31. Es sei $P[x]$ die Menge aller Polynome $\sum_{i=0}^{N} a_i x^i$, $N \in \mathbb{N}_0$, $a_i \in \mathbb{Z}$, $a_N \neq 0$ für $N > 0$, sowie $P_+[x]$ die Menge aller Polynome $\sum_{i=0}^{N} a_i x^i$ mit $a_N > 0$. Auf $P[x] \times P_+[x]$ sei die Relation $\sim$ durch

$$(p, q) \sim (\hat{p}, \hat{q}) \quad \Leftrightarrow \quad p\hat{q} = \hat{p}q$$

definiert. Zeigen Sie, dass $\sim$ eine Äquivalenzrelation ist.

Beweis: Reflexivität: $(p,q) \sim (p,q) \Leftrightarrow pq = pq$

Symmetrie: $(p,q) \sim (\hat{p},\hat{q}) \Leftrightarrow p\hat{q} = \hat{p}q \Leftrightarrow \hat{p}q = p\hat{q} \Leftrightarrow (\hat{p},\hat{q}) \sim (p,q)$

Transitivität: Seien $(p,q) \sim (\hat{p},\hat{q})$ und $(\hat{p},\hat{q}) \sim (\bar{p},\bar{q})$, also $p\hat{q} = \hat{p}q$ und $\hat{p}\bar{q} = \bar{p}\hat{q}$. Dann ist

$$p(\hat{p}\bar{q}) = p(\bar{p}\hat{q}) = p(\hat{q}\bar{p}) = (p\hat{q})\bar{p} = (\hat{p}q)\bar{p} = \hat{p}(q\bar{p}) = \hat{p}(\bar{p}q) \Leftrightarrow p\bar{q} = \bar{p}q$$

Weil beim ersten und letzten Term $\hat{p}$ gekürzt werden kann, folgt $p\bar{q} = \bar{p}q \Leftrightarrow (p,q) \sim (\bar{p},\bar{q})$.

32. Definieren Sie auf $P[x] \times P_+[x]$ eine Addition $^+$ und Multiplikation $\cdot$, die sich auf die Äquivalenzklassen $[(p,q)]_\sim$ übertragen lässt, sodass die Menge

$$\{[(p,q)]_\sim : (p,q) \in P[x] \times P_+[x]\}$$

mit diesen Operationen zu einem Körper K wird. Es reicht, wenn Sie die Aussage für die Addition beweisen, d.h. wenn Sie zeigen dass K mit der so definierten Addition auf K und einem Nullelement $0_K \in K$ eine Kommutative Gruppe ist.

Hinw.: $\mathbb{Q}$

Wir definieren die Addition auf $P[x] \times P_+[x]$ wie folgt:

$$+ : \begin{cases} (P[x] \times P_+[x])^2 \to P[x] \times P_+[x] \\ (p,q) + (\hat{p},\hat{q}) \mapsto (p\hat{q} + \hat{p}q,\ q\hat{q}) \end{cases}$$

Somit ist $(K, +)$ eine abel'sche Gruppe.

Beweis: Assoziativität: $((p,q) + (\hat{p},\hat{q})) + (\bar{p},\bar{q}) =$
$(p\hat{q} + \hat{p}q,\ q\hat{q}) + (\bar{p},\bar{q}) = ((p\hat{q} + \hat{p}q)\bar{q} + \bar{p}q\hat{q},\ q\hat{q}\bar{q}) =$
$(p\hat{q}\bar{q} + \hat{p}q\bar{q} + \bar{p}q\hat{q},\ q\hat{q}\bar{q}) = (p\hat{q}\bar{q} + (\hat{p}\bar{q} + \bar{p}\hat{q})q,\ q\hat{q}\bar{q}) =$
$(p,q) + (\hat{p}\bar{q} + \bar{p}\hat{p},\ \hat{q}\bar{q}) = (p,q) + ((\hat{p},\hat{q}) + (\bar{p},\bar{q}))$.

