Inhaltsverzeichnis

Blatt 1, Aufgabe 11

Beh.: $C_2 \times C_2 \not\cong C_4$, d.h. es gibt keinen Gruppeniso $C_2 \times C_2 \to C_4$.

Bew.: C_4 ist zyklisch. Wäre $C_2 \times C_2$ isomorph zu C_4, so müsste auch $C_2 \times C_2$ zyklisch sein. (*)

Aber $C_2 \times C_2$ ist nicht zyklisch:

Sei $C_2 = \{1, \sigma\}$.

Dann ist $C_2 \times C_2 = \{(1,1), (1,\sigma), (\sigma,1), (\sigma,\sigma)\}$.

Keines dieser vier Elemente ist ein Erzeuger von $C_2 \times C_2$:

$\langle (1,1) \rangle = \{(1,1)\} \subsetneqq C_2 \times C_2$

$\langle (1,\sigma) \rangle = \{(1,1), (1,\sigma)\} \subsetneqq C_2 \times C_2$

$\langle (\sigma,1) \rangle = \{(1,1), (\sigma,1)\} \subsetneqq C_2 \times C_2$

$\langle (\sigma,\sigma) \rangle = \{(1,1), (\sigma,\sigma)\} \subsetneqq C_2 \times C_2$.

Also ist $C_2 \times C_2$ in der Tat ~~zy~~ nicht zyklisch.

Beh.: Es gibt endliche Gruppen gleicher Ordnung, welche nicht zueinander isomorph sind.

Bew.: C_4 und $C_2 \times C_2$ besitzen beide jeweils vier Elemente, sind jedoch nicht isomorph.

Zu (*): (allgemein)

Beh.: Sei $\varphi: G \to H$ ein Gruppenisomorphismus. Sei $x \in G$ beliebig. Dann gilt:

x ist ein Erzeuger von G $\Leftrightarrow$ $\varphi(x)$ ist ein Erzeuger von H.

Bew.: „$\Rightarrow$": Sei $y \in H$ beliebig. Dann ist $\varphi^{-1}(y)$ ein Element von G.

$\underset{\substack{x \text{ Erzeuger} \\ \text{von } G}}{\Longrightarrow}$ $\varphi^{-1}(y) = x^n$ für ein $n \geq 0$.

$\Rightarrow$ $y = \varphi(x^n) = \varphi(x)^n$, also ist y eine Potenz von $\varphi(y)$, das war zu zeigen.

„$\Leftarrow$": Analog, oder: Wende Argumentation auf φ^{-1} statt φ an.

Beh.: Sei $\varphi: G \to H$ ein Gruppenisomorphismus. Dann gilt:

G zyklisch $\Leftrightarrow$ H ~~ist~~ zyklisch.

Bew.: „$\Rightarrow$": G zyklisch $\Leftrightarrow$ $\exists g \in G$: g Erzeuger von G $\Leftrightarrow$ $\exists g \in G$: $\varphi(g)$ Erzeuger von H

$\Downarrow$

H zyklisch

„$\Leftarrow$": analog.

Blatt 3, Aufgabe 4

$G \circlearrowright X, \quad |G| = 91 = 7 \cdot 13, \quad |X| = 71.$

Beh.: Die Wirkung von G auf X besitzt ~~einen~~ mindestens einen Fixpunkt, d.h. einen Punkt $x \in X$ mit

$$gx = x \quad \text{für alle } g \in G,$$

d.h. ein Element von X^G.

Bew.: Nach der Bahnengleichung gilt:

Standgruppe von x

$$|X| = \sum_{[x] \in G\backslash X} |[x]| = \sum_{[x]\in G\backslash X} |Gx| = \sum_{[x]\in G\backslash X} |G/G_x| = \sum_{[x]\in G\backslash X} [G : G_x]$$

Summe über die Längen jeder Bahn

Nach dem Satz von Lagrange gilt: $[G : G_x] \in \{1, 7, 13, 91\}$

Menge der positiven Teiler von 91

Somit folgt:

$$|X| = 71 = 1 \cdot \underbrace{(\text{Anzahl der Bahnen, die nur ein Element enthalten})}_{=:a}$$
$$+ 7 \cdot \underbrace{(\text{—— " ——, die genau 7 Elemente "})}_{=:b}$$
$$+ 13 \cdot \underbrace{(\text{—— " ——, die genau 13 —"—})}_{=:c}$$
$$+ 91 \cdot \underbrace{(\text{—— " ——, die genau 91 —"—})}_{=:d}$$

für gewisse $a, b, c, d \in \mathbb{N}_0$.

Wir müssen zeigen, dass $a \geq 1$, denn bei einer Bahn, die nur aus einem Punkt besteht, ist dieser Punkt dann ein Fixpunkt.

Offensichtlich gilt $d = 0$, denn $71 < 91$.

Angenommen, $a = 0$. Dann gilt also:

$$|X| = 71 = 7b + 13c.$$

$$\Rightarrow 6 \equiv 7b \mod 13 \Rightarrow b \equiv \underbrace{7^{-1}}_{= 2 \bmod 13, \text{ denn } 2\cdot 7 \equiv 1 \bmod 13} \cdot 6 \mod 13 \Rightarrow b \equiv 12 \mod 13$$

Somit: 1. Fall: $b = 12$: $\lightning$, denn $71 < 7 \cdot 12$

2. Fall: $b = 25$ oder noch größer: $\lightning$, noch schlimmer. $\lightning$

Blatt 3, Aufgabe 5

(α) G Gruppe, $(N_i)_{i\in I}$ Familie von Normalteilern in G.

Beh.: $N := \bigcap_{i\in I} N_i$ ist ein Normalteiler in G.

Bew.: 1) N ist eine Untergruppe: klar nach Vorlesung oder direkt:

Neutrales Element: $1 \in N_i$ f.a. $i \in I$, also auch $1 \in N$.

Abgeschlossenheit bzgl. "·": Seien $x, y \in N$, also $x, y \in N_i$ f.a. $i \in I$.
$\Rightarrow xy \in N_i$ f.a. $i \in I \Rightarrow xy \in N$.

Inverse Elemente: Sei $x \in N$, also $x \in N_i$ f.a. $i \in I$.
$\Rightarrow x^{-1} \in N_i$ f.a. $i \in I \Rightarrow x^{-1} \in N$.

2) N ist ein Normalteiler von G:

Seien $u \in N$, $g \in G$ beliebig z.z.: $gug^{-1} \in N$.

Es gilt $u \in N_i$ f.a. $i \in I$.

Da N_i in G ein Normalteiler ist,

folgt daher $gug^{-1} \in N_i$, f.a. $i \in I$.

$\Rightarrow gug^{-1} \in N$.

Vorsicht Falle: Man muss nicht zeigen, dass $gug^{-1} = u$!

(β) G Gruppe, $H \subseteq G$ Untergruppe, $(N_i)_{i\in I}$ Familie aller Normalteiler, welche H enthalten.

Beh.: $\bigcap_{i\in I} N_i = G_H$ ← normaler Abschluss von H in G, definiert als $\langle U \rangle$ (die von U erzeugte Untergruppe), wobei $U = \{ghg^{-1} \mid g \in G, h \in H\}$.

Bew.: "⊆": Klar, denn da nach Vorlesung G_H ein Normalteiler von G ist, welcher H enthält, kommt G_H unter den N_i vor.

"⊇": Sei ein beliebiges Element aus G_H gegeben. Dieses lässt sich schreiben als ein Produkt von gewissen Elementen aus U und gewissen Inversen von Elementen aus U. Da $\bigcap_{i\in I} N_i$ eine Untergruppe ist, genügt es daher, zu zeigen, dass alle Elemente aus U in $\bigcap_{i\in I} N_i$ liegen. Denn dann liegen ihre Produkte und Inversen auch in $\bigcap_{i\in I} N_i$.

Sei also $ghg^{-1} \in U$ beliebig. Dann gilt in der Tat auch $ghg^{-1} \in N_i$ für alle $i \in I$, denn $h \in H \subseteq N_i$ und N_i ist in G ein Normalteiler.

Blatt 3, Aufgabe 6

G, H Gruppen, $f: G \to H$ Gruppenhomomorphismus,
$N \subseteq G$ Normalteiler in G, $N \subseteq \ker f$.

Beh.: Die Abbildung

$$\bar{f}: G/N \longrightarrow H$$
$$[g] \longmapsto f(g)$$

ist ein wohldefinierter Gruppenhomomorphismus mit

$$\ker \bar{f} = (\ker f)/N = \{ [g] \in G/N \mid g \in \ker f \}.$$

Bew.: 1) Wohldefiniertheit...

...der Definitionsmenge: okay, da N in G ein Normalteiler ist.

...der Funktionsvorschrift: Es gelte $[g] = [\tilde{g}]$, also $\tilde{g}^{-1} g \in N$.

$$\Rightarrow \underbrace{f(\tilde{g}^{-1} g)}_{= f(\tilde{g})^{-1} f(g)} = 1, \text{ da } \tilde{g}^{-1} g \in N \subseteq \ker f. \quad \Rightarrow \quad \underset{\bar{f}([\tilde{g}])}{\underset{\parallel}{f(\tilde{g})}} = \underset{\bar{f}([g])}{\underset{\parallel}{f(g)}}.$$

2) Gruppenhomomorphieeigenschaft:

i) $\bar{f}([1]) = f(1) = 1.$ ✓

ii) $\bar{f}([g] \cdot [h]) = \bar{f}([gh]) = f(gh) = f(g) f(h) = \bar{f}([g])\, \bar{f}([h]).$ ✓

3) $\ker \bar{f} = \{ [g] \in G/N \mid \underbrace{\bar{f}([g]) = 1}_{\Leftrightarrow f(g) = 1 \Leftrightarrow g \in \ker f} \} = \{ [g] \in G/N \mid g \in \ker f \}.$ ✓

Blatt 3, Aufgabe 7 (bzw. Blatt 4, Aufgabe 1)

(Q1) Gs: Darstellung von D_n über Erzeuger und Relationen, $n \geq 3$.

Dazu: $D_n \cong \langle r, s \mid r^{n}, s^2, srsr \rangle$.

Gesuchter Isomorphismus, wenn man

$$D_n = \{R_0, R_1, \dots, R_{n-1}, S_0, \dots, S_{n-1}\}$$

schreibt:

$$\varphi: \langle r, s \mid r^n, s^2, srsr \rangle \longrightarrow D_n$$

auf den Erzeugern definiert als:

$$r \longmapsto R_0$$
$$s \longmapsto S_0.$$

(Es gibt auch andere Möglichkeiten)

(Q2) Seien G, H Gruppen.

Gs: Wirkung von H auf G derart, dass $G \rtimes H \cong G \times H$.

Dazu: Definiere Wirkung von H auf G:

$$H \longrightarrow \mathrm{Aut}(G)$$
$$h \longmapsto h_* := \mathrm{id}_G.$$

Isomorphismus: $G \rtimes H \xrightarrow{\varphi} G \times H$, $(g,h) \longmapsto (g,h)$

Dabei sind Injektivität und Surjektivität klar. Zur Homomorphieeigenschaft:

$$\varphi((1,1)) = (1,1) = 1 \checkmark$$

$$\varphi((g,h)\cdot(\tilde{g},\tilde{h})) = \varphi((g\, h_*(\tilde{g}), h\tilde{h})) = \varphi((g\tilde{g}, h\tilde{h})) = (g\tilde{g}, h\tilde{h}) = (g,h)\cdot(\tilde{g},\tilde{h}). \checkmark$$

(Q3) $G \circlearrowright X$, G endlich, X endlich.

Beh.: $|Gx| \mid |G|$ für alle $x \in X$, also für die Bahnen $Gx \subseteq X$.

Bew.: $\underset{\substack{\uparrow \\ \text{Bahn von } x}}{|Gx|} = |G/\underset{\substack{\uparrow \\ \text{Standgruppe}}}{G_x}| = |G| / |G_x| \Rightarrow |G| = \underbrace{|G_x|}_{\in \mathbb{Z}} \cdot |Gx|$, also ist $|G|$ ein Vielfaches von $|Gx|$.

Blatt 4 Aufgabe 3

Beh.: $\varphi: \mathbb{R}^3 \rtimes SO_3(\mathbb{R}) \longrightarrow GL_4(\mathbb{R})$ ist ein injektiver Gruppenhomo.

$$(b, A) \longmapsto \left(\begin{array}{c|c} A & b \\ \hline 0\,0\,0 & 1 \end{array}\right) \quad \text{(Blockmatrixform)}$$

Bew.: Die Gruppenverknüpfung auf $\mathbb{R}^3$ schreiben wir als $+$,
die auf $SO_3(\mathbb{R})$ als $\cdot$
und die Wirkung von $SO_3(\mathbb{R})$ auf $\mathbb{R}^3$ auch als $\cdot$.

nämlich: $M \cdot x := Mx$ für $M \in SO_3(\mathbb{R}^3)$, $x \in \mathbb{R}^3$.

Wohldefiniertheit: Zu zeigen ist, dass $\left(\begin{array}{c|c} A & b \\ \hline 000 & 1 \end{array}\right) \in GL_4(\mathbb{R})$ für $A \in SO_3(\mathbb{R})$, $b \in \mathbb{R}^3$.
Das ist klar mit der Determinantenmultiplikationsformel:

$$\det\left(\begin{array}{c|c} A & b \\ \hline 000 & 1 \end{array}\right) = (\det A) \cdot (\det (1)) = \det A = 1 \neq 0. ✓$$

Injektivität: klar.

Homomorphie: $\varphi((b, A) \cdot (\tilde{b}, \tilde{A})) = \varphi((b + A\tilde{b}, A\tilde{A})) = \left(\begin{array}{c|c} A\tilde{A} & b + A\hat{b} \\ \hline 0\,0\,0 & 1 \end{array}\right)$

$\varphi((b, A)) \cdot \varphi((\hat{b}, \tilde{A})) = \left(\begin{array}{c|c} A & b \\ \hline 000 & 1 \end{array}\right) \left(\begin{array}{c|c} \tilde{A} & \hat{b} \\ \hline 000 & 1 \end{array}\right) = \left(\begin{array}{c|c} A\tilde{A} & b + A\hat{b} \\ \hline 0\,0\,0 & 1 \end{array}\right)$ $= ✓$

in Gedanken die Matrizen und Vektoren ausschreiben und dann die Multiplikation ausführen

Bew.: Da φ also ein injektiver Gruppenhomomorphismus ist, folgt, dass

$\mathbb{R}^3 \rtimes SO_3(\mathbb{R})$

isomorph zu im $\varphi = \left\{ \left(\begin{array}{c|c} A & b \\ \hline 000 & 1 \end{array}\right) \,\middle|\, A \in SO_3(\mathbb{R}), b \in \mathbb{R}^3 \right\} \subseteq GL_4(\mathbb{R})$ ist, also zu einer Untergruppe von $GL_4(\mathbb{R})$.

Blatt 4, Aufgabe 4

(a) $f: G \longrightarrow H$ Gruppenhomomorphismus, $K \leq H$ Untergruppe.

Beh.: $f^{-1}[K] = \{g \in G \mid f(g) \in K\} \leq G$ ist eine Untergruppe.

Bew.: Wir zeigen die Untergruppenaxiome:

1) $1 \in f^{-1}[K]$, denn $f(1) = 1 \in K$.

2) $g, \tilde{g} \in f^{-1}[K]$ beliebig, dann auch $g\tilde{g} \in f^{-1}[K]$, denn $f(g\tilde{g}) = \underbrace{f(g)}_{\in K} \underbrace{f(\tilde{g})}_{\in K} \in K$.

3) $g \in f^{-1}[K]$, dann auch $g^{-1} \in f^{-1}[K]$,
denn $f(g^{-1}) = \underbrace{f(g)}_{\in K}{}^{-1} \in K$.

(b) $f: G \to H$ Gruppenhomomorphismus, $N \leq H$ Normalteiler in H.

Beh.: $f^{-1}[N]$ ist ein Normalteiler in G.

Bew.: Nach (a) ist $f^{-1}[N]$ eine Untergruppe.
Nun ist noch zu zeigen:

$$\forall g \in f^{-1}[N]\ \forall h \in G:\ hgh^{-1} \in f^{-1}[N]$$

Falle: Es ist nicht zu zeigen, dass $hgh^{-1} = g$!

