim und sei $f = a_n T^n + \cdots + a_0 \in R[T]$ primitiv und von Grad $n \geq 1$.
Falls gilt: $p \mid a_j$ für $j = 0, \ldots, n-1$ und $p \nmid a_n$ und $p^2 \nmid a_0$, so ist f irreduzibel.

Beweis:
Angenommen, $f = g \cdot h$ mit $\deg(g), \deg(h) \geq 1$, also $g = b_k T^k + \cdots + b_0$ und $h = c_l T^l + \cdots + c_0$.
Außerdem $a_0 = b_0 c_0$ mit $p \mid c_0$ und » $p \mid b_0$. Da $p^2 \nmid a_0$ folgt $p \nmid c_0$. Sei m minimal mit $p \nmid b_m$ (also $p \mid b_0, \ldots, p \mid b_{m-1}$).
Da g primitiv ist, gilt $m \leq k$.

$$a_m = \underbrace{b_0 c_m + b_1 c_{m-1} + \cdots + b_{m-1} c_1}_{\text{wird von } p \text{ geteilt}} + \underbrace{b_m c_0}_{\text{wird nicht von } p \text{ geteilt}}$$

$$p \nmid a_m \Rightarrow m = n \not\downarrow_{\deg(k) \geq 1}$$

□

Mit dem **Eisenstein-Kriterium** folgt z.B. sofort: ist $p \in \mathbb{N}$ eine Primzahl, so ist für $m \geq 1$ das Polynom

$$T^m \pm p \in \mathbb{Z}[T] \text{ irreduzibel in } \mathbb{Q}[T]$$

5.18 Substitution

Sei R ein kommutativer Ring, sei $u \in R^*$ und $k \in R[T]$.
Für $f = a_n T^n + \cdots + a_0 \in R[T]$ schreibe

$$f(uT+k) = a_n(uT+k)^n + \cdots + a_0 \in R[T]$$

(substituiere/ersetze T durch $uT+k$).
Die Abbildung

$$f \mapsto f(uT+k),\ \phi : R[T] \to R[T]$$

ist ein Ringisomorphismus mit Inversen

$$g \mapsto g(u^{-1}(t-k)),\ \psi : R[T] \to R[T]$$

Denn:

$$\psi \circ \phi(f) = \psi(f(uT+k)) = f(u(u^{-1}(T-k))+k) = f(T-h+h) = f(T) = f$$

Also gilt:

$$f \text{ irreduzibel} \Leftrightarrow f(uT+k) \text{ irreduzibel}$$

5.19 Lemma 13

Sei $p \in \mathbb{N}$ eine Primzahl. Dann ist $f = T^{p-1} + \cdots + T + 1 \in \mathbb{Z}[T]$ irreduzibel.

Beweis:
$(T-1)f = T^p - 1$ (geometrische Summe)
Substitution: $T \mapsto T * 1$: zu zeigen $f(T+1) = \tilde{f}$ ist irreduzibel.

$$\Rightarrow (T+1-1)\tilde{f} = (T+1)^p - 1 \Rightarrow T \cdot \tilde{f} = \sum_{k=0}^{p} \binom{p}{k} T^k - 1$$

$$\Rightarrow T \cdot \tilde{f} = \sum_{k=1}^{p} \binom{p}{k} T^k = \binom{p}{1} T + \cdots + \binom{p}{p} T^p$$

$$\Rightarrow \tilde{f} = \binom{p}{1} + \cdots + \binom{p}{p} T^{p-1} \Rightarrow \tilde{f} = p + \binom{p}{2} T + \cdots + T^{p-1}$$

$$\Rightarrow p \mid \binom{p}{k} \in \mathbb{N} \text{ für } k = 1, \ldots, p-1$$

Nach Eisenstein ist $\tilde{f}$ irreduzibel, also ist f irreduzibel. □

5.20 Konstruktion von regelmäßigen n-Ecken mit Zirkel und Lineal

Sei $n \in \mathbb{N},\ n \geq 3$.

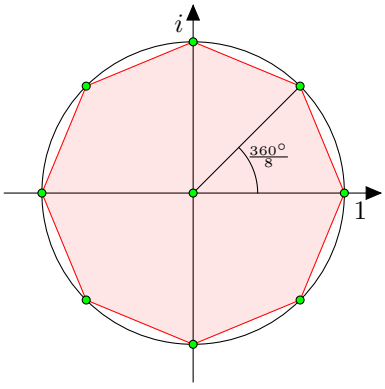


Abbildung 17: Konstruktion eines 8-Ecks

Beispiel: für $n = 8$ müssen wir den Winkel $\frac{360^\circ}{8}$ konstruieren.

