Determinante (Existenz)

Aufgaben 3

```
> restart;
  with(LinearAlgebra):
```

Laplace-Entwicklung

Zur Erinnerung aus dem letzten Worksheet:

MATH: Sei V ein K-Vektorraum der Dimension n und $B \in V^n$ eine Basis von V.
Die (bezüglich B normierte) Determinante von V ist eine Abbildung

$$det_B : V^n \to K : (v_1, ..., v_n) \mapsto det_B(v_1, ..., v_n)$$

mit den folgenden drei Eigenschaften:

1) det_B ist **multilinear**, d.h.

$$det_B(x_1, ..., x_{i-1}, a \cdot x_i + b \cdot x_i', x_{i+1}, ..., x_n) = a \cdot det_B(x_1, ..., x_{i-1}, x_i, x_{i+1}, ..., x_n) + b \cdot det_B(x_1, ..., x_{i-1}, x_i', x_{i+1}, ..., x_n)$$

für alle $x \in V^n$, $1 \le i \le n$, $x_i' \in V$.

2) det_B ist **alternierend**, d.h. $det_B(x) = 0$ für alle $x \in V^n$, für die $1 \le i \ne j \le n$ existieren mit $x_i = x_j$.

3) det_B ist **normiert**, d.h. $det_B(B) = 1$.

MATH: Für eine Matrix $A \in K^{n \times n}$ definieren wir

$$\mathrm{Det}(A) := det_S(A_{-,1}, ..., A_{-,n})$$

wobei S die Standardbasis von $K^{n \times 1}$ ist.

MATH: Die Skizze des Eindeutigkeitsbeweises aus "Determinante (Eindeutigkeit)" hat den Nachteil, dass sie uns keine explizite Formel für die Determinante liefert, die man dann für den Existenzbeweis benutzen könnte, indem man die beiden Eigenschaften (unserer Definition aus dem Abschnitt) 1.) und 2.) mit Hilfe dieser Formel überprüft. Eine solche Formel wollen wir jetzt erarbeiten.

Wir wollen mit ein paar Vermutungen versuchen eine Formel für die Determinante zu entwickeln. Für diese Formel kann man dann zeigen, dass sie die (eindeutige) Determinante festlegt.

Wir vermuten, dass die Determinante eine Polynomfunktion der Matrixeinträge A_{ij} von $A \in K^{n \times n}$ ist.

Die Formel

$$\mathrm{Det}(\mathrm{Diag}([1,\ldots, 1, s, 1,\ldots, 1]) \cdot A) = s \cdot \mathrm{Det}(A)$$

sagt uns, dass in jedem Summand des Polynoms ein Eintrag A_{ij} nur zur ersten Potenz vorkommen kann und dass wahrscheinlich keine zwei Faktoren A_{ij} mit demselben i in einem solchen Summanden auftauchen können.

Die Formel

$$\mathrm{Det}(s \cdot A) = s^n \cdot \mathrm{Det}(A)$$

legt nahe, dass die Summanden immer genau n Faktoren haben.

Man beachte nun, dass wir für monomiale Matrizen (d.h. Matrizen, die in jeder Zeile und jeder Spalte nur einen Eintrag ungleich 0 besitzen) bereits eine Formel für die Determinante gefunden haben:

```
> sym:=proc(n::posint)
    local i, L;
    if n=1 then
      return [[1]];
    end if;
   L:=NULL;
    for i from 1 to n do
     L:=L,op(map(r->[op(r[1..i-1]),n,op(r[i..n-1])],sym(n-1))
  );
    end do;
    return [L];
  end proc:
> L4:=sym(4);
```

$L4 := [[4, 3, 2, 1], [4, 3, 1, 2], [4, 2, 3, 1], [4, 1, 3, 2], [4, 2, 1, 3], [4, 1, 2, 3], [3, 4, 2, 1], [3, 4, 1, 2], [2, 4, 3, 1], [1, 4, 3, 2], [2, 4, 1, 3], [1, 4, 2, 3], [3, 2, 4, 1], [3, 1, 4, 2], [2, 3, 4, 1], [1, 3, 4, 2], [2, 1, 4, 3], [1, 2, 4, 3], [3, 2, 1, 4], [3, 1, 2, 4], [2, 3, 1, 4], [1, 3, 2, 4], [2, 1, 3, 4], [1, 2, 3, 4]]$ **(1.1.1)**

```
> DD:=DiagonalMatrix([a,b,d,c]);
  SubMatrix(DD,1..4,L4[2]);
  Determinant(%);
```