Neutrales Element: $(p,q) + (0,1) = (p \cdot 1 + 0 \cdot q,\ q \cdot 1)$
$= (p,q)$

Inverses Element: $(p,q) + (-p,q) = (pq - pq,\ qq) =$
$(0, qq) \sim (0,1)$, weil $0 \cdot 1 = 0 \cdot qq$

In sich geschlossen: $(p,q) + (\hat{p},\hat{q}) = (p\hat{q} + \hat{p}q, q\hat{q})$, wobei $p\hat{q} + \hat{p}q \in P[x]$ ($a_i \in \mathbb{Z}$, $a_N \neq 0$, weil bei $q, \hat{q}$ gilt $a_N > 0$ und somit $a_N \neq 0$) und $q\hat{q} \in P_+[x]$ ($a_N > 0$, weil bei $q, \hat{q}$ gilt $a_N > 0$ und somit $a_N^q \cdot a_N^{\hat{q}} = a_N^{q\hat{q}} > 0$).
Daher gilt $(p\hat{q} + \hat{p}q, q\hat{q}) \in P[x] \times P_+[x]$.

Kommutativität: $(p,q) + (\hat{p},\hat{q}) = (p\hat{q} + \hat{p}q, q\hat{q}) = (\hat{p}q + p\hat{q}, \hat{q}q)$
$= (\hat{p},\hat{q}) + (p,q)$.

Die Operation $+$ lässt sich auf Äquivalenzklassen übertragen, da $a+b$ nicht von den gewählten Repräsentanten (p,q) und $(\hat{p},\hat{q})$ abhängig ist.

$a + b := [(p,q) + (\hat{p},\hat{q})]_\sim$ mit $a = (p,q)$ und $b = (\hat{p},\hat{q})$.

Das liegt daran, dass wenn $(p,q) \sim (\hat{p},\hat{q})$ und $(r,s) \sim (\hat{r},\hat{s})$, also $p\hat{q} = \hat{p}q$ und $r\hat{s} = \hat{r}s$, dann $(p,q) + (r,s) \sim (\hat{p},\hat{q}) + (\hat{r},\hat{s})$.
Dazu zeigen wir vorerst $(p,q) + (r,s) \sim (\hat{p},\hat{q}) + (r,s)$:
$(p,q) + (r,s) = (ps + rq, qs)$ und —"— $= (\hat{p}s + r\hat{q}, \hat{q}s)$
und daher $(ps + rq)\hat{q}s = (\hat{p}s + r\hat{q})qs$, weil

$(ps + rq)\hat{q}s = ps\hat{q}s + rq\hat{q}s = 0 + ps\hat{q}s + rq\hat{q}s \overset{(p\hat{q} = \hat{p}q)}{=}$
$(\hat{p}q - p\hat{q})ss + ps\hat{q}s + rq\hat{q}s = \hat{p}qss - p\hat{q}ss + p\hat{q}ss + rq\hat{q}s =$
$\hat{p}qss + rq\hat{q}s = (\hat{p}s + r\hat{q})qs$

Analog kann $(\hat{p},\hat{q}) + (r,s) \sim (\hat{p},\hat{q}) + (\hat{r},\hat{s})$ gezeigt werden (Kommutativität gilt) und dann muss man sich lediglich noch der Transitivität befleißigen.

□

33. Sei $K_+ = \{[(p,q)]_\sim \in K : (p,q) \in P_+ \times P_+\}$. Zeigen Sie, dass damit eine Ordnung auf K wohldefiniert ist, mit der K zu einem angeordneten Körper wird, der nicht Archimedisch angeordnet ist.

Beweis: Es existiert eine Menge $\{0_K\} = \{[(0,1)]_\sim\} \subseteq K$, weil für $N = 0$ auch $a_N = 0$ möglich ist, also $0 \in P[x]$. $K_- = K \setminus (\{0_K\} \cup K_+\}$, also $K_- \dot\cup \{0_K\} \dot\cup K_+ = K$, wobei $\{0_K\} \cap K_+ = \emptyset$ durch die Voraussetzung von $P_+[x]$, also $a_N > 0$, folgt $(0 \notin P_+[x])$ und $K_- \cap (\{0_K\} \cup K_+) = \emptyset$ ist trivial. Daher sind alle Mengen disjunkt.
Für die Abgeschlossenheit von $+$ in K_+ betrachte man Beispiel 32. Diese gilt auch für $\cdot$. Seien dazu $p, \hat{p} \in P_+[x]$, dann ist $a_N > 0 < \hat{a}_N$, also $a_N \cdot \hat{a}_N > 0$ und somit $p \cdot \hat{p} \in P_+[x]$.
Der Körper ist nicht archimedisch angeordnet, weil (eine Bijektion von) $\mathbb{N} \subseteq K$ nach oben, durch $N \in \mathbb{N}_0$ (es wird ja festgelegt), beschränkt ist. $\square$

34. Für welche $n \in \mathbb{N}$ wird $\mathbb{Z}_n := \{0, 1, \dots, n-1\}$ mit Addition und Multiplikation modulo n zu einem Körper?