Setze $q(n) = \cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right)$
Frage:für welche n gilt

$$q(n) \in \mathcal{K}(\{0,1\})$$

Vorüberlegung

Reduzierung der Frage: für welche Primzahlen p gilt $q(p) \in \mathcal{K}(\{0,1\})$?
Denn:

$$n = p_1 p_2 \rightsquigarrow \underbrace{q(n)\cdots q(n)}_{p_2} \hat{=} \underbrace{\frac{360^\circ}{n}\cdots\frac{360^\circ}{n}}_{p_2}$$
$$= p_2 \cdot \frac{360^\circ}{p_1 p_2} = \frac{360^\circ}{p_1} \hat{=} q(p_1)$$

Wir erhalten: Wenn

$$q(n) \in \mathcal{K}(\{0,1\}) \Rightarrow q(p_i) \in \mathcal{K}(\{0,1\}) \text{ für } i = 1,\ldots,k \text{ und } n = p_1 \cdots p_k$$

Für $q(p)$ gilt

$$q(p)^p = 1 \Leftrightarrow q(p)^p - 1 = 0$$

für das Minimalpolynom $\mu_{q(p)}$ von $q(p)$ über $\mathbb{Q}$ gilt also:

$$\mu_{q(p)} \mid T^p - 1 = (T-1)\underbrace{(T^{p-1} + \cdots + 1)}_{\text{irreduzibel, 5.19}}$$

$$\Rightarrow \mu_{q(p)} = T^{p-1} + \cdots + 1$$

Falls also $q(p) \in \mathcal{K}(\{0,1\})$, so ist

$$\deg(\mu_{q(p)}) = p - 1 = 2^l \text{ für ein } l \geq 2$$

Solche Primzahlen nennt man **Fermatsche Primzahlen**,

$$2^l + 1 = p$$

Frage: Struktur von l?

Lemma

Ist $2^l + 1$ eine Primzahl, so ist l eine Zweierpotenz.

Beweis:
$l = 1$ dann $l = 2^0 = 1$ ✓
Sei nun $l > 1$. Wir schreiben $l = \underbrace{g}_{\text{gerade oder } g=1} \underbrace{u}_{\text{ungerade}}$.

$\mathbb{Z} \ni u = 1$

$$z = 2^g \rightsquigarrow 2^l = (s^g)^u = z^u$$

Dann folgt:

$$\begin{aligned} p = 2^l + 1 = z^u + 1 &\overset{u \text{ ungerade}}{=} 1 - (-z)u \\ &= \underbrace{(1-(-z))}_{=1+z\geq 3}\underbrace{((-z)^{u-1} + (-z)^{u-2} + \cdots + 1)}_{=\frac{1-(-z)^u}{1-(-z)}} \\ &\overset{p \text{ prim}}{\Rightarrow} 1 = \frac{1-(-z)^u}{1-(-z)} \\ &\Rightarrow u = 1 \end{aligned}$$

□

Setze $F_j = 2^{2^j} + 1$. Dann sind $F_0 = 3,\ F_1 = 5,\ F_2 = 2^4 + 1 = 17,\ F_3 = 257,\ F_4 = 65537$ Primzahlen. Dagegen ist F_5 keine Primzahl. Es ist ein offenes Problem, ob es außer $F_1, \ldots, F_4$ noch weitere Fermatsche Zahlen gibt.

Zusammenfassung

- $n \in \mathbb{N},\ n \geq 3$. Für welche n ist $q(n) \in \mathcal{K}(\{0,1\})$?
  Wenn $q(n = p_1 \cdots p_k) \in \mathcal{K}(\{0,1\}) \Rightarrow q(p_i) \in \mathcal{K}(\{0,1\})$ für $i = 1, \ldots, k$.
- Für welche Primzahlen p ist $q(p) \in \mathcal{K}(\{0,1\})$?
- Wenn $q(p) \in \mathcal{K}(\{0,1\})$, dann $p = 2^l + 1,\ l \in \mathbb{N}$ mit $l = 2^k$ für ein $k \in \mathbb{N}$.