$$DD := \begin{bmatrix} a & 0 & 0 & 0 \\ 0 & b & 0 & 0 \\ 0 & 0 & d & 0 \\ 0 & 0 & 0 & c \end{bmatrix}$$

$$\begin{bmatrix} 0 & 0 & a & 0 \\ 0 & 0 & 0 & b \\ 0 & d & 0 & 0 \\ c & 0 & 0 & 0 \end{bmatrix}$$

$$-c\,d\,a\,b$$ **(1.1.2)**

DENKANSTOSS: Nutze die Methoden aus dem Abschnitt "Determinante

(Eindeutigkeit)" um die obige Determinante auszurechnen.

Für jedes Elements aus **L4** muss ein Summand in der Determinantenformel vorkommen, also addieren wir sie alle auf:

```
> ex:=proc(A::Matrix,pi::list)
    local i,B;
    B:=Matrix(Dimension(A));
    for i from 1 to nops(pi) do
      B[i,pi[i]]:=A[i,pi[i]]
    end do;
    return B;
  end proc:
```

```
> A:=Matrix(4,4,symbol=a);
```

$$A := \begin{bmatrix} a_{1,1} & a_{1,2} & a_{1,3} & a_{1,4} \\ a_{2,1} & a_{2,2} & a_{2,3} & a_{2,4} \\ a_{3,1} & a_{3,2} & a_{3,3} & a_{3,4} \\ a_{4,1} & a_{4,2} & a_{4,3} & a_{4,4} \end{bmatrix} \quad \textbf{(1.1.3)}$$

```
> ex(A,L4[2]);
```

$$\begin{bmatrix} 0 & 0 & 0 & a_{1,4} \\ 0 & 0 & a_{2,3} & 0 \\ a_{3,1} & 0 & 0 & 0 \\ 0 & a_{4,2} & 0 & 0 \end{bmatrix} \quad \textbf{(1.1.4)}$$

```
> dA:=add(Determinant(ex(A,L4[i])),i=1..nops(L4));
```

$$\begin{aligned} dA := {} & a_{1,1} a_{2,2} a_{3,3} a_{4,4} - a_{1,1} a_{2,2} a_{3,4} a_{4,3} - a_{1,1} a_{2,3} a_{3,2} a_{4,4} \\ & + a_{1,1} a_{2,3} a_{3,4} a_{4,2} + a_{1,1} a_{2,4} a_{3,2} a_{4,3} - a_{1,1} a_{2,4} a_{3,3} a_{4,2} \\ & - a_{1,2} a_{2,1} a_{3,3} a_{4,4} + a_{1,2} a_{2,1} a_{3,4} a_{4,3} + a_{1,2} a_{2,3} a_{3,1} a_{4,4} \\ & - a_{1,2} a_{2,3} a_{3,4} a_{4,1} - a_{1,2} a_{2,4} a_{3,1} a_{4,3} + a_{1,2} a_{2,4} a_{3,3} a_{4,1} \\ & + a_{1,3} a_{2,1} a_{3,2} a_{4,4} - a_{1,3} a_{2,1} a_{3,4} a_{4,2} - a_{1,3} a_{2,2} a_{3,1} a_{4,4} \\ & + a_{1,3} a_{2,2} a_{3,4} a_{4,1} + a_{1,3} a_{2,4} a_{3,1} a_{4,2} - a_{1,3} a_{2,4} a_{3,2} a_{4,1} \\ & - a_{1,4} a_{2,1} a_{3,2} a_{4,3} + a_{1,4} a_{2,1} a_{3,3} a_{4,2} + a_{1,4} a_{2,2} a_{3,1} a_{4,3} \\ & - a_{1,4} a_{2,2} a_{3,3} a_{4,1} - a_{1,4} a_{2,3} a_{3,1} a_{4,2} + a_{1,4} a_{2,3} a_{3,2} a_{4,1} \end{aligned} \quad \textbf{(1.1.5)}$$

```
> coeff(dA,a[4,4],1);
```

$$\begin{aligned} & a_{1,1} a_{2,2} a_{3,3} - a_{1,1} a_{2,3} a_{3,2} - a_{1,2} a_{2,1} a_{3,3} + a_{1,2} a_{2,3} a_{3,1} + a_{1,3} a_{2,1} a_{3,2} \\ & - a_{1,3} a_{2,2} a_{3,1} \end{aligned} \quad \textbf{(1.1.6)}$$

ÜBUNG [01]:

1) Verstehe obige Überlegungen zur Formel der Determinante. Insbesondere: Welche Annahmen treffen wir? Was folgt aus diesen Annahmen? Wieso sind die Annahmen/Folgerungen sinnvoll?
2) Zeige, dass **coeff(dA,a[4,4],1)** gleich dem ist, was wir nach den obigen Überlegungen als Determinante von **SubMatrix(A,1..3,1..3)** erwarten würden.