Hinw.: Zeigen Sie mit einem Schubfachargument, dass ein endlicher Integritätsbereich (nullteilerfreier kommutativer Ring mit Eins) ein Körper ist.

$\mathbb{Z}_n$ ist genau dann ein Körper, wenn n eine Primzahl ist.

Beweis: Wir wissen, dass $\forall n \in \mathbb{N} : \exists a, b \in \mathbb{N} : a \leq b \leq n \wedge a \cdot b = n$. Sollte n eine Primzahl sein, so ist eindeutig $a = 1$ (und $b = n$).

In dem Restkörper $\mathbb{Z}_n$ gilt also auch $a \cdot b = n$ und somit $\overline{a \cdot b} = \overline{n}$. Weil $\overline{n} = \overline{0}$ und $\overline{a \cdot b} = \overline{a} \cdot \overline{b}$, ist $\overline{a} \cdot \overline{b} = \overline{0}$. Ein Körper ist „nullteilerfrei", also ist $\overline{a} = \overline{0} \vee \overline{b} = \overline{0}$. Sei also $\overline{b} = \overline{0}$, dann auch $\overline{b} = \overline{n}$. Somit ist b ein Vielfaches von n, aber laut Voraussetzung auch $b \leq n$. Also ist $b = n$ und durch $a \cdot n = n$ auch $1 \leq n \leq n$ die Einzige Lösung für die obere Ungleichung: n ist eine Primzahl! $\square$

35. Zeigen Sie, dass kein endlicher Körper angeordnet werden kann.

Hinw.: Betrachten Sie $1, 1+1, 1+1+1, \dots$.

Beweis: Wir wissen, dass P endlich und somit ein $\sup P$ hat. Nun gilt aber

$$\sum_{n=1}^{\lfloor \sup P \rfloor} n/n \cdot 1_K + 1_K > \sup P$$

Wenn ein endlicher Körper wirklich angeordnet wäre, dann wäre P aber durch $+$ abgeschlossen. Dies widerspricht jedoch dem oberen Argument. $\square$

36. Bsp. 2.16 Man stelle eine Formel für ($n \in \mathbb{N}$)

$$p(n) := \sum_{k=1}^{n} (2k-1)^2 = 1^2 + 3^2 + \dots + (2n-1)^2$$

auf und beweise diese mittels vollständiger Induktion.

Hinweis: Setzen Sie unbestimmt $p(n) = an^3 + bn^2 + cn + d$ an, und ermitteln Sie die unbekannten Koeffizienten durch Einsetzen von $n = 1$, $n = 2$, usw..

Dazu werden 4 unabhängige Gleichungen benötigt:

$$\begin{aligned}
\mathrm{I}&: \; a \cdot 1^3 + b \cdot 1^2 + c \cdot 1 + d = 1^2 \\
\mathrm{II}&: \; a \cdot 2^3 + b \cdot 2^2 + c \cdot 2 + d = 1^2 + 3^2 \\
\mathrm{III}&: \; a \cdot 3^3 + b \cdot 3^2 + c \cdot 3 + d = 1^2 + 3^2 + 5^2 \\
\mathrm{IV}&: \; a \cdot 4^3 + b \cdot 4^2 + c \cdot 4 + d = 1^2 + 3^2 + 5^2 + 7^2
\end{aligned}$$

