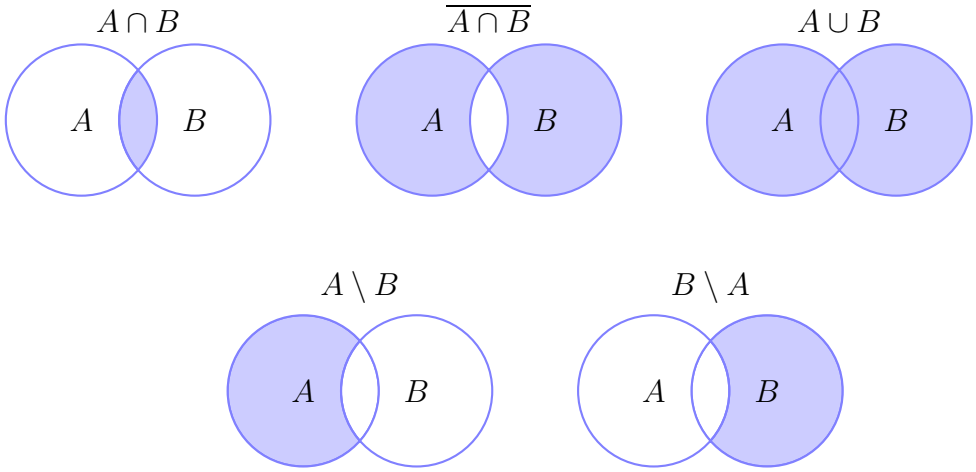
Im Folgenden seht ihr die eingeführten Begriffe nochmal graphisch dargestellt.



1.2 Rechenregeln für Mengen

1.6 Satz

Seien A, B und C Mengen. Dann gelten folgende Rechenregeln für Mengen:

(a) Kommutativgesetz*:* $A \cap B = B \cap A$ *und* $A \cup B = B \cup A$

(b) Assoziativgesetz*:* $A \cap (B \cap C) = (A \cap B) \cap C$ *und* $A \cup (B \cup C) = (A \cup B) \cup C$.

(c) Distributivgesetz*:*
$$\begin{cases} A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \\ A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \end{cases}$$

Beweis. Der Beweis ergibt sich einfach aus den entsprechenden Regeln für „und“ und „oder“:

a.

$$\begin{aligned} A \cup B &\overset{Def}{=} \{x \mid x \in A \text{ oder } x \in B\} \\ &= \{x \mid x \in B \text{ oder } x \in A\} \\ &\overset{Def}{=} B \cup A \end{aligned}$$

Das zweite Gleichheitszeichen folgt dabei aus der Wahrheitstabelle.

1.11 Bemerkung (Vollständige Induktion)
Bevor wir den Satz beweisen schauen wir uns eine in der Mathematik geläufige Beweismethode an, die vollständige Induktion. Sei $z \in \mathbb{Z}$ und jedem $n \in \mathbb{Z}$ mit $n \geq z$ sei eine Aussage $X(n)$ zugeordnet. Ziel ist es, die Gültigkeit von $X(n)$ für alle $n \geq z$ zu zeigen. Dazu bedarf es zweier Beweisschritte:

a. *Induktionsanfang*: $X(z)$ ist richtig

b. *Induktionsschritt*: Unter der Annahme, dass $X(n)$ richtig ist für alle $z \leq m \leq n$, wird die Richtigkeit von $X(n+1)$ gezeigt.

Satz 1.10. Setze $z = 0$, $X(n)$: Ist $\big|A\big|$=n, so ist $\big|\mathcal{P}(A)\big| = 2^n$

a. *Induktionsanfang*
$X(0)$ ist richtig, das heißt es ist zu zeigen:
Ist $\big|$A$\big|$=0, so ist $\big|\mathcal{P}(A)\big| = 2^0 = 1$. Dies ist klar, da $A = \emptyset$ und $\big|\mathcal{P}(\emptyset)\big| = \big|\{\emptyset\}\big| = 1$

b. *Induktionsschritt*:
Annahme: $X(m)$ ist richtig für alle $0 \leq m \leq n$. Das heißt für alle Mengen B mit $\big|B\big|$= n , dann gilt $\big|\mathcal{P}(B)\big| = 2^n$.
Bleibt zu zeigen: Ist A eine Menge mit $\big|A\big|$=n+1 $\big|\mathcal{P}(A)\big| = 2^{n+1}$. Sei nun A={a,b,c,...} mit $\big|A\big|$=n+1. Dann ist $A \neq \emptyset$.
Sei $a \in A$ beliebig und setze $A' = A \setminus \{a\}$. Dann ist $\big|A'\ \big|$=n.
Betrachten wir nun eine beliebige Teilmenge B von A, so unterscheiden wir 2 verschiedene Fälle:
1.Fall: $a \in B$ (wir sagen B ist vom Typ 1). Dann hat B die Gestalt:
$B = \{a\} \cup B'$, wobei $B' = B \setminus \{a\} \subseteq A'$. Ist andererseits $C \subseteq A'$, so ist $C \cup \{a\}$ eine Teilmenge von A vom Typ 1. Dabei gilt :
Sind B_1, B_2 vom Typ 1 mit ${B_1}' = {B_2}'$, so ist $B_1 = B_2$.
Sind $C_1, C_2 \subseteq A'$ mit $C_1 \cup \{a\} = C_2 \cup \{a\}$, so ist $C_1 = C_2$.
Also ist die Anzahl der Teilmengen von A vom Typ 1 gleich der Anzahl der Teilmengen von A', mit $2^{|A|} = 2^n$.
2.Fall: Sei $a \notin B$ (wir sagen dann B ist vom Typ 2).
Dann gilt offensichtlich $a \notin B \Leftrightarrow B \subseteq A$. Also ist die Anzahl der Teilmengen von A vom Typ 2 gleich $\big|(A')\big| = 2^n$.
Insgesamt ergibt sich dann:
$\big|\mathcal{P}(A)\big| = \big|$(Teilmengen vom Typ 1)$\big| \dot\cup \big|$(Teilmengen vom Typ 2)$\big| = 2^n + 2^n = 2 * 2^n = 2^{n+1}$.
Der Punkt über dem Vereinigungszeichen bedeutet, dass die Vereinigung disjunkt ist.

(2) Gilt $m \sim m'$, so gilt auch $m' \sim m$.(*Symmetrie*)

(3) Gilt $m \sim m'$, $m' \sim m$",so gilt auch $m \sim m$".(*Transitivität*)

1.16 Beispiel
Sei $M = \mathbb{N}$. Dann wird durch $R = \{(m,m)\big|\ m \in M\}$, also durch die Gleichheit eine Äquivalenzrelation definiert, das heißt „$\sim$ "= „= ".

1.17 Satz
Sei M eine Menge.

(a) Sei $\sim$ eine Äquivalenzrelation auf M. Ist $m \in M$, so definieren wir
$T(m) = \{m'\big|m' \in M, m' \sim m\}$.
Dann gilt: $M = \bigcup_{m\in M} T(m)$.*Ferner ist*

$$T(m) \cap T(m') = \begin{cases} 0, & \text{für } m' \notin T(m) \\ T(m) = T(m'), & \text{für } m' \in T(m) \end{cases}$$

Die Mengen $T(m)$ heißen Äquivalenzklassen *in M zu $\sim$. Wählen wir aus jedem $T(m)$ ein Element m' und nennen wir die so gebildete Menge V, so gilt:*
$M = \dot{\bigcup}_{m'\in V}$, *mit der Eigenschaft $T(a) \cap T(b) = \emptyset$ für $a, b \in V$ und $a \neq b$.*
M ist also die disjunkte Vereinigung der $T(m')$mit $m' \in V$. Daran erkennen wir, dass $\sim$ eine Zerlegung von M liefert.