Seien also $g \in f^{-1}[N]$, $h \in G$ beliebig.
Dann gilt $f(hgh^{-1}) = f(h) \underbrace{f(g)}_{\in N} f(h)^{-1} \in N$, also $hgh^{-1} \in f^{-1}[N]$.

Bem.: Es gilt sogar folgende stärkere Aussage: (#)
(*) Sei $f: G \to H$ Gruppenhomomorphismus, $U \leq H$ Untergruppe, $N \leq U$ Normalteiler in U.
Dann ist auch $f^{-1}[N] \leq f^{-1}[U]$ ein Normalteiler in $f^{-1}[U]$ (nicht notwendigerweise in G).

(c) G endliche Gruppe, $N \leq G$ Normalteiler.

Beh.: G auflösbar $\Longleftrightarrow$ G/N und N auflösbar.

Bew.: „$\Leftarrow$": Sei $G/N = H_0 \geq H_1 \geq \dots \geq H_n = 1$ eine auflösbare Kompositionsreihe von G/N,
Sei $N = N_0 \geq N_1 \geq \dots \geq N_m = 1$ eine —— " —— N.
Sei $\pi: G \longrightarrow G/N$, $g \mapsto [g]$ die kanonische Projektionsabbildung.
Wir zeigen: $G = \pi^{-1}[H_0] \geq \pi^{-1}[H_1] \geq \dots \geq \pi^{-1}[H_n] = N = N_0 \geq \dots \geq N_m = 1$
ist eine auflösbare Kompositionsreihe von G.
Für den hinteren Teil (ab N_0) ist alles klar.
Im vorderen Teil ist zu zeigen:
i) $\pi^{-1}[H_{i+1}]$ ist in $\pi^{-1}[H_i]$ ein Normalteiler.
ii) $|\pi^{-1}[H_i] / \pi^{-1}[H_{i+1}]|$ ist eine Primzahl.

Zu i): Das ist klar nach (#).

Zu ii): Nach einem der Isomorphiesätze ist

$$\pi^{-1}[H_i] / \pi^{-1}[H_{i+1}]$$

isomorph zur Gruppe

$$H_i / H_{i+1},$$

deren Anzahl von Elementen eine Primzahl ist.

[Für Spaß hier noch ein Beweis der Isomorphie:

Die Abbildungskomposition

$$\begin{aligned} \pi^{-1}[H_i] &\longrightarrow H_i \longrightarrow H_i/H_{i+1} \\ g &\longmapsto [g] \longmapsto [[g]] \end{aligned}$$

ist surjektiv mit

$$\ker = \{ g \in G \mid \underbrace{[[g]] = 1 \text{ in } H_i/H_{i+1}}_{\Leftrightarrow\ [g] \in H_{i+1} \ \Leftrightarrow\ g \in \pi^{-1}[H_{i+1}]} \} = \pi^{-1}[H_{i+1}]$$

Nach dem ersten Isomorphiesatz folgt somit, dass

$$\begin{aligned} \pi^{-1}[H_i] / \pi^{-1}[H_{i+1}] &\longrightarrow H_i/H_{i+1} \\ [g] &\longmapsto [[g]] \end{aligned}$$

ein wohldefinierter Isomorphismus.

„$\Rightarrow$": Beispielsweise aus Algebra I ist bekannt, dass Untergruppen auflösbarer Gruppen auflösbar sind.
Es ist also nur noch zu zeigen, dass G/N auflösbar ist.

Sei dazu $G = G_0 \geq G_1 \geq \cdots \geq G_\ell = 1$ eine auflösbare Kompositionsreihe von G.
Betrachte die Reihe $G/N = \pi[G_0] \geq \cdots \geq \pi[G_\ell] = 1$, wobei $\pi : G \to G/N$ wie ob
Wir behaupten nicht, dass diese Reihe eine auflösbare Kompositionsreihe von G/N ist.

Stattdessen zeigen wir:

i) $\pi[G_{i+1}]$ ist in $\pi[G_i]$ ein Normalteiler.

ii) $|\pi[G_i] / \pi[G_{i+1}]|$ ist entweder 1 oder eine Primzahl.

Zu i): Seien $g \in G_{i+1}$, $h \in G_i$ beliebig. Dann gilt $[h][g][h]^{-1} = [\underbrace{hgh^{-1}}_{\in G_{i+1}}] \in \pi[G_{i+1}]$

Zu ii): Betrachte den Gruppenhomomorphismus

$$\begin{aligned} G_i/G_{i+1} &\xrightarrow{\ \varphi\ } \pi[G_i]/\pi[G_{i+1}] \\ [g] &\longmapsto [[g]]. \end{aligned}$$

Dieser ist wohldefiniert, denn:

Gelte $[g] = [\tilde{g}]$ in G_i/G_{i+1}, also $\tilde{g}^{-1} g \in G_{i+1}$.

Dann folgt $[\tilde{g}]^{-1} [g] \in \pi[G_{i+1}]$,

Somit $[[g]] = [[\tilde{g}]]$ in $\pi[G_i]/\pi[G_{i+1}]$.

Außerdem ist φ offensichtlich surjektiv.

Nach Voraussetzung ist ~~der Kern von φ~~ G_i/G_{i+1} einfach, also gibt es für den Kern nur zwei Möglichkeiten:

Fall 1: $\ker \varphi = 1$.

Dann ist φ injektiv und somit (nach oben) ein Isomorphismus. Somit hat $\pi[G_i]/\pi[G_{i+1}]$ genauso viele Elemente wie G_i/G_{i+1}, ist also von Primzahlordnung.

Fall 2: $\ker \varphi = G_i/G_{i+1}$.

Dann ist, da φ surjektiv ist, jedes Element in $\pi[G_i]/\pi[G_{i+1}]$ gleich der Identität. Somit gilt $|\pi[G_i]/\pi[G_{i+1}]| = 1$. $(\lozenge)$

Jetzt sind wir schnell fertig: Aus der Reihe

$$G/N = \pi[G_0] \geq \ldots \geq \pi[G_\ell] = 1$$

streichen wir ~~ddd~~ doppelt (oder sogar häufiger) auftretende Glieder. Übrig bleibt dann eine auflösbare Kompositionsreihe von G/N.

Zu $(\lozenge)$: Somit folgt $\pi[G_i] = \pi[G_{i+1}]$.

Blatt 5, Aufgabe 5

Sei G Gruppe mit $|G| = 56 = 2^3 \cdot 7$.

Beh.: G besitzt einen nichttrivialen Sylowschen Normalteiler.

Bew.: $n_7 \in \{1, 2, 4, 8\} \cap \{1, 8, 15, \dots\} = \{1, 8\}$, $n_2 \in \{1, 7\} \cap \{1, 3, 5, 7, \dots\} = \{1, 7\}$

1. Fall: $n_7 = 1$: ✓

2. Fall: $n_7 = 8$:

Die acht 7-Sylowgruppen können sich nur in $\{1\}$ überlappen.

Daher können wir folgende Zwischenbilanz ziehen:

1 Element der Ordnung 1 (das neutrale Element von G),

$8 \cdot 6$ Elemente der Ordnung 7 in den acht 7-Sylowgruppen.

Bleiben also $56 - 1 - 8 \cdot 6 = 7$ bisher unzugeordnete Elemente.

Da jede 2-Sylowgruppe acht Elemente enthält, kann es nur eine 2-Sylowgruppe geben, fertig.

Warnung: Gäbe es mehrere 2-Sylowgruppen, so könnten sich diese durchaus überlappen, da 8 nicht nur die Teiler 1 und 8 besitzt. Zwei 2-Sylowgruppen können sich aber höchstens in vier Elementen überlappen,

also bräuchten die hypothetischen sieben 2-Sylowgruppen jeweils vier eigene Elemente, insgesamt also $7 \cdot 4 = 28 > 7$.

Blatt 5, Aufgabe 7

p, q Primzahlen mit $p<q$, $p \nmid q-1$,
G Gruppe mit $|G| = pq$.

Beh.: G ist zyklisch.

Bew.: Anzahl p-Sylowgruppen: ~~$n_p \in \{1, q\}$~~

$n_p \mid q \Rightarrow n_p = 1$ oder $n_p = q$.

Sollte $n_p = q$ sein, dann gilt also auch $n_p = q \equiv 1 \mod p$, also $p \mid q-1$, ↯.

Folglich: $n_p = 1$.

Anzahl q-Sylowgruppen:

$n_q \mid p \Rightarrow n_q = 1$ oder $n_q = p$.

Sollte $n_q = p$ sein, dann gilt also $n_q = p \equiv 1 \mod q$, also $q \mid p-1$, ↯ zu $p<q$.

Folglich: $n_q = 1$.

Die einzige p-Sylowgruppe sei P, die einzige q-Sylowgruppe sei Q.

Nun gibt es zwei Möglichkeiten, weiter zu machen:

1) Da Ordnungen von Elementen Teiler der Gruppenordnung sind, gibt es in G nur Elemente der Ordnungen $1, p, q$ und pq. Gesucht ist ein Element der Ordnung pq.

Anzahl Elemente von Ordnung 1: 1 (nur das neutrale Element)

... Ordnung p: $p-1$ (alle in P bis auf das neutrale Element)

... Ordnung q: $q-1$ (alle in Q bis auf das neutrale Element)

Sei m die Anzahl von Elementen mit Ordnung pq, wir wollen zeigen: $m \geq 1$.

Es gilt: $1 + (p-1) + (q-1) + m = |G| = pq$,

also: $m = pq - 1 - (p-1) - (q-1) = pq - p - q + 1 \underset{p<q}{>} pq - q - q + 1 = \underbrace{(p-2)}_{\geq 0,\ \text{da } p \geq 2} q + 1 \geq 1$.

Fertig!

2) P und Q sind jeweils zyklisch, da sie von Primordnung sind. Ferner vertauschen Elemente von P und Q untereinander:

Sei $p \in P$, $q \in Q$ beliebig. Betrachte $(pq)(qp)^{-1} = pqp^{-1}q^{-1} \in G$.

Es gilt: $pqp^{-1}q^{-1} = p\underbrace{(qp^{-1}q^{-1})}_{\in P,\ \text{da } p^{-1} \in P \text{ und } P \text{ Normalteiler}} \in P$, andererseits $pqp^{-1}q^{-1} = \underbrace{(pqp^{-1})}_{\in Q,\ \text{da } q \in Q \text{ und } Q \text{ Normalteiler}} q^{-1} \in Q$.

Folglich gilt $(pq)(qp)^{-1} \in P \cap Q = \{1\}$, also $(pq)(qp)^{-1} = 1$, also $pq = qp$.

p- und q-Sylowgruppen können sich nur trivial überlappen

Somit folgt:

$$\begin{aligned} P \times Q &\xrightarrow{\varphi} G \\ (p,q) &\longmapsto pq \end{aligned}$$

ist ein Gruppeniso, denn:

a) φ ist ein Gruppenhomo: $\varphi((1,1)) = 1 \cdot 1 = 1$ ✓

$\varphi((p,q)(\tilde{p},\tilde{q})) = \varphi((p\tilde{p}, q\tilde{q})) = p\tilde{p}q\tilde{q} = pq\tilde{p}\tilde{q} = \varphi((p,q))\varphi((\tilde{p},\tilde{q}))$ ✓

b) φ ist injektiv, denn:

Sei $\varphi(pq) = 1$. $\Rightarrow pq = 1 \Rightarrow \underbrace{p}_{\in P} = \underbrace{q^{-1}}_{\in Q}$, also $p = q^{-1} \in P \cap Q = \{1\}$.

$\Rightarrow p = 1,\ q^{-1} = 1$

$\Rightarrow (p,q) = (1,1)$.

c) φ ist surjektiv, da injektiv und $|P \times Q| = |P| \cdot |Q| = pq = |G|$.

Also: $G \cong P \times Q \cong \mathbb{Z}/(p) \times \mathbb{Z}/(q) \cong \mathbb{Z}/(pq)$. ← ist zyklische Gruppe

Vorlesung, da p,q zueinander teilerfremd

Blatt 5, Aufgabe 8

Beh.: $\mathbb{Z}/(2) \times \mathbb{Z}/(3)$ ist zyklisch, d.h. kann durch ein einzelnes Element erzeugt werden.

Bew.: Zwei Beweismöglichkeiten:

1) Direkt, per Hand:

Es gilt $\mathbb{Z}/(2) = \{[0], [1]\}$, $\mathbb{Z}/(3) = \{[0], [1], [2]\}$,

also $\mathbb{Z}/(2) \times \mathbb{Z}/(3) = \{([0],[0]), ([0],[1]), ([0],[2]), ([1],[0]), ([1],[1]), ([1],[2])\}$.

Dann ist $([1],[1])$ ein Erzeuger von $\mathbb{Z}/(2) \times \mathbb{Z}/(3)$:

$$\left.\begin{aligned}
0 \cdot ([1],[1]) &= ([0],[0]) \\
1 \cdot ([1],[1]) &= ([1],[1]) \\
2 \cdot ([1],[1]) &= ([0],[2]) \\
3 \cdot ([1],[1]) &= ([1],[0]) \\
4 \cdot ([1],[1]) &= ([0],[1]) \\
5 \cdot ([1],[1]) &= ([1],[2])
\end{aligned}\right\} \text{ also sind alle sechs Gruppenelemente Vielfache von } ([1],[1]). \checkmark$$

2) „Fancy": Nach Vorlesung gilt $\mathbb{Z}/(2) \times \mathbb{Z}/(3) \cong \mathbb{Z}/(2 \cdot 3) = \mathbb{Z}/(6)$,
und $\mathbb{Z}/(6)$ ist natürlich zyklisch.

da 2, 3 teilerfremd zueinander

Frage: Wieso ist das kein Widerspruch zu Hilfssatz 6.112?

Dazu: Voraussetzung des Hilfssatzes ist, dass die Zahlen d_i (aus der Behauptung des Hilfssatzes) jeweils eine Teilerkette bilden. Das ist hier nicht der Fall, da weder $2 \mid 3$ noch $3 \mid 2$.

Bem.: In abelschen Gruppen schreibt man ja oft $+$ statt $\cdot$, so auch hier.
Der Konsistenz wegen schreibt man dann auch $n \cdot g := \underbrace{g + \dots + g}_{n \text{ Mal}}$ statt $g^n := \underbrace{g \cdots g}_{n \text{ Mal}}$.

Blatt 5, Aufgabe 9

$d \in \mathbb{Z}$, $A \in \mathbb{Z}^{n \times n}$, $u \in \mathbb{Z}^n$, $Au \equiv 0 \mod d$ komponentenweise

d.h. $(Au)_i \equiv 0 \mod d$ für alle $i = 1, \dots, n$

Bh.: $(\det A) \cdot u \equiv 0 \mod d$.

Bew.: Für die Adjunkte $\mathrm{ad}\, \cancel{\det} A$ von $\cancel{\det} A$ gilt:

$$(\mathrm{ad}\, \cancel{\det} A) \cdot A = (\det A) \cdot \mathbb{1}_n$$

$n \times n$-Einheitsmatrix

Daher gilt:

$$(\det A) \cdot u = (\det A) \cdot \mathbb{1}_n u = (\mathrm{ad}\, A) \underbrace{A u}_{\substack{\equiv 0 \\ \mathrm{mod}\ d}} \equiv 0 \mod d.$$

Blatt 6, Aufgabe 5

$A \in \mathbb{Z}^{n\times m}$ mit Elementarteilern $d_1, \dots, d_r$, $r = \min\{n,m\}$.

Sei $\lambda_i := ggT(\text{alle } i\text{-Minoren von } A)$ für $i = 1, \dots, \min\{n,m\}$.

Beh.: $\lambda_i = d_1 \cdots d_i$ für $i = 1, \dots, r$.

Bew.: $\lambda_i = ggT(\text{alle } i\text{-Minoren von } A) = ggT(\text{alle } i\text{-Minoren von } S) = ggT(0, \text{alle Produkte von je } i \text{ vielen } d_j) = d_1 \cdots d_i$.