MATH: Mit dem obigen Beispiel können wir nun die Existenz der Determinanten zeigen, indem wir die definierenden Eigenschaften aus der Formel heraus nachrechnen.
Wir entdecken, dass unsere Formel für die Determinante eine faszinierende induktive Struktur hat: Der Koeffizient von $a_{i,j}$ ist bis aufs Vorzeichen gleich der Determinante derjenigen Teilmatrix von A, die durch Streichung der i-ten Zeile und der j-ten Spalte entsteht.

DENKANSTOSS: Verifiziere dies und überzeuge dich von dem schachbrettartigen Vorzeichenschema:

```
> Matrix(4,4,(i,j)->(-1)^(i+j));
```

$$\begin{bmatrix} 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 \\ 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 \end{bmatrix} \tag{1.1.7}$$

MATH: Folgerung (Laplace-Entwicklung): Wir haben eine induktive Formel für die Determinante, etwa durch Entwicklung nach der ersten Spalte, d.h. wir können die Determinante wie folgt zerlegen:

```
> Det(A) = add((-1)^(1+i)*a[i,1]*Det(SubMatrix(A,[seq(j,j=1..
  i-1),seq(j,j=i+1..4)],2..4)),i=1..4);
```

$$\begin{aligned} Det\left(\begin{bmatrix} a_{1,1} & a_{1,2} & a_{1,3} & a_{1,4} \\ a_{2,1} & a_{2,2} & a_{2,3} & a_{2,4} \\ a_{3,1} & a_{3,2} & a_{3,3} & a_{3,4} \\ a_{4,1} & a_{4,2} & a_{4,3} & a_{4,4} \end{bmatrix}\right) &= a_{1,1}\, Det\left(\begin{bmatrix} a_{2,2} & a_{2,3} & a_{2,4} \\ a_{3,2} & a_{3,3} & a_{3,4} \\ a_{4,2} & a_{4,3} & a_{4,4} \end{bmatrix}\right) \\ &\quad - a_{2,1}\, Det\left(\begin{bmatrix} a_{1,2} & a_{1,3} & a_{1,4} \\ a_{3,2} & a_{3,3} & a_{3,4} \\ a_{4,2} & a_{4,3} & a_{4,4} \end{bmatrix}\right) + a_{3,1}\, Det\left(\begin{bmatrix} a_{1,2} & a_{1,3} & a_{1,4} \\ a_{2,2} & a_{2,3} & a_{2,4} \\ a_{4,2} & a_{4,3} & a_{4,4} \end{bmatrix}\right) \end{aligned} \tag{1.1.8}$$

$$-a_{4,1}\,Det\left(\left[\begin{array}{ccc} a_{1,2} & a_{1,3} & a_{1,4} \\ a_{2,2} & a_{2,3} & a_{2,4} \\ a_{3,2} & a_{3,3} & a_{3,4} \end{array}\right]\right)$$

```
> eval(subs(Det=Determinant, rhs(%)));
```

$$a_{1,1}\left(a_{2,2}a_{3,3}a_{4,4}-a_{2,2}a_{3,4}a_{4,3}-a_{2,3}a_{3,2}a_{4,4}+a_{2,3}a_{3,4}a_{4,2}+a_{2,4}a_{3,2}a_{4,3}-a_{2,4}a_{3,3}a_{4,2}\right)-a_{2,1}\left(a_{1,2}a_{3,3}a_{4,4}-a_{1,2}a_{3,4}a_{4,3}-a_{1,3}a_{3,2}a_{4,4}+a_{1,3}a_{3,4}a_{4,2}+a_{1,4}a_{3,2}a_{4,3}-a_{1,4}a_{3,3}a_{4,2}\right)+a_{3,1}\left(a_{1,2}a_{2,3}a_{4,4}-a_{1,2}a_{2,4}a_{4,3}-a_{1,3}a_{2,2}a_{4,4}+a_{1,3}a_{2,4}a_{4,2}+a_{1,4}a_{2,2}a_{4,3}-a_{1,4}a_{2,3}a_{4,2}\right)-a_{4,1}\left(a_{1,2}a_{2,3}a_{3,4}-a_{1,2}a_{2,4}a_{3,3}-a_{1,3}a_{2,2}a_{3,4}+a_{1,3}a_{2,4}a_{3,2}+a_{1,4}a_{2,2}a_{3,3}-a_{1,4}a_{2,3}a_{3,2}\right) \quad \textbf{(1.1.9)}$$

```
> expand(%-dA);
```