(b) Sei $M = \dot{\bigcup}_{j\in J} M_j$ mit $M_j \neq \emptyset$. Setze nun $m \sim m'$, falls m und m' in demselben M_j liegen. Dann wird durch $\sim$ eine Äquivalenzrelation auf M definiert.

Beweis. (a) Sei $m \in M$
Wegen $m \sim m$ ist $m \in T(m) \neq \emptyset$. Daher gilt: $M \subseteq \bigcup_{m\in M} T(m) \subseteq M$. Also gilt $M = \bigcup_{m\in M} T(m)$.
Sei nun $m' \in T(m)$, dann gilt nach Definition $m' \sim m$.
Sei nun $m_0 \in T(m')$, das heißt $m_0 \sim m'$. Wegen der Transitivität gilt dann auch $m_0 \sim m$, das heißt $m_0 \in T(m)$. Daraus folgt dann $T(m') \subseteq T(m)$. Aus Symmetriegründen gilt aber auch $m \sim m'$. Daher folgt analog $T(m) \subseteq T(m')$ und es ergibt sich $T(m) = T(m')$.
Sei nun $m' \notin T(m)$. Angenommen, es existiert ein $m_0 \in T(m) \cap T(m')$. Analog zum ersten Teil folgt aber dann $T(m) = T(m_0) = T(m') \ni m'$.

(b) Diese Aussage lässt sich ganz einfach nachrechnen und ist dem Leser als Übungsaufgabe überlassen.

□

2.4 Beispiel

(a) Die Abbildung f aus 2.2 a) ist surjektiv.
Die Abbildung f aus 2.2 b) ist nicht surjektiv.

(b) Definiere $f \in Hom(\mathbb{Q}, \mathbb{Q})$ durch $f(a) = 2a + 3$ für $a \in \mathbb{Q}$
f ist injektiv :
Sei

$$f(a_1) = f(a_2)$$
$$2a_1 + 3 = 2a_2 + 3$$
$$a_1 = a_2$$

f ist surjektiv :
Sei $b \in \mathbb{Q}$. Dann ist natürlich auch $\frac{b}{2} - \frac{3}{2} \in \mathbb{Q}$.
Daraus folgt dann: $f(\frac{b}{2} - \frac{3}{2}) = 2 * (\frac{b}{2} - \frac{3}{2}) = b$
Aus dieser Rechnung ergibt sich dann die Surjektivität und damit ist f bijektiv.

(c) Betrachte nun die Abbildung $f \in Hom(\mathbb{Q}, \mathbb{Q})$ definitert durch $f(a) = a^2$
Dann ist f nicht injektiv, da $f(1) = 1^2 = (-1)^2 = f(-1)$. f ist aber auch nicht surjektiv, da es kein Element $a \in \mathbb{Q}$ gibt mit $a^2 = -1$.(Man beachte, dass $a \in \mathbb{Q}$ sein muss, denn wir werden später bei der Definition der komplexen Zahlen sehen, dass wir eine Lösung für diese Gleichung finden können.)

2.5 Definition (Komposition von Abbildungen)
Sei $f \in Hom(A, B)$ und $g \in Hom(B, C)$. Dann heißt $g \circ f \in Hom(A, C)$ die *Komposition* oder Hintereinanderausführung von f mit g. Die Komposition ist dann definiert durch $(g \circ f)(a) = g(f(a))$ für alle $a \in A$. Die graphische Darstellung soll die Komposition weiter verdeutlichen:

$$\begin{array}{ccccc} A & \xrightarrow{f} & B & \xrightarrow{g} & C \\ a & \longmapsto & f(a) & \longmapsto & g(f(a)) \\ & & & \overset{g \circ f}{\searrow} & \end{array}$$

2.6 Beispiel
Sei $f \in Hom(\mathbb{Z}, \mathbb{Q})$ definiert durch $f(a) = a^2$ und $g \in Hom(\mathbb{Q}, \mathbb{R})$ definiert durch $g(b) = b + 1$.
Dann ist $g \circ f \in Hom(\mathbb{Z}, \mathbb{R})$ mit $(g \circ f)(a) = g(f(a)) = g(a^2) = a^2 + 1$

(a) Es existiert genau dann eine Abbildung $g \in Hom(A,B)$ mit $g \circ f = id_A$, wenn f injektiv *ist.(f hat dann eine Linkskuve)*

(b) Es existiert genau dann eine Abbildung $h \in Hom(B,A)$ mit $f \circ h = id_B$, falls f surjektiv *ist.(f hat eine Rechtskurve)*

(c) Es existiert genau dann eine Abbildung $g \in Hom(B,A)$ mit $g \circ f = id_A, f \circ g = id_B$, wenn f bijektiv ist .Die Abbbildung g ist dabei durch f eindeutig bestimmt und sie ist bijektiv. *g heißt dann auch die zu f* inverse Abbildung *oder nur* Inverse *und wird mir f^{-1} bezeichnet.*

Beweis. (a)

- Es gebe nun $g \in Hom(A,B)$ mit $g \circ f = id_A$. Sei nun $f(a_1) = f(a_2)$ mit $a_1, a_2 \in A$.
  Zu zeigen ist nun, dass dann $a_1 = a_2$. Nun gilt:
  $a_1 = id_A(a_1) = (g \circ f)(a_1) = g(f(a_1)) = g(f(a_2)) = (g \circ f)(a_2) = id_A(a_2) = a_2$
- Sei nun f injektiv. Wir müssen nun $g \in Hom(B,A)$ finden mit $g \circ f = id_A$. Da f injektiv ist, gibt es zu $b \in B$ höchstens ein $a \in A$ mit $f(a) = b$. Wir definieren nun eine Funktion g :
  $g : B \mapsto A$ durch $g(b) = \begin{cases} a, & fallsb = f(a) \in Bildf \\ a_0, & fallsb \notin Bildf \text{ mit } a_0 \in A \text{ beliebig} \end{cases}$
  Sei nun $a \in A$. Dann ist $(gf)(a) = g(f(a)) = a = id_A$ Also ist $gf = id_A$.

(b)

- Es gebe nun ein $h \in Hom(B,A)$ mit $fh = id_B$.
  Sei nun $b \in B$ beliebig. Dann gilt $b = id_B(b) = (fh)(b) = f(h(b)) \in Bildf$.
  Also ist f surjektiv.
- Sei f nun surjektiv. Dann existiert zu jedem $b \in B$ ein $a \in A$ mit $f(a) = b$.
  Definiere nun $h \in Hom(B,A)$ durch $h(b) = a$ mit obigem a.
  Dann ist aber $(fh)(b) = f(h(b)) = f(a) = b = id_B(b)$.
  Also ist $fh = id_B$.

(c)

- Es gebe nun ein $g \in Hom(B,A)$ mit $gf = id_A, fg = id_B$. Nach a) und b) ist f dann surjektiv und injektiv und daher f bijektiv.
- Es sei nun f bijektiv. Nach a) existiert ein $g \in Hom(B,A)$ mit $gf = id_A$ und nach b) existiert ein $\in Hom(B,A)$ mit $fh = id_B$. Dabei gilt dann :
  $g = g * id_B = g(fh) = (gf)h = id_A * h = h$:
  Man sieht auch, dass g durch f eindeutig bestimmt ist und g nach a) und b) bijektiv ist.

