Für die Anwendungen von Polynomen in Linearer Algebra müssen wir Nullstellen von Polynomen verstehen.

1.19 **Def:** Eine Nullstelle (NS) von $p \in K[X]$ ist ein Element $a \in K$ mit $p(a) = 0$.

1.20 **Bsp:**

(a) Sei $p = X^2 + 1$. Für alle $a \in \mathbb{R}$ gilt $a^2 + 1 > 0$.
Also hat p keine NS als Polynom in $\mathbb{R}[X]$.
Als Polynom in $\mathbb{C}[X]$ gilt $p = (X+i)(X-i)$.
Damit ist i und $-i$ jeweils NS von $p \in \mathbb{C}[X]$.
Sei $z \in \mathbb{C} \setminus \{\pm i\}$. Dann ist $z + i \neq 0$, $z - i \neq 0$.
Nach Lemma 1.11 ist damit $p(z) = (z+i)(z-i) \neq 0$.
Also sind $\pm i$ die einzigen NS von $p \in \mathbb{C}[X]$.

(b) Sei $f = X^2 - 7X + 12$. In $\mathbb{R}[X]$ faktorisiert das Polynom f durch:

$f =$ __________

Analog wie in (a) folgt: Polynom $f \in \mathbb{R}[X]$ hat die NS: $a_1 =$ ______ $a_2 =$ ______

(c) Sei $h = X^4 - 7X^2 + 12$.
In $\mathbb{R}[X]$ hat h die NS: __________
Es gibt also vier verschiedene Nullstellen.
In $\mathbb{Q}[X]$ hat h ~~genau~~ ______ Nullstellen.

1.21 Prop: Sei K Körper und $p \in K[X]$.
Es sind äquivalent:
(a) Element $a \in K$ ist NS von p dh. $p(a) = 0$
(b) $X-a$ ist ein Faktor von p, dh. es ex $q \in K[X]$ mit $p = (X-a) \cdot q$.

Beweis:
"(b) ⟹ (a)": Einsetzen von a liefert:
$$p(a) = ((X-a) \cdot q)(a) = \_\_\_\_\_\_\_\_$$

"(a) ⟹ (b)": Sei $a \in K$ NS von $p \in K[X]$.
Nach Thm 1.17 ex $q, r \in K[X]$ mit $p = (X-a) \cdot q + r$, wobei $\deg(r) < \deg(X-a) = 1$ ist.
⟹ r ist konstante Polynom mit
$$r(a) = (p - (X-a) \cdot q)(a)$$
$$= p(a) - \underbrace{(a-a)}_{=0} \cdot q(a) = p(a) \overset{\text{Vor.}}{=} 0.$$

Also ist $p = (X-a) \cdot q$.

1.22 Bsp: Sei $g = X^3 - 6X^2 + 5X + 12 \in \mathbb{R}[X]$.
Durch Raten / Einsetzen kleiner Werte findet man die NS $a_1 =$
Polynomdivision liefert
$$X^3 - 6X^2 + 5X + 12 = (X - \quad) \cdot (\qquad\qquad)$$

Also hat g die drei Nullstellen: ________

1.23 <u>Thm</u>: Sei $0 \neq p \in K[X]$. Dann gilt:

(a) Das Polynom p hat eine Darstellung

$$p = (X-a_1)^{n_1} \cdot \ldots \cdot (X-a_r)^{n_r} \cdot q \qquad (*)$$

mit $r \in \mathbb{N}_0$ und paarweise verschiedenen $a_1, -, a_r \in K$, sowie Exponenten $n_1, \ldots, n_r \in \mathbb{N}$ und einem Polynom $q \in K[X]$ ohne Nullstelle.

(b) Die Nullstellen von p sind genau $a_1, \ldots, a_r$.

(c) Darstellung $(*)$ von p ist eindeutig bis auf Permutation der Faktoren.

<u>Bem</u>: Wir nennen den Exponenten n_i die <u>Vielfachheit</u> der Nullstelle a_i.

<u>Beweis</u>:

(a) Wir machen Induktion nach $\deg(p)$

(i) Hat p keine Nullstelle, so ist $r=0$ und $q=p$. Dies gilt zum Beispiel für Polynome vom Grad Null, und liefert damit den Induktionsanfang.

(ii) Wir nehmen an, die Behauptung gilt für Polynome vom Grad $< \deg(p)$ und p habe eine Nullstelle $a \in K$. Nach Prop 1.21 existiert $\tilde{p} \in K[X]$ mit $p = (X-a)\tilde{p}$. Nach Prop 1.15 folgt:

$$\deg(\tilde{p}) = \deg(p) - \deg(X-a)$$
$$= \deg(p) - 1 \lneq \deg(p).$$

Nach Ind. Vor. hat dann $\tilde{p}$ eine Darstellung wie in $(*)$. Die Darstellung von p ergibt sich hieraus durch Multiplikation mit $(X-a)$

(b) Sei $b \in K$ mit $p(b) = 0$. So folgt:

$$0 = p(b) \overset{(*)}{=} (b-a_1)^{n_1} \cdot \ldots \cdot (b-a_r)^{n_r} q(b).$$

Nach Lemma 1.11 ist einer der Faktoren Null. Da q keine Nullstelle hat (nach Voraussetzung), existiert $1 \leq i \leq r$ mit $b = a_i$. Umgekehrt ist nach 1.21 jedes a_i, $1 \leq i \leq r$, eine Nullstelle.