$$0 \quad \textbf{(1.1.10)}$$

Als weiteres Beispiel können wir z.B. nach der zweiten Zeile entwickeln:

```
> Det(A) = add((-1)^(i)*a[2,i]*Det(SubMatrix(A,[1,3,4],[seq(j,
  j=1..i-1),seq(j,j=i+1..4)])),i=1..4);
```

$$Det\left(\left[\begin{array}{cccc} a_{1,1} & a_{1,2} & a_{1,3} & a_{1,4} \\ a_{2,1} & a_{2,2} & a_{2,3} & a_{2,4} \\ a_{3,1} & a_{3,2} & a_{3,3} & a_{3,4} \\ a_{4,1} & a_{4,2} & a_{4,3} & a_{4,4} \end{array}\right]\right) = -a_{2,1}\,Det\left(\left[\begin{array}{ccc} a_{1,2} & a_{1,3} & a_{1,4} \\ a_{3,2} & a_{3,3} & a_{3,4} \\ a_{4,2} & a_{4,3} & a_{4,4} \end{array}\right]\right) + a_{2,2}\,Det\left(\left[\begin{array}{ccc} a_{1,1} & a_{1,3} & a_{1,4} \\ a_{3,1} & a_{3,3} & a_{3,4} \\ a_{4,1} & a_{4,3} & a_{4,4} \end{array}\right]\right) - a_{2,3}\,Det\left(\left[\begin{array}{ccc} a_{1,1} & a_{1,2} & a_{1,4} \\ a_{3,1} & a_{3,2} & a_{3,4} \\ a_{4,1} & a_{4,2} & a_{4,4} \end{array}\right]\right) + a_{2,4}\,Det\left(\left[\begin{array}{ccc} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{3,1} & a_{3,2} & a_{3,3} \\ a_{4,1} & a_{4,2} & a_{4,3} \end{array}\right]\right) \quad \textbf{(1.1.11)}$$

```
> eval(subs(Det=Determinant, rhs(%)));
```

$$-a_{2,1}\left(a_{1,2}a_{3,3}a_{4,4}-a_{1,2}a_{3,4}a_{4,3}-a_{1,3}a_{3,2}a_{4,4}+a_{1,3}a_{3,4}a_{4,2}+a_{1,4}a_{3,2}a_{4,3}-a_{1,4}a_{3,3}a_{4,2}\right)+a_{2,2}\left(a_{1,1}a_{3,3}a_{4,4}-a_{1,1}a_{3,4}a_{4,3}-a_{1,3}a_{3,1}a_{4,4}+a_{1,3}a_{3,4}a_{4,1}+a_{1,4}a_{3,1}a_{4,3}-a_{1,4}a_{3,3}a_{4,1}\right)-a_{2,3}\left(a_{1,1}a_{3,2}a_{4,4}-a_{1,1}a_{3,4}a_{4,2}-a_{1,2}a_{3,1}a_{4,4}+a_{1,2}a_{3,4}a_{4,1}+a_{1,4}a_{3,1}a_{4,2}-a_{1,4}a_{3,2}a_{4,1}\right)+a_{2,4}\left(a_{1,1}a_{3,2}a_{4,3}-a_{1,1}a_{3,3}a_{4,2}\right. \quad \textbf{(1.1.12)}$$

$-a_{1,2}\,a_{3,1}\,a_{4,3}+a_{1,2}\,a_{3,3}\,a_{4,1}+a_{1,3}\,a_{3,1}\,a_{4,2}-a_{1,3}\,a_{3,2}\,a_{4,1})$

```
> expand(%-dA);
```

$$0 \qquad (1.1.13)$$

Allgemein lautet die Formel mittels Laplace-Entwicklung:
Für die j-te Zeile:

$$Det(A) = \sum_{i=1}^{n} (-1)^{i+j} \cdot A_{j,\,i} \cdot Det(B_{j,\,i})$$

Für die k-te Spalte:

$$Det(A) = \sum_{i=1}^{n} (-1)^{i+k} \cdot A_{i,\,k} \cdot Det(B_{i,\,k})$$

Hierbei ist $B_{i,\,j}$ die Matrix, welche aus A durch Streichung der i-ten Zeile und j-ten Spalte entsteht.