□

(1) Jedem $(a,b) \in G \times G$ ist genau ein Element $c \in G$ zugeordnet. Wir schreiben: $c = a \circ b$, " $\circ$ " heißt die Verknüpfung (oder Produkt) auf G (später: $a \circ b = ab$ oder $a + b$).

(2) Für alle a, b, c gilt
$(a \circ b) \circ c = a \circ (b \circ c)$

(3) Es gibt $e \in G$ mit

i. $e \circ a = a$ für alle $a \in G$

ii. Zu jedem $a \in G$ gibt es ein $b \in G$ mit $b \circ a = e$

b. gilt außer (1),(2),(3) auch

(5) $a \circ b = b \circ a$ für alle $a, b \in G$, so heißt G *abelsch*. (N.A. Abel, 1802-1829)

c. Ist G eine endliche Menge, so nennen wir $|G|$ die *Ordnung* von G.

d. Wird nur (1) und (2) gefordert, so heißt G eine *Halbgruppe*.

3.2 Beispiel a. Jede Menge $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ bildet bezüglich der Addition + eine Gruppe (abelsche Gruppe). Diese Gruppen bezeichnen wir mit $\mathbb{Z}^+, \mathbb{Q}^+, \mathbb{R}^+$.

b. Die Menge der natürlichen Zahlen $\mathbb{N}$ ist bezüglich + keine Gruppe: (aber Halbgruppe) Es gibt kein $e \in \mathbb{N}$ mit $e + 1 = 1$.

c. Setze $\mathbb{R}^\times = \{r \mid r \in \mathbb{R}, r \neq 0\}$ und verwende als Verknüpfung die Multiplikation. (abelsche Gruppe)

d. Genauso ist $\mathbb{Q}^\times$ eine abelsche Gruppe

e. Sei $M \neq \emptyset$.
Setze: $S(M) = \{f \in \mathrm{Hom}(M,M) \mid f\text{bijektiv}\}$. Sind $f, g \in S(M)$, so definiere fg wie in 2.5. Nach 2.7 ist 3.1.a.(1) erfüllt. 3.1.a.(2) ist ebenfalls nach 2.7 erfüllt. Nach 2.10 sind $f^{-1}, g^{-1} \in S(M)$. 3.1.a.(3) wird erfüllt mit $e = id_M$. Enthält M mindestens 3 elemente, so ist $S(M)$ nicht abelsch. (Seien (m_1, m_2, m_3) drei verschiedene Elemente aus M:
Definiere $f, g \in S(M)$ durch:

$f(m_1) = m_2, f(m_2) = m_1, f(m_3) = m_3$
$g(m_1) = m_1, g(m_2) = m_3, g(m_3) = m_2$
und $f(m) = g(m) = m$ für alle $m \in M \setminus \{m_1, m_2, m_3\}$
$(fg)(m_1) = f(g(m_1)) = f(m_1) = m_2$
$(gf)(m_1) = g(f(m_1)) = g(m_2) = m_3$
Also: $fg \neq gf$

b. Ist $M = \{a, b, c, \dots\}$, so schreibe auch $\langle M\rangle = \langle a, b, c, \dots\rangle$ und setze $\langle M_1 \cup \dots \cup M_k\rangle = \langle M_1, \dots, M_k\rangle$

4.5 Satz
Sei G eine Gruppe und $M \subseteq G$. Setze $M^{-1} = \{m^{-1} | m \in M\}$. Dann: $\langle M\rangle = \{e, x_1 \cdot \dots \cdot x_n | x_j \in M \bigcup M^{-1}, n \in \mathbb{N}\}$.

Beweis. Sei $U = \{e, x_1 \cdot \dots \cdot x_n | x_j \in M \cup M^{-1}, n \in \mathbb{N}\}$. Offensichtlich ist das Produkt zweier Elemente aus U wieder in U und $(x_1 \cdot \dots \cdot x_n)^{-1} = x_n^{-1} \cdot \dots \cdot x_1^{-1} \in U$. Also ist $M \subseteq U \leq G$ und demnach $\langle M\rangle \leq U$. Sei $u = x_1 \cdot x_2 \cdot \dots \cdot x_n \in U$. Dann ist $x_i \in M \bigcup M^{-1} \subseteq < M >$. Also $u = x_1 \cdot \dots \cdot x_n \in \langle M\rangle$. Damit ist $U \leq \langle M\rangle$ und somit $U = \langle M\rangle$. □

4.6 Definition
Sei G eine Gruppe und $U \leq G$. Ist $g \in G$, so setze $gU = \{gu | u \in U\}$ die *Linksnebenklasse von g nach U* und entsprechend $Ug = \{ug | u \in U\}$ die *Rechtsnebenklasse von g nach U*. Dabei ist $gU = U \Leftrightarrow g \in U$, denn
$\Rightarrow$ Sei $gU = U$. Dann ist $g = ge \in gU = U$
$\Leftarrow$ Sei $g \in U$. Klar: $gU \subseteq U$. Sei $u \in U$. Dann ist $g^{-1}u \in U$ und somit $u = g \cdot (g^{-1}u) \in gU$. Also $U \subseteq gU$.

4.7 Definition
Sei G eine Gruppe und $U \leq G$. Sind $g, h \in G$, so schreibe $g \sim h \Leftrightarrow g^{-1}h \in U \Leftrightarrow h \in gU$. $\sim$ ist eine Äquivalenzrelation auf G denn:

a. $g \in gU$. Also $g \sim g \Rightarrow g^{-1}g = e \in U$.

b. Sei $g \sim h$. Dann ist $h \in gU$. Das heißt $h = gu$ mit $u \in U$. Dann ist auch $u^{-1} \in U$ und $h \cdot u^{-1} = g$. Es ist also $g \in gU = h \cdot u^{-1}U = hU$. Also $h \sim g$.

c. Sei $g \sim h, s \sim k$. Dann ist $h \in gU$ und $k \in hU$. Etwa $h = gu_1$ und $k = hu_2$ mit $u_1, u_2 \in U$. Also ist $k = (gu_1)u_2 = g\underbrace{u_1u_2}_{\in U}$. Also $k \in kU = gu_1u_2U = gU$. Also ist $g \sim k$.