Sei S die Smithsche Normalform von A, $S = \begin{pmatrix} d_1 & & & & & \\ & \ddots & & & & \\ & & d_r & 0 & \cdots & 0 \end{pmatrix}$ oder $S = \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_r \\ & & \vdots \\ & & 0 \end{pmatrix}$ („rechteckige Diagonalmatrix“).
Das Gleichheitszeichen gilt dann nach dem gegebenen Tipp.

da $d_1 | d_2 | \cdots | d_r$

Bem.: Da jede ~~natürliche~~ ganze Zahl ein Teiler von 0 ist, gilt stets $ggT(0, a_1, \dots, a_\ell) = ggT(a_1, \dots, a_\ell)$.

Bsp.: Sei $S = \begin{pmatrix} d_1 & 0 & 0 & 0 \\ 0 & d_2 & 0 & 0 \end{pmatrix}$.

Dann sind die 1-Minoren von S: $d_1, 0, 0, 0, 0, d_2, 0, 0$.

... 2-Minoren von S: $\det\begin{pmatrix} d_1 & 0 \\ 0 & d_2 \end{pmatrix}$, $\det\begin{pmatrix} d_1 & 0 \\ 0 & 0 \end{pmatrix}$, $\det\begin{pmatrix} d_1 & 0 \\ 0 & 0 \end{pmatrix}$, $\det\begin{pmatrix} 0 & 0 \\ d_2 & 0 \end{pmatrix}$, $\det\begin{pmatrix} 0 & 0 \\ d_2 & 0 \end{pmatrix}$, $\det\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$,

also $d_1 d_2, 0, 0, 0, 0, 0$.

Somit $ggT(\text{alle 1-Minoren von } S) = ggT(d_1, d_2) = d_1$, da $d_1 | d_2$,
$ggT(\text{alle 2-Minoren von } S) = ggT(d_1 d_2) = d_1 d_2$.

Bsp.: Sei $S = \begin{pmatrix} d_1 & & \\ & d_2 & \\ & & d_3 \end{pmatrix}$.

Dann sind die 1-Minoren von S: $d_1, d_2, d_3, 0, \dots, 0$.

... 2-Minoren von S: $d_1 d_2, d_1 d_3, d_2 d_3, 0, \dots, 0$.

... 3-Minoren von S: $d_1 d_2 d_3$.

Somit $ggT(\text{alle 1-Minoren von } S) = ggT(d_1, d_2, d_3) = d_1$,
$ggT(\text{alle 2-Minoren von } S) = ggT(d_1 d_2, d_1 d_3, d_2 d_3) = d_1 d_2$,
$ggT(\text{alle 3-Minoren von } S) = ggT(d_1 d_2 d_3) = d_1 d_2 d_3$.

Blatt 6, Aufgabe 5 (Forts.)

Bsp: Sei $A = \begin{pmatrix} 2 & 6 & 8 \\ 3 & 1 & 2 \\ 9 & 5 & 4 \end{pmatrix}$.

Dann gilt:

$\lambda_1 = \text{ggT}(\text{alle 1-Minoren}) = \text{ggT}(2, 6, 8, 3, 1, 2, 9, 5, 4) = 1.$

$\lambda_2 = \text{ggT}(\text{alle 2-Minoren}) = \text{ggT}\left(\begin{vmatrix} 2 & 6 \\ 3 & 1 \end{vmatrix}, \begin{vmatrix} 2 & 8 \\ 3 & 2 \end{vmatrix}, \begin{vmatrix} 6 & 8 \\ 1 & 2 \end{vmatrix}, \begin{vmatrix} 3 & 1 \\ 9 & 5 \end{vmatrix}, \begin{vmatrix} 3 & 2 \\ 9 & 4 \end{vmatrix}, \begin{vmatrix} 1 & 2 \\ 5 & 4 \end{vmatrix}, \begin{vmatrix} 2 & 6 \\ 9 & 5 \end{vmatrix}, \begin{vmatrix} 2 & 8 \\ 9 & 4 \end{vmatrix}, \begin{vmatrix} 6 & 8 \\ 5 & 4 \end{vmatrix} \right)$

$= \text{ggT}(-18, -20, 4, 6, -6, -6, -44, -64, -16)$

$= 2$

$\lambda_3 = \text{ggT}(\text{alle 3-Minoren}) = \text{ggT}(\det A) = |\det A| = \ldots = 72.$

Somit:

$d_1 = \lambda_1 = 1$

$d_2 = \lambda_2 / d_1 = 2$

$d_3 = \lambda_3 / (d_1 d_2) = 36.$

Bem.: Dieses Verfahren zum Ausrechnen der Elementarteiler empfiehlt sich bei größeren Matrizen nicht, viel schneller bringt man die Matrix auf Smithsche Normalform.

Blatt 6, Aufgabe 6

(Q1) R kommutativer Ring, $R \neq \{0\}$ (Nullring)

Beh.: $M_n(R)$ kommutativ $\Leftrightarrow$ $n=1$

Bew.: Für $n=1$ ist $M_n(R)$ isomorph zu R selbst,

$$M_1(R) \xrightarrow{\cong} R$$
$$(r) \longmapsto r,$$

1×1-Matrix

daher muss $M_1(R)$ ~~die~~ kommutativ sein.

Für $n \geq 2$ betrachte folgendes Gegenbeispiel zur Kommutativität:

$$A := \begin{pmatrix} 1 & 0 & & \\ 0 & 0 & & \\ & & 0 & \\ & & & \ddots \\ & & & & 0 \end{pmatrix}, \quad B := \begin{pmatrix} 0 & 1 & & \\ 0 & 0 & & \\ & & 0 & \\ & & & \ddots \\ & & & & 0 \end{pmatrix},$$

Dann gilt:

$$AB = \begin{pmatrix} 1 & 0 & & \\ 0 & 0 & & \\ & & 0 & \\ & & & \ddots \\ & & & & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 & & \\ 0 & 0 & & \\ & & 0 & \\ & & & \ddots \\ & & & & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 & & \\ 0 & 0 & & \\ & & 0 & \\ & & & \ddots \\ & & & & 0 \end{pmatrix}$$

$$\neq$$

$$BA = \begin{pmatrix} 0 & 1 & & \\ 0 & 0 & & \\ & & 0 & \\ & & & \ddots \\ & & & & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & & \\ 0 & 0 & & \\ & & 0 & \\ & & & \ddots \\ & & & & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & & \\ 0 & 0 & & \\ & & 0 & \\ & & & \ddots \\ & & & & 0 \end{pmatrix}$$

(Q2) Beh.: $\mathbb{R}^{\mathbb{R}} = \{f : \mathbb{R} \to \mathbb{R}\}$ wird vermöge der üblichen Addition und Multiplikation von Funktionen zu einem Ring.

Bew.: Wir müssen alle Ringaxiome nachprüfen.

1) Abgeschlossenheit von $+$: klar, für $f, g \in \mathbb{R}^{\mathbb{R}}$ ist auch $f+g \in \mathbb{R}^{\mathbb{R}}$.

2) Assoziativität von $+$:

Seien $f,g,h \in \mathbb{R}^{\mathbb{R}}$ beliebig. Dann $f+(g+h) = (x \mapsto f(x) + \underbrace{(g+h)(x)}_{=(g(x)+h(x))}) = (x \mapsto (f+g)(x) + h(x))$
$= (f+g)+h$

3) Neutrales Element für $+$:

Sei 0 die Nullfunktion $(x \mapsto 0)$.

Sei $f \in \mathbb{R}^{\mathbb{R}}$ beliebig. Dann $0+f = (x \mapsto \underbrace{0(x)}_{=0} + f(x)) = (x \mapsto f(x)) = f$,

$f + 0 = (x \mapsto f(x) + \underbrace{0(x)}_{=0}) = (x \mapsto f(x)) = f$.

die Nullfunktion

die reelle Zahl 0

4) Negative Elemente für $+$:

Sei $f \in \mathbb{R}^{\mathbb{R}}$ beliebig.

Definiere $-f := (x \mapsto -f(x))$.

Dann: $f + (-f) = (x \mapsto f(x) + (-f)(x))$
$= (x \mapsto f(x) - f(x)) = (x \mapsto 0)$, ~~lebt~~ $= 0$ (Nullfunktion),

ebenso $(-f) + f =$ Nullfunktion.

5) Abgeschlossenheit von $\cdot$: klar, für $f,g\in\mathbb{R}^\mathbb{R}$ ist auch $fg\in\mathbb{R}^\mathbb{R}$.

6) Assoziativität von $\cdot$:

Seien $f,g,h\in\mathbb{R}^\mathbb{R}$ beliebig.

Dann $(fg)h = (x\mapsto \underbrace{(fg)(x)}_{=(f(x)g(x))} h(x)) = (x\mapsto f(x)(gh)(x)) = f(gh)$.

7) Neutrales Element für $\cdot$:

Sei 1 die Einsfunktion $(x\mapsto 1)$.

Sei $f\in\mathbb{R}^\mathbb{R}$ beliebig.

Dann $\underbrace{1}_{\text{Einsfunktion}} f = (x\mapsto \underbrace{1(x)}_{=1 \text{ (Zahl 1)}} f(x)) = (x\mapsto f(x)) = f$, ebenso $f\cdot 1 = f$.

8) Distributivgesetze:

Seien $f,g,h\in\mathbb{R}^\mathbb{R}$ beliebig.

Dann $(f+g)h = (x\mapsto (f+g)(x)\,h(x)) = (x\mapsto (f(x)+g(x))h(x))$
$= (x\mapsto f(x)h(x) + g(x)h(x)) = (x\mapsto (fh)(x)+(gh)(x)) = fh + gh$,

ebenso $f(g+h) = fg + fh$.

Bem.: In $\mathbb{R}^\mathbb{R}$ ist nicht jedes Element bzgl. $\cdot$ invertierbar, genauer gilt:

$f\in\mathbb{R}^\mathbb{R}$ ist in $\mathbb{R}^\mathbb{R}$ invertierbar bzgl. $\cdot$ $\iff$ f besitzt keine Nullstellen.

Bem.: Die Identitätsfunktion $(x\mapsto x)$ ist weder bzgl. $+$ noch bzgl. $\cdot$ neutrales Element.

Bem.: Auf analoge Art und Weise kann man zeigen, dass für eine beliebige Menge M auch

$\mathbb{R}^M = \{f : M\to\mathbb{R}\}$,

also die Menge aller Funktionen von M nach ~~[illegible]~~ $\mathbb{R}$, ein Ring ist.

Bem.: $\mathbb{R}^\mathbb{R}$ (und $\mathbb{R}^M$) sind kommutative Ringe, d.h. es gilt $fg=gf$ für alle f,g des Rings.

(Q3) R kommutativer Ring, S R-Algebra

Beh.: $\phi: R\to S,\ x\mapsto x\cdot 1$ ist ein Ringhomomorphismus.

Bew.: $\phi(0) = 0\cdot 1 = 0$ ✓, $\phi(x+y) = (x+y)\cdot 1 = (x\cdot 1)+(y\cdot 1) = \phi(x)+\phi(y)$ ✓

$\phi(1) = 1\cdot 1 = 1$ ✓, $\phi(xy) = (xy)\cdot 1 = (xy)\cdot(1\cdot 1) = (x\cdot 1)\cdot(y\cdot 1) = \phi(x)\phi(y)$ ✓

Blatt 7, Aufgabe 3

(a) p Primzahl, $\mathbb{Z}_p = \{ x \in \mathbb{Q} \mid$ in vollständig gekürzter Bruchdarstellung von $\mathbb{Q}$ ist der Nenner nicht durch p teilbar $\} \subseteq \mathbb{Q}$.

Beh.: $\mathbb{Z}_p$ ist ein Unterring von $\mathbb{Q}$.

Bew.: $0 = \frac{0}{1} \in \mathbb{Z}_p$, da $p \nmid 1$.

$1 = \frac{1}{1} \in \mathbb{Z}_p$, da $p \nmid 1$.

Für $x = \frac{a}{b}$, $y = \frac{c}{d} \in \mathbb{Z}_p$ (vollständig gekürzt) gilt:

$x + y = \frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ (vielleicht nicht vollständig gekürzt),

also $x+y \in \mathbb{Z}_p$, da $p \nmid bd$ (da $p \nmid b$, $p \nmid d$ und p prim) und somit p auch nicht Teiler des (nicht angeschriebenen) ~~des~~ Nenners in der vollständig gekürzten Darstellung ist.

Ganz analog gilt auch $xy = \frac{ac}{bd} \in \mathbb{Z}_p$.

Schließlich gilt $-x = \frac{-a}{b} \in \mathbb{Z}_p$.

Ges.: $(\mathbb{Z}_p)^\times = \{ x \in \mathbb{Z}_p \mid x$ invertierbar in $\mathbb{Z}_p \}$.

Dazu: Sei $x = \frac{a}{b} \in \mathbb{Z}_p$ (vollständig gekürzt).

Dann gilt:

x in $\mathbb{Z}_p$ invertierbar $\iff \frac{b}{a}$ existiert und liegt in $\mathbb{Z}_p$

$\iff a \neq 0$ und $p \nmid a$.

Also: $(\mathbb{Z}_p)^\times = \{ \frac{a}{b} \in \mathbb{Q} \mid a, b \neq 0,\ p \nmid a, b \}$.

Bem.: $\mathbb{Z}_p$ ist die Lokalisierung von $\mathbb{Z}$ nach der multiplikativen Menge $\mathbb{Z} \setminus (p)$.

(b) Ges.: $(\mathbb{Z}[i])^\times = \{ x \in \mathbb{Z}[i] \mid x$ in $\mathbb{Z}[i]$ invertierbar $\}$.

Dazu: Sei $x = a + ib \in \mathbb{Z}[i]$ beliebig.

Dann gilt:

x in $\mathbb{Z}[i]$ invertierbar $\iff x$ in $\mathbb{C}$ invertierbar und $x^{-1} \in \mathbb{Z}[i]$

$\iff |x|^2 = a^2 + b^2 \neq 0$ und $x^{-1} = \cancel{\frac{1}{a+ib}}\ \frac{1}{a^2+b^2} \cdot (a - ib) \in \mathbb{Z}[i]$

$\iff a^2 + b^2 \neq 0$ und $a^2 + b^2 \mid a, b$

$\iff a^2 + b^2 = 1$

$\iff a, b \in \{-1, 0, 1\}$ und $a^2 + b^2 = 1$

$\iff x \in \{1, -1, i, -i\}$.

Also $(\mathbb{Z}[i])^\times = \{ \pm 1, \pm i \}$.

Blatt 7, Aufgabe 7

K Körper.

Beh.: char $K = n \iff \ker\varphi = (n)$, wobei φ der eindeutig bestimmte Ringhomomorphismus von $\mathbb{Z}$ nach K ist.

Bew.: Der Ringhomo ~~[illegible]~~ φ sieht so aus:

$$\varphi: \mathbb{Z} \longrightarrow K$$
$$z \longmapsto z\cdot 1 := \begin{cases} 1+1+\dots+1 & (z \text{ Summanden}), \text{ falls } z>0 \\ 0, & \text{falls } z=0 \\ (-1)+(-1)+\dots+(-1) & (-z \text{ Summanden}), \text{ falls } z<0 \end{cases}$$

Somit gilt für $n \geq 1$:

$$\ker\varphi = (n) \overset{(*)}{\iff} \varphi(n) = 0 \text{ und } \varphi(i) \neq 0 \text{ für } 1 \leq i < n$$
$$\iff n\cdot 1 = 0 \text{ und } i\cdot 1 \neq 0 \text{ für } 1 \leq i < n$$
$$\iff \text{char } K = n$$

Null in K

Für $n = 0$ gilt:

$$\ker\varphi = (0) \iff \varphi \text{ injektiv} \iff n\cdot 1 \neq 0 \text{ für alle } n \neq 0 \iff \text{char } K = 0.$$

Erklärung von (*): Das Ideal $(n) \subseteq \mathbb{Z}$ ist $\{0, n, 2n, 3n, \dots, -n, -2n, -3n, \dots\}$.
Folglich ist die kleinste positive Zahl in (n) die Zahl n selbst.

Bem.: Diese Aufgabe liefert einen guten Grund dafür, die Charakteristik von Körpern K mit $n\cdot 1 \neq 0$ in K für alle $n \neq 0$ als 0 statt ∞ festzusetzen.

Blatt 7, Aufgabe 9

Sei $\phi: R \to S$ ein Homomorphismus von Ringen, $b \subseteq S$ ein Ideal.

Beh.: Die Urbildmenge

$$\phi^{-1}(b) = \{ x \in R \mid \phi(x) \in b \} \subseteq R$$

ist ein Ideal von R.

Bew.: 1) $0 \in \phi^{-1}(b)$, denn $\phi(0) = 0 \in b$.

2) $x + y \in \phi^{-1}(b)$ für $x, y \in \phi^{-1}(b)$, denn $\phi(x+y) = \underbrace{\phi(x)}_{\in b} + \underbrace{\phi(y)}_{\in b} \in b$.

3) $ax \in \phi^{-1}(b)$

für $a \in R$, $x \in \phi^{-1}(b)$,

denn $\phi(ax) = \underbrace{\phi(a)}_{\in S} \underbrace{\phi(x)}_{\in b} \in b$.

Bem.: Nicht jedes Ideal eines beliebigen Rings ist ein Hauptideal.
Man kann daher nicht voraussetzen, dass b von der Form $(s_0) = \{ s s_0 \mid s \in S \}$ für ein $s_0 \in S$ ist.

Bem.: Für $\phi^{-1}(b)$ schreibt man oft auch „$R \cap b$".
Das ist aber keinesfalls wörtlich zu verstehen, denn da im Allgemeinen $R \cap S = \emptyset$, wäre auch $R \cap b = \emptyset$.

Frage: Sind auch Bildmengen von Idealen i.A. Ideale?

Dazu: Nein, i.A. nicht. Betrachte folgendes Gegenbeispiel:

$$\phi: \mathbb{Z} \longrightarrow \mathbb{Q}$$
$$z \longmapsto \frac{z}{1}$$

Dann ist ϕ in der Tat ein Ringhomomorphismus und das Einsideal $(1) = \mathbb{Z}$ ist ein Ideal von $\mathbb{Z}$.
Aber das Bild dieses Ideals,

$$\phi(\mathbb{Z}) = \{ \tfrac{z}{1} \mid z \in \mathbb{Z} \} \subseteq \mathbb{Q},$$

ist kein Ideal von $\mathbb{Q}$. Denn die „Magneteigenschaft" ist verletzt:

Beispielsweise liegt 3 in $\phi(\mathbb{Z})$ und $\frac{1}{2} \in \mathbb{Q}$.

Aber $\frac{1}{2} \cdot 3$ liegt nicht in $\phi(\mathbb{Z})$.

Blatt 8, Aufgabe 1

(a2) R komm. Ring, $f \in R$ invertierbar.

Gesucht: Kanonischer Ringisomorphismus $R \longrightarrow R[f^{-1}]$.

Dazu: Betrachte die kanonische Abbildung

$$\varphi: R \longrightarrow R[f^{-1}]$$
$$r \longmapsto \frac{r}{1}.$$

Nach Vorlesung ist φ wohldefiniert und ein Ringhomomorphismus.
Hier ist φ außerdem bijektiv.

Injektivität: Sei $\varphi(r) = \frac{r}{1} = 0$. $\left(= \frac{0}{1}\right)$

$\Rightarrow$ ex. $m \geq 0$: $f^m r \cdot 1 = f^m \cdot 0 \cdot 1$, also $f^m r = 0$. (in R)

$\Rightarrow (f^m)^{-1} f^m r = (f^m)^{-1} 0$ (in R)

f invertierbar in R

$$\underbrace{(f^m)^{-1} f^m r}_{= r} = \underbrace{(f^m)^{-1} 0}_{= 0} \quad \checkmark$$

Surjektivität: Sei ein beliebiges Element $\frac{r}{f^n} \in R[f^{-1}]$ gegeben.

Dann gilt

$$\frac{r}{f^n} = \frac{r(f^n)^{-1}}{1},$$ denn $\exists s \in \{f^0, f^1, f^2, \ldots\}: s r \cdot 1 = s r (f^n)^{-1} f^n$,

nämlich $s = f^0 = 1$.

Folglich gilt

$$\frac{r}{f^n} = \frac{r(f^n)^{-1}}{1} = \varphi(r(f^n)^{-1}).$$

Blatt 8, Aufgabe 4

(a) R komm. Ring, $s_1, \dots, s_n$ Zerlegung der Eins (d.h. $1 = s_1 + \dots + s_n$).

Seien $f, g \in R$ beliebig.

Beh.: $f = g$ in R $\iff$ $f = g$ in $R[s_i^{-1}]$ für alle $i \in \{1, \dots, n\}$.

Bem.: Die Aussage

$$f = g \text{ in } R[h^{-1}]$$

bedeutet allgemein, dass die beiden Elemente

$$\frac{f}{1}, \quad \frac{g}{1}$$

des Rings $R[h^{-1}]$ gleich sind, d.h. dass es ein $m \geq 0$ gibt mit

$$m f = m g \in R.$$

Bew.: „$\Rightarrow$": klar.

„$\Leftarrow$": Da $f = g$ in $R[s_i^{-1}]$, gibt es ein $m_i \geq 0$ mit $s_i^{m_i} f = s_i^{m_i} g$, $i = 1, \dots, n$.

Wenn wir $m := \max\{m_1, \dots, m_n\}$ setzen, können wir bequemer schreiben

$$s_i^m f = s_i^m g$$

für alle $i = 1, \dots, n$ (einfach die gegebenen Gleichungen erweitern, mit $s_i^{m-m_i}$).

Multipliziert man $(s_1 + \dots + s_n)^{n(m-1)+1}$ aus, sieht man, dass man

$$1 = (s_1 + \dots + s_n)^{n(m-1)+1} = \sum_{i=1}^n a_i s_i^m$$

für gewisse $a_1, \dots, a_n \in R$ schreiben kann.

Somit folgt:

$$f = 1 \cdot f = \sum_{i=1}^n a_i s_i^m f = \sum_{i=1}^n a_i s_i^m g = 1 \cdot g = g,$$

das war zu zeigen.

Blatt 8, Aufgabe 4 (Forts.)

(b) R komm. Ring, $s_1, \dots, s_n$ Zerlegung der Eins, $f \in R$.

Beh.: f ist in R invertierbar $\iff$ f ist in $R[s_i^{-1}]$ invertierbar, für alle $i = 1, \dots, n$.

Bem.: Die Aussage, dass f in R invertierbar ist, bedeutet

$$\exists g \in R: \quad fg = gf = 1 \quad (\text{in } R).$$

Die Aussage, dass f in $R[s_i^{-1}]$ invertierbar ist, bedeutet, dass $\frac{f}{1} \in R[s_i^{-1}]$ invertierbar ist, also dass

$$\exists g \in R[s_i^{-1}]: \quad g \frac{f}{1} = \frac{f}{1} g = 1 \quad (\text{in } R[s_i^{-1}]).$$

Bew.: „$\Rightarrow$": Die Lokalisierungen $R[s_i^{-1}]$, $i = 1, \dots, n$, kommen zusammen mit den Ringhomomorphismen

$$\varphi_i : R \longrightarrow R[s_i^{-1}]$$
$$r \longmapsto \frac{r}{1}.$$

Da Bilder invertierbarer Ringelemente unter Ringhomomorphismen wieder invertierbar sind, folgt sofort, dass

$$\frac{f}{1} = \varphi_i(f) \in R[s_i^{-1}]$$

invertierbar ist.

„$\Leftarrow$": Nach Voraussetzung gibt es Ringelemente $g_i \in R[s_i^{-1}]$ mit

$$g_i \cdot \frac{f}{1} = \frac{f}{1} \cdot g_i = 1 \quad \text{in } R[s_i^{-1}].$$

Um die Proposition über die eindeutige Verklebbarkeit aus der Vorlesung (7.59) anzuwenden, zeigen wir

$$g_i = g_j \quad \text{in } R[s_i^{-1} s_j^{-1}]$$

für alle $i, j = 1, \dots, n$. Damit ist gemeint

$$\varphi_{i \to ij}(g_i) = \varphi_{j \to ij}(g_j),$$

wobei

$$\varphi_{i \to ij}: R[s_i^{-1}] \longrightarrow R[s_i^{-1} s_j^{-1}]$$
$$\varphi_{j \to ij}: R[s_j^{-1}] \longrightarrow R[s_i^{-1} s_j^{-1}]$$

die kanonischen Ringhomomorphismen sind.

Dazu: Wegen $g_i \cdot f/_1 = f/_1 \cdot g_i = 1$ in $R[s_i^{-1}]$ gilt auch $\varphi_{i \to ij}(g_i \cdot f/_1) = \varphi_{i \to ij}(g_i) \cdot \frac{f}{1} = \frac{f}{1} \cdot \varphi_{i \to ij}(g_i)$

Somit ist $\varphi_{i \to ij}(g_i)$ ein Inverses von $f/_1$ in $R[s_i^{-1} s_j^{-1}]$. $\quad \parallel \; \varphi_{i \to ij}(\frac{f}{1} \cdot g_i) \; \parallel \; 1$ in $R[s_i^{-1} s_j^{-1}]$

Analog ist $\varphi_{j \to ij}(g_j)$ ein Inverses von $f/_1$ in $R[s_i^{-1} s_j^{-1}]$.

Da Inverse eindeutig sind, folgt $\varphi_{i \to ij}(g_i) = \varphi_{j \to ij}(g_j)$.

$\downarrow$

Blatt 8, Aufgabe 4 (Forts.)

Somit gibt es nach Vorlesung ein
$g \in R$ mit $g = g_i$ in $R[s_i^{-1}]$ für alle $i = 1, \ldots, n$.

Wir zeigen jetzt, dass g in der Tat ein Inverses von f ist; dann ist nämlich f invertierbar und wir sind fertig.

Also zu zeigen: $fg = gf = 1$ in R.
Nach Teilaufgabe (a) genügt es dazu zu zeigen, dass
$fg = gf = 1$ in $R[s_i^{-1}]$
Das ist klar:
in $R[s_i^{-1}]$: $fg = fg_i = 1 = g_i f = gf$.

Vorschlag zu Aufgabe 5 von Blatt 8

Teilaufgabe (I)

R kommutativer Ring, $S \subseteq R$ multiplikativ abgeschlossene Menge.

Frage: Welche Probleme hat die Definition

$$\frac{a}{s} = \frac{b}{t} \quad :\Leftrightarrow \quad at = bs?$$

Dazu: Ganz allgemein erwartet man von einer Definition des Symbols „=“, dass sie reflexiv, symmetrisch und transitiv ist, denn diese Eigenschaften verwendet man ständig, wenn man mit Gleichheiten arbeitet.

Die vorgeschlagene Definition führt zwar noch zu einer reflexiven und symmetrischen Relation, allerdings ist die Transitivität im Allgemeinen verletzt:

Gelte $\frac{a}{s} = \frac{b}{t}$ und $\frac{b}{t} = \frac{c}{u}$, wir wollen $\frac{a}{s} = \frac{c}{u}$ zeigen.

Nach Voraussetzung wissen wir $at = bs$ und $bu = ct$. Somit gilt die Rechnung

$$t \cdot au = u \cdot at = u \cdot bs = s \cdot bu = s \cdot ct = t \cdot cs.$$

Im Allgemeinen folgt daraus aber nicht die Behauptung $au = cs$, denn im Allgemeinen muss t nicht notwendigerweise regulär sein.

Bem.: Der Grund, wieso die in dieser Aufgabe gegebene Definition im Spezialfall $R = \mathbb{Z}$ und $S = \mathbb{Z} \setminus \{0\}$ (also den üblichen Brüchen) doch funktioniert, ist, dass in $\mathbb{Z}$ bis auf die Null alle Zahlen reguläre Elemente sind.

Zur Erinnerung: Denkt man nur an Zahlen, so ist das Konzept der Nicht-Regularität von Ringelementen sicherlich sehr ungewohnt. Bei Matrizen aber kennt man ja da Phänomen, beispielsweise gilt

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

Teilaufgabe (II)

Frage: Warum ist es nicht so einfach, Lokalisierungen nichtkommutativer Ringe zu definieren?

Dazu: Zunächst mal erscheint die Definition der Gleichheit zweier Brüche der Vorlesung,

$$\frac{a}{s} = \frac{b}{t} \quad :\Leftrightarrow \quad uat = ubs \text{ für ein } u \in S,$$

im nichtkommutativen Kontext willkürlich: Genauso denkbar wären

1. $\frac{a}{s} = \frac{b}{t} \quad :\Leftrightarrow \quad uat = usb$ für ein $u \in S$,
2. $\frac{a}{s} = \frac{b}{t} \quad :\Leftrightarrow \quad uta = usb$ für ein $u \in S$,

3. $\frac{a}{s} = \frac{b}{t} \quad :\Leftrightarrow \quad uta = ubs$ für ein $u \in S$,
4. $\frac{a}{s} = \frac{b}{t} \quad :\Leftrightarrow \quad tau = bsu$ für ein $u \in S$,
5. u. s. w.

Keine dieser Definitionen führt zu einer Äquivalenzrelation.

Zum anderen ist nicht mal im Spezialfall, dass s invertierbar ist, klar, was der Bruch $\frac{a}{s}$ bedeuten soll: Sowohl $s^{-1}\,a$ als auch $a\,s^{-1}$ sind denkbar, man spricht von Links- und Rechtsdivision.

Bem.: In der homologischen Algebra definiert man zur Kategorie $\mathrm{Kom}(\mathcal{A})$ der Kettenkomplexe mit Objekten in einer abelschen Kategorie $\mathcal{A}$ die lokalisierte Kategorie $\mathrm{Kom}(\mathcal{A})[S^{-1}]$ nach der Klasse der sog. Quasiisomorphismen. Da die Verkettung von Abbildungen i. A. nicht kommutativ ist, gibt es dort eine ähnliche Schwierigkeit.

Anmerkung zu Aufgabe 1 von Blatt 9

Zu Teilaufgabe (b): Man kann sich noch überlegen (das ist nicht verlangt, hilft aber für (d)), dass es für alle $j \in I$ kanonisch definierte R-Algebrenhomomorphismen

$$\lambda_j \colon A_j \longrightarrow \varinjlim A_i$$

gibt, welche außerdem die Eigenschaft

$$\lambda_k \circ \phi_{jk} = \lambda_j$$

für alle $j, k \in I$ mit $j \leq k$ erfüllen. Die ϕ_{jk} bezeichnen dabei die Strukturmorphismen des gerichteten Systems $(A_i)_{i \in I}$.

Zu Teilaufgabe (d): Die Aufgabenstellung muss noch leicht verschärft werden, sonst funktioniert (e) nicht. Die eigentlich zu zeigende universelle Eigenschaft lautet: Zu jeder R-Algebra B zusammen mit R-Algebrenhomomorphismen

$$\psi_i \colon A_i \longrightarrow B$$

für alle $i \in I$, welche

$$\psi_j \circ \phi_{ij} = \psi_i$$

für alle $i, j \in I$ mit $i \leq j$ erfüllen, gibt es genau einen R-Algebrenhomomorphismus

$$\psi \colon \varinjlim A_i \longrightarrow B$$

mit der Eigenschaft

$$\psi \circ \lambda_i = \psi_i \tag{1}$$

für alle $i \in I$. Dabei bezeichnet λ_i die R-Algebrenhomomorphismen von oben.

Tipp: Man kann die gesuchte Abbildung ψ kanonisch definieren und muss dann nur noch nachrechnen, dass alle geforderten Eigenschaften erfüllt sind. Um die Eindeutigkeit (aus „genau ein") zu zeigen, muss man die Bedingung (1) verwenden.

Zu Teilaufgabe (e): Zu zeigen ist hier: Sei X eine R-Algebra zusammen mit R-Algebrenhomomorphismen

$$\widetilde{\lambda}_i \colon A_i \longrightarrow X$$

für alle $i \in I$, welche

$$\widetilde{\lambda}_j \circ \phi_{ij} = \widetilde{\lambda}_i$$

für alle $i, j \in I$ mit $i \leq j$ erfüllen und gelte die universelle Eigenschaft aus (d) (für X). Dann ist X kanonisch isomorph zu $\varinjlim A_i$.

Tipp: Man kann ausnutzen, dass X und $\varinjlim A_i$ beide die (jeweilige) universelle Eigenschaft erfüllen. Auf diese Weise kann man schonmal R-Algebrenhomomorphismen von X nach $\varinjlim A_i$ und umgekehrt erhalten. Dann muss man noch zeigen, dass ihre Verkettung (in beiden Reihenfolgen) die jeweilige Identität ist.

Blatt 9, Aufgabe 6

Beh.: $3+2i \in \mathbb{Z}[i]$ ist irreduzibel.

Bew.: Definiere die Normabbildung

$$N: \mathbb{Z}[i] \longrightarrow \mathbb{N}_{\geq 0}$$
$$a+ib \longmapsto a^2+b^2 = |a+ib|^2$$

komplexer Betrag

Es gilt:

1) $N(1) = 1$

2) $N(uv) = N(u)N(v)$

3) $N(u) = 1 \iff u$ in $\mathbb{Z}[i]$ invertierbar.

Bew. zu 3):

„$\Rightarrow$": Sei $N(u) = 1$ mit $u = a+ib$.

$\Rightarrow a^2+b^2 = 1$

$\Rightarrow (a^2 = 1,\ b = 0)$ oder $(a = 0,\ b^2 = 1)$

$\Rightarrow u = 1$ oder $u = -1$ oder $u = i$ oder $u = -1$

$\Rightarrow u$ ist in $\mathbb{Z}[i]$ invertierbar.

„$\Leftarrow$": Sei u in $\mathbb{Z}[i]$ invertierbar, also $u \in \mathbb{Z}[i]^\times = \{1, -1, i, -i\}$.
Dann gilt in jedem der vier möglichen Fälle $N(u) = 1$.

Nun zum Beweis der Behauptung.

$3+2i$ ist regulär, da in $\mathbb{Z}[i]$ bis auf die 0 alle Elemente regulär sind.

$3+2i$ ist nicht invertierbar, denn $N(3+2i) = 9+4 = 13 \neq 1$.

Sei $3+2i \sim uv$ („$\sim$": „assoziiert zu").

$\Rightarrow 3+2i = x\,uv$ für ein $x \in \mathbb{Z}[i]^\times$.

$$\Rightarrow \underset{13}{\underset{\shortparallel}{N(3+2i)}} = \underset{1}{\underset{\shortparallel}{N(x)}}\, N(u)\, N(v)$$

$$\Rightarrow 13 = \underbrace{N(u)}_{\geq 0}\ \underbrace{N(v)}_{\geq 0} \quad \underset{\text{13 Primzahl}}{\Longrightarrow} \quad N(u) = 1 \text{ oder } N(v) = 1$$

$N(u) = 1 \Downarrow$ u invertierbar $\Downarrow$ $3+2i \sim v$ ✓

$N(v) = 1 \Downarrow$ v invertierbar $\Downarrow$ $3+2i \sim u$ ✓

Blatt 8, Aufgabe 7

Zur Erinnerung:

Sei R ein Ring mit eindeutiger Primfaktorzerlegung.
Dann ist der Inhalt definiert als:

$$c: R[X]\setminus\{0\} \longrightarrow R/\sim = \{[r] \mid r \in R\}, \text{ wobei } [r]=[\tilde{r}] :\Leftrightarrow r\sim\tilde{r}$$
$$f \longmapsto \text{ein ggT der Koeffizienten von } f$$

$:\Leftrightarrow r$ ist zu $\tilde{r}$ assoziiert
$:\Leftrightarrow r = u\tilde{r}$ für ein $u\in R^\times$

Da der größte gemeinsame Teiler nur bis auf Assoziiertheit definiert ist, kann man nicht sagen:

$$c: R[X]\setminus\{0\} \longrightarrow R.$$

Ges.: Fortsetzung von c auf $K[X]\setminus\{0\}$, sodass auch die Fortsetzung multiplikativ ist.
Dabei sei $K = \text{Quot } R = \{\frac{r}{s} \mid r\in R, s\in R, s\neq 0\}$ der Quotientenkörper von R.

Dazu: Definiere:

$$\bar{c}: K[X]\setminus\{0\} \longrightarrow K/\approx = \{[k] \mid k\in K\}, \text{ wobei } [k]=[\tilde{k}] :\Leftrightarrow k\approx\tilde{k}$$
$$f \longmapsto c(af)/a,$$

$:\Leftrightarrow k = u\tilde{k}$ für ein $u\in R^\times$

nicht $K^\times$! Das wäre nicht sinnvoll, denn $K^\times = K\setminus\{0\}$.

wobei $a\in R$ irgendein Element ist, sodass $af\in R[X]\setminus\{0\}$.
Die Division soll in K durchgeführt werden.

Dann gilt:

1) Wohldefiniertheit, erster Teil:
Da wir als a beispielsweise das Produkt aller in f auftretenden Nenner wählen können, ist die Existenz eines a gesichert.

2) Wohldefiniertheit, zweiter Teil:
Seien $a, \tilde{a}\in R$ derart, dass $af, \tilde{a}f\in R[X]$.
Zu zeigen ist, dass $c(af)/a = c(\tilde{a}f)/\tilde{a}$.
Dazu folgende Rechnung:

$$\frac{c(af)}{a} \underset{b\neq 0}{=} \frac{b\,c(af)}{ba} \underset{c \text{ multiplikativ, } b\in R\setminus\{0\}}{=} \frac{c(baf)}{ba} \overset{c \text{ multiplikativ, } a\in R\setminus\{0\}}{=} \frac{a\,c(bf)}{ba} = \frac{c(bf)}{b}.$$

3) $\overline{c}$ ist in der Tat eine Fortsetzung von c, denn:

Sei $f \in R[X] \setminus \{0\}$ beliebig.

Dann gilt:

$$\overline{c}(f) \underset{\substack{1 \text{ hat die Eigenschaft,} \\ \text{dass } 1 \in R \text{ und } 1f \in R[X]\setminus\{0\}}}{=} c(1f)/1 = c(f).$$

4) $\overline{c}$ ist multiplikativ, denn:

Seien $f, g \in K\cancel{R}[X] \setminus \{0\}$ beliebig.

Seien $a, b \in R$ so, dass $af, bg \in R[X] \setminus \{0\}$.

Somit gilt:

$$\overline{c}(fg) \underset{\substack{(ab) \in R \text{ hat die} \\ \text{Eigenschaft, dass} \\ (ab)(fg) \in R[X]\setminus\{0\}}}{=} \frac{c(ab\,fg)}{ab} \underset{\substack{c \text{ ist multiplikativ,} \\ af,\, bg \in R[X]\setminus\{0\}}}{=} \frac{c(af)\; c(bg)}{a \cdot b} = \frac{c(af)}{a} \cdot \frac{c(bg)}{b} = \overline{c}(f)\; \overline{c}(g).$$

Bem.: Es gibt nur obige Möglichkeit, um c multiplikativ auf $K[X] \setminus \{0\}$ fortzusetzen.

Bew.: Sei $\tilde{c}: K[X] \setminus \{0\} \longrightarrow K/\mathcal{E}$ irgendeine multiplikative Fortsetzung von c.

Sei $f \in K[X] \setminus \{0\}$ beliebig, wir zeigen $\tilde{c}(f) = \overline{c}(f)$.

Sei dazu $a \in R$ so, dass $af \in R[X] \setminus \{0\}$ (Existenz gesichert).

Dann gilt:

$$\tilde{c}(f) = \tilde{c}\left(\tfrac{1}{a}\, a\, f\right) \underset{\tilde{c} \text{ multiplikativ}}{=} \underbrace{\tilde{c}\left(\tfrac{1}{a}\right)}_{= \frac{1}{a}} \underbrace{\tilde{c}(af)}_{= c(af)} = \tfrac{1}{a}\, c(af) = \overline{c}(f).$$

$= c(af)$, denn $af \in R[X] \setminus \{0\}$ und $\tilde{c}$ Fortsetzung von c

$= \frac{1}{a}$, denn $\tilde{c}(1) \underset{\tilde{c} \text{ multiplikativ}}{=} 1 = \tilde{c}(a \cdot \tfrac{1}{a}) \underset{\tilde{c} \text{ multiplikativ}}{=} \underbrace{\tilde{c}(a)}_{\substack{= c(a) \\ = a}} \tilde{c}\left(\tfrac{1}{a}\right) = a\, \tilde{c}(1/a)$

$\tilde{c}$ Fortsetzung von c, $a \in R\setminus\{0\}$

Bem.: Es gibt auch andere Möglichkeiten, die Fortsetzung $\tilde{c}$ zu definieren.
Die Behauptung garantiert, dass diese stets dieselben Ergebnisse liefern.

Bsp.: Sei $R = \mathbb{Z}$, somit $K = \mathbb{Q}$.
Dann gilt:

$$\tilde{c}\left(\tfrac{1}{3}X^2 - 5X + \tfrac{1}{8}\right) = c\left(8X^2 - 120X + 3\right) / (3 \cdot 8) = 1/24.$$

Blatt 9, Aufgabe 9

R komm. Ring, $N \in \mathbb{N}$.

Beh.: Die Abbildung

$$\tilde{\Phi} : \{ f \in R[X,Y] \mid f \text{ hat in } X \text{ Grad echt kleiner als } N \} \longrightarrow R[X]$$

$$f \longmapsto f(X, X^N)$$

also für X X einsetzen, für Y X^N einsetzen

ist injektiv.

Bew: Seien f, g zwei beliebige Elemente der Definitionsmenge mit $\tilde{\Phi}(f) = \tilde{\Phi}(g)$. Wir müssen zeigen, dass $f = g$.

Nach Voraussetzung lässt sich f schreiben als

$$f = \sum_{i=0}^{?} a_i(X)\, Y^i \quad \text{für gewisse Polynome } a_i \in R[X] \text{ mit } \deg a_i < N,$$

analog g als

$$g = \sum_{i=0}^{?} b_i(X)\, Y^i \quad \text{für gewisse Polynome } b_i \in R[X] \text{ mit } \deg b_i < N.$$

Betrachte:

$$\tilde{\Phi}(f) = \sum_{i=0}^{?} \underbrace{a_i(X)\, X^{Ni}} = \sum_{i=0}^{?} \underbrace{b_i(X)\, X^{Ni}} = \tilde{\Phi}(g)$$

hier können nur die X-Potenzen $X^{Ni}, X^{Ni+1}, \ldots, X^{Ni+(N-1)}$ vorkommen.

Somit kommen in jedem Summanden unterschiedliche X-Potenzen vor!
Das erlaubt es, mit Koeffizientenvergleich

$$a_i = b_i \quad \text{für alle } i = 0, \ldots, ?$$

zu folgern. Also gilt $f = g$.

Blatt 10, Aufgabe 1 (komplizierte Lösung)

(a) Ges: Primfaktorzerlegung von $\underbrace{X^4+4Y^4}_{=:f}$ in $\mathbb{Z}[X,Y]$.

Dazu: Im Verfahren der Vorlesung können wir $N=5$ wählen und also

$$X^4+4(X^5)^4 = X^4+4X^{20} \in \mathbb{Z}[X]$$

faktorisieren. Das gibt:

$$X^4+4X^{20} = X^4(4X^{16}+1) = X^4\overbrace{(2X^8-2X^4+1)}^{=:p}\overbrace{(2X^8+2X^4+1)}^{=:q}$$

Dass die beiden hinteren Faktoren irreduzibel sind, kann man beispielsweise mit dem Verfahren über die elementarsymmetrischen Funktionen sehen, per Hand dauert das jedoch recht lange.

Mögliche Aufteilungen:

1) $X^4pq \cdot 1$: trivial.

2) $X^4p \cdot q = (2X^{12}-2X^8+X^4)\cdot(2X^8+2X^4+1)$,

kommt von $(2X^2Y^2-2X^3Y+X^4)\cdot(2X^3Y+2X^4+1)$,

das ist aber nicht gleich f.

3) $X^4q \cdot p = (2X^{12}+2X^8+X^4)\cdot(2X^8-2X^4+1)$,

scheitert ähnlich.

4) $X^4 \cdot pq = X^4\cdot(4X^{16}+1)$,

kommt von $X^4\cdot(4XY^3+1)$, scheitert.

5) $X^3p \cdot Xq = (2X^{11}-2X^7+X^3)(2X^9+2X^5+X)$,

kommt von $(2XY^2-2X^2Y+X^3)(2X^4Y+2Y+X)$, scheitert.

6) $X^3q \cdot Xp$ scheitert ebenso.

7) $X^3 \cdot Xpq$ auch.

8) $X^2p \cdot X^2q = (2X^{10}-2X^6+X^2)(2X^{10}+2X^6+X^2)$,

kommt von $(2Y^2-2XY+X^2)(2Y^2+2XY+X^2)$,

funktioniert!

Wir können also an dieser Stelle abbrechen, eine Zerlegung von f ist

$$f = (2Y^2-2XY+X^2)(2Y^2+2XY+X^2).$$

Wir müssen jetzt noch prüfen, ob diese Faktoren irreduzibel sind. Fasst man diese als Polynome in X (über $\mathbb{Z}[Y]$) auf, ist das klar mit Eisenstein $(p=2)$. Oder komplizierter:

Im Verfahren der Vorlesung können wir $N=3$ wählen und müssen dann

$$2(X^3)^2 - 2X(X^3) + X^2 = 2X^6 - 2X^4 + X^2$$

faktorisieren. Das gibt:

$$2X^6 - 2X^4 + X^2 = X^2 \overbrace{(2X^4 - 2X^2 + 1)}^{=:r}$$

Der hintere Term ist irreduzibel, das kann man mit den Verfahren aus Algebra I sehen.

Mögliche Aufteilungen:

1) $X^2 r \cdot 1$: trivial.

2) $X^2 \cdot r$, kommt von $X^2 \cdot (2XY - 2X^2 + 1)$, scheitert.

3) $X \cdot Xr$, kommt von $X \cdot (2X^2Y - 2Y + 1)$, scheitert.

4) $Xr \cdot X$, genauso.

5) $r \cdot X^2$, genauso.

6) $1 \cdot X^2 r$, trivial.

Also ist das Polynom $2Y^2 - 2XY + X^2 \in \mathbb{Z}[X,Y]$ irreduzibel.
Analog kann man den anderen Faktor behandeln.

(b) Bh.: $X^2 + Y \in \mathbb{Z}[X,Y]$ ist irreduzibel.

Bew.: Klar mit Eisenstein: Aufgefasst als Element von $(\mathbb{Z}[Y])[X]$, $p = Y$.
Kompliziert: Im Verfahren wählen wir $N=3$, dann ergibt sich

$$X^2 + X^3 = X^2(1+X)$$

als irreduzible Zerlegung. Mögliche Aufteilungen:

1) $X^2(1+X) \cdot 1$: trivial.

2) $X(1+X) \cdot X$: kommt von $(X + X^2) \cdot X$, scheitert.

3) $X^2 \cdot (1+X)$: kommt von $X^2 \cdot (1+X)$, scheitert.

4), 5), 6) wie oben, scheitern.

Damit ist gezeigt, dass $X^2 + Y$ in $\mathbb{Z}[X,Y]$ irreduzibel ist.

Blatt 10, Aufgabe 3

R Integritätsbereich, $I \subseteq R$ Ideal mit $I \neq (1)$.

$f \in R[X]$ normiert.

Sei φ die Abbildung

$$\begin{aligned} \varphi: R[X] &\longrightarrow (R/I)[X] \\ f &\longmapsto \varphi(f) \\ \sum a_k X^k &= f, \quad \varphi(f) = \sum [a_k] X^k \end{aligned}$$

Es ist φ ein Ringhomomorphismus.

Sei $\varphi(f) \in (R/I)[X]$ irreduzibel.

Beh.: $f \in R[X]$ ist irreduzibel.

Bew.: 1) f ist regulär, da normiert. (Oder: Da $\neq 0$ und R ein Integritätsbereich ist.)

2) f ist nicht invertierbar, denn sonst wäre $\varphi(f)$ invertierbar, aber $\varphi(f)$ ist ja irreduzibel.

3) Sei $f \sim gh$ für $g, h \in R[X]$.