MATH: Unsere Formel für die Determinante, gegeben durch Laplace-Entwicklung, - im Folgenden auch wieder kurz mit Det bezeichnet - hat drei Eigenschaften, wenn man sie als Formel für die Spalten A_i der Matrix A versteht:
I.) Die Determinante ist **multilinear** in jeder Spalte, d.h.

$$\mathrm{Det}(A_1,\ldots,A_{k-1},A_k+B_k,A_{k+1},\ldots,A_n) = \mathrm{Det}(A_1,\ldots,A_{k-1},A_k,A_{k+1},\ldots,A_n) + \mathrm{Det}(A_1,\ldots,A_{k-1},B_k,A_{k+1},\ldots,A_n)$$

und

$$\mathrm{Det}(A_1,\ldots,A_{k-1},a\cdot A_k,A_{k+1},\ldots,A_n) = a\cdot\mathrm{Det}(A_1,\ldots,A_{k-1},A_k,A_{k+1},\ldots,A_n).$$

II.) Die Determinante ist **alternierend**, d. h. falls zwei Spalten gleich sind, ist der Wert der Determinante Null.
III.) Die Determinante ist **normiert**: $\mathrm{Det}(I_n) = 1$

DENKANSTOSS: Verifiziere diese drei Eigenschaften aus der obigen Formel heraus.

MATH: Dadurch, dass die Formel für die Determinante I.) - III.) erfüllt, haben wir die Existenz der Determinante (nach der "korrekten" Definition) gezeigt.

MATH: Mit Hilfe von I.) bis III.) kann man jetzt unsere definierenden Eigenschaften 1) und 2) überprüfen. Dabei folgt 1.) trivial aus der Formel, so dass nur 2.) offen bleibt:
Die i-te Spalte von $A\cdot B$ ist eine Linearkombination der Spalten von A mit Koeffizienten $B_{1,\,i},\ldots,B_{n,\,i}$:

```
> A:=Matrix(4,4,symbol=a);
  B:=Matrix(4,4,symbol=b);
```

$$A := \begin{bmatrix} a_{1,1} & a_{1,2} & a_{1,3} & a_{1,4} \\ a_{2,1} & a_{2,2} & a_{2,3} & a_{2,4} \\ a_{3,1} & a_{3,2} & a_{3,3} & a_{3,4} \\ a_{4,1} & a_{4,2} & a_{4,3} & a_{4,4} \end{bmatrix}$$

$$B := \begin{bmatrix} b_{1,1} & b_{1,2} & b_{1,3} & b_{1,4} \\ b_{2,1} & b_{2,2} & b_{2,3} & b_{2,4} \\ b_{3,1} & b_{3,2} & b_{3,3} & b_{3,4} \\ b_{4,1} & b_{4,2} & b_{4,3} & b_{4,4} \end{bmatrix} \tag{1.1.14}$$

```
> Column(A.B,3);
```

$$\begin{bmatrix} a_{1,1} b_{1,3} + a_{1,2} b_{2,3} + a_{1,3} b_{3,3} + a_{1,4} b_{4,3} \\ a_{2,1} b_{1,3} + a_{2,2} b_{2,3} + a_{2,3} b_{3,3} + a_{2,4} b_{4,3} \\ a_{3,1} b_{1,3} + a_{3,2} b_{2,3} + a_{3,3} b_{3,3} + a_{3,4} b_{4,3} \\ a_{4,1} b_{1,3} + a_{4,2} b_{2,3} + a_{4,3} b_{3,3} + a_{4,4} b_{4,3} \end{bmatrix} \tag{1.1.15}$$

```
> A.Column(B,3);
```

$$\begin{bmatrix} a_{1,1} b_{1,3} + a_{1,2} b_{2,3} + a_{1,3} b_{3,3} + a_{1,4} b_{4,3} \\ a_{2,1} b_{1,3} + a_{2,2} b_{2,3} + a_{2,3} b_{3,3} + a_{2,4} b_{4,3} \\ a_{3,1} b_{1,3} + a_{3,2} b_{2,3} + a_{3,3} b_{3,3} + a_{3,4} b_{4,3} \\ a_{4,1} b_{1,3} + a_{4,2} b_{2,3} + a_{4,3} b_{3,3} + a_{4,4} b_{4,3} \end{bmatrix} \tag{1.1.16}$$