Die zugehörigen Äquivalenzklassen sind $T(g) = \{h \in G | h \sim g\} = \{h \in G | h \in gU\} = gU$. Nach 1.8 gilt $gU \cap hU = \begin{cases} \emptyset & \text{, falls } h \notin gU \\ gU = hU & \text{, falls } h \in gU \end{cases}$
Wähle aus jeder Äquivalenzklasse gU genau ein Element und bilde aus diesen Elementen eine Menge L. Dann ist $G = \bigcup\limits_{l \in L} lU$.

a. Sei e' das Einselement von H.
Dann: $e'(\alpha e) = \alpha e = \alpha(e^2) = (\alpha e) \cdot (\alpha e)$
Nach 3.4: $\alpha e = e'$.

b. $(\alpha g^{-1}) \cdot (\alpha g) = \alpha(g^{-1}g) = \alpha e = e'$ (nach 1.)
$(\alpha g) \cdot (\alpha g^{-1}) = \alpha(gg^{-1}) = \alpha e = a'$ (nach 1.)
Also: $(\alpha g^{-1}) = (\alpha g)^{-1}$ wegen der Eindeutigkeit der Inversen.

c. Sei $\alpha g_1, \alpha g_2 \in Bild(\alpha), \quad g_1, g_2 \in G$.
$\alpha g_1 \alpha g_2 = \alpha(g_1 g_2) \quad \in Bild(\alpha) \quad \Rightarrow \quad (\alpha g_1)^{-1} = \alpha(g_1^{-1}) \quad \in Bild(\alpha)$
Also: $Bild(\alpha) \leq H$.

d. Seien $g_1, g_2 \in Kern(\alpha)$, d.h. $\alpha g_1 = \alpha g_2 = e'$.
$\alpha(g_1 g_2) = \alpha(g_1)\alpha(g_2) = e'e' = e'$, d.h $g_1 g_2 \in Kern(\alpha)$.
$\alpha(g^{-1}) = (\alpha g_1)^{-1} = (e')^{-1} = e'$, d.h. $g_1^{-1} \in Kern(\alpha)$.
Also: $Kern(\alpha) \leq G$.
Seien nun $g_1, g_2 \in G$ und $x \in Kern(\alpha)$, d.h. $\alpha x = e'$.
$\alpha(g^{-1}xg) = \alpha g^{-1} \cdot \alpha x \cdot \alpha g = (\alpha g^{-1})(e')(\alpha g) = \alpha(g^{-1})\alpha(g) = \alpha(g^{-1}g) = \alpha e = e'$
Also: $g^{-1}xg \in Kern(\alpha)$.

e.
- Sei $Kern(\alpha) = \{e\}$:
Sei $\alpha g_1 = \alpha g_2$. Dann: $e' = (\alpha g_1)^{-1}(\alpha g_2) = (\alpha g_1^{-1})(\alpha g_2) = \alpha(g_1^{-1} g_2)$.
Also: $g_1^{-1} g_2 \in Kern(\alpha) = \{e\}$, also: $g_1^{-1} g_2 = e \quad \Rightarrow \quad g_1 = g_2$.

- Sei α injektiv:
Dann gibt es nur ein $y \in G$ mit $\alpha y = e'$, nämlich $y = e$ (nach 1.).
Also: $Kern(\alpha) = \{e\}$.

□

5.5 Motivation
Wir wollen nun versuchen, Gruppen auf einfachere Gruppen zurückzuführen. Dafür benötigen wir zunächst die Struktur der *Normalteiler*, und später dann die sogenannten *Faktorgruppen*.

5.6 Definition (Normalteiler)
Sei G eine Gruppe.

a. Für $a, b \in G$ setze:

$$a^b := b^{-1}ab.$$

Nenne a *konjugiert* zu a^b vermöge b.

b. Ist $M \subseteq G$, so setze:

$$M^b = \{m^b \mid m \in M\}$$

.

c. Sei $N \leq G$. N heißt *Normalteiler* von G, falls

$$g^{-1}Ng = N^g \leq N \quad \forall g \in G.$$

Schreibe: $N \trianglelefteq G, N \lhd G$.

5.7 Beispiel
In den folgenden Beispielen stellen wir einige typische Normalteiler vor:

a. $\{e\} \trianglelefteq G, \quad G \trianglelefteq G$

b. *Ist G abelsch*, so ist *jede* Untergruppe von G *Normalteiler* von G.

c. Ist $\alpha : G \to H$ Homomorphismus, so ist $Kern(\alpha) \trianglelefteq G$. (nach 5.4.4.)

5.8 Satz
Sei $U \leq G$. Dann sind äquivalent:

a. $U \trianglelefteq G$, d.h. $g^{-1}Ug \subseteq U$ für alle $g \in G$.

b. $\forall g \in G$ ist $g^{-1}Ug = U$.

c. $\forall g \in G$ ist $Ug = gU$.

d. Jede Linksnebenklasse von U in G ist eine Rechtsnebenklasse von U in G.

e. Jede Rechtsnebenklasse von U in G ist eine Linksnebenklasse von U in G.

f. $\forall g_1, g_2 \in G$ ist $(g_1U)(g_2U)$ eine Linksnebenklasse.

g. $\forall g_1, g_2 \in G$ ist $(g_1U)(g_2U) = (g_1g_2)U$.

Beweis.

- 1. $\Rightarrow$ 2.:
  Nach Vorr.: $g^{-1}Ug \subseteq U \quad \forall g \in G$.
  Also auch: $gUg^{-1} \subseteq U$.
  $U = (g^{-1}g)U(g^{-1}g) = g^{-1}(gUg^{-1})g \subseteq g^{-1}Ug \subseteq U$.
  Also: $g^{-1}Ug = U$.

multiplikativen neutralen Elements angibt, das dem additiven neutralen Element entspricht.

7.1 Definition
Eine Menge K mit zwei Verknüpfungen + und · heißt ein *Körper*, falls

a. K ist bzgl. + eine *abelsche Gruppe* mit neutralem Element 0 (*Nullelement von K*). (*Diese Gruppe heißt die additive Gruppe* K^+ von K.)

(1) K ist nicht leer.

$$K \neq \oslash \tag{I.16}$$

(2) Es gilt das Assoziativgesetz: Für alle $a, b, c \in K$

$$(a + b) + c = a + (b + c) \tag{I.17}$$

(3) Es gibt ein Element 0, dem Nullelement in K

$$0 + a = a \qquad \forall\ a \in K \tag{I.18}$$

(4) Zu jedem $a \in K$ gibt es $b \in K$ mit

$$a + b = 0 \tag{I.19}$$

Schreibe: $b = -a$ invertierbar

(5) Es gilt das Kommutativgesetz: Für alle $a, b \in K$

$$a + b = b + a \qquad \forall\ a, b \in K \tag{I.20}$$

b. $K \setminus \{0\}$ ist bzgl. · eine *abelsche Gruppe* mit neutralem Element 1 (*Einselement von K*). (*Diese Gruppe heißt die multiplikative Gruppe* K^X von K.)

(1) $K \setminus \{0\}$ ist nicht leer.

$$K \setminus \{0\} \neq \oslash, \tag{I.21}$$

d.h. jeder Körper: $|K| \geq 2$

(2) Es gilt das Assoziativgesetz: Für alle $a, b, c \in K$

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \tag{I.22}$$

(3) Es gibt ein Element $1 \neq 0$, dem Einselement in K

$$1 \cdot a = a \qquad \forall\ a \in K \setminus \{0\} \tag{I.23}$$

$$\begin{pmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{pmatrix} \cdot \begin{pmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{pmatrix} := \begin{pmatrix} a_1a_2 - b_1b_2 & a_1b_2 + a_2b_1 \\ -(a_2b_1 + a_1b_2) & -b_1b_2 + a_1a_2 \end{pmatrix} \in \mathbb{C} \tag{I.56}$$