Man kann zeigen:

$$q(n) \in \mathcal{K}(\{0,1\}) \Leftrightarrow n = 2^m p_1 \cdots p_k,\ p_1 < \cdots < p_k \text{ alles Fermatsche Primzahlen, } m \in \mathbb{N}$$

Der Beweis benutzt Galois-Theorie, vgl. Jacobsen 4.11. Gauß gab als erster eine Konstruktion eines regelmaäßigen 17-Ecks an.
Wir betrachten jetzt transzendente Zahlen und zeigen, dass

$$e = \exp(1) = \sum_{k=0}^{\infty} \frac{1}{k!} \text{ nicht algebraisch über } \mathbb{Q} \text{ ist.}$$

5.21 Definition algebraische Hülle

Sei $K \subseteq L$ eine Körpererweiterung. Die **algebraische Hülle** von K in L ist

$$\mathrm{acl}_L(K) = \{u \in L \mid u \text{ algebraisch über } K\} \qquad (\text{acl='algebraic cloure'})$$

Satz

Ist $K \subseteq L$ eine Körpererweiterung, so ist

$$K \subseteq \mathrm{acl}_L(K) \subseteq L$$

ein Teilkörper.
Es gilt:

$$\mathrm{acl}_L(\mathrm{acl}_L(K)) = \mathrm{acl}(K).$$

Beweis:
Sei $u, v \in L$ algebraisch über K. Es folgt

$$u \pm v,\ u \cdot v,\ \frac{u}{v} \in K(u,v)$$

und

$$[K(u,v) : K] = \underbrace{[K(u,v) : K(u)]}_{\text{endlich}} \cdot \underbrace{[K(u) : K]}_{\text{endlich}}$$

weil u, v algebraisch sind. Nach ÜA 11.4 ist jedes Element von $K(u,v)$ algebraisch über K. Also ist $\mathrm{acl}_L(K) \subseteq L$ ein Körper. Sei $K' = \mathrm{acl}_L(K)$ und $u \in \mathrm{acl}_L(K')$. Dann gibt es $w_1, \ldots, w_r \in K'$ mit

$$u \in \mathrm{acl}_L\, K(w_1, \ldots, w_r)$$

Damit folgt, dass

$$[K(u, w_1, \ldots, w_r) : K] = [K(u, w_1, \ldots, w_r) : K(w_1, \ldots, w_r)] \cdot [K(w_1, \ldots, w_r) : K]$$

Beide Faktoren sind endlich $\rightsquigarrow u$ algebraisch über K nach ÜA 11.4 $\Rightarrow u \in \mathrm{acl}_L(K)$. □

Eine Vorüberlegung zur Existenz reeller Zahlen, die transzendent über $\mathbb{Q}$ sind. $\mathbb{Q}$ ist abzählbar, jedes Polynom $f \in \mathbb{Q}[T]$ hat endlich viele rationale Koeffizienten $\rightsquigarrow \mathbb{Q}[T]$ ist abzählbar. Jedes Polynom in $\mathbb{Q}[T]$ hat nur endliche viele Nullstellen (überlegen wir später nochmal!) daraus folgt, dass $\mathrm{acl}_{\mathbb{C}}(\mathbb{Q})$ und $\mathrm{acl}_{\mathbb{R}}(\mathbb{Q})$ sind beides abzählbare Körper. Da $\mathbb{R}$ und $\mathbb{C}$ überabzählbar sind, ist 'fast jede' reelle oder komplexe Zahl transzendent über $\mathbb{Q}$.

5.22 Definition formale Ableitung

Für $f = a_n T^n + \cdots + a_0 \in R[T]$ setzen wir

$$Df = n a_n T^{n-1} + \cdots + a_1 \in R[T]$$

als **formale Ableitung**, sowie

$$F = (1 + D + \cdots + D^n) f,\ n = \deg(f)$$

(F löst dann formal die DGL $(1 - D)F = f$).
Für $f = \frac{1}{n!} T^n \in \mathbb{Q}[T]$ ergibt sich

$$F = 1 + T + \frac{1}{2} T^2 + \cdots + \frac{1}{n!} T^n = \sum_{k=0}^{n} \frac{1}{k!} T^k \qquad *$$

5.23 Lemma 14

Sei $f = \sum_{k=0}^{n} a_k T^k \in \mathbb{C}[T]$. Sei $F = (1 + D + \cdots + D^n) f$. Für jedes $z \in \mathbb{C}$ gilt dann

$$|F(0) \exp(z) - F(z)| \leq \sum_{k=0}^{n} |a_k| \cdot |z|^k \exp(z)$$

Beweis:

$$
\begin{aligned}
|F(0)\exp(z) - F(z)| &= \left| \sum_{k=0}^{n} a_k k! \cdot \sum_{k=0}^{n} \frac{z^l}{l!} - \sum_{k=0}^{n} a_k \underbrace{\sum_{k=0}^{n} \frac{k!}{l!} z^l}_{\text{nach } *} \right| \\
&= \left| \sum_{k=0}^{n} a_k \cdot \sum_{l \geq k} \frac{k!}{l!} z^l \right| \leq \sum_{k=0}^{n} \sum_{l \geq k} |a_k| \, \frac{k!}{l!} \, |z|^l \\
&\leq \sum_{k=0}^{n} \sum_{l \geq k} |a_k| \, |z|^k \, \frac{1}{(l-k)!} \, |z|^{l-k} \quad \text{weil } \binom{l}{k} = \frac{l!}{k!(l-k)!} \geq 1 \\
&\leq \sum_{k=0}^{n} |a_k| \cdot |k|^k \exp|z|
\end{aligned}
$$

□

5.24 Bemerkung zu Nullstellen

Sei $p \in \mathbb{N}$ eine Primzahl und sei $n \geq 1$. Betrachte

$$
f = \frac{1}{(p-1)!} \cdot \underbrace{T^{p-1}}_{p-1\text{-fache NS}} \cdot \prod_{k=1}^{n} \underbrace{(k-T)^p}_{p\text{-fache NS}} \in \mathbb{C}[T]
$$

Es folgt

$$
\begin{aligned}
D^m f(v) &= 0 \text{ für } m \leq p-2, \ v = 0, \ldots, n \\
D^{p-1} f(v) &= 0 \text{ für } v = 1, \ldots, n \\
D^{p-1} f(0) &= \frac{(p-1)!}{(p-1)!}(n!)^p = (n!)^p
\end{aligned}
$$

Für $m \geq p$ hat $D^m f$ ganzzahlige Koeffizienten, die alle von p geteilt werden. (Das folgt alles mit der Produktregel für Ableitungen.)
Sei $F = (1 + D + \cdots + D^n)f, \ N = \deg(f)$. Es folgt

$$
F(0) \equiv (n!)^p \mod p, \ F(v) \equiv 0 \mod p
$$

Schreibe $f = \sum_{n=1}^{N} a_n T^n, \ a_n \in \mathbb{Q}$.

5.25 Satz 25 (Hermite 1873)

Die Zahl $e = \exp(1) \approx 2.71..$ ist transzendent.

Beweis:
Es genügt, folgendes zu zeigen. Ist $q_0, \ldots, q_n \in \mathbb{Z}$ mit $q_0 \neq 0$, so ist

$$
q_0 + \cdots + q_n e^n \neq 0,
$$

denn wenn e algebraisch wäre, gäbe es ein Polynom $f \in \mathbb{Q}[T]$ mit $f(e) = 0, \ \deg(f) \geq 1$. Nach Durchmultiplizieren mit dem Hauptnenner hätten wir $f \in \mathbb{Z}[T]$ mit $f(e) = 0, \ \deg(f) \geq 1$ und nach Division durch eine e-Potenz, dass $f(0) \neq 0$.

Sei nun $p \in \mathbb{N}$ eine Primzahl mit $p > m$ und $p > |q_0|$. Esfolgt (mit der Bezeichnung aus 5.24 für dieses p und n)

$$\sum_{v=0}^{n} q_v F(v) \equiv q_0 \cdot (n!)^p \not\equiv 0 \mod p$$
$$\Rightarrow \sum_{v=0}^{n} q_v F(0) e^v = \sum_{v=0}^{n} q_v F(v) + \epsilon$$

und

$$|\epsilon| \leq \underbrace{\sum_{v=0}^{n} |q_v|\, e^v}_{\text{hängt nicht von } p \text{ ab}} \quad \underbrace{\sum_{k=1}^{N} |a_k| \cdot |v^k|}_{\text{hängt von } p \text{ ab}}$$