Wegen der Multilinearität erhält man also
$\mathrm{Det}(A \cdot B) =$ Summe von Determinanten von Matrizen, deren Spalten von A kommen, mit Vorfaktoren, die Produkte in den B_{ij} sind.
Jede dieser Determinanten ist Null, falls eine Spalte von A mehrfach auftaucht.
Die übrigen sind bis aufs Vorzeichen gleich $\mathrm{Det}(A)$.
Ergebnis:

$$\mathrm{Det}(A \cdot B) = f(B) \cdot \mathrm{Det}(A)$$

wo $f(B)$ irgendeine Funktion ist, deren Wert durch die Einträge der Matrix B bestimmt ist.
Aus Symmetriegründen (mit Zeilen von B arbeiten):

$$\mathrm{Det}(A \cdot B) = g(A) \cdot \mathrm{Det}(B)$$

Insgesamt:

$$\mathrm{Det}(A \cdot B) = \mathrm{Det}(A) \cdot \mathrm{Det}(B) \cdot k$$

mit $k \in K$, welches nicht mehr von A oder B abhängt.
Wir setzen $A = B =$ Einheitsmatrix und sehen, dass wir $k = 1$ setzen müssen.
Beweisende.

ÜBUNG [02]:

Zeige:
$$\mathrm{Det}(A^{tr}) = \mathrm{Det}(A)$$

Wir sind im allgemeinen nicht nur an Determinanten von Matrizen, sondern auch an Determinanten von Endomorphismen interessiert.

ÜBUNG [03]:

1) Definiere die Determinante eines Endomorphismus φ. Diese Definition darf (soll!) von der Wahl einer Basis des Vektorraumes abhängen.
2) Zeige, dass deine Wahl doch unabhängig von der gewählten Basis ist.
3) Warum betrachten wir keine Determinanten von allgemeinen Homomorphismen und nur von Endomorphismen?

Ringe und Ideale

Aufgaben: 6

```
> restart;
```

Ringe, Restklassenringe, Ideale

MATH: Im Folgenden werden Ringe immer kommutativ sein und ein Einselement haben. Unter diesen sind die Körper ausgezeichnet. Ein Ring *R* ist genau dann ein Körper, wenn jedes Element ungleich 0 in *R* invertierbar ist, also ein multiplikatives Inverses hat, kurz eine **Einheit** ist.

ÜBUNG [04]:

Was sind die Einheiten in $\mathbb{Z}$, $\mathbb{R}[x]$, $\mathbb{Q}$, $\mathbb{Z}[x]$? Welche dieser Ringe sind Körper? Gib eine Nichteinheit $\neq 0$ an, wenn kein Körper vorliegt.

MATH: Ein interessantes Spiel besteht darin, in einem Ring ein (oder mehrere) Element(e) Null zu setzen, also die Gleichheit durch eine gewisse Äquivalenzrelation zu ersetzen, aber ansonsten genau wie vorher zu rechnen, so dass man wieder einen Ring bekommt. Die Elemente dieses Ringes wären dann die Äquivalenzklassen und die Addition und Multiplikation dieser Klassen dann vertreterweise durchzuführen.

BEISPIELE:

1.) In einem Körper K setzen wir ein Element

$$a \neq 0$$

zu Null, was wir so schreiben:

$$a \equiv 0.$$

Dann folgt

$$1 = a^{-1}a \equiv a^{-1}0 = 0$$

also

$$1 \equiv 0$$

und damit

$$b \equiv 0$$

für alle $b \in K$.

Damit hätte der neue Ring nur ein einziges Element. So etwas betrachten wir nicht . Man verlangt meistens bei einem Ring

$$1 \neq 0.$$

2.) In $\mathbb{Z}$ setzen wir

$$2 \equiv 0$$

und bekommen

$$\mathbb{Z}/2\mathbb{Z} = \mathbb{F}_2$$

den Körper aus zwei Elementen.

3.) In $\mathbb{R}[x]$ setzen wir

$$x^2 + 1 \equiv 0$$

und bekommen

$$\mathbb{R}[x]/\mathbb{R}[x]\left(x^2+1\right) = \mathbb{C}$$

den Körper der komplexen Zahlen.

ÜBUNG [05]:
Zeige, dass $$\mathbb{C}[x]/\mathbb{C}[x]\left(x^2+1\right)$$ kein Körper ist.

MATH: Sei R ein Ring (also kommutativ mit Eins, wie oben vereinbart). Eine nicht leere Teilmenge

$$I \subseteq R$$

heißt **Ideal** von R, falls

$$a, b \in I \;\Rightarrow\; a + b \in I$$

und

$$a \in I, r \in R \Rightarrow ra, ar \in I$$

gilt.