Dann ist $\mathbb{C}$ ein Körper mit

$$\textit{Nullelement} := \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \textit{ und } \textit{Einselement} := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

b. Die Abbildung f mit

$$f(a) = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \tag{I.57}$$

ist ein Isomorphhismus von $\mathbb{R}$ auf den Unterkörper

$$\left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a \in \mathbb{R} \right\} \tag{I.58}$$

von $\mathbb{C}$:

$$\begin{aligned} f(a_1 + a_2) &= \begin{pmatrix} a_1 + a_2 & 0 \\ 0 & a_1 + a_2 \end{pmatrix} \\ &= \begin{pmatrix} a_1 & 0 \\ 0 & a_1 \end{pmatrix} + \begin{pmatrix} a_2 & 0 \\ 0 & a_2 \end{pmatrix} \\ &= f(a_1) + f(a_2) \end{aligned} \tag{I.59}$$

f bijektiv: klar. Also:

$$\mathbb{R} \cong \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a \in \mathbb{R} \right\} \tag{I.60}$$

c. Setze:

$$i := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \tag{I.61}$$

Somit erhält man bei der Multiplikation von i mit sich selber:

$$\begin{aligned} i^2 &= \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \\ &= -\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \end{aligned} \tag{I.62}$$

(c) *Sind* $A_{\mathcal{U}}$ *und* $A_{\mathcal{V}/\mathcal{U}}$ *Monomorphismen, so ist auch* A *ein Monomorphismus. Analoges gilt auch für Epimorphismen und Isomorphismen.*

(d) *Ist* $\dim_K \mathcal{V} < \infty$ *und ist* A *ein Isomorphisms, so sind auch* $A_{\mathcal{U}}, A_{\mathcal{V}/\mathcal{U}}$ *Isomorphismen.*

Beweis. (a) Das folgt sofort durch Nachrechnen der erforderlichen Eigenschaften.

(b) Wir zeigen die Wohldefiniertheit von $A_{\mathcal{V}/\mathcal{U}}$:
Seien $v_1, v_2 \in \mathcal{V}$ beliebig mit $v_1 + \mathcal{U} = v_2 + \mathcal{U}$. Dann gilt, da $v_2 - v_1 \in \mathcal{U}$:

$$Av_2 - Av_1 = A(v_2 - v_1) \in \mathcal{U}.$$

Also folgt $Av_1 + \mathcal{U} = Av_2 + \mathcal{U}$. Außerdem ist $A_{\mathcal{V}/\mathcal{U}}$ linear, denn es gilt

$$\begin{aligned} A_{\mathcal{V}/\mathcal{U}}((v_1 + \mathcal{U}) + (v_2 + \mathcal{U})) &= A_{\mathcal{V}/\mathcal{U}}((v_1 + v_2) + \mathcal{U}) \\ &= A(v_1 + v_2) + \mathcal{U} = Av_1 + Av_2 + \mathcal{U} = (Av_1 + \mathcal{U}) + (Av_2 + \mathcal{U}) \\ &= A_{\mathcal{V}/\mathcal{U}}(v_1 + \mathcal{U}) + A_{\mathcal{V}/\mathcal{U}}(v_2 + \mathcal{U}) \end{aligned}$$

sowie für alle $\lambda \in K$:

$$\begin{aligned} A_{\mathcal{V}/\mathcal{U}}(\lambda(v + \mathcal{U})) &= A_{\mathcal{V}/\mathcal{U}}(\lambda v + \mathcal{U}) \\ &= A(\lambda v) + \mathcal{U} = \lambda(Av) + \mathcal{U} \\ &= \lambda(Av + \mathcal{U}) \\ &= \lambda(A_{\mathcal{V}/\mathcal{U}}(v + \mathcal{U})). \end{aligned}$$

(c) Seien $A_{\mathcal{U}}$ und $A_{\mathcal{V}/\mathcal{U}}$ Monomorphismen. Sei $v \in \mathrm{Kern}A$. Dann gilt $Av = 0$ und somit:

$$\mathcal{U} = 0 + \mathcal{U} = Av + \mathcal{U} = A_{\mathcal{V}/\mathcal{U}}(v + \mathcal{U}).$$

Daraus folgt also, dass $v + \mathcal{U} \in \mathrm{Kern}A_{\mathcal{V}/\mathcal{U}} = \{\mathcal{U}\}$. Somit ist $v + \mathcal{U} = \mathcal{U}$, d.h. $v \in U$. Weiterhin gilt nun
$0 = Av = A_{\mathcal{U}}v$, also $v \in \mathrm{Kern}A_{\mathcal{U}} = \{0\}$. Folglich ist $v = 0$ und da v beliebig gewählt war $\mathrm{Kern}A = \{0\}$. Damit ist A ein Monomorphismus.
Seien nun $A_{\mathcal{U}}$ und $A_{\mathcal{V}/\mathcal{U}}$ Epimorphismen und sei $v \in \mathcal{V}$.
Da $A_{\mathcal{V}/\mathcal{U}}$ ein Epimorphismus ist, gibt es $v_1 \in \mathcal{V}$ mit $v + \mathcal{U} = A_{\mathcal{V}/\mathcal{U}}(v_1 + \mathcal{U}) = Av_1 + \mathcal{U}$.
Somit ist $v - Av_1 \in \mathcal{U}$.
Ananlog dazu gibt es, da $A_{\mathcal{U}}$ ein Epimorphismus ist, ein $u \in \mathcal{U}$ mit

Beweis. **a.** Nach Satz 2.10.c. gibt es genau ein B mit $BA = E_{\mathfrak{V}_1}$ und $AB = E_{\mathfrak{V}_2}$. Es bleibt zu zeigen, dass B linear ist. Seien $\nu_2, \nu_2' \in \mathfrak{V}_2$. Dann gilt:

$$\begin{aligned} A\left(B(\nu_2 + \nu_2')\right) &= (AB)(\nu_2 + \nu_2') \\ &= \nu_2 + \nu_2' \\ &= (AB)\nu_2 + (AB)\nu_2' \\ &= A(B\nu_2) + A(B\nu_2') \\ &= A(B\nu_2 + B\nu_2'). \end{aligned}$$

Da A injektiv ist, folgt zusätzlich

$$B(\nu_2 + \nu_2') = B\nu_2 + B\nu_2'.$$

Mit den gleichen Argumenten gilt für $\nu_2 \in \mathfrak{V}_2$ und $k \in K$:

$$\begin{aligned} A\left(B(k\nu_2)\right) &= (AB)(k\nu_2) \\ &= k\nu_2 \\ &= k\left((AB)\nu_2\right) \\ &= k\left(A(B\nu_2)\right) \\ &= A\left(k(B\nu_2)\right). \end{aligned}$$

Mit der Injektivität von A folgt

$$B(k\nu_2) = k(B\nu_2).$$

b. Die Aussage gilt offensichtlich.

□

1.9 Definition (reguläre Matrizen, general linear group)

a. Ist $A \in Hom_K(\mathfrak{V}, \mathfrak{V})$ ein Automorphismus, d.h. A^{-1} existiert nach Satz 1.8, so heißt A *regulär* oder *invertierbar*. Ist A nicht regulär, so heißt A *singulär*. In diesem Fall ist A ein Endomorphismus.

b. Setze $Gl(\mathfrak{V}) = \{A \in Hom_K(\mathfrak{V}, \mathfrak{V}) \mid \text{A regulär}\}$. Dann ist $Gl(\mathfrak{V})$ bezüglich der auf $Hom_K(\mathfrak{V}, \mathfrak{V})$ definierten Multiplikation eine Gruppe, die sogenannte *general linear group*, da alle Gruppeneigenschaften erfüllt werden:

a. Seien $A, B \in Gl(\mathfrak{V})$. Nach Satz 1.8 gilt $AB \in Gl(\mathfrak{V})$ und somit ist die Gruppe abgeschlossen.

b. Die Assoziativität $(AB)C = A(BC)$ gilt bereits in $Hom_K(\mathfrak{V}, \mathfrak{V})$ und überträgt sich direkt auf $Gl(\mathfrak{V})$.

und n *Spalten* $s_j = \begin{pmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{pmatrix}$, $j = 1, \ldots, n$

mit Koeffizienten $a_{ij} \in K$.