Wir schreiben sie zur besseren Übersicht in ein Raster:

$$\begin{array}{c|cccc|c}
\mathrm{I} & 1 & 1 & 1 & 1 & 1 \\
\mathrm{II} & 8 & 4 & 2 & 1 & 10 \\
\mathrm{III} & 27 & 9 & 3 & 1 & 35 \\
\mathrm{IV} & 64 & 16 & 4 & 1 & 84
\end{array}
\xrightarrow{\text{Gauß'scher Eliminations-Algoritmus}}
\begin{array}{c|cccc|c}
\mathrm{I} & 1 & 1 & 1 & 1 & 1 \\
\mathrm{II} & 0 & ? & ? & ? & ? \\
\mathrm{III} & 0 & 0 & ? & ? & ? \\
\mathrm{IV} & 0 & 0 & 0 & ? & ?
\end{array}$$

(1): $\mathrm{I} = \mathrm{I} \cdot 8$; $\mathrm{II} = \mathrm{II} - \mathrm{I}$;

$$\begin{array}{c|cccc|c}
\mathrm{I} & 8 & 8 & 8 & 8 & 8 \\
\mathrm{II} & 0 & -4 & -6 & -7 & 2 \\
\mathrm{III} & 27 & 9 & 3 & 1 & 35 \\
\mathrm{IV} & 64 & 16 & 4 & 1 & 84
\end{array}$$

(2): $I = I \cdot 27;\quad III = III \cdot 8;\quad III = III - I;$

$$\begin{array}{c|cccc|c}
I & 216 & 216 & 216 & 216 & 216 \\
II & 0 & -4 & 6 & 7 & 2 \\
III & 0 & -144 & -192 & -208 & 64 \\
IV & 64 & 16 & 4 & 1 & 84
\end{array}$$

(3): $I = I \cdot 64;\quad IV = IV \cdot 27;\quad IV = IV - I;$

$$\begin{array}{c|cccc|c}
I & 1728 & 1728 & 1728 & 1728 & 1728 \\
II & 0 & -4 & -6 & -7 & 2 \\
III & 0 & -144 & -192 & -208 & 64 \\
IV & 0 & -1296 & -1620 & -1701 & 540
\end{array}$$

(4): $II = II \cdot 36;\quad III = III - II;$

$$\begin{array}{c|cccc|c}
I & 1728 & 1728 & 1728 & 1728 & 1728 \\
II & 0 & -144 & -216 & -252 & 72 \\
III & 0 & 0 & 24 & 44 & -8 \\
IV & 0 & -1296 & -1620 & -1701 & 540
\end{array}$$

(5): $II = II \cdot 9;\quad IV = IV - II;$

$$\begin{array}{c|cccc|c}
I & 1728 & 1728 & 1728 & 1728 & 1728 \\
II & 0 & -1296 & -1944 & -2268 & 648 \\
III & 0 & 0 & 24 & 44 & -8 \\
IV & 0 & 0 & 324 & 567 & -108
\end{array}$$

(6): $III = III \cdot 27;\quad IV = IV \cdot 2;\quad IV = IV - III;$

$$
\begin{array}{c|cccc|c}
\mathrm{I} & 1728 & 1728 & 1728 & 1728 & 1728 \\
\mathrm{II} & 0 & -1296 & -1944 & -2268 & 648 \\
\mathrm{III} & 0 & 0 & 648 & 1188 & -216 \\
\mathrm{IV} & 0 & 0 & 0 & -54 & 0
\end{array}
$$

Jetzt erkennen wir, dass:

- $\underline{\mathrm{IV}}$: $-54 \cdot d = 0 \Rightarrow d = 0$
- $\underline{\mathrm{III}}$: $648 \cdot c + 1188 \cdot 0 = -216 \Rightarrow c = -1/3$
- $\underline{\mathrm{II}}$: $-1296 \cdot b - 1944 \cdot (-1/3) - 2268 \cdot 0 = 648$
  $\Rightarrow b = 0$
- I: $1728 \cdot a + 1728 \cdot 0 + 1728 \cdot (-1/3) + 1728 \cdot 0 =$
  $1728 \Rightarrow a = 4/3$

Es ist also davon auszugehen, dass die folgende Formel hinreichend ist:

$$p(n) = \sum_{k=1}^{n} (2k-1)^2 = \frac{4}{3} \cdot n^3 - \frac{1}{3} \cdot n$$

Beweis: IA: $(2 \cdot 1 - 1)^2 = \frac{4}{3} \cdot 1^3 - \frac{1}{3} \cdot 1$

IS: $\sum_{k=1}^{n+1} (2k-1)^2 = \sum_{k=1}^{n} (2k-1)^2 + (2(n+1)-1)^2 \overset{IV}{=}$