„assoziiert zu"

$\Rightarrow$ Leitkoeffizient von f $\sim$ Leitkoeffizient von g $\cdot$ Leitkoeffizient von h

R Int'bereich

Leitkoeffizient von f $= 1$

$\Rightarrow$ Leitkoeffizienten von g und h sind invertierbar, liegen somit insbesondere nicht in I, da sonst $I = (1)$ wäre. $(*)$

Da φ ein Ringhomomorphismus ist, folgt ~~...~~

$$\varphi(f) \sim \varphi(g)\,\varphi(h).$$

Da $\varphi(f)$ irreduzibel ist, folgt $\varphi(f) \sim \varphi(g)$ oder $\varphi(f) \sim \varphi(h)$.

O.E.d.A. trete der erste Fall ein (sonst Rollen von g, h vertauschen).

$\Rightarrow$ $\varphi(h)$ invertierbar, denn: $\varphi(f) = u\,\varphi(g)\,\varphi(h)$ für ein $u \in (R/I)[X]^\times$, außerdem $\varphi(f) = v\,\varphi(g)$ für ein $v \in (R/I)[X]^\times$.

$$\Rightarrow u\varphi(g)\varphi(h) = v\,\varphi(g) \Rightarrow u\,\varphi(h) = v \Rightarrow \varphi(h) \text{ invertierbar}$$

$\varphi(g)$ regulär, da $\varphi(f)$ regulär und $\varphi(f) \sim \varphi(g)$, da $\varphi(f)$ normiert, da f normiert

allgemein gilt in komm. Ringen: xy invertierbar $\Leftrightarrow$ x, y invertierbar

$\Rightarrow$ $\varphi(h)$ konstant, $h = c + \tilde{h}$ für ein $\tilde{h} \in I[X]$, $c \in R$

Sollte $\deg \tilde{h} \geq 1$ sein, dann

Leitkoeffizient(h) = Leitkoeffizient$(\tilde{h}) \in I$,

im Widerspruch zu $(*)$.

Also $\deg \tilde{h} = 0$, $\tilde{h} = d$ für ein $d \in R$, $d = h$ = (Leitkoeffizient von h) invertierbar.

Fazit: h ist invertierbar. Das war zu zeigen.

Beispiel: Das Polynom $X^2 + Y \in \mathbb{Q}[X, Y]$ ist irreduzibel,
denn für die Reduktion modulo $I = (Y-1)$ gilt:

$$\varphi(X^2+Y) = X^2 + Y = X^2 + Y - 1 + 1 = X^2 + 1 \in \mathbb{Q}[X,Y]/(Y-1) \cong \mathbb{Q}[X]$$

bekanntermaßen irreduzibel

Verfeinerungen von Zerlegungen der Eins

Sei R ein kommutativer Ring und sei

$$1 = s_1 + \cdots + s_n$$

eine Zerlegung der Eins von R, $s_1, \ldots, s_n \in R$. Seien weiter für jeden der lokalisierten Ringe $R[s_i^{-1}]$ Zerlegungen

$$1 = t_{i,1} + \cdots + t_{i,m_i}$$

der Eins von $R[s_i^{-1}]$ gegeben, $t_{i,1}, \ldots, t_{i,m_i} \in R[s_i^{-1}]$.

Behauptung. *Dann gibt es eine Zerlegung*

$$1 = u_1 + \cdots + u_N$$

von R, $u_1, \ldots, u_N \in R$ derart, dass es zu jedem der lokalisierten Ringe $R[u_j^{-1}]$ jeweils ein $i \in \{1, \ldots, n\}$ und ein $k \in \{1, \ldots, m_i\}$ gibt, sodass s_i und $t_{i,k}$ in $R[u_j^{-1}]$ invertierbar sind.

Beweis. Jedes $t_{i,k}$ hat die Form $t_{i,k} = t'_{i,k}/s_i^{\ell_{i,k}}$ für ein $t'_{i,k} \in R$ und $\ell_{i,k} \geq 0$. Ohne Einschränkung können wir davon ausgehen, dass die $\ell_{i,k}$ für alle $k \in \{1, \ldots, m_i\}$ gleich sind (nötigenfalls einfach die Brüche noch mit geeigneten Potenzen von s_i erweitern). Somit können wir $t_{i,k} = t'_{i,k}/s_i^{\ell_i}$ für ein allen k gemeinsamem Exponenten $\ell_i \geq 0$ schreiben.

Dass die $t_{i,k}$, $k = 1, \ldots, m_i$ eine Zerlegung der $1 \in R[s_i^{-1}]$ bilden, bedeutet, dass wir einen Exponenten $r_i \geq 0$ mit

$$s_i^{r_i} s_i^{\ell_i} = s_i^{r_i}(t'_{i,1} + \cdots + t'_{i,m_i})$$

finden. Sei $r := \max_{i=1,\ldots,n}(r_i + \ell_i)$. Dann können wir für alle $i \in \{1, \ldots, n\}$

$$s_i^r = t''_{i,1} + \cdots + t''_{i,m_i}$$

schreiben, wenn wir $t''_{i,k} := s_i^{r-\ell_i} t'_{i,k} \in R$ setzen.

Nach der üblichen Überlegung, wie wir sie schonmal in Übung und Vorlesung hatten, finden wir Koeffizienten $b_1, \ldots, b_n \in R$ derart, dass

$$1 = \sum_{i=1}^{n} b_i s_i^{r+1} = \sum_{i=1}^{n} \sum_{k=1}^{m_i} b_i s_i t''_{i,k}$$

gilt. Das ist unsere gesuchte Zerlegung der Eins, denn in $R[(b_i s_i t''_{i,k})^{-1}]$ sind $b_i s_i t''_{i,k}$ und damit insbesondere s_i und $t''_{i,k}$, und damit wiederum $t_{i,k}$, invertierbar. $\square$

Aufgabe 4(b)

Gesucht: Zerlegung der Eins in $R = \mathbb{Z}[\sqrt{-13}]$ derart, dass das Ideal $(7, u)$ mit $u := 1 + \sqrt{-13}$ in den lokalisierten Ringen jeweils ein Hauptideal ist.

Es gilt $u \cdot \overline{u} = (1 + \sqrt{-13}) \cdot (1 - \sqrt{-13}) = 1 + 13 = 14$.

Dazu: Wir wählen $1 = 8 + (-7)$ als Zerlegung der Eins. In $R[8^{-1}]$ gilt dann

$$(7, u) = (14, u) = (u\overline{u}, u) = (u),$$

wobei der erste Schritt deswegen folgt, weil mit 8 auch 2 in $R[8^{-1}]$ invertierbar ist, und in $R[(-7)^{-1}]$ gilt

$$(7, u) = (1),$$

da 7 in $R[(-7)^{-1}]$ invertierbar ist.

Bemerkung zum Vorgehen: Die Zahl u erfüllt die Beziehung $u^2 - 2u + 14 = 0$, daher gilt $2 \cdot 7 = 14 = 2u - u^2$. So kann man zum Gedanken geleitet werden, dass es gut wäre, wenn die Zahl 2 invertierbar wäre, denn dann wäre 7 einfach ein Vielfaches von u (nämlich das $(u - u^2/2)$-fache).

Nun benötigt man für eine nichttriviale Zerlegung der Eins natürlich mindestens zwei Zahlen, die dann in den lokalisierten Ringen invertierbar sein sollen und sich zur Eins aufaddieren müssen. Daher kann man sich auf die Suche nach einer zu 2 teilerfremden Zahl begeben, denn teilerfremde ganze Zahlen induzieren ja eine Darstellung der Eins.

Ein Beispiel für eine Zahl, welche teilerfremd zu 2 ist, ist 7. Diese hat den schönen Nebeneffekt, dass es gut ist, wenn sie invertierbar ist, denn dann wird das Ideal zum Einsideal. Eine durch die Teilerfremdheit von 2 und 7 induzierte Darstellung der Eins ist $1 = 4 \cdot 2 + (-1) \cdot 7$, das ist dann die gewünschte Zerlegung.

Aufgabe 7

Wir benötigen zwei Vorüberlegungen.

Wenn wir konstruktiv arbeiten wollen, benötigen wir sogar noch eine weitere:

Behauptung. *Ein endlich erzeugtes Ideal $\mathfrak{a} = (x_1, \ldots, x_n) \subseteq R$ eines Integritätsbereichs R ist genau dann nicht das Nullideal, wenn es ein reguläres Element enthält.*

Beweis. Die Rückrichtung ist klar. Zur Hinrichtung können wir, da R ein Integritätsbereich ist, von jedem Erzeuger x_i prüfen, ob er null oder regulär ist. Der Fall, dass alle Erzeuger null sind, kann nach Voraussetzung nicht eintreten, daher gibt es ein Erzeuger, der nicht nicht null und somit regulär ist. □

Behauptung. *Sei R ein prüferscher Bereich und seien $\mathfrak{p}, \mathfrak{q}$ Primideale in R mit $\mathfrak{p} \subseteq \mathfrak{q}$. Ferner enthalte $\mathfrak{p}$ ein reguläres Element. Dann gilt sogar schon $\mathfrak{p} = \mathfrak{q}$.*

Beweis. Da R prüfersch ist, können wir $\mathfrak{p} = (\mathfrak{p} : \mathfrak{q})(\mathfrak{p} + \mathfrak{q}) = (\mathfrak{p} : \mathfrak{q}) \cdot \mathfrak{q}$ schreiben. Wegen der Primalität von $\mathfrak{p}$ gilt $\mathfrak{p} = \mathfrak{p} : \mathfrak{q}$ oder $\mathfrak{p} = \mathfrak{q}$. Im zweiten Fall sind wir fertig. Der erste kann nicht eintreten: Denn dann würde $\mathfrak{p} \cdot (1) = (\mathfrak{p} : \mathfrak{q}) \cdot \mathfrak{q} = \mathfrak{p}\mathfrak{q}$ folgen, also, da $\mathfrak{p}$ nach den Voraussetzungen invertierbar ist, $(1) = \mathfrak{q}$. □

Behauptung. *Sei R ein prüferscher Bereich. Dann sind Zerlegungen von Idealen (welche ein reguläres Element enthalten) in Primideale bis auf Umordnung eindeutig, falls sie existieren.*

Beweis. Sei $\mathfrak{a}$ ein Ideal, welches ein reguläres Element enthält, und seien $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ und $\mathfrak{q}_1, \ldots, \mathfrak{q}_m$ Primideale mit

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_n = \mathfrak{q}_1 \cdots \mathfrak{q}_m.$$

Nach der ersten Vorüberlegung enthalten auch alle aufgelisteten Primideale jeweils ein reguläres Element, denn es kann jeweils nicht der Fall sein, dass sie das Nullideal sind.

Insbesondere gilt $\mathfrak{q}_1 \cdots \mathfrak{q}_m \subseteq \mathfrak{p}_1$, also gibt es wegen der Primidealeigenschaft von $\mathfrak{p}_1$ ein $i \in \{1, \ldots, m\}$ mit $\mathfrak{q}_i \subseteq \mathfrak{p}_1$. Nach der Vorüberlegung gilt sogar $\mathfrak{p}_1 = \mathfrak{q}_i$, und da $\mathfrak{p}_1 = \mathfrak{q}_i$ invertierbar ist, folgt

$$\mathfrak{p}_2 \cdots \mathfrak{p}_n = \mathfrak{q}_1 \cdots \widehat{\mathfrak{q}_i} \cdots \mathfrak{q}_m.$$

Induktiv folgt die Behauptung. □

Teilaufgabe (α)

Behauptung. *Sei R ein dedekindscher Bereich, in dem jedes endlich erzeugte Ideal $\mathfrak{a} \subseteq R$ irreduzibel oder in echte Faktoren zerlegbar ist. Dann lässt sich jedes nichtverschwindende endlich erzeugte Ideal eindeutig als Produkt von Primidealen schreiben.*

Beweis. Die Eindeutigkeit haben wir bereits oben bewiesen. Zur Existenz können wir prüfen, ob ein gegebenes nichtverschwindendes Ideal $\mathfrak{a} \subseteq R$ irreduzibel ist. Falls ja, sind wir fertig, falls nicht, können wir es in zwei echte Ideale zerlegen. Diese können wir wieder auf Irreduzibilität prüfen, und so weiter.

Wir müssen noch zeigen, dass dieses Verfahren irgendwann endet. Dazu können wir uns die Situation als (nach unten wachsenden) verzweigten Baum veranschaulichen: Ganz oben an die Wurzel setzen wir das gegebene Ideal $\mathfrak{a}$. Die beiden Faktoren von $\mathfrak{a}$ setzen wir als die beiden Kinder der Wurzel. Deren Faktoren fügen wir wiederum als deren Kinder ein, und so weiter.

Insgesamt erhalten wir einen Baum, der mit endlich erzeugten Idealen beschriftet ist. In klassischer Logik gilt nun: Da der Ring R noethersch ist, stabilisiert sich jeder von der Wurzel ausgehende Pfad, da die Ideale entlang eines jeden Pfads aufsteigende Ketten bilden. Insgesamt kommen daher also nur endlich viele Ideale vor, daher endet das angegebene Faktorisierungsverfahren. (Wer die letzte Schlussfolgerung genauer nachlesen will, kann sich auf Wikipedia das Lemma von König anschauen.) □

Teilaufgabe (β)

Eine Vorüberlegung:

Behauptung. *Sei R ein dedekindscher Bereich, in dem jedes endlich erzeugte Ideal, welches nicht das Einsideal ist, maximal ist oder durch ein Ringelement echt zu einem weiteren Ideal, welches nicht das Einsideal ist, erweitert werden kann. Dann liegt jedes endlich erzeugte Ideal, welches nicht das Einsideal ist, in einem maximalen Ideal.*

Beweis. Wir beschreiben ein Verfahren, welches ausgehend von einem gegebenen endlich erzeugten Ideal $\mathfrak{a}$ ein aufsteigende Kette endlich erzeugter Ideale produziert: Ist das gegebene Ideal $\mathfrak{a}$ maximal, so produziere $\mathfrak{a}$. Sonst gibt es ein $x \in R$ mit $\mathfrak{a} \subsetneq \mathfrak{a} + (x) \subsetneq (1)$, produziere $\mathfrak{a} + (x)$. Fahre immer so fort.

Da R noethersch ist, muss die so produzierte Kette eine Stoppstelle aufweisen. Das jeweils neu produzierte Ideal ist aber genau dann gleich dem Ausgangsideal, wenn das Ausgangsideal maximal war. Damit folgt die Behauptung. □

Behauptung. *Sei R ein dedekindscher Bereich, in dem jedes endlich erzeugte Ideal maximal ist oder durch ein Ringelement echt zu einem weiteren Ideal, welches nicht das Einsideal ist, erweitert werden kann. Dann lässt sich jedes nichtverschwindende endlich erzeugte Ideal, welches nicht das Einsideal ist, eindeutig als Produkt von Primidealen schreiben.*

Beweis. Wie produzieren eine aufsteigende Kette endlich erzeugter Ideale nach folgendem Verfahren: Ein gegebenes endlich erzeugtes Ideal $(0) \subsetneq \mathfrak{a} \subsetneq (1)$ prüfen wir auf Maximalität. Falls es maximal ist, produzieren wir $\mathfrak{a}$ und fahren damit fort. Sonst finden wir ein maximales Ideal $\mathfrak{m}$ mit $\mathfrak{a} \subseteq \mathfrak{m}$. Da R prüfersch ist, gilt $\mathfrak{a} = (\mathfrak{a} : \mathfrak{m})(\mathfrak{a} + \mathfrak{m}) = (\mathfrak{a} : \mathfrak{m}) \cdot \mathfrak{m}$. Wir produzieren das über $\mathfrak{a}$ liegende Ideal $(0) \subsetneq \mathfrak{a} : \mathfrak{m} \subsetneq (1)$ und fahren damit fort. (Es kann nicht der Fall sein, dass $\mathfrak{a} = \mathfrak{a} : \mathfrak{m}$. Denn sonst wäre $\mathfrak{a} = (\mathfrak{a} : \mathfrak{m}) \cdot \mathfrak{m} = \mathfrak{a}\mathfrak{m}$ und damit, da $\mathfrak{a}$ invertierbar, $\mathfrak{m} = (1)$.)

Da R noethersch ist, muss diese Kette eine Stoppstelle aufweisen. Das ist genau dann der Fall, wenn das jeweilige Ausgangsideal maximal war. Somit erhalten wir eine endliche Zerlegung als Produkt maximaler Ideale. Da maximale Ideale insbesondere prim sind, folgt die Behauptung. $\square$

Aufgabe 8

Sei R ein prüferscher Bereich, welcher nicht notwendigerweise noethersch ist. Wir benötigen folgende Vorüberlegung:

Behauptung. *Seien $x, y \in R$ zwei beliebige Elemente. Dann gibt es eine Zerlegung $1 = s_1 + \cdots + s_N$ der Eins derart, dass in den lokalisierten Ringen $R[s_i^{-1}]$ jeweils gilt:*

$$x \mid y \quad \textit{oder} \quad y \mid x.$$

Beweis. Wenn x oder y null sind (das können wir prüfen, da R ein Integritätsbereich ist), ist die Behauptung mit der trivialen Zerlegung $1 = 1$ klar.

Zum endlich erzeugten Ideal (x, y) gibt es eine Zerlegung $1 = t_1 + \cdots + t_n$ derart, dass die Erweiterungen dieses Ideals in den lokalisisierten Ringen $R[t_i^{-1}]$ jeweils Hauptideale (d_i) sind. Ohne Einschränkung der Allgemeinheit können wir annehmen, dass alle t_i regulär sind. (Da R ein Integritätsbereich ist, können wir auf Regularität prüfen.)

Für jedes $i \in \{1, \ldots, n\}$ können wir somit Multiplikatoren $a_i, b_i \in R[t_i^{-1}]$ und $u_i, v_i \in R[t_i^{-1}]$ derart finden, dass

$$\begin{aligned} d_i &= a_i x + b_i y \\ x &= u_i d_i \\ y &= v_i d_i \end{aligned}$$

gilt. Da $d_i \neq 0$ und $R[t_i^{-1}]$ auch ein Integritätsbereich ist, können wir

$$1 = a_i u_i + b_i v_i$$

zeigen. Im erneut lokalisierten Ring $R[t_i^{-1}][(a_i u_i)^{-1}]$ ist u_i invertierbar, somit x assoziiert zu d_i und somit x ein Teiler von y. Analog ist y in $R[t_i^{-1}][(b_i v_i)^{-1}]$ ein Teiler von x.

Zu jedem i erhalten wir also jeweils eine Zerlegung der Eins des lokalisierten Rings $R[t_i^{-1}]$. Diese können wir zu einer Zerlegung $1 = s_1 + \cdots + s_{2n}$ der Eins von R zusammenfassen; es gilt dann für alle $j = 1, \ldots, 2n$ jeweils

$$x \mid y \quad \text{oder} \quad y \mid x$$

in $R[s_j]$, das war zu zeigen. □

Als Korollar ergibt sich:

Behauptung. *Seien $x_1, \ldots, x_m \in R$ gegebene Ringelemente. Dann gibt es eine Zerlegung der Eins derart, dass in den lokalisierten Ringen jeweils eines der Elemente ein Teiler aller anderen ist.*

Beweis. (durch Induktion)

Induktionsanfang $m = 1$: Klar.

Induktionsschritt $m \to m+1$: Wir wenden die Induktionsvoraussetzung auf $x_1, \ldots, x_m$ an und betrachten einen festen der sich dadurch ergebenden lokalisierten Ringe. Es sei darin x_j ein Teiler aller $x_1, \ldots, x_m$. Nach der Vorüberlegung finden wir eine Zerlegung der Eins, sodass in den weiter lokalisierten Ringen x_j ein Teiler von x_{m+1} ist oder umgekehrt. In beiden Fällen sind wir fertig. □

Sei $A \in M_{n,m}(R)$ eine Matrix.

Behauptung. *Der Kern von A ist lokal endlich erzeugt.*

Beweis.

1. Ganz allgemein, unabhängig von den Eigenschaften von R, gilt für jede multiplikative Menge $S \subseteq R$:

   $$\ker(A \in M_{n,m}(R[S^{-1}])) \cong (\ker A)[S^{-1}]$$

   Ein Isomorphismus ist durch
   $$\frac{x}{s} \longmapsto \frac{x}{s}$$
   gegeben: Wohldefiniertheit, Injektivität und Homomorphieeigenschaft kann man sich schnell überlegen. Zur Surjektivität sei ein beliebiges Element $\frac{y}{s}$ der rechten Seite vorgegeben. Da $A\frac{y}{s} = \frac{Ay}{s} = 0$, gibt es ein $u \in S$ mit $uAy = 0$, also mit $A(uy) = 0$. Somit gilt $\frac{y}{s} = \frac{uy}{us}$ und $\frac{uy}{us}$ ist ein Element der linken Seite, da uy im Kern von A liegt.

   Diese Vorüberlegung erlaubt folgende Schlussweise: Um zu zeigen, dass der Kern von A lokal endlich erzeugt ist, genügt es, eine Zerlegung der Eins derart anzugeben, dass die Kern der Bilder der Matrizen über den lokalisierten Ringen endlich erzeugt sind.

2. Über beliebigen Integritätsbereichen sind Kerne von (rechteckigen) Diagonalmatrizen stets endlich erzeugt, nämlich genau durch diejenigen Standardeinheitsvektoren e_i, für die der i-te Diagonaleintrag der Matrix null ist.

3. Nun zur eigentlichen Aufgabe. Wir werden eine Zerlegung der Eins finden, sodass über den lokalisierten Ringen A jeweils ähnlich zu Diagonalmatrizen ist.

   Dazu benutzen wir eine starke Vereinfachung des Smithschen Diagonalisierungsverfahrens: Nach der Vorüberlegung finden wir eine Zerlegung der Eins derart, dass in den lokalisierten Ringen jeweils eines der Matrixelemente ein Teiler aller anderen ist. Dieses können wir nach oben links bringen und damit alle anderen Elemente der ersten Zeile und Spalte auslöschen.

   Diesen Schritt können wir für die entstehende Restmatrix rekursiv wiederholen, dabei müssen wir die Zerlegung der Eins immer weiter verfeinern. Nach endlich vielen Schritten sind wir fertig.

□

Aufgabe 9

Sei R ein noetherscher kommutativer Ring. Ein Algorithmus produziere m Ketten

$$\begin{array}{ccccccc} \mathfrak{a}_{10} & \subseteq & \mathfrak{a}_{11} & \subseteq & \mathfrak{a}_{12} & \subseteq & \cdots \\ \vdots & & \vdots & & \vdots & & \\ \mathfrak{a}_{m0} & \subseteq & \mathfrak{a}_{m1} & \subseteq & \mathfrak{a}_{m2} & \subseteq & \cdots \end{array}$$

von endlich erzeugten Idealen in R.

Behauptung. *Es gibt ein n derart, dass*

$$\mathfrak{a}_{jn} = \mathfrak{a}_{j,n+1}$$

für alle $j \in \{1, \ldots, m\}$.

Beweis. (durch Induktion über m)

Induktionsanfang $m = 1$: Klar, da R noethersch.

Induktionsschritt $m \to m + 1$: Nach Induktionsvoraussetzung können wir algorithmisch eine streng monotone Folge $(i_n)_n$ von Indizes finden, sodass $\mathfrak{a}_{j,i_n} = \mathfrak{a}_{j,i_n+1}$ für alle $j \in \{1, \ldots, m\}$ und alle $n \geq 1$ gilt.

Genauer geht das so: Als erstes verwenden wir die Induktionsvoraussetzung, um einen Index i_1 mit $\mathfrak{a}_{j,i_1} = \mathfrak{a}_{j,i_1+1}$ für alle $j \in \{1, \ldots, m\}$ zu erhalten. Um den nächsten Index i_2 zu finden, wenden wir die Induktionsvoraussetzung auf die Teilfolgen $(\mathfrak{a}_{j,i_1+1+n})_{n\geq 0}$, $j \in \{1, \ldots, m\}$ an (wir schneiden also die ersten $i_1 + 1$ Folgenglieder ab). Wir könnig ewig so fortfahren.

Nun betrachten wir die Teilfolge

$$\mathfrak{a}_{m+1,i_1} \subseteq \mathfrak{a}_{m+1,i_2} \subseteq \mathfrak{a}_{m+1,i_3} \subseteq \cdots$$

von $(\mathfrak{a}_{m+1,n})_n$. Da R noethersch ist, gibt es ein n mit $\mathfrak{a}_{m+1,i_n} = \mathfrak{a}_{m+1,i_{n+1}}$. Somit gilt auch

$$\mathfrak{a}_{m+1,i_n} = \mathfrak{a}_{m+1,i_n+1} = \mathfrak{a}_{m+1,i_n+2} = \cdots = \mathfrak{a}_{m+1,i_{n+1}-1} = \mathfrak{a}_{m+1,i_{n+1}},$$

da die zwischen Anfang und Ende stehenden Folgenglieder in dieser Aufzählung vom Rand „gesandwicht“ werden. Folglich gilt

$$\mathfrak{a}_{j,i_n} = \mathfrak{a}_{j,i_n+1}$$

für alle $j \in \{1, \ldots, m + 1\}$, womit der Induktionsschritt abgeschlossen ist. □

Bemerkung. Nach ein bisschen Nachdenken kommt man vielleicht irrtümlicherweise auf die Idee, dass die zu zeigende Behauptung gar nicht stimmt: Betrachte die Gegenbeispielsituation

$$\begin{array}{l} \mathfrak{a}_{10} \subsetneq \mathfrak{a}_{11} = \mathfrak{a}_{12} \subsetneq \mathfrak{a}_{13} = \mathfrak{a}_{14} \subsetneq \mathfrak{a}_{15} = \mathfrak{a}_{16} \subsetneq \cdots \\ \mathfrak{a}_{20} = \mathfrak{a}_{21} \subsetneq \mathfrak{a}_{22} = \mathfrak{a}_{23} \subsetneq \mathfrak{a}_{24} = \mathfrak{a}_{25} \subsetneq \mathfrak{a}_{26} = \cdots \end{array}$$

Offensichtlich gibt es dann kein n, für den sowohl $a_{1n} = a_{1,n+1}$ als auch $a_{2n} = a_{2,n+1}$ gilt. Es ist aber auch die Noether-Voraussetzung verletzt, was man an der unendlich aufsteigenden Teilfolge

$$a_{11} \subsetneq a_{13} \subsetneq a_{15} \subsetneq a_{17} \subsetneq \cdots$$

sieht.

Bemerkung. Wir verwenden im Beweis das abzählbare Auswahlaxiom, das ist aber nur ein sprachliches Problem. Genauer:

Das abzählbare Auswahlaxiom ist das Hilfsmittel, was einem erlaubt, aus einer Folge von Algorithmen A_i, die jeweils ein Objekt produzieren, einen Algorithmus zu erhalten, der alle Ergebnisse der gegebenen Algorithmen A_i in einer Folge zusammenfasst und diese zurückgibt.

Von der Berechenbarkeitsperspektive ist klar, dass das Unsinn ist: Denn jeder Algorithmus A_i benötigt von null verschieden Zeit zur Berechnung seines Ergebnisses; wöllte man alle Ergebnisse zu einer Folge zusammenfassen, müsste man zunächst alle Algorithmen A_i ablaufen lassen, das dauert aber unendlich lange.

Im Beweis haben wir für jedes $n \geq 1$ einen Algorithmus beschrieben, der den Index i_n berechnet. Das abzählbare Auswahlaxiom kam ins Spiel, als wir all diese Indizes i_n zu einer Folge $(i_n)_n$ zusammengefasst haben. Das hätten wir aber gar nicht machen müssen. (Auch die gegebenen Ideale $a_{j,0}, a_{j,1}, a_{j,2}, \ldots$ haben wir sprachlich auch zu einer ganzen Folge $(a_{j,n})_{n \geq 0}$ zusammengefasst, das hätte auch nicht sein müssen.)

Aufgabe 10

Sei $x \in \overline{\mathbb{Q}}$ eine Nullstelle von $f = X^4 - X^2 - 3X + 7$, sei $K = \mathbb{Q}(x)$. Es gilt $7 = x(3 + x - x^3)$, diese Tatsache werden wir mehrmals benutzen.

Wir suchen eine teilweise Faktorisierung der Ideale $\mathfrak{a} := (14, x + 7)$ und $\mathfrak{b} := (35, x - 14)$ in $\mathcal{O}_K$, dazu gehen wir nach dem Verfahren von Seite 327 des Skripts vor. Glücklicherweise terminiert das Verfahren schon nach dem ersten Schritt.

Das Resultat ist:

$$\mathfrak{a} = \mathfrak{d} \cdot \tilde{\mathfrak{a}}, \quad \mathfrak{b} = \mathfrak{d} \cdot \tilde{\mathfrak{b}},$$

wobei:

$$\begin{aligned}
\mathfrak{d} &:= \mathfrak{a} + \mathfrak{b} = (14, x + 7, 35, x - 14) = (14, 7, 35, x) = (7, x) \\
&= (x)
\end{aligned}$$

$$\begin{aligned}
\tilde{\mathfrak{a}} &:= \mathfrak{a} : \mathfrak{d} = (2 \cdot 7, x + 7) : (x) = (2x(3 + x - x^3), x(4 + x - x^3)) : (x) \\
&= (2(4 + x - x^3) - 2, 4 + x - x^3) = (2, 4 + x - x^3) \\
&= (2, x - x^3)
\end{aligned}$$

$$\begin{aligned}
\tilde{\mathfrak{b}} &:= \mathfrak{b} : \mathfrak{d} = (5 \cdot 7, x - 2 \cdot 7) : (x) = (5x(3 + x - x^3), x - 2x(3 + x - x^3)) : (x) \\
&= (5 \cdot (3 + x - x^3), 1 - 2 \cdot (3 + x - x^3)) = (5 + x - x^3, -5 - 2x + 2x^3) \\
&= (5 + x - x^3, -x + x^3) \\
&= (5, x - x^3)
\end{aligned}$$

Denn die Ideale $\tilde{\mathfrak{a}}$ und $\tilde{\mathfrak{b}}$ sind direkt nach Konstruktion koprim, und für die restlichen beiden Kombinationen gilt:

$$\begin{aligned}
\tilde{\mathfrak{a}} + \mathfrak{d} &= (2, x - x^3, x) = (2, x) = (2, x, x(3 + x - x^3)) = (2, x, 7) = (1) \\
\tilde{\mathfrak{b}} + \mathfrak{d} &= (5, x - x^3, x) = (5, x) = (5, x, x(3 + x - x^3)) = (5, x, 7) = (1)
\end{aligned}$$

Bemerkung zum Vorgehen: Alle auftretenden Ideale möglichst gut vereinfachen, die Rechenregel fürs Teilen durch Hauptideale verwenden, die Darstellung des konstanten Glieds von f nutzen.

Blatt 14 Aufgabe 2

Bh.: Sei K ein Körper mit 25 Elementen.
Dann gibt es in K eine Quadratwurzel aus $2=1+1$.

Bew.: Der Körper $K_0 := \mathbb{F}_5[X]/(X^2-2)$ hat 25 Elemente.
(Dass es sich bei K_0 wirklich um einen Körper handelt, liegt daran, dass X^2-2 über $\mathbb{F}_5$ irreduzibel ist. Um das einzusehen, genügt es zu zeigen, dass X^2-2 über $\mathbb{F}_5$ keine Nullstelle besitzt, da X^2-2 Grad 2 hat. Dazu:

$$0^2-2 = -2 \neq 0$$
$$1^2-2 = -1 \neq 0$$
$$2^2-2 = 2 \neq 0$$
$$3^2-2 = 2 \neq 0$$
$$4^2-2 = 4 \neq 0)$$

Nach Vorlesung sind je zwei endliche Körper mit gleich vielen Elementen (nicht-eindeutig) isomorph. Somit genügt es, die Behauptung für K_0 zu zeigen.

Bh.: In $K_0 := \mathbb{F}_5[X]/(X^2-2)$ gibt es eine Quadratwurzel aus 2.

Bew.: Klar, denn $[X] \in K_0$ ist eine Quadratwurzel aus 2, da gilt:
$$[X]^2-2 = [X^2-2] = 0, \quad \text{also} \quad [X]^2 = 2.$$

Ges.: Erzeuger der multiplikativen Gruppe $K_0^\times$ von K_0.