Als Kurzform schreiben wir (a_{ij}), wobei i der Zeilenindex und j der Spaltenindex ist. Die *Menge aller Matrizen* vom Typ (m, n) heißt $(K)_{m,n}$ (oder $K^{m \times n}$).

Ist $m = n$, so heißt (a_{ij}) *quadratisch*. In diesem Fall schreiben wir auch $(K)_n$ statt $(K)_{n,n}$.

Als *Hauptdiagonale* einer quadratischen Matrix bezeichnen wir die Einträge $a_{11}, a_{22}, \ldots, a_{nn}$, welche nachfolgend fett gedruckt sind.

$$\begin{pmatrix} \boldsymbol{a_{11}} & a_{12} & \ldots & a_{1n} \\ a_{21} & \boldsymbol{a_{22}} & \ldots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \ldots & \boldsymbol{a_{mn}} \end{pmatrix}$$

Ferner wollen wir drei Spezialfälle vorstellen.

a. Bei einer *unteren Dreiecksmatrix* sind gilt $a_{ij} = 0$ für alle Einträge mit $i < j$. Die mit $*$ gekennzeichneten Einträge sind beliebig.

$$\begin{pmatrix} * & 0 & \ldots & 0 & 0 \\ * & * & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & & \vdots \\ * & * & \ldots & * & 0 \\ * & * & \ldots & * & * \end{pmatrix}$$

Eine untere Dreiecksmatrix kann beispielsweise folgendermaßen aussehen:

$$\begin{pmatrix} 1 & 0 & 0 \\ 8 & 2 & 0 \\ 7 & 6 & 5 \end{pmatrix}$$

b. Analog sind bei einer *oberen Dreiecksmatrix* für $i > j$ alle Einträge $a_{ij} = 0$.

$$\begin{pmatrix} * & * & \ldots & * & * \\ 0 & * & \ldots & * & * \\ \vdots & \vdots & \ddots & & \vdots \\ 0 & 0 & \ldots & * & * \\ 0 & 0 & \ldots & 0 & * \end{pmatrix}$$

$k = 1, \ldots, n_3$. Daraus folgt:

$$\begin{aligned}(AB)\nu_j &= A(B\nu_j)\\ &= A\left(\sum_{i=1}^{n_2} b_{ij}\omega_i\right)\\ &= \sum_{i=1}^{n_2} b_{ij}(A\omega_i)\\ &= \sum_{i=1}^{n_2}\left(b_{ij}\left(\sum_{k=1}^{n_3} a_{ki}\mu_k\right)\right)\\ &= \sum_{k=1}^{n_3}\left(\sum_{i=1}^{n_2} b_{ij}a_{ki}\right)\mu_k\\ &= \sum_{k=1}^{n_3} c_{kj}\mu_k\end{aligned}$$

wobei wir im letzten Schritt ausnutzen, dass $b_{ij}a_{ki} = a_{ki}b_{ij}$ und somit $\sum_{k=1}^{n_3} a_{ki}b_{ij} = c_{kj}$ gilt.

□

2.6 Definition
Seien $(a_{ki}) \in (K)_{l,\boldsymbol{m}},\ (b_{ij}) \in (K)_{\boldsymbol{m},n}$. Dann:

$$(a_{ki})(b_{ik})(c_{kj}) \in (K)_{l,n}$$

mit $c_{kj} = \sum_{i=1}^{m} a_{ki}b_{ij}$.

Mit dieser Definition gilt in Satz 2.5.b.:

$${}_{\mathcal{L}_3}(AB)_{\mathcal{L}_1} = {}_{\mathcal{L}_3}A_{\mathcal{L}_2}{}_{\mathcal{L}_2}B_{\mathcal{L}_1}.$$

2.7 Beispiel

$$\begin{pmatrix}1&2&3\\0&1&2\end{pmatrix}\begin{pmatrix}1\\0\\1\end{pmatrix} = \begin{pmatrix}1\cdot 1 & + & 0\cdot 2 & + & 1\cdot 3\\ 1\cdot 0 & + & 0\cdot 1 & + & 1\cdot 2\end{pmatrix} = \begin{pmatrix}4\\2\end{pmatrix}$$

$$\begin{pmatrix}1&2&3\\0&1&2\end{pmatrix}\begin{pmatrix}1&1&0\\2&0&1\\3&1&2\end{pmatrix} = \begin{pmatrix}1\cdot 1+2\cdot 2+3\cdot 3 & 1\cdot 1+0\cdot 2+1\cdot 3 & 0\cdot 1+1\cdot 2+2\cdot 3\\ 1\cdot 0+2\cdot 1+3\cdot 2 & 1\cdot 0+0\cdot 1+1\cdot 1 & 0\cdot 0+1\cdot 1+2\cdot 2\end{pmatrix}$$

$$= \begin{pmatrix}14&4&8\\8&2&5\end{pmatrix}$$

hat die Matrix bezüglich der Basen $\mathfrak{B}_1$ und $\mathfrak{B}_2$ folgende Form:

$$\underset{\mathfrak{B}_1\mathfrak{B}_2}{A} = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{pmatrix}$$

b. Gelten folgende Gleichungen,

$$\begin{aligned} Av_1 &= w_1 \\ Av_2 &= 3w_1 - w_2 \\ Av_3 &= w_2 \end{aligned}$$

dann erhalten wir für die Matrix A bezüglich der Basen $\mathfrak{B}_1$ und $\mathfrak{B}_2$:

$$\underset{\mathfrak{B}_1\mathfrak{B}_2}{A} = \begin{pmatrix} 1 & 3 & 0 \\ 0 & -1 & 1 \end{pmatrix}$$

3.5 Bemerkung
Auch an dieser Stelle ist der *Unterschied* zwischen einer *Menge* von Vektoren und einem *System* von Vektoren wesentlich. Umnummerieren der Basen aendert im Allgemeinen die zugehörigen Matrizen.

Als Beispiel betrachten wir dafür jetzt die Gleichungen wie in Beispiel 3.4 2) und nummerieren unsere Basiseinträge wie folgt um :

$$\begin{aligned} v_i' &= v_i \qquad \text{mit } i = 1,2,3 \\ w_1' &= w_2 \qquad \text{und } w_2' = w_1. \end{aligned}$$

Dann gilt:

$$\left.\begin{aligned} Av_1' &= w_2' \\ Av_2' &= -w_1' + 3w_2' \\ Av_3' &= w_1' \end{aligned}\right\} \Rightarrow \underset{\mathfrak{B}_1'\mathfrak{B}_2'}{A} = \begin{pmatrix} 0 & -1 & 1 \\ 1 & 3 & 0 \end{pmatrix}$$

Die zugehörige Matrix bezüglich der Basen $\mathfrak{B}_1'$ und $\mathfrak{B}_2'$ hat andere Einträge als die Matrix in Beispiel 3.4.

