Norbert Klingen

Algebra

Übungen zur Vorlesung

(mit Lösungen)

Aufgabenstellungen: F.-P. Heider, H.-D. Steckel

Universität zu Köln WS 1980/81

Inhaltsverzeichnis

Algebra
Übung 1

Aufgabe 1. (m)
Sei G eine Gruppe und $H \subseteq G$ eine Teilmenge. Zeigen Sie:

$$H \text{ ist Untergruppe von } G \iff H \neq \emptyset \ \wedge \bigwedge_{a,b \in H} ab^{-1} \in H\,.$$

Lösung:
$\Rightarrow$ ist klar, da die Untergruppe H ein Einselement enthält und gegenüber den Gruppenoperationen Multiplikation und Inversenbildung abgeschlossen ist.
ad $\Leftarrow$: $H \neq \emptyset$, also gibt es ein $a \in H$ und nach Voraussetzung ist dann $aa^{-1} = e \in H$; H besitzt also ein Einselement. Für alle $b \in H$ ist dann $eb^{-1} = b^{-1} \in H$ und für alle $a, b \in H$ dann $ab = a \cdot (b^{-1})^{-1} \in H$. H ist somit Untergruppe von G (Vorlesung Bemerkung I.1.7).

Aufgabe 2. (m)
Es sei der *Exponent* einer Gruppe G definiert durch

$$\exp(G) = \inf\{n \in \mathbb{N}_+ \mid \bigwedge_{g \in G} g^n = e\} \in \mathbb{N}_+ \cup \{\infty\} \qquad (\inf \emptyset = \infty)\,.$$

a) Für eine endliche Gruppe G gilt $\exp(G) = \mathrm{kgV}\{\mathrm{ord}(g) \mid g \in G\}$.

b) Jede Gruppe vom Exponenten 2 ist abelsch.

c) Für zyklisches G gilt $\exp(G) = \#G$. Gilt hier die Umkehrung?

Lösung:
a) Wegen der Endlichkeit von G gilt $g^{\#G} = e$ (Satz von Lagrange, Korollar I.1.13, p. 9) also haben alle $g \in G$ endliche Ordnung $\mathrm{ord}\ g$ und es gilt $\exp(G) \leq \#G < \infty$. Mit $\exp := \exp(G)$ und $\mathrm{kgV} := \mathrm{kgV}(\mathrm{ord}(g) \mid g \in G)$ gilt gemäß Prop. 1.10 d), p. 8

$$\bigwedge_{g \in G} g^{\exp} = e \implies \bigwedge_{g \in G} \mathrm{ord}(g) \mid \exp \implies \mathrm{kgV} \leq \exp$$

und umgekehrt

$$\bigwedge_{g \in G} \mathrm{ord}(g) \mid \mathrm{kgV} \implies \bigwedge_{g \in G} g^{\mathrm{kgV}} = e \implies \exp \leq \mathrm{kgV}\,.$$

b) Seien $a, b \in G$ beliebig. Dann gilt nach Voraussetzung

$$a^2 = b^2 = (ab)^2 = e \implies a = a^{-1}\,,\ b = b^{-1}\,,\ ab = (ab)^{-1} = b^{-1}a^{-1} = ba\,.$$

c) Wegen $g^{\#G} = e$ für alle g (Satz von Lagrange, s.o.) ist $\exp(G) \leq \#G$ und für zyklisches $G = \langle a \rangle$ gilt nach a) $\#G = \mathrm{ord}(a) \mid \exp(G)$.
Die Umkehrung gilt nicht: Die 6 Elemente der symmetrischen Gruppe S_3 haben die Ordnungen 1 (Identität), 2 (drei Transpositionen) und 3 (zwei 3-Zyklen). Also ist $\exp S_3 = \mathrm{kgV}(1, 2, 3) = 6 = \#S_3$, aber S_3 ist nicht zyklisch, nicht einmal abelsch.

Aufgabe 3. (m)
Sei G eine endliche Gruppe.

a) Kann G Vereinigung zweier echter Untergruppen sein?

b) Kann für eine Untergruppe $H \leq G$ gelten

$$G = \bigcup_{g \in G} gHg^{-1} \ ?$$

c) Jede Untergruppe N von G vom Index 2 ist ein Normalteiler.

Lösung:
a) Nein. Angenommen $G = H_1 \cup H_2$ mit $H_i < G$. Seien $h_1 \in H_1 \setminus H_2$ und $h_2 \in H_2 \setminus H_1$. Nach Voraussetzung gilt $h_1 h_2 \in G = H_1 \cup H_2 \implies h_1 h_2 \in H_1$ oder $h_1 h_2 \in H_2$.
$h_1 h_2 \in H_1 \implies h_2 = h_1^{-1}(h_1 h_2) \in H_1$, Wid., und genauso für $h_1 h_2 \in H_2$.
b) Bei Schwierigkeiten hier ein Tipp: Gruppenindex und Abzählen! Wieviele verschiedene Konjugierte gHg^{-1} von H gibt es höchstens? Wie groß ist dann die Vereinigung höchstens?
b) Hier die Antwort und Lösung: Ja, falls $H = G$, sonst nicht. Sei $d = (G : H)$ und $G = \bigcup_{i=1}^{d} g_i H$ die Nebenklassenzerlegung von G nach H. Dann gilt $d \cdot \#H = \#G$ (Satz von Lagrange, Vorlesung I.1.12 e), p. 9) und für jedes g existiert ein i mit $g \in g_i H$, also $gHg^{-1} = g_i H g_i^{-1}$. Also gilt

$$G = \bigcup_{g \in G} gHg^{-1} = \bigcup_{i=1}^{d} g_i H g_i^{-1} \implies \#G \leq \sum_{i=1}^{d} \#g_i H g_i^{-1} = \sum_{i=1}^{d} \#H = d \cdot \#H = \#G$$

In der letzten Abschätzungkette muss also an allen Stellen Gleichheit gelten und das bedeutet, dass die Vereinigungsmenge disjunkt sein muss. Da aber Untergