Mathematik I WiSe 2010/2011 – Lösung Blatt 4

4.2. Für $p=2$:

In $\mathbb{R}$ gilt: $(a+b)^2 = a^2 + 2ab + b^2$.

In $\mathbb{Z}/2\mathbb{Z}$ gilt entsprechend: $(a+b)^2 = a^2 + \underbrace{[2]}_{=[0]} ab + b^2 = a^2 + b^2$.

Für $p=3$:

In $\mathbb{R}$ gilt $(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$.

In $\mathbb{Z}/3\mathbb{Z}$ gilt entsprechend:

$$(a+b)^3 = a^3 + \underbrace{[3]}_{=[0]} a^2b + \underbrace{[3]}_{=[0]} ab^2 + b^3 = a^3 + b^3.$$

Für $p=5$:

In $\mathbb{R}$ gilt: $(a+b)^5 = a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5$

In $\mathbb{Z}/5\mathbb{Z}$ gilt entsprechend:

$$(a+b)^5 = a^5 + \underbrace{[5]}_{=[0]} a^4b + \underbrace{[10]}_{=[0]} a^3b^2 + \underbrace{[10]}_{=[0]} a^2b^3 + \underbrace{[5]}_{=[0]} ab^4 + b^5$$
$$= a^5 + b^5.$$

Wir bemerken: In diesen Beispielen sind die Koeffizienten vor den „gemischten" Termen $a^k b^{p-k}$, $1 \le k \le p-1$, stets durch p teilbar und liefern somit in $\mathbb{Z}/p\mathbb{Z}$ keinen Beitrag.

Vermutung: Das gilt immer!

⟹ Behauptung: Ist p prim, so gilt im Körper $\mathbb{Z}/p\mathbb{Z}$:

$$\forall a, b \in \mathbb{Z}/p\mathbb{Z}: \quad (a+b)^p = a^p + b^p.$$

1. Schritt: Allgemeine binomische Formel:

Für $n \in \mathbb{N}$, $0 \leq k \leq n$ setze

$$\binom{n}{k} := \frac{n!}{k!\,(n-k)!} = \frac{n(n-1)\cdots(n-k+1)}{1 \cdot 2 \cdot \ldots \cdot k}.$$

Dann gilt für $1 \leq k \leq n$:

$$\binom{n}{k-1} + \binom{n}{k} = \frac{n!}{(k-1)!\,(n-k+1)!} + \frac{n!}{k!\,(n-k)!}$$

$$= \frac{n!\,(k + (n-k+1))}{k!\,(n-k+1)!} = \frac{(n+1)!}{k!\,((n+1)-k)!} = \binom{n+1}{k}.$$

(vgl. „Pascalsches Dreieck"!)

Behauptung: Für alle $a, b \in \mathbb{R}$, $n \in \mathbb{N}$ gilt:

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

Beweis: Induktion nach n:

Sei $I := \left\{ n \in \mathbb{N} \mid \forall a, b \in \mathbb{R}: (a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} \right\}$.

Induktionsanfang: $0 \in I$:

$$(a+b)^0 = 1 = \binom{0}{0} a^0 b^{0-0} = \sum_{k=0}^{0} \binom{0}{k} a^k b^{0-k} \Rightarrow 0 \in I.$$

Induktionsschritt: $n \in I \Rightarrow n+1 \in I$:

$$(a+b)^{n+1} = (a+b)(a+b)^n \underset{n \in I}{=} (a+b) \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

$$\underset{\text{ausmultiplizieren}}{=} \sum_{k=0}^{n} \binom{n}{k} a^{k+1} b^{n-k} + \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k+1}$$

$$= \sum_{k=1}^{n+1} \binom{n}{k-1} a^k \underbrace{b^{n-(k-1)}}_{= b^{(n+1)-k}} + \sum_{k=0}^{n} \binom{n}{k} a^k \underbrace{b^{n-k+1}}_{= b^{(n+1)-k}}$$

↑ Indexverschiebung: $k \to k-1$

$$= a^{n+1} + \sum_{k=1}^{n} \underbrace{\left(\binom{n}{k-1} + \binom{n}{k} \right)}_{\overset{\text{s.o.}}{=} \binom{n+1}{k}} a^k b^{(n+1)-k} + b^{n+1}$$

↑ Zusammenfassen

$$= \sum_{k=0}^{n+1} \binom{n+1}{k} a^k b^{(n+1)-k} \Rightarrow n+1 \in I.$$

↑ Zusammenfassen

Nach dem Induktionsprinzip ist $I = \mathbb{N}$, woraus die Behauptung folgt.

<u>2. Schritt:</u> Sei p prim und seien $a, b \in \mathbb{Z}/p\mathbb{Z}$ beliebig.