3.6 Satz *a. Seien $\mathbb{V}$, $\mathbb{W}$ K-Vektorräume mit Basen $\mathfrak{B}_1 = (v_1, \ldots, v_n)$ und $\mathfrak{B}_2 = (w_1, \ldots, w_n)$. Die Abbildung :*

$$\underset{\mathfrak{B}_1\mathfrak{B}_2}{f} : Hom_k(\mathbb{V}, \mathbb{W}) \to (K)_{m,n}$$

*mit $\underset{\mathfrak{B}_1\mathfrak{B}_2}{f}\, A = \underset{\mathfrak{B}_1\mathfrak{B}_2}{A}$ ist ein K-*Vektorraum-Isomorphismus.
$Hom_k(\mathbb{V}, \mathbb{W})$ und $(K)_{m,n}$ sind also isomorph zueinander. (kurz geschrieben: $Hom_k(\mathbb{V}, \mathbb{W}) \cong (K)_{m,n}$)

Nach Satz 3.18 gilt (b_{kl}) regulär und $(b_{kl})^{-1} = (E_{\mathfrak{W}})_{\mathfrak{b}_2\mathfrak{b}_2'}$. Damit erhalten wir:

$$\begin{aligned} {}_{\mathfrak{b}_2'\mathfrak{b}_1'}A &= (E_{\mathfrak{W}})_{\mathfrak{b}_2'\mathfrak{b}_2'} A E_{\mathfrak{V}} \\ &= (E_{\mathfrak{W}})_{\mathfrak{b}_2'\mathfrak{b}_2'} {}_{\mathfrak{b}_2\mathfrak{b}_1}A (E_{\mathfrak{V}})_{\mathfrak{b}_1'\mathfrak{b}_1'} \\ &= (b_{kl})^{-1} {}_{\mathfrak{b}_2\mathfrak{b}_1}A (a_{ij}) \end{aligned}$$

Wobei die 2 Gleichung aus Definition 3.7 folgt.

b. folgt sofort aus 1.

c. Sei $\mathfrak{b}_1 = (v_1, \ldots, v_n)$ Basis von $\mathfrak{V}$ und $\mathfrak{b}_2 = (w_1, \ldots, w_m)$ Basis von $\mathfrak{W}$. Ausserdem sei $B = (b_{jk})$.
Definiere $A \in Hom_k(\mathfrak{V}, \mathfrak{W})$ durch $Av_k = \sum_{j=1}^{m} b_{jk} w_j$. Dann ist aber klar dass: ${}_{\mathfrak{b}_2\mathfrak{b}_1}A = B$.
Sei jetzt : $X^{-1} = (\bar{x}_{ij})$ und $Y = (y_{ij})$.
Ausserdem sei

$$v_j' = \sum_{i=1}^{n} y_{ij} v_i$$

mit $j = 1, \ldots, n$ und

$$w_l' = \sum_{k=1}^{m} \bar{x}_{kl} w_k$$

mit $l = 1, \ldots, m$.

Setzen wir jetzt: $\mathfrak{b}_1' = (v_1', \ldots, v_n')$ und $\mathfrak{b}_2' = (w_1', \ldots, w_m)$, dann gilt :

$${}_{\mathfrak{b}_2'\mathfrak{b}_1'}A \underset{a}{=} (X^{-1})^{-1} {}_{\mathfrak{b}_2\mathfrak{b}_1}A \, Y = XBY$$

□

3.23 Bemerkung a. Seien $\mathfrak{V}$ und $\mathfrak{W}$ endlich dimensionale K-Vektoräume und sei $A \in Hom_k(\mathfrak{V}, \mathfrak{W})$.
Problemstellung:
Wie kann man Basen $\mathfrak{b}_1$ und $\mathfrak{b}_2$ von $\mathfrak{V}$ beziehungsweise $\mathfrak{W}$ so wählen, dass ${}_{\mathfrak{b}_2\mathfrak{b}_1}A$ eine möglich einfache Gestalt hat? (In Sprache der Matrizen: Sei eine Matrix B gegeben, dann suchen wir invertierbare Matrizen X, und Y derart, dass XBY möglichst einfache Gestalt hat.

b. Sei $A \in Hom_k(\mathfrak{V}, \mathfrak{W})$ und $dim_k \mathfrak{W} < \infty$.
Problemstellung:

Ist $\pi_i \leq i$ für $i = 1, \ldots, r$, so ist $\pi_i = i$ für $i = 1, \ldots, r$.

Induktionsanfang: $r = 1$: $\pi_1 \leq 1$, folglich also $\pi_1 = 1$

Induktionsschritt: Sei gezeigt:

$$\left.\begin{array}{ll} \pi_i = i & \text{für } i \leq r-1 \\ \pi_i \leq i & \text{für } i = r \end{array}\right\} \text{Daraus folgt: } \pi_r = r$$

Also: Ist $\pi \neq \mathrm{id}$, so gibt es ein $i_o \in \{1, \ldots, n\}$ mit $\pi_{i_0} > i_0$

Dann gilt: $a_{i_0,\pi_{i_0}} = 0$

und damit: $\det A = a_{11} \cdots a_{nn} + \sum\limits_{\pi \neq \mathrm{id}} \operatorname{sgn}\pi \cdot \underbrace{a_{1,\pi_1} \cdots a_{n,\pi_n}}_{=0} = a_{11} \cdots a_{nn}$

5.3 Lemma
Sei $A = (a_{ij}) \in (\mathbb{R})_n$ und A' die Transponierte von A. (siehe 12.19)
Dann gilt: det A =det A'.

Beweis. Sei $A' = (b_{ij})$, also $b_{ij} = a_{ji}$ für $i, j = 1, \ldots, n$.

$\det A' = \sum\limits_{\pi \in S_n} \operatorname{sgn} \pi \cdot b_{1,\pi_1} \ldots b_{n,\pi_n} = \sum\limits_{\pi \in S_n} \operatorname{sgn} \pi \cdot a_{\pi_1,1} \ldots a_{\pi_n,n}$

Zu $j \in \{1, \ldots, n\}$ gibt es genau ein $k \in \{1, \ldots, n\}$ mit $\pi_k = j$.

Dabei gilt: $k = \pi_j^{-1}$ also folglich auch: $a_{\pi_k,k} = a_{j,\pi_j^{-1}}$.

Und da $\mathbb{R}$ kommutativ ist, ergibt sich die Gleichung:

$\det A' = \sum\limits_{\pi \in S_n} \operatorname{sgn} \pi \cdot a_{1,\pi_1^{-1}} \ldots a_{n,\pi_n^{-1}}$

Beachte außerdem: $\operatorname{sgn} \pi \cdot \operatorname{sgn} \pi^{-1} = \operatorname{sgn} \pi \cdot \pi^{-1} = \operatorname{sgn} \mathrm{id} = 1$

Womit gezeigt wäre, daß: $\operatorname{sgn} \pi = \operatorname{sgn} \pi^{-1}$ Fortführend können wir nun zeigen:

$$\begin{aligned} \det A' &= \sum_{\pi \in S_n} \operatorname{sgn} \pi^{-1} \cdot a_{1,\pi_1^{-1}} \ldots a_{n,\pi_n^{-1}} \qquad (\text{setze: } \pi^{-1} = \tau) \\ &= \sum_{\tau \in S_n} \operatorname{sgn} \tau \cdot a_{1,\tau_1} \ldots a_{n,\tau_n} \\ &= \det A \end{aligned}$$

□

5.4 Lemma *(a) Sei $A = (a_{ij}) \in (\mathbb{R})_n$. Sei $i \neq j$ und es gelte $z_i = z_j$ für die zwei Zeilen z_i und z_j von A. Dann gilt: det $A = 0$.*

(b) Analog für zwei gleiche Spalten.