Schreibweise: $I \trianglelefteq R$.

Diese beiden Regeln sind leicht zu merken, da die Restklasse der 0 ein Ideal bildet, und ebensoleicht motiviert durch

$$0+0=0$$

und

$$0\,r=r0=0.$$

Ist $I \trianglelefteq R$ und $r \in R$, so heißt

$$r+I := \{r+i \mid i \in I\}$$

die **Restklasse** von r nach I.
Die Menge aller Restklassen nach I bilden mit der vertreterweisen Addition und Multiplikation einen Ring, der mit

$$R/I$$

bezeichnet wird.

DENKANSTOSS: Woher kennst du dieses Konzept?

ÜBUNG [06]:

Die ungeraden Zahlen bilden eine Restklasse in $\mathbb{Z}$.
Zeige dies, bestimme das zugehörige Ideal und erinnere dich an die Division mit Rest, um den Namen Restklasse zu motivieren.

DENKANSTOSS: Der Schnitt einer Menge von Idealen eines Ringes ist wieder ein Ideal.

Hauptidealbereiche, Teilbarkeit

MATH: Wichtige Beispiele von Idealen sind Hauptideale. Das von

$$r \in R$$

erzeugte Ideal, also der Schnitt aller Ideale, die r enthalten ist, ist gegeben durch

$$rR = Rr := \{ra \mid a \in R\}$$

und heißt das von r erzeugte **Hauptideal** von R.
Übrigens sind die beiden trivialen Ideal $\{0\}$ und R auch Hauptideale , denn

$$\{0\} = 0\,R \quad \text{und} \quad R = 1\,R.$$

Beachte R/R ist der bereits oben geschmähte Nullring.

DENKANSTOSS: Die Summe und das Produkt zweier Ideale sind wieder Ideale:

$$I_1, I_2 \trianglelefteq R \Rightarrow I_1 + I_2 := \{a+b \mid a \in I_1,\ b \in I_2\} \trianglelefteq R.$$

$$I_1, I_2 \trianglelefteq R \Rightarrow I_1 I_2 := \{a_1 b_1 + \ldots + a_n b_n \mid n \in \mathbb{N}, a_i \in I_1,\ b_i \in I_2\} \trianglelefteq R.$$

ÜBUNG [07]:

Zeige, dass in einem Euklidischem Ring jedes Ideal ein Hauptideal ist.
Bestimme den Hauptidealerzeuger von

$$(133412\mathbb{Z} + 33412\mathbb{Z}) \trianglelefteq \mathbb{Z}$$

und

$$((x^{12} + x^8 + 1)\mathbb{F}_2[x] + (x^{15} + x^{10} + 1)\mathbb{F}_2[x]) \trianglelefteq \mathbb{F}_2[x]$$

(Erinnerung: Man hat eine Division mit Rest und kann von dem Rest sagen dass er "kleiner" also der Divisor, sodass man einen Euklidischen Algorithmus hat) .

MATH: Ringe, bei denen das Produkt zweier von Null verschiedener Elemente wieder von Null verschieden ist, heißen **Integritätsbereich**e.
Integritätsbereiche, deren sämtliche Ideale Hauptideale sind heißen **Hauptidealbereich**e.

Offenbar sind Euklidische Ringe Hauptidealbereiche. $\mathbb{Z}$ und $K[x]$, wobei K ein Körper ist, sind die wichtigsten Beispiele.

MATH: Sind R und S Ringe, so heißt eine Abbildung

$$\alpha : R \to S$$

Ringhomomorphismus, falls sie additiv und multiplikativ ist, sowie

$$\alpha(1_R) = 1_S$$

erfüllt.

DENKSANSTOSS: Ist ein Ringhomomorphismus bijektiv, so ist sein Inverses auch Ringhomomorphimus. Man spricht von einem **Ringisomorphismus**.