Dann sind $a = [\alpha]$, $b = [\beta]$, $\alpha, \beta \in \{0, \dots, p-1\}$, und es gilt:

$$(a+b)^p = \left([\alpha] + [\beta]\right)^p = \left[(\alpha+\beta)^p\right]$$

$$= \left[\sum_{k=0}^{p} \binom{p}{k} \alpha^k \beta^{p-k} \right] = \sum_{k=0}^{p} \left[\binom{p}{k}\right] [\alpha]^k [\beta]^{p-k}$$

↑ 1 Schritt

$$= \sum_{k=0}^{p} \left[\binom{p}{k}\right] a^k b^{p-k}.$$

Für $k \in \{1, \dots, p-1\}$ gilt:

Der Faktor p kommt in der Primfaktorzerlegung von $p!$ vor, nicht aber in der von $k!\,(p-k)!$

$\Rightarrow \binom{p}{k} = \frac{p!}{k!\,(p-k)!}$ ist durch p teilbar

$\Rightarrow \left[\binom{p}{k}\right] = [0]$ in $\mathbb{Z}/p\mathbb{Z}$.

Es folgt:

$$(a+b)^p = \sum_{k=0}^{p} \underbrace{\left[\binom{p}{k}\right]}_{= [0] \text{ außer für } k=0,\ k=p} a^k b^{p-k} = a^p + b^p$$

Bemerkung: Die Aussage

$$\forall a, b \in K: (a+b)^p = a^p + b^p$$

gilt nicht nur im Körper $K = \mathbb{Z}/p\mathbb{Z}$, p prim, sondern allgemeiner in jedem Körper K, in dem gilt:

$$\underbrace{1 + \dots + 1}_{p\text{-mal},\ p \text{ prim}} = 0$$

(Man sagt: „K hat die Charakteristik p.")

4.3. Über $\mathbb{Z}/3\mathbb{Z}$:

Sei $A = \begin{pmatrix} [2] & [0] & [1] \\ [2] & [1] & [2] \end{pmatrix} = \begin{pmatrix} [0] & [0] & [1] \\ [2] & [1] & [2] \end{pmatrix} \in \left(\mathbb{Z}/3\mathbb{Z}\right)^{2\times 3}$.

ges.: $\mathbb{L}_A = \left\{ x \in \left(\mathbb{Z}/3\mathbb{Z}\right)^3 \mid A \cdot x = 0 \right\}$.

Vorgehen wie im Beweis des Fundamentallemmas:

Schreibe $A = (a_{ij})_{\substack{i=1,2 \\ j=1,2,3}}$. Dann ist $a_{11} = [0]$

$\rightsquigarrow$ Vertausche die Zeilen von A:

$$\mathbb{L}_A = \mathbb{L}_{A^{(1)}} \text{ mit } A^{(1)} := (a_{ij}^{(1)})_{\substack{i=1,2 \\ j=1,2,3}} := \begin{pmatrix} [2] & [1] & [2] \\ [0] & [0] & [1] \end{pmatrix}.$$

Betrachte die Matrix

$$A^{(2)} := (a_{ij}^{(1)})_{\substack{i=2 \\ j=2,3}} = \left([0], [1]\right) \in \left(\mathbb{Z}/3\mathbb{Z}\right)^{1\times 2}$$

$$\Rightarrow \mathbb{L}_{A^{(2)}} = \left\{ (\lambda, [0]) \mid \lambda \in \mathbb{Z}/3\mathbb{Z} \right\} \subset \left(\mathbb{Z}/3\mathbb{Z}\right)^2.$$

Damit folgt:

$$\mathbb{L}_{A^{(1)}} = \left\{ (\mu, \lambda, [0]) \mid \mu, \lambda \in \mathbb{Z}/3\mathbb{Z},\ A^{(1)} (\mu, \lambda, [0]) = 0 \right\}.$$

Für $\mu, \lambda \in \mathbb{Z}/3\mathbb{Z}$ gilt:

$$A^{(1)} (\mu, \lambda, [0]) = 0 \iff [2]\mu + \lambda = [0]$$

$$\iff \mu = -[2]^{-1}\lambda = -[2]\lambda = \lambda.$$

Wir erhalten:

$$\mathbb{L}_A = \mathbb{L}_{A^{(1)}} = \left\{ (\lambda, \lambda, [0]) \mid \lambda \in \mathbb{Z}/3\mathbb{Z} \right\}$$

$$= \left\{ ([0], [0], [0]),\ ([1], [1], [0]),\ ([2], [2], [0]) \right\}.$$

Über $\mathbb{Z}/5\mathbb{Z}$:

Sei $A = \begin{pmatrix} [2] & [0] & [1] \\ [2] & [1] & [2] \end{pmatrix} \in (\mathbb{Z}/5\mathbb{Z})^{2\times 3}$.

ges.: $\mathbb{L}_A = \left\{ x \in (\mathbb{Z}/5\mathbb{Z})^3 \mid A \cdot x = 0 \right\}$.