nach 5.23, mit $f = \sum_{k=1}^{N} a_k T^k$.
Nun gilt für jedes v

$$\begin{aligned}\sum_{k=1}^{N} |a_k| \cdot |v|^k &= \sum_{k=1}^{N} |a_k| \cdot v^k \\ &\overset{(**)}{\leq} \frac{v^{p-1}}{(p-1)!} \prod_{k=1}^{N} (k+v)^p \\ &= \frac{1}{(p-1)!} \underbrace{\prod_{k=1}^{N} (k+v)}_{=\alpha} \underbrace{\left(v \prod_{k=1}^{N} (k+v) \right)^p}_{=\beta} = \alpha \frac{\beta^p}{(p-1)!}\end{aligned}$$

wobei α, β nur von n und v abhängen, nihct von p.
Für $p \gg 1$ wird $\alpha \frac{\beta^p}{(p-1)!}$ beliebig klein. Da es beliebig große Primzahlen p gibt, können wir also durch geeignete Wahl von $p \gg 1$ erreichen, dass

$$|\epsilon| \leq \sum_{v=0}^{N} |q_v|\, e^v \cdot \alpha \frac{\beta^p}{(p-1)!} > \frac{1}{2}$$

gilt. Da $\sum_{v=0}^{N} q_v F(v) \in \mathbb{Z} \backslash \{0\}$ gilt, olgt

$$F(0) \cdot \sum_{v=0}^{N} q_v e^v \neq 0$$

Zu $(**)$:

$$(k-T)^p = \sum_{l=0}^{p} \binom{p}{l} k^{p-l} (-1)^l T^l$$
$$(k+T)^p = \sum_{k=0}^{p} \binom{p}{l} k^{p-l} t^l$$

Ausmultiplizieren liefert die Abschätzung. □

Der vorige Beweis stammt aus E. Landaus Zahlentheorie-Buch (Lindenmann 1882). Ein etwas anderer Beweis steht bei Jacobsen.

Korollar

Die Zahl e ist nicht mit Zirkel und Lineal aus $\{0, 1\}$ konstruierbar.

Bemerkung

Mit ähnlichen Methoden kann man zeigen, dass $\pi \approx 3.14..$ transzendent über $\mathbb{Q}$ ist. Der Beweis ist allerdings erheblich länger (siehe Landau oder Jacobsen) - im Prinzip aber genauso elementar.

Korollar

Die 'Quadratur des Kreises' mit Zirkel und Lineal ist unmöglich, d.h. man kann aus $\{0, 1\}$ mit Zirkel und Lineal kein Quadrat mit Fläche π konstruieren.

6 Zerfällungskörper und algebraischer Abschluss

6.1 Lemma 15

Sei K ein Körper, sei $f \in K[T]$ mit $\deg(f) = n \geq 1$. Angenommen $u_1, \ldots, u_m \in K$ sind Nullstellen von f, d.h.

$$f(u_j) = 0 \text{ für } j = 1, \ldots, m$$

Wenn für alle $i < j$ gilt $u_i \neq u_j$,so gibt es $g \in K[T]$ mit

$$f = (T - u_1)(T - u_2) \cdots (T - u_m) \cdot g$$

Insbesondere ist $m \leq n$.

Beweis:
Angenommen, $u \in K$ ist eine Nullstelle von f. Teilen mit Rest wie in 4.11:

$$f = (T - u) \cdot q + r \qquad \deg(r) < \deg(T - u) = 1 \Rightarrow r \in K \text{ konstant}$$

da

$$0 = f(u) = (u - u) \cdot q(u) + r$$

Es folgt $f = (T - u) \cdot q$. Ist $v \neq u$ eine weitere Nullstelle von f, so folgt

$$0 = f(v) = \underbrace{v - u}_{\neq 0} \cdot q(v) \rightsquigarrow v \text{ ist Nullstelle von } q = q_1 \neq 0$$

Daraus folgt $q = (T - v)q_2$ und

$$f = (T - u_1) \cdots (T - u_m) q_m, \; q_m \neq 0$$

und

$$\deg(f) = m + \deg(q_m)$$

□

6.2 Definition normiert

Ein Polynom f dessen Leitkoeffizient 1 ist, also $f = T + a_{n-1}T^{n-1} + \cdots + a_0$ heißt **normiert**. Ist K ein Körper,so ist jedes $f \in K[T], \; f \neq 0$ von der Form $f = a \cdot \tilde{f}, \; \tilde{f} \in K[T]$ normiert, $a \in K^*$ und $f, \tilde{f}$ haben die gleichen Nullstellen (klar). Ist $f \in K[T]$ normiert und gibt es $u_1, \ldots, u_m \in K$ mit

$$f = (T - u_1) \cdots (T - u_m),$$

so **zerfällt** f in **Linearfaktoren** über K ($\rightsquigarrow$ Jordannormalform).

