1.11 Lemma: Sei $a, b \in K \setminus \{0\}$. Dann ist $ab \neq 0$.

Beweis: Angenommen $a \cdot b = 0$ mit $a \neq 0$.

Dann ex $a^{-1} \in K$, und es folgt:

$$0 = a^{-1} \cdot 0 = a^{-1}(ab) = (a^{-1}a) \cdot b = 1 \cdot b = b.$$

1.12 Bem/Def: Sei R kommutativer Ring mit 1.

(a) Ein Element $a \in R$ heißt Nullteiler, falls $a \neq 0$ und es ex. $b \in R \setminus \{0\}$ mit $ab = 0$ (oder $ba = 0$).

Beispielsweise: $\bar{2}, \bar{3}$ sind Nullteiler in $\mathbb{Z}_6$, denn $\bar{2} \cdot \bar{3} = \bar{6} = \bar{0}$.

Ein kommutativer Ring mit 1 ohne Nullteiler ist ein Integritätsbereich (IB).

(b)(i) Lemma 1.11 besagt, daß jeder Körper ein Integritätsbereich ist.

(ii) Sei $a \in R^\times$ eine Einheit. Dann ist a kein Nullteiler, denn:

(iii) Der Ring $M_n(K)$ hat Nullteiler

z.B.

(iv) Seien R, S Ringe. Dann ist $R \times S = \{(r,s) \mid r \in R, s \in S\}$ ein Ring mit komponentenweiser Addition und Multiplikation

$$(r,s) \dot{+} (a,b) := (r \dot{+} a, s \dot{+} b)$$

für alle $r, a \in R$ und $s, b \in S$. Dieser Ring $R \times S$ hat Nullteiler

z.B.

(v) Sei $n \geq 2$ und $R = \mathbb{Z}_n$. Dann ist $a + n\mathbb{Z} \neq 0 + n\mathbb{Z}$ ein Nullteiler genau dann, wenn $ggT(a,n) \neq 1$.

Beweis:

1.13 Def: Der Grad eines Polynoms $p = \sum a_i X^i \in k[X]$ ist definiert als

$$\deg(p) := \begin{cases} \max\{i \mid a_i \neq 0\} & \text{falls } p \neq 0, \\ -\infty & \text{falls } p = 0. \end{cases}$$

Ist $d := \deg(p) \neq -\infty$, so heißt der Koeffizient a_d auch Leitkoeffizient von p, der Summand $a_d X^d$ heißt Leitsummand. Polynom p heißt normiert, falls der Leitkoeffizient Eins ist.

1.14 Bsp: (a) $\deg(X-a) = 1$, für alle $a \in K$

. $\deg(2X^3 - 7X + 5) =$ ____

. Polynom $p \in k[X]$ ist konstant
$\Leftrightarrow \deg p \leq 1$.

(b) Definiere $p = 2x+1$, $q = 3x^2$.
Dann ist $p \cdot q =$ _____.
In $\mathbb{R}[X]$ ist $\deg(p \cdot q) =$ ____
In $\mathbb{Z}_6[X]$ ist $\deg(p \cdot q) =$ ____.

1.15 Prop: (Gradformel)

Für alle $p, q \in K[X]$ gilt:

(a) $\deg(p \cdot q) = \deg(p) + \deg(q)$

(b) $\deg(p+q) \leq \max\{\deg p, \deg q\}$ und hierbei gilt Gleichheit, falls $\deg p \neq \deg q$ ist.

Beweis:

(a) Sei $p = 0$ oder $q = 0$. Dann ist

$$\deg(p \cdot q) = \deg(0) = -\infty = \deg(p) + \deg(q).$$

Sei also $p \neq 0$ und $q \neq 0$ mit $p = \sum_{i=0}^{n} a_i X^i$

$$q = \sum_{i=0}^{m} b_i X^i$$

mit $a_n \neq 0, b_m \neq 0$, also $\deg p = n$, $\deg q = m$.

Sei $p \cdot q = \left(\sum a_i X^i\right)\left(\sum b_i X^i\right) =: \sum c_k X^k$.

Dann ist $c_k = 0$ für alle $k \geq n+m$.

Der Koeff $c_{n+m} = a_n \cdot b_m \neq 0$ nach Lemma 1.11.

Also ist $\deg(p \cdot q) = n+m = \deg(p) + \deg(q)$.

(b) Übungsaufgabe.

Übung: Zeigen Sie $K[X]^\times = K^\times (\subsetneq K \setminus \{0\})$, wobei Elemente aus K hierbei mit der entsprechenden konstanten Funktion identifiziert werden.

1.16 Korollar: Seien $p, q, r \in K[X]$.

(a) Ist $pq = 0$, so ist $p = 0$ oder $q = 0$,
dh. $K[X]$ ist Nullteiler-frei, dh. $K[X]$ IB

(b) Ist $pq = pr$ und $p \neq 0$, so ist $q = r$.
d.h. Kürzungsregel gilt.