Vorgehen wie im Beweis des Fundamentallemmas:

Schreibe $A = (a_{ij})_{\substack{i=1,2 \\ j=1,2,3}}$. Dann ist $a_{11} = [3] \neq [0]$

$\rightsquigarrow$ Addiere das $(-[2]\cdot[3]^{-1}) = [1]$ - fache der ersten Zur zweiten Zeile von A:

$$\mathbb{L}_A = \mathbb{L}_{A^{(1)}} \quad \text{mit} \quad A^{(1)} := (a_{ij}^{(1)})_{\substack{i=1,2 \\ j=1,2,3}} := \begin{pmatrix} [3] & [0] & [1] \\ [0] & [1] & [3] \end{pmatrix}.$$

Betrachte die Matrix

$$A^{(2)} := (a_{ij}^{(1)})_{\substack{i=2 \\ j=2,3}} = ([1], [3]) \in (\mathbb{Z}/5\mathbb{Z})^{1\times 2}$$

$$\Rightarrow \mathbb{L}_{A^{(2)}} = \left\{ (\lambda\cdot[2], \lambda) \mid \lambda \in \mathbb{Z}/5\mathbb{Z} \right\} \subset (\mathbb{Z}/5\mathbb{Z})^2.$$

Damit folgt:

$$\mathbb{L}_{A^{(1)}} = \left\{ (\mu, \lambda\cdot[2], \lambda) \mid \mu, \lambda \in \mathbb{Z}/5\mathbb{Z},\ A^{(1)}\cdot(\mu, \lambda\cdot[2], \lambda) = 0 \right\}.$$

Für $\mu, \lambda \in \mathbb{Z}/5\mathbb{Z}$ gilt:

$$A^{(1)}(\mu, \lambda\cdot[2], \lambda) = 0 \iff [3]\mu + \lambda = [0]$$

$$\iff \mu = -[3]^{-1}\lambda = -[2]\lambda = [3]\lambda.$$

Wir erhalten:

$$\mathbb{L}_A = \mathbb{L}_{A^{(1)}} = \left\{ ([3]\lambda, [2]\lambda, \lambda) \mid \lambda \in \mathbb{Z}/5\mathbb{Z} \right\}$$

$$= \left\{ ([0],[0],[0]), ([3],[2],[1]), ([1],[4],[2]), ([4],[1],[3]), ([2],[3],[4]) \right\}.$$

4.4. Sei $\mathbb{F}$ Körper, $0 \neq A = (a_1, \dots, a_n) \in \mathbb{F}^{1\times n}$.

Beh.: $\exists$ $n-1$ linear unabhängige $x \in \mathbb{F}^n$ mit $A \cdot x = 0$

Beweis: $A \neq 0 \Rightarrow \exists i \in \{1, \dots, n\} : a_i \neq 0$.

Für $j \in \{1, \dots, n\} \setminus \{i\}$ setze

$$x^{(j)} := (x_1^{(j)}, \dots, x_n^{(j)}) \in \mathbb{F}^n$$

mit

$$x_k^{(j)} := \begin{cases} -a_j & , \text{ falls } k = i, \\ a_i & , \text{ falls } k = j, \\ 0 & , \text{ sonst.} \end{cases}$$

Dann gilt:

- Für alle $j \in \{1, \dots, n\} \setminus \{i\}$:

$$A \cdot x^{(j)} = \sum_{k=1}^{n} a_k \underbrace{x_k^{(j)}}_{=0 \text{ für } k \neq \{i,j\}} = a_i x_i^{(j)} + a_j x_j^{(j)}$$

$$= -a_i a_j + a_j a_i = 0.$$

- Die $x^{(j)}$, $j \in \{1, \dots, n\} \setminus \{i\}$ sind linear unabhängig, denn:
Seien λ_j, $j \in \{1, \dots, n\} \setminus \{i\}$, aus $\mathbb{F}$ gegeben mit

$$\sum_{j \neq i} \lambda_j x^{(j)} = 0.$$

In der k-ten Koordinate, $k \in \{1, \dots, n\} \setminus \{i\}$, erhält man:

$$0 = \sum_{j \neq i} \lambda_j \underbrace{x_k^{(j)}}_{=0 \text{ für } j \neq k} = \lambda_k x_k^{(k)} = \lambda_k \underbrace{a_i}_{\neq 0} \Rightarrow \lambda_k = 0$$

Also sind die $x^{(j)}$ linear unabhängig. Insbesondere sind es tatsächlich $n-1$ Vektoren.