6.3 Definition Zerfällungskörper

Sei K ein Körper, $f \in K[T]$ normiert. Eine Körpererweiterung $K \subseteq L$ heißt **Zerfällungskörper** von f, wenn es $u_1, \ldots, u_m \in L$ gibt es mit

(i) $f = (T - u_1) \cdots (T - u_m)$

(ii) $L = K(u_1, \ldots, u_m)$ (folglich $[L : K] < \infty$)

Beispiel

$$f = T^2 + 1 \in \mathbb{R}[T] \qquad f = (T - i)(T + i),\ i \in \mathbb{C}$$

$\mathbb{C} = \mathbb{R}(i) \rightsquigarrow \mathbb{C}$ ist Zerfällungskörper von $T^2 + 1$.

6.4 Satz 26

Sei K ein Körper und sei $f \in K[T]$ normiert mit $n = \deg(f) \geq 1$. Dann existiert ein Zerfällungskörper $L \supseteq K$ mit

$$[L : K] \leq n!$$

Beweis:
Induktion nach n:
$n = 1$: $f = T - u,\ u \in K \rightsquigarrow L = K$ fertig.
Sei jetzt $n \geq 2$: Schreibe $f = g \cdot h$ mit $g \in K[T]$ normiert und irreduzibel. Dann ist $K' = {}^{K[T]}/_{(g)}$ ein Körper nach 4.5.
Via $K \hookrightarrow K[T] \xrightarrow{\pi} K'$ können wir K als Teilkörper von K' auffassen - die Elemente von K' sind von der Form

$$f + (g),\ f \in K[T].$$

Setze $u = \pi(T) \in K',\ u = T + (g) \rightsquigarrow u^k = T^k + (g)$ dann folgt

$$g = T^n + \cdots + a_0 \Rightarrow g(u) = \underbrace{T^n + \cdots + a_0}_{=g} + (g) = (g)$$

also ist u eine Nullstelle von g.
In $K'[T]$ folgt $g = (T - u) \cdot \tilde{g}$. Weiter gilt $\mu_u = g$,da g irreduzibel ist, also gilt für $K' = K(u)$, dass

$$[K' : K] = \deg(g) \leq n.$$

Nun $\deg(\tilde{g} \cdot h) = n - 1 \rightsquigarrow$ es gibt ein Zerfällungskörper $L \supseteq K'$ für $\tilde{g} \cdot h$ mit

$$L = K'(u_2, \ldots, u_m) = K(u_1, \ldots, u_m),\ u = u_1$$

also

$$[L : K] = \underbrace{L : K'}_{\leq (n-1)!} \cdot \underbrace{[K' : K]}_{\leq n} \leq n!$$

□

Wir zeigen jetzt, dass ein Zerfällungskörper bis auf Isomorphie eindeutig bestimmt ist.

6.5 Definition Homomorphismus

Sei $\varphi : K \to K'$ ein Isomorphismus von Körpern.

(a) Für $f \in K[T],\ f = a_n T^n + \cdots + a_0$ setze $\varphi(f) = \varphi(a_n)T^n + \cdots + \varphi(a_0) \in K'[T]$. Dann ist

$$\varphi : K[T] \to K'[T]$$

ein Isomorphismus.

(b) Wenn $L \supseteq K$ und $L' \supseteq K'$ Körpererweiterungen sind und $\psi : L \to L'$ ein Homomorphismus mit

$$\psi|_K = \varphi$$

so heißt ψ **Homomorphismus** über ϕ.

$$\begin{array}{ccc} L & \xrightarrow{\psi} & L' \\ \uparrow & & \uparrow \\ K & \xrightarrow{\varphi} & K' \end{array}$$

Abbildung 18: Homomorphismus

6.6 Lemma 16

Sei $\varphi : K \to K'$ ein Isomorphismus von Körpern, seien $L \supseteq K$ und $L' \supseteq K'$ Körpererweiterungen. Sei $u \in L$ mit normierten Minimalpolynom $\mu_u = g$.

(i) Wenn $v \in L'$ eine Nullstelle von $\varphi(g)$ ist, gibt es genau ein Isomorphismus

$$K(u) \xrightarrow{\psi} K'(u)$$

über φ mit $\psi(u) = v$.