Beweis:

(a) Ist $p \neq 0$, $q \neq 0$, so ist $\deg(p \cdot q) \overset{1.15}{=} \deg p + \deg q \geq 0$.
Also ist $pq \neq 0$.

(b) Ist $pq = pr$ mit $p \neq 0$, so ist $p(q-r) = 0$.
Da $p \neq 0$ nach Voraussetzung
$\overset{(a)}{\Longrightarrow}$ $q - r = 0$, also $q = r$.

1.17 Thm (Division mit Rest für Polynome)
Sei K ein Körper. Im Polynomring $K[X]$ gilt
Division mit Rest bezüglich der Gradfunktion:
Zu $f, g \in K[X]$, $g \neq 0$, existieren $q, r \in K[X]$

mit $$f = q \cdot g + r$$

mit $\deg(r) < \deg(g)$.
Die Polynome q, r sind hierbei eindeutig
durch f und g bestimmt.

Beweis:

(a) Existenz: Wir machen Induktion nach $\deg(f) =: n$.
Ist $\deg(f) < \deg(g)$, wähle $q = 0$ und $r = f$,
und die Behauptung folgt.
Sei nun $\deg(f) \geq \deg(g)$. Sei $f = \sum_{i=0}^{n} a_i X^i$
$g = \sum_{j=0}^{m} b_j X^j$.

Setze $f_1 := f - a_n b_m^{-1} X^{n-m} \cdot g$
Dann ist $\deg(f_1) < \deg(f)$.
Nach Induktionsvoraussetzung ex. also $q_1, r_1 \in K[X]$
mit $f_1 = q_1 g + r_1$ und $\deg(r_1) < \deg(g) = m$.
Es folgt:

$$f = f_1 + a_n b_m^{-1} X^{n-m} g = (q_1 \cdot g + r_1) + a_n b_m^{-1} X^{n-m} g$$

$$= \underbrace{(q_1 + a_n b_m^{-1} X^{n-m})}_{=:q} g + r_1$$

mit $\deg(r_1) < m = \deg(g)$.

(b) Eindeutigkeit: Ang. $q \cdot g + r = \tilde{q} \cdot g + \tilde{r}$ mit
$\deg(r), \deg(\tilde{r}) < m = \deg(g)$.

$\Rightarrow (q - \tilde{q}) g = \tilde{r} - r$.

$\overset{1.15}{\Rightarrow}$ $m = \deg(g) > \deg(r - \tilde{r}) = \deg((q - \tilde{q}) \cdot g)$

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

$\Rightarrow \deg(q - \tilde{q}) < 0$, d.h. $q - \tilde{q} = 0$, also $q = \tilde{q}$.
Einsetzen ergibt auch $r = \tilde{r}$.

1.17 Bem: Der Beweis von Thm 1.16 liefert einen Algorithmus zur Bestimmung von q und r:

Solange $\deg(f) \geq \deg(g)$ ist:

- Bestimme $c_{n-m} := a_n b_m^{-1}$ aus Leitkoeff a_n bzw b_m von f bzw g, und notiere den Summanden $c_{n-m} X^{n-m}$.
- Starte erneut mit f_1 ~~statt~~ f wobei $f_1 = f - c_{n-m} X^{n-m} g$.

Wenn $\deg(f) < \deg(g)$ ist:

- Dann ist $r = f$ und q die Summe der notierten Summanden.

Der Algorithmus endet dann.

1.18 Bsp: Der Algorithmus für $f = 2X^4+1$, $g = X^2+1$ liefert:

(a) Sei $f = 2X^4+1$, $g = X^2+1$. Dann ist

- $c_{4-2} = c_2 = 2 \cdot 1^{-1} = 2$. Notiere $2X^2$.
- $f_1 = f - c_2 X^2 g = 2X^4+1 - 2(X^4+X^2)$
  $= -2X^2+1$.

(b) Sei $f = -2X^2+1$, $g = X^2+1$. Es ist

-
-

(c) Sei $f = 3$, $g = X^2+1$. Es ist $\deg f < \deg g$. Dann ist $r = 3$ und $q = 2X^2-2$.

Also $f = 2X^4+1 = (2X^2-2) \cdot g + 3$.

Die Kurznotation für diesen Algorithmus in der Schule ist

$$2X^4+1 = (X^2+1)(2X^2-2X^0)+3$$
$$-(2X^4+2X^2)$$
$$-2X^2+1$$
$$-(-2X^2-2)$$
$$3$$

Übung: Rechnen Sie in $\mathbb{Z}_3[X]$:

$$X^5+X^4+X^3+2X^2+X-1 = (2X^2+1)(\quad\quad)+\quad\quad$$