(c) Wir machen Induktion nach $\deg(p)$.

(i) Angenommen $p \in K[X]$ hat keine Nullstelle in K. Dann ist $q = p$ in $(*)$ und $r = 0$ (andernfalls wäre $a_1 \in K$ eine NS von p ↯). Also ist die Darstellung in $(*)$ eindeutig in diesem Fall. Dies gilt zum Beispiel für Polynome vom Grad Null, und liefert also den Ind. Anfang.

(ii) Sei $p \in K[X]$ mit mindestens einer Nullstelle. Seien $\prod_{i=0}^{r} (X-a_i)^{n_i} q = p = \prod_{i=0}^{s} (X-b_i)^{m_i} u$ zwei Darstellungen von p. Da p nach Vor. eine NS hat, ist $r \geq 1$. Nach Voraussetzung hat u keine NS, also ist $u(a_1) \neq 0$. Also ist $0 = p(a_1) = \prod_{i=0}^{s} (a_1 - b_i) \underbrace{u(a_1)}_{\neq 0}$

$\overset{1.11}{\Rightarrow}$ $0 = \prod_{i=0}^{s} (a_1 - b_i)$, und es ex $1 \leq i \leq s$ mit $a_1 = b_i$.

Nach Anwendung einer Permutation der Faktoren, sei o. E. $a_1 = b_1$. Nach 1.16 dürfen wir kürzen (um den Faktor $(X-a_1)$), und erhalten

$$(X-a_1)^{n_1-1} \cdot \ldots \cdot (X-a_r)^{n_r} q = (X-b_1)^{m_1-1} \cdot \ldots \cdot (X-b_s)^{m_s} u, \quad (**)$$

ein Polynom vom Grad $\deg(p)-1$. ~~Nach~~ Ind. Vorauss. folgt (bis auf Permutation der Faktoren) die Eindeutigkeit für die Darst. $(**)$, und damit auch für die Darst. von p.

1.24 Korollar: Sei $0 \neq p \in K[X]$.

(a) Polynom p hat höchstens $\deg(p)$ viele paarweise verschiedene NS.

(b) Polynom p hat höchstens $\deg(p)$ viele NS, wenn man diese mit ihrer Vielfachheit zählt.

Beweis: Benutze Notation aus Thm 1.23.

(a) Nach ~~Prop~~ 1.23 hat p genau r paarweise verschiedene NS mit

$$\deg(p) \underset{(*)}{\overset{1.15}{=}} \deg(q) + \sum_{i=1}^{r} n_i \geq 0 + \sum_{j=1}^{r} 1 = r.$$

(b) Nach Prop 1.15 und Thm 1.23 hat p genau $\sum_{i=1}^{r} n_i$ viele NS, mit Vielfachheit gezählt, wobei

$$\sum_{i=1}^{r} n_i \underset{(q\neq 0)}{\leq} \deg(q) + \sum_{i=1}^{r} n_i \underset{(*)}{\overset{1.15}{=}} \deg(p).$$

1.25 Bsp: Sei $p = X^2+1$. Siehe auch Bsp 1.20(a).

(a) In $\mathbb{C}[X]$ hat $p = (X+i)(X-i)$ zwei verschiedene NS, nämlich i und $-i$, beide mit Vielfachheit Eins.

(b) In $\mathbb{R}[X]$ hat p keine NS.

(c) In $\mathbb{Z}_5[X]$ ist $X^2+1 = (X-2)(X+2)$ mit $+2 = -3$ in $\mathbb{Z}_5$. Also hat p die NS 2 und 3, jeweils mit Vielfachheit Eins.

(d) In $\mathbb{Z}_2[X]$ ist $X^2+1 =$ ________
In diesem Fall hat p genau die NS: ______;
die Vielfachheit ist ______.

1.26 **Def:** Ein Polynom $0 \neq f \in K[X]$ heißt <u>unzerlegbar</u> oder <u>irreduzibel</u>, falls f nicht konstant ist wenn $f = g \cdot h$ ist für $g, h \in K[X]$, dann ist entweder g konstant oder h konstant.