$\frac{4}{3} \cdot n^3 - \frac{1}{3} \cdot n + (2n+1)^2 \overset{(?)}{=} \frac{4}{3} \cdot (n+1)^3 - \frac{1}{3} \cdot (n+1) \Leftrightarrow$

$\frac{4}{3} \cdot n^3 - \frac{1}{3} \cdot n + 4n^2 + 4n + 1 = \frac{4}{3} \cdot (n^3 + 3n^2 + 3n + 1) - \frac{1}{3} n - \frac{1}{3} \Leftrightarrow$

$\frac{4}{3} \cdot n^3 - \frac{1}{3} n + 4n^2 + 4n + 1 = \frac{4}{3} \cdot n^3 + 4n^2 + 4n + \frac{4}{3} - \frac{1}{3} n - \frac{1}{3} \Leftrightarrow$

$0 = 0$ $\square$

37. Bsp. 2.17 Zeige mittels vollständiger Induktion, dass für $n \in \mathbb{N}$, $n \geq 2$,

$$\sum_{k=2}^{n} \frac{1}{k^2-1} = \frac{3}{4} - \frac{2n+1}{2n(n+1)} .$$

Beweis: IA: $\frac{1}{2^2-1} = \frac{3}{4} - \frac{2n+1}{2n(n+1)} \Leftrightarrow 1/3 = 1/3$

IS: $\sum_{k=2}^{n+1} \frac{1}{k^2-1} = \sum_{k=2}^{n} \frac{1}{k^2-1} + \frac{1}{(n+1)^2-1} \overset{IV}{=}$

$\frac{3}{4} - \frac{2n+1}{2n(n+1)} + \frac{1}{n^2+2n} = \frac{3}{4} - \frac{(2n+1)(n^2+2n) - 2n(n+1)}{2n(n+1)(n^2+2n)} =$

$\frac{3}{4} - \frac{2n^3+4n^2+n^2+2n-2n^2-2n}{2n^2(n+1)(n+2)} = \frac{3}{4} - \frac{2n^3+3n^2}{2n^2(n+1)(n+2)} =$

$\frac{3}{4} - \frac{2n+2+1}{2(n+1)(n+2)} = \frac{3}{4} - \frac{2(n+1)+1}{2(n+1)((n+1)+1)}$ $\square$

38. Bsp. 2.19 Zeige mittels vollständige Induktion, dass für $n \in \mathbb{N}$, $n \geq 2$,

$$\prod_{k=1}^{n} \left(1 + \frac{1}{n+k}\right) = 2 - \frac{1}{n+1}.$$

Beweis: IA: $\left(1 + \frac{1}{2+1}\right)\left(1 + \frac{1}{2+2}\right) = 2 - \frac{1}{2+1}$

$\Leftrightarrow 5/3 = 5/3$

IS: $\prod_{k=1}^{n+1} \left(1 + \frac{1}{(n+1)+k}\right) = \prod_{k=2}^{n+2} \left(1 + \frac{1}{n+k}\right) =$

$\prod_{k=2}^{n} \left(1 + \frac{1}{n+k}\right) \cdot \left(1 + \frac{1}{n+(n+1)}\right) \cdot \left(1 + \frac{1}{n+(n+2)}\right) \overset{(IV)}{=}$

$\left(2 - \frac{1}{n+1}\right) \cdot \left(\frac{1}{1 + 1/(n+1)}\right)\left(\frac{2n+2}{2n+1}\right)\left(\frac{2n+3}{2n+2}\right) =$

$\left(\frac{2(n+1)-1}{n+1}\right)\left(\frac{1}{\frac{n+2}{n+1}}\right)\left(\frac{2n+3}{2n+1}\right) =$

$(2n+1)\left(1/(n+2)\right)\left(\frac{2n+3}{2n+1}\right) = \frac{2n+4-1}{n+2} = \frac{2(n+2)-1}{n+2} =$

$\frac{2(n+2)}{n+2} - \frac{1}{n+2} = 2 - \frac{1}{(n+1)+1}$ $\square$

39. Bsp. 2.20 Zeige mittels vollständiger Induktion, dass für $n \in \mathbb{N}$, $n \geq 2$,

$$\prod_{k=2}^{n} \left(1 - \frac{2}{k(k+1)}\right) = \frac{1}{3}\left(1 + \frac{2}{n}\right).$$