Beweis. (a) Sei $\tau = (i, j) \in S_n$. Nach 6.6 gilt, daß $S_n = A_n \bigcup A_n\tau$

$$\begin{aligned} \det A &= \sum_{\pi \in S_n} \operatorname{sgn} \pi \cdot a_{1,\pi_1} \cdots a_{n,\pi_n} \\ &= \sum_{\alpha \in A_n} (\operatorname{sgn} \alpha \cdot a_{1,\alpha_1} \cdots a_{n,\alpha_n} + \operatorname{sgn} \alpha\tau \cdot a_{1,\alpha\tau_1} \cdots a_{n,\alpha\tau_n}) \end{aligned}$$

Dabei gilt: $\operatorname{sgn} \alpha\tau = \operatorname{sgn} \alpha \cdot \operatorname{sgn} \tau = 1 \cdot (-1) = -1$

$$\begin{aligned} \det A &= \sum_{\alpha \in A_n} (a_{1,\alpha_1} \cdots a_{n,\alpha_n} - a_{1,\alpha\tau_1} \cdots a_{n,\alpha\tau_n}) \\ &= \sum_{\alpha \in A_n} \left(a_{1,\alpha_1} \cdots a_{i,\alpha_i} \cdots a_{j,\alpha_j} \cdots a_{n,\alpha_n} - a_{1,\alpha_1} \cdots a_{i,\alpha_j} \cdots a_{j,\alpha_i} \cdots a_{n,\alpha_n}\right) \end{aligned}$$

$$h_i := c_2 \prod_{j=2, j\neq i}^{n} f_j \text{ für } i \geq 2$$

$$g = 1 - c_1 f_1 = 1 + h_1 f_1$$

$$g = c_2 f_2 \cdots f_n = h_i f_i \text{ für } i \geq 2$$

□

2.20 Definition
Sei R ein kommutativer Ring mit 1.

(a) Sei $\dot{\nu} \in R, \dot{\nu} \neq \emptyset$. $\dot{\nu}$ heißt ein **Ideal** von R, falls:

- Ist $f_1, f_2 \in \dot{\nu}$, so ist $f_1 \pm f_2 \in \dot{\nu}$
- Ist $f \in \dot{\nu}, g \in R$, so ist $f \cdot g \in \dot{\nu}$

Beispiel:

(a) Ist $R = \mathbb{Z}$ und $n \in \mathbb{Z}$, dann ist $\dot{\nu} = n\mathbb{Z}$ ein Ideal von $\mathbb{Z}$.

(b) Ist $R = K[x]$ und $f \in K[x]$, dann ist $\dot{\nu} = fK[x]$ ein Ideal von $K[x]$.

(b) Gibt es ein $f \in R$ mit $\dot{\nu} = fR = \{fr \mid r \in R\}$, so heißt $\dot{\nu}$ ein **Hauptideal** von R.

Ist jedes Ideal eines Rings ein Hauptideal, so nennen wir den Ring **Hauptidealring**.

2.21 Satz
$K[x]$ ist ein Hauptidealring.

Beweis. Ist $\dot{\nu} = \{0\}$, so ist $\dot{\nu} = 0 \cdot K[x]$ ein Hauptideal.
Sei also $\dot{\nu} \neq \{0\}$. Betrachte $M = \{\text{Grad } f \mid 0 \neq f \in \dot{\nu}\} \subseteq \mathbb{N} \cup \{0\}$. Offensichtlich ist $M \neq \emptyset$. Sei $n = \text{Grad } g$ ein kleinstes Element aus M mit $g \in \dot{\nu}$ und $f \in \dot{\nu}$ beliebig. Durch Anwenden des Euklidischen Algorithmus (17.6) folgt $f = gq + r$ mit Grad $r <$ Grad g. Daraus folgt

$$r = \underbrace{f}_{\in \dot{\nu}} - \underbrace{gq}_{\in \dot{\nu}} \in \dot{\nu},$$

aber Grad $r \notin M$, da Grad $r <$ Grad g. Also gilt $r = 0$ und $f = gq$. Damit ergibt sich $f \in gK[x] \subseteq \dot{\nu}$. Da die umgekehrte Inklusion klar ist, erhalten wir $\dot{\nu} = gK[x]$. □

Anmerkung: Genauso ergibt sich: $\mathbb{Z}$ ist ein Hauptidealring. Ersetze dazu Grad durch $|\cdot|$.

(d) Sei $\mathfrak{A} = (K)_n$. Dann ist $\alpha_A : K[x] \to \mathfrak{A}$ mit
$\alpha_A(a_0+a_1x+...+a_nx) = a_0E+a_1A+...+a_nA^n$ ein K-Algebrenautomorphismus.
Sei $\alpha_A(f) = f(A), K = \{0,1\}$ ein Körper, $f = x^2 - x \in K[x]$ und
$A = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \in \mathfrak{A}$. Dann ist $f(A) = A^2 - A = -A \neq 0$.

(e) Seien $K[x]$ und $K[y]$ Polynomringe. Dann gilt: $K[x] \cong K[y]$ als K-Algebren und $\alpha_y : K[x] \to K[y]$ ist ein K-Algebrenautomorphismus mit Inverse α_x.

3.3 Definition
Sei $f \in K[x], L$ ein Körper mit $K \leq L$ und $b \in L$. Ist $f(b) = 0$, so heißt b eine **Nullstelle** von f in L.

3.4 Satz
Sei $f \in K[x]$.

(a) Seien $b_1, ..., b_n$ paarweise verschiedene Nullstellen von f und $b_i \in K$. Dann gibt es ein $g \in K[x]$ mit $f = (x - b_1) \cdots (x - b_n) \cdot g$.

(b) Ist Grad $f = m \geq 0$, *so hat f in K höchstens m Nullstellen.*

(c) Ist Grad $f \geq 2$ *und hat f eine Nullstelle, so ist f nicht irreduzibel.*

Beweis. (a) Nach (17.6) gibt es $q, r \in K[x]$ mit $f = (x - b_1)q + r$ und
Grad $r <$ Grad $(x - b_n) = 1$. Wegen $0 = f(b_1) = r(b_1)$ folgt also $r = 0$. Das zeigt die Behauptung für $n = 1$.
Sei nun bereits für $k < n$ gezeigt: $f = (x - b_1) \cdots (x - b_k)g_k$ mit $g_k \in K[x]$. Dann haben wir

$$0 = f(b_{k+1}) = \underbrace{(b_{k+1} - b_1)}_{\neq 0} \cdots \underbrace{(b_{k+1} - b_k)}_{\neq 0} \cdot g_k(b_{k+1}).$$

Damit folgt $g_k(b_{k+1}) = 0$. Also $g_k = (x - b_{k+1})g_{k+1}$ mit $g_{k+1} \in K[x]$.

(b) Seien $b_1, ..., b_m$ paarweise verschiedene Nullstellen von f. Nach (a) gilt

$$f = (x - b_1) \cdots (x - b_m)g$$

mit Grad $f = \underbrace{1 + ... + 1}_{m-\text{mal}}$ + Grad $g \geq m$.

(c) Sei $f(b) = 0$ mit $b \in K$. Nach (a) gilt $f = (x-b)g$ mit $2 \leq$ Grad $f = 1+$Grad g, also Grad $g \leq 1$. Daraus folgt, dass g keine Einheit ist. Also ist f reduzibel.

□