Dazu: Wir müssen also ein Element $x_0 \in K_0^\times$ der Ordnung $24 = |K_0^\times|$ finden.
Da jedes Element in $K_0^\times$ als Ordnung 1, 2, 3, 4, 6, 8, 12 oder 24 hat, genügt es als Nachweis, dass ein Element Ordnung 24 hat, ein Nachweis, dass es nicht die Ordnungen 1, 2, 3, 4, 6, 8, oder 12 hat.
Definiere $x_0 := 3+1\cdot\sqrt{2}$. Dann gilt:
$$x_0 \neq 1, \quad x_0^2 = 1+\sqrt{2} \neq 1, \quad x_0^3 = 4\sqrt{2} \neq 1, \quad x_0^4 = 3+2\sqrt{2} \neq 1,$$
$$x_0^6 = 2 \neq 1, \quad x_0^8 = 2+2\sqrt{2} \neq 1, \quad x_0^{12} = 4 \neq 1.$$
Also ist x_0 ein Erzeuger von $K_0^\times = \{a \in K_0 \mid a \neq 0\}$.

Blatt 14 Aufgabe 4

R komm. Ring, char R = p.

Def: $\varprojlim_i R^{p^i} := \{ (x_0, x_1, x_2, \dots);\ x_i \in R,\ x_{i+1}^{p} = x_i$ für alle $i \geq 0 \}$,

$0 := (0, 0, 0, \dots) \in \varprojlim_i R^{p^i}$

$1 := (1, 1, 1, \dots) \in \varprojlim_i R^{p^i}$

$(x_0, x_1, \dots) + (\tilde{x}_0, \tilde{x}_1, \dots) := (x_0 + \tilde{x}_0, x_1 + \tilde{x}_1, \dots) \in \varprojlim_i R^{p^i}$

— " — · — " — $:= (x_0 \cdot \tilde{x}_0, x_1 \cdot \tilde{x}_1, \dots) \in \varprojlim_i R^{p^i}$

Beh.: Jedes Element in $E := \varprojlim_i R^{p^i}$ besitzt eine p-te Wurzel.

Bew.: Sei $a = (x_0, x_1, \dots) \in E$ beliebig.

Definiere $b := (x_1, x_2, \dots)$. Dann gilt:

1. $b \in E$: klar.
2. $b^p = a$: $b^p = (x_1^p, x_2^p, \dots) = (x_0, x_1, \dots) = a$.

Also ist b eine p-te Wurzel von a in E.

Sei nun R ein Körper.

Beh.: E ist ein Körper.

Bew.: Sei $a = (x_0, x_1, \dots) \in E$ beliebig.

Da R ein Körper ist, gilt

entweder: $x_0 = 0$ in R. Da der Frobenius injektiv ist, folgt dann $x_1 = 0$, und induktiv folgt $x_i = 0$ für alle $i \geq 0$, also $a = 0$.

oder: x_0 ist in R invertierbar. Dann sind auch $x_1, x_2, \dots$ in R invertierbar: Beispielsweise gilt $x_1 \cdot x_1 \cdot \ldots \cdot x_1 = x_0$ (p Mal), x_0 ist invertierbar, somit ist x_1 invertierbar. Induktiv macht man weiter.

Es folgt nun, dass die Folge $(x_0^{-1}, x_1^{-1}, \dots)$ ein Element von E ist, denn

$$(x_{i+1}^{-1})^p = (x_{i+1}^p)^{-1} = x_i^{-1} \text{ für alle } i \geq 0,$$

und dass sie ein Inverses von a ist, denn

$$a \cdot (x_0^{-1}, x_1^{-1}, \dots) = (x_0 x_0^{-1}, x_1 x_1^{-1}, \dots) = (1, 1, \dots) = 1$$

Also ist a in E invertierbar.

Das war zu zeigen.

Bh.: E wird vermöge der Abbildung

$$\varphi: U\,E \longrightarrow R$$
$$(x_0, x_1, \ldots) \longmapsto x_0$$

zu einem Unterkörper von R.

Bew.: Klar: φ ist ein Ringhomomorphismus und automatisch injektiv.

Bh.: E ist vollkommen.

Bew.: klar (Satz 8.23 auf Seite 356).

Bh.: E kann mit $M := \{x \in R;\ x$ besitzt eine q-te Wurzel, für alle p-Potenzen $q\} \subseteq R$ identifiziert werden.

Bew.: Gemeint ist, dass $\varphi[E] = M$ ist.

„$\subseteq$": Sei $x_0 \in \varphi[E]$, d.h. x_0 ist das erste Folgenglied einer Folge $(x_0, x_1, \ldots) \in E$. Dann ist x_1 eine p-te Wurzel von x_0, x_2 eine p^2-te Wurzel von x_0, usw. Also $x_0 \in M$.

„$\supseteq$": Sei $x_0 \in M$. Nach Voraussetzung existiert eine p-te Wurzel x_1 von x_0, und zwar auch nur eine, da der Frobenius injektiv ist.
Weiter existiert (genau) eine p^2-te Wurzel x_2 von x_0. Aufgrund der Eindeutigkeit erfüllt diese $x_2^p = x_1$.
Rekursiv erhalten wir eine Folge $(x_0, x_1, \ldots)$ derart, dass $x_{i+1}^p = x_i$ für alle $i \geq 0$.
Somit gilt $(x_0, x_1, \ldots) \in E$ und $x_0 \in \varphi[E]$.

Blatt 14, Aufgabe 5

Ges: Alle 7-ten Wurzeln aller Elemente von $\mathbb{F}_7$.

Dazu: In $\mathbb{F}_7$ gilt für alle Elemente $x \in \mathbb{F}_7$: $x^7 = x$.

Ferner sind 7-te Wurzeln in $\mathbb{F}_7$ eindeutig, da der Frobenius injektiv ist.

Folglich ist jedes Element aus $\mathbb{F}_7$ seine eigene 7-te Wurzel.

Blatt 14, Aufgabe 6

Sei K ein Körper mit char $K = p$.

Bh.: K ist vollkommen $\Longleftrightarrow$ der Frobenius von K nach K ist ein Isomorphismus.

Bew.: K vollkommen $\overset{\text{Satz 8.23}}{\Longleftrightarrow}$ jedes Element in K besitzt eine p-te Wurzel

$\Longleftrightarrow$ der Frobenius ist surjektiv

$\Longleftrightarrow$ der Frobenius ist ein Isomorphismus (denn er ist stets injektiv und stets ein Ringhomo).

Blatt 14 Aufgabe 7

$L \supseteq K$. Sei $S := \{x \in L;\ x \text{ ist rein inseparabel über } K\} \subseteq L$.

Beh.: $K \subseteq S$ und S ist ein Körper.

Bew.: Zur Erinnerung: $x \in L$ heißt genau dann rein inseparabel über K, wenn $x \in K$ oder wenn char $K = p$ und $x^{(p^e)} \in K$ für ein $e \geq 0$.

Damit ist klar, dass $K \subseteq S$.

Somit ist ebenfalls klar, dass $0, 1 \in S$.

Noch zu zeigen:

~~a) $x \in K \Rightarrow -x \in K$ und $x^{-1} \in K$ (f~~

a) $x \in S \Rightarrow -x \in S$ und $x^{-1} \in S$ (falls $x \neq 0$)

b) $x, y \in S \Rightarrow x + y \in S$, $x \cdot y \in S$.

Zu a): Sei $x \in S$. Dann gilt:

1. Fall: $x \in K$. Dann sind auch $-x$ und x^{-1} (falls $x \neq 0$) Elemente von K und damit von S.

2. Fall: char $K = p$ und $x^{(p^e)} \in K$ für ein $e \geq 0$.
Dann gilt auch $(-x)^{p^e} = (-1)^{p^e} \cdot x^{p^e} \in K$, also $-x \in S$.
Weiter gilt $(x^{-1})^{p^e} = (x^{p^e})^{-1} \in K$, da $x^{p^e} \in K$; somit auch $x^{-1} \in S$.

Zu b): Seien $x, y \in S$. Dann gilt:

1. Fall: $x, y \in K$. Dann auch $x + y, x \cdot y \in K \subseteq S$.

2. Fall: $x \in K$ und char $K = p$, $y^{p^e} \in K$ für ein $e \geq 0$.
Dann auch $(x+y)^{p^e} = x^{p^e} + y^{p^e} \in K$; somit $x + y \in S$.
Weiter $(xy)^{p^e} = x^{p^e} y^{p^e} \in K$, somit $x \cdot y \in S$.

3. Fall: char $K = p$ und $x^{p^e} \in K$ für ein $e \geq 0$, und $y \in K$:
Analog wie der 2. Fall.

4. Fall: char $K = p$ und $x^{p^e} \in K$, $y^{p^f} \in K$ für ein $e, f \geq 0$.
Es gilt dann auch $x^{p^i}, y^{p^i} \in K$, wobei $i := \max\{e, f\}$.
Dann folgt, dass $(x+y)^{p^i} = x^{p^i} + y^{p^i}$ und $(xy)^{p^i} = x^{p^i} y^{p^i}$ Elemente von K sind.
Somit gilt $x + y, x \cdot y \in S$.

Blatt 14, Aufgabe 8

Wir können sogar eine Verschärfung der Aufgabe zeigen:

Sei $L \supseteq K$ eine beliebige Körpererweiterung.

Sei ferner $L \supseteq K$ sowohl separabel als auch rein inseparabel.

Bh. $L = K$.

Bew: „$\supseteq$": klar.

„$\subseteq$": Sei $x \in L$ beliebig. Da $L \supseteq K$ rein inseparabel, folgt:

1. Fall: $x \in K$: Dann fertig.

2. Fall: char $K = p$ und $x^{p^e} \in K$ für ein $e \geq 0$:

Dann folgt mit Hilfssatz 8.17:

$$x \in K(x^{p^e}) \subseteq K,$$

also $x \in K$, fertig.

Mit der zusätzlichen Voraussetzung der Augabe, dass die Erweiterung endlich ist, kann man den Beweis noch verkürzen:

Da L über K separabel ist, gilt $[L:K]_i = 1$.

Da L über K rein insep. ist, gilt $[L:K]_s = 1$.

Somit folgt $[L:K] = [L:K]_i \cdot [L:K]_s = 1 \cdot 1 = 1$, also $L = K$.

Blatt 14, Aufgabe 9

$L \supseteq K$ endliche Erweiterung, $x \in L$ separabel über K, $y \in L$ rein inseparabel über K.

Bh.: $K(x,y) = K(x+y)$.

Bew.: „$\supseteq$": ✓

„$\subseteq$": Da y rein inseparabel über K, gilt:

1. Fall: $y \in K$: Dann fertig, denn $K(x,y) = K(x) = K(x+y)$.

2. Fall: $y^{p^e} \in K$ für ein $e \geq 0$ und char $K = p$:

Dann $x \in K(x) \underset{8.17}{=} K(x^{p^e}) \underset{\overset{\nearrow}{y^{p^e} \in K}}{=} K(x^{p^e} + y^{p^e}) = K((x+y)^{p^e}) \subseteq K(x+y)$,

also $x \in K(x+y)$.

Außerdem gilt $y = \underbrace{(x+y)}_{\in K(x+y)} - \underbrace{x}_{\in K(x+y)} \in K(x+y)$. Damit ist alles gezeigt.

Aufgabe 10a

Sei $L \supseteq K$ eine endliche Körpererweiterung. Sei für $x \in L$ die Abbildung $\varphi_x \colon L \to L$ durch $\varphi_x(a) = ax$ für alle $a \in L$ definiert.

Seien $\sigma_1, \ldots, \sigma_{[L:K]_\mathrm{s}} \colon L \to \Omega$ die verschiedenen K-Algebrenhomomorphismen von L in einen algebraisch abgeschlossenen Oberkörper Ω.

Sei $\overline{K}$ der separable Abschluss von K in L.

Wir wollen die Gültigkeit folgender Formel zeigen:

$$N_{L/K}(x) = \det \varphi_x = \left(\prod_{i=1}^{[L:K]_\mathrm{s}} \sigma_i(x) \right)^{[L:K]_\mathrm{i}} .$$

Reduktion auf separable Elemente

Wir wollen zunächst annehmen, dass die Formel für alle $x \in \overline{K}$ bereits bewiesen worden ist. Sei dann $x \in L$ beliebig. Da L über $\overline{K}$ rein inseparabel ist, können wir zwei Fälle unterscheiden:

1. Fall: $x \in \overline{K}$. Dann stimmt die Formel für x nach Annahme.

2. Fall: Die Charakteristik von K ist eine Primzahl p und x^{p^e} liegt in $\overline{K}$ für ein $e \geq 0$. Wegen der Multiplikativität der Determinante folgt dann

$$N_{L/K}(x)^{p^e} = N_{L/K}(x^{p^e}) = \left(\prod_{i=1}^{[L:K]_\mathrm{s}} \sigma_i(x^{p^e}) \right)^{[L:K]_\mathrm{i}} = \left(\left(\prod_{i=1}^{[L:K]_\mathrm{s}} \sigma_i(x) \right)^{[L:K]_\mathrm{i}} \right)^{p^e} ,$$

wobei die mittlere Gleichheit nach der Annahme folgt. Die Injektivität des Frobenius erlaubt es dann, die Gültigkeit der Formel auch für x zu zeigen.

Der Fall separabler Elemente

Sei nun $x \in \overline{K}$. Da $L \supseteq \overline{K}$ eine endliche Erweiterung ist, besitzt L eine Basis $a_1, \ldots, a_{[L:K]_\mathrm{i}}$ über $\overline{K}$. Da $\overline{K} \supseteq K(x)$ eine endliche Erweiterung ist, besitzt $\overline{K}$ eine Basis $b_1, \ldots, b_d$ über $K(x)$. Und schließlich besitzt $K(x)$ die Basis $1, x, x^2, \ldots, x^{n-1}$ über K, wenn n den Grad von x über K bezeichnet.

Nach dem Satz über die Gradformel ist dann eine Basis von L über K durch die $a_i b_j x^k$ gegeben. Da $\varphi_x(a_i b_j x^k) = a_i b_j \, \varphi_x(x^k)$, erhalten wir, dass die Matrix von φ_x bezüglich dieser Basis Blockdiagonalform hat,

$$M := M(\varphi_x; (a_i b_j x^k), (a_i b_j x^k)) = \begin{pmatrix} N & & \\ & \ddots & \\ & & N \end{pmatrix} \in K^{nd[L:K]_\mathrm{i} \times nd[L:K]_\mathrm{i}},$$

wobei N die Matrix der Einschränkung $\varphi_x|_{K(x)}$ bezüglich der Basis $1, x, x^2, \ldots, x^{n-1}$ ist. Diese heißt auch *Begleitmatrix von* m_x, wobei $m_x \in K[X]$ das Minimalpolynom von x über K bezeichne, und hat die Form

$$N = \begin{pmatrix} 0 & 0 & \cdots & 0 & -c_0 \\ 1 & 0 & \cdots & 0 & -c_1 \\ 0 & 1 & \cdots & 0 & -c_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -c_{n-1} \end{pmatrix} \in K^{n \times n},$$

wobei $m_x = X^n + c_{n-1}X^{n-1} + \cdots + c_1 X + c_0$.

Aus der Linearen Algebra ist bekannt, dass das charakteristische Polynom dieser Matrix gerade $(-1)^n m_x$ ist. Somit besitzt M als charakteristisches Polynom die Potenz $((-1)^n m_x)^{d[L:K]_\mathrm{i}}$, womit die Formel

$$N_{L/K}(x) = \det M = ((-1)^n m_x(0))^{d[L:K]_\mathrm{i}} = \left(\left(\prod_{\ell=1}^{n} x_i\right)^d\right)^{[L:K]_\mathrm{i}}$$

folgt, wobei $x_1, \ldots, x_n$ die galoisschen Konjugierten von x in Ω, also die Nullstellen von m_x in Ω, seien. Das ist noch nicht die Formel, die wir zeigen sollten, aber auch schon nett!

Umformung auf die Form der Angabe

Wer noch daran interessiert ist, die Formel auf die vorgegebene Form zu bringen, sei auf [1] und [2, Kap. 8.1] verwiesen.

Literatur

[1] K. Conrad. Trace and norm, 2008.

[2] S. Roman. *Field Theory*, volume 158 of *Graduate Texts in Mathematics*. Springer-Verlag, second edition, 2006.