Beweis: IA: $1 - \frac{2}{2(2+1)} = \frac{1}{3}\left(1 + \frac{2}{2}\right) \Leftrightarrow 2/3 = 2/3$

IS: $$\prod_{k=2}^{n+1} \left(1 - \frac{2}{k(k+1)}\right) = \prod_{k=2}^{n}\left(1 + \frac{2}{k(k+1)}\right)\left(1 - \frac{2}{(n+1)(n+2)}\right) \overset{IV}{=}$$

$$\frac{1}{3}\left(1 + \frac{2}{n}\right)\left(\frac{n^2+3n+2-2}{(n+1)(n+2)}\right) = \frac{1}{3}\left(\frac{n+2}{n}\right)\left(\frac{n^2+3n}{(n+1)(n+2)}\right) =$$

$$\frac{1}{3}\left(\frac{n+3}{n+1}\right) = \frac{1}{3}\left(\frac{2+(n+1)}{n+1}\right) = \frac{1}{3}\left(\frac{2}{n+1} + \frac{n+1}{n+1}\right) =$$

$$\frac{1}{3}\left(1 + \frac{2}{n+1}\right)$$

$\square$

40. Bsp 2.21 Zeige mittels vollständiger Induktion:

(a) $2^n > n$ für $n \in \mathbb{N}$ und $2^n > n^2$ für $n \in \mathbb{N}, n \geq 5$.

(b) Für ein beliebiges $x \geq 2$ aus einem angeordneter Körper, folgere man $x^n > n$ für $n \in \mathbb{N}$ und $x^n > n^2$ für alle $n \in \mathbb{N}, n \geq 5$.

Beweis: IA: $2^1 = 2 > 1$

IS: $2^{n+1} = 2^n \cdot 2 > n+1 \Leftrightarrow 2^n > n \geq \frac{n+1}{2} \Leftrightarrow$

IA: $1 \geq \frac{1+1}{2}$

IS: $n+1 \geq \frac{n+1+1}{2} = \frac{n+1}{2} + \frac{1}{2} \Leftrightarrow n \geq \frac{n+1}{2} - \frac{1}{2}$

Laut IV gilt diese Aussage erst recht.

IA: $2^5 > 5^2 \Leftrightarrow 32 > 25$

IS: $2^{n+1} > (n+1)^2 \Leftrightarrow 2^n \cdot 2 > n^2 + 2n + 1 \Leftrightarrow$

$2^n > n^2 \geq \frac{n^2+2n+1}{2}$

IA: $5^2 \geq \frac{5^2 + 2 \cdot 5 + 1}{2} \Leftrightarrow 25 \geq \frac{25+10+1}{2} = \frac{36}{2} = 18$

IS: $(n+1)^2 \geq \frac{(n+1)^2 + 2(n+1) + 1}{2} \Leftrightarrow n^2 + 2n + 1 \geq \frac{n^2 + 2n + 1 + 2n + 2 + 1}{2}$

$= \frac{n^2 + 4n + 4}{2} \Leftrightarrow n^2 \geq n^2/2 + 1 \Leftrightarrow n^2 - 1 \geq n^2/2 \Leftrightarrow$

$2n^2 - 2 \geq n^2 \Leftrightarrow 2n^2 \geq n^2 + 2$

IA: $2 \cdot 5^2 \geq 5^2 + 2 \Leftrightarrow 50 \geq 27$

IS: $2(n+1)^2 \geq (n+1)^2 + 2 \Leftrightarrow 2n^2 + 4n + 2 \geq n^2 + 2n + 3$

$\Leftrightarrow n^2 + 2n \geq 1$

Die Beweisführung in (b) erfolgt analog, mit den zusätzlichen Argumenten: $2 \leq x \Rightarrow 2^{-1} \geq x^{-1}$ und der Rechenregel $0 \leq a \leq b \wedge 0 \leq c \leq d \Rightarrow ac \leq bd$. Manchmal ist es auch praktisch $x = 2 + \epsilon$ mit $\epsilon \geq 0$ zu betrachten. $\square$