(ii) Wenn $\varphi(g)$ keine Nullstelle in L' hat, gibt es kein Homomorphismus

$$\psi : K(u) \to L'$$

über φ.

Beweis:
zu (i):
Da g irreduzibel ist und $\varphi : K[T] \to K'[T]$ ein Isomorphismus ist, ist $\varphi(g)$ irreduzibel. Betrachte

$$\begin{array}{ccccccc} K(u) & \xrightarrow{\cong} & {}^{K[T]}\!/_{(g)} & \xrightarrow{\cong} & {}^{K'[T]}\!/_{(\varphi(g))} & \xrightarrow{\cong} & K(u) \\ \uparrow & & \uparrow & & \uparrow & & \uparrow \\ K & = & K & \xrightarrow{\phi} & K' & = & K' \end{array}$$

Abbildung 19: Beweis Lemma 16

Es folgt die Existenz von $\psi : K(u) \xrightarrow{\cong} K(u)$ mit $\psi(u) = v$. Jedes Element $z \in K(u)$ ist von der Form

$$z = a_l u^l + \cdots + a_0 \text{ und } a_j \in K,$$

also ist $\psi(z)$ festgesetzt durch $\psi(u)$. □
zu (ii):
Ist $\psi : K(u) \to L'$ ein Homomorphismus über φ, so folgt für $\psi(u) = v$, dass

$$\varphi(g)(v) = \psi(g(u)) = 0$$

□

6.7 Satz 27

Sei $\varphi : K \to K'$ ein Isomorphismus von Körpern,sei $f \in K[T]$ normiert, seien $L \supseteq K$ sowie $L' \supseteq K'$ Zerfällungskörper von f bzw. $\varphi(f)$. Sei

$$H = \{\psi : L \to L' \mid \psi \text{ Isoorphismus über } \varphi\}$$

Dann gilt

$$1 \leq \#H \leq [L : K]$$

(d.h. es gibt solche Isomorphismen über φ, aber höchstens $[L : K]$ viele).

Beweis:
Induktion nach $n = \deg(f)$.
$\underline{n = 1:}$ $f = T - u$ und $\varphi(f) = T - \varphi(u),\ u \in K,\ \varphi(u) \in K'$. Dann folgt

$$L = K,\ L' = K' \Rightarrow \psi = \phi \text{ fertig.}$$

$\underline{n \geq 2:}$ Schreibe $f = g \cdot h,\ g$ßK[T] normiert und irreduzibel. Da f in $L[T]$ in Linearfaktoren zerfällt, zerfällt auch g in $L[T]$ in Linearfaktoren. Sei $u \in L$ eine Nullstelle von g. Sei $v \in L'$ eine Nullstelle von $\varphi(g)$ ($\varphi(g)$ zerfällt in $L'[T]$ in Linearfaktoren).
Nach Lemma 6.6 gibt es genau ein Isomorphismus $\zeta : K(u) \to K'[T]$ über φ mit $\zeta(u) = v$. Setze $M = K(u) \subseteq L$ sowie $M' = K'(u) \subseteq L'$. Dann folgt

$$g(T - u)\tilde{g} \text{ für } \tilde{g} \in M[T]$$

und

$$f = (t - u) \cdot \tilde{g} \cdot h \text{ für } \tilde{g} \in M[T].$$

Nach Induktionsschritt gibt es ein Isomorphismus ψ über ζ, also über φ.

$$\begin{array}{ccc} L & \xrightarrow{\psi} & L' \\ \uparrow & & \uparrow \\ M & \xrightarrow{\zeta} & M' \\ \uparrow & & \uparrow \\ K & \xrightarrow{\varphi} & K' \end{array}$$

Abbildung 20: Beweis Satz 27

Für ψ über ζ gibt es höchstens $[L : M]$ Möglichkeiten. Ist ψ über φ, so gibt es höchstens $\deg(g)$ viele Möglichkeiten für $\psi(u) = v$, zu jeder davon höchstens $[M : K]$ Möglichkeiten über $K(u) \xrightarrow{\varphi} K'(u)$, also höchstens

$$[L : M] \cdot [M : K] = [L : K]$$

Möglichkeiten. □

Index

Die Seitenzahlen *sind mit Hyperlinks zu den entsprechenden Seiten versehen, also anklickbar!*

Abbildungsverzeichnis