Man überlegt sich leicht:
M ATH: $I \trianglelefteq R \Rightarrow \nu : R \to R/I : r \mapsto r + I$ ist ein **Ringepimorphismus**, also ein surjektiver Ringhomomorphismus.
Umgekehrt:
Ist $\alpha : R \to S$ ein Ringhomomorphismus und $I \trianglelefteq S$ ein Ideal, so folgt $\alpha^{-1}(I) \trianglelefteq R.$ Insbesondere ist

$$\mathrm{Kern}\,(\alpha) := \alpha^{-1}(\{0_S\}) \trianglelefteq R.$$

Weiter:
Ist $\alpha : R \to S$ ein Ringepimorphismus und $I \trianglelefteq R \Rightarrow \alpha(I) \trianglelefteq S.$

ÜBUNG [08]:

Zeige $\mathbb{Z}/100\mathbb{Z}$ ist kein Hauptidealbereich, obwohl seine sämtlichen Ideale Hauptideale sind. Zeige also insbesondere, dass sämtliche Ideale Hauptideale sind.

MATH: Ein Körper *K* hat nur die beiden **trivialen Ideale** $\{0\}$ und *K*.
Offenbar ist ein Ring $K \neq \{0\}$, welcher keine nicht-triviale Ideale enthält, ein Körper (**DENKANSTOSS**: Warum?).
Also: Ist $R \neq \{0\}$ ein Ring und $I \trianglelefteq R$, so folgt:

R/I ist Körper genau dann, wenn *I* **maximales Ideal** von *R* ist.

(Dabei heißt $I \trianglelefteq R$ maximales Ideal, wenn $I \neq R$ gilt und *R* das einzige *I* umfassende Ideal ist.)

BEISPIEL:
$x\mathbb{Z}[x]$ ist kein maximales Ideal von $\mathbb{Z}[x]$, denn $\mathbb{Z}[x]/x\mathbb{Z}[x] \cong \mathbb{Z}$ ist kein Körper.
$2\,\mathbb{Z}[x]$ ist kein maximales Ideal von $\mathbb{Z}[x]$, denn $\mathbb{Z}[x]/2\,\mathbb{Z}[x] \cong \mathbb{F}_2[x]$ ist kein Körper.
$x\mathbb{Z}[x] + 2\,\mathbb{Z}[x]$ ist ein maximales Ideal von $\mathbb{Z}[x]$, denn $\mathbb{Z}[x]/(2\,\mathbb{Z}[x] + x\mathbb{Z}[x]) \cong \mathbb{F}_2$ ist ein Körper.

DENKANSTOSS: Finde alle Restklassenkörper von $\mathbb{Z}/100\,\mathbb{Z}$.

MATH: Auf Hauptidealbereiche R und $a \in R$ angewandt bedeutet dies die Äquivalenz der folgenden drei Aussagen:
1.) Ra ist ein maximales Ideal von R.
2.) *R/Ra* ist ein Körper.
3.) *a* ist **unzerlegbar (= irreduzibel)**, d. h. *a* lässt nur triviale Faktorierungen zu, also solche, in denen ein Faktor eine Einheit ist.

Wir wollen jetzt einen Schritt weitergehen und eine vollständige Teilbarkeitstheorie in Hauptidealbereichen skizzieren, Zunächst eine allgemeine Vorbereitung:

MATH: Sei *R* ein Ring, $a, b \in R$. Man sagt a **teilt** b (kurz $a \mid b$), falls $b \in Ra$ (oder äquivalent $Rb \subseteq Ra$) gilt.
Falls $a \mid b$ und $b \mid a$ gilt, dann heißen a, b **assoziiert**.
Ein Element $p \in R$ heißt **prim**, falls für alle $a, b \in R$ gilt:

$p \mid ab$ 0 $p \mid a$ oder $p \mid b$.

Offenbar gilt in Integritätsbereichen: Ein primes Element ist irreduzibel.

Die Umkehrung hiervon ist der Kernpunkt bei Hauptidealbereichen
MATH: Sei R ein Hauptidealbereich und $u \in R$ irreduzibel. Dann ist *u* prim.

Beweis: Angenommen $u \nmid a$ und $u \nmid b$. Da Ru ein maximales Ideal ist, folgt dann

$$Ru + Ra = R \quad \text{und} \quad Ru + Rb = R.$$

Also haben wir $r_i \in R$ mit

$$r_1 u + r_2 a = 1 \quad \text{und} \quad r_3 u + r_4 b = 1,$$

sodass durch Produktbildung folgt:

$$r_5 u + r_6 ab = 1$$

mit $r_5, r_6 \in R$ geeignet. Das heißt aber $u \nmid ab$.

q.e.d.

ÜBUNG [09]:

Sei R ein Hauptidealbereich und $a, b \in R$. Zeige:
$a, b \in R$ sind **teilerfremd**, d. h. haben nur genau dann Einheiten als einzige gemeinsame Teiler, wenn

$$Ra + Rb = R$$

gilt.