1.27 **Bem/Bsp:**

(a) Irreduzible Polynome in $K[X]$ sind das Analogon zu Primzahlen in $\mathbb{Z}$. Die Primfaktorzerlegung in $\mathbb{Z}$ ist eindeutig bis auf Reihenfolge und Einheiten, dh. bis auf ein Vorzeichen. Die Primfaktorzerlegung in $K[X]$, also die Faktorisierung von $f \in K[X]$ als Produkt irreduzibler Polynome ist ebenfalls eindeutig, bis auf Reihenfolge und Einheiten in $K[X]$, dh. bis auf konstante Faktoren. Bewiesen wird dies in der Algebravorlesung.

(b) Sei $f = X^2 + 1 \in \mathbb{Z}_3[X]$. Angenommen $f = g \cdot h$ mit $g, h \in K[X] \setminus K[X]^*$ mit $K[X]^* = K$. Nach 1.15 ist $2 = \deg f = \deg(gh) = \deg g + \deg h$. Da g, h nicht konstant, ist $\deg g = \deg h = 1$.

$\overset{1.21}{\Rightarrow}$ f hat eine Nullstelle in $\mathbb{Z}_3[X]$.

Es ist aber $f(0) = 1$, $f(1) = 2$, $f(2) = 2^2 + 1 = 5 = 2$. ↯

Also ist f irreduzibel in $\mathbb{Z}_3[X]$.

(c) Die irreduziblen Polynome $f \in \mathbb{Z}_3[X]$ mit f normiert und $\deg f = 2$ sind:

Ein Polynom $f \in \mathbb{Z}_3[X]$ mit $\deg(f) = 4$ und f hat keine Nullstelle in $\mathbb{Z}_3$, ist aber dennoch nicht irreduzibel ist zum Beispiel das Polynom $f =$

(d) Sei $f \in K[X]$ mit $\deg f \in \{2, 3\}$.
Dann ist f irreduzibel, genau dann wenn f keine Nullstelle hat.

Beweis:

1.28 Thm: (Fundamentalsatz der Algebra)
Jedes Polynom in $\mathbb{C}[X]$ vom Grad mindestens Eins hat mindestens eine Nullstelle in $\mathbb{C}$.

Beweis: Funktionentheorie- oder Topologievorlesung (oder Algebravorlesung)

1.29 Korollar: Ein Polynom $p \in \mathbb{C}[X]$ hat genau $\deg(p)$ viele NS in $\mathbb{C}$, mit Vielfachheiten gezählt, d.h. p zerfällt über $\mathbb{C}$ vollständig in Linearfaktoren:

$$p = c \cdot \prod_{i=1}^{\deg p} (X - a_i), \quad a_i \in \mathbb{C}, \; c \in \mathbb{C}.$$
(nicht notw. verschieden)

Beweis: Folgt aus Thm 1.28 und mit Induktion.
Die Details sind:

Übung: Sei $f \in \mathbb{C}[X]$ und seien alle Koeffizienten von f aus $\mathbb{R}$.

(a) Zeigen Sie: Ist $z \in \mathbb{C}$ Nullstelle von f, dann ist auch $\bar{z} \in \mathbb{C}$ Nullstelle von f.

(b) Folgern Sie, daß die unzerlegbaren Elemente in $\mathbb{R}[X]$ entweder lineare Polynome (mit Koeff in $\mathbb{R}$) sind oder quadratische Polynome für $\mathbb{R}[X]$ sind (also $\deg = 2$) mit negativer Diskriminante $D = b^2 - 4ac$, wobei $f = aX^2 + bX + c$ ist.

Allgemeiner definiert man:

Def: Ein Körper $\bar{K}$ heißt <u>algebraisch abgeschlossen</u>, falls jedes nicht-konstante Polynom in $\bar{K}[X]$ eine Nullstelle in $\bar{K}$ hat.

Bsp: Nach Thm 1.28 ist $\mathbb{C}$ algebraisch abgeschlossen.

Bem: In der Algebra-Vorlesung können Sie lernen, daß es zu jedem Körper K einen Körper $\bar{K}$ gibt mit $K \leq \bar{K}$ Teilkörper (also Teilring) mit $\bar{K}$ ist algebraisch abgeschlossen. Gilt zusätzlich, daß es keinen (algebr. abg.) Körper L gibt mit $K \subsetneq L \subsetneq \bar{K}$, dann heißt $\bar{K}$ <u>algebraischer Abschluß</u> von K. Die Standardnotation für den algebraischen Abschluß von K ist $\bar{K}$. Beispielsweise ist $\bar{\mathbb{R}} = \mathbb{C}$. Man kann zeigen, daß jeder Körper einen algebraischen Abschluß hat, und daß dieser in einem gewissen Sinne (bis auf K-Isomorphie) eindeutig ist.

Übung: Sei K algebraisch abgeschlossen. Dann hat K unendlich viele Elemente.

Beweis: Angenommen $K = \{a_1, \ldots, a_n\}$ endlich. Definiere Polynom f in $K[X]$ als $f :=$

$\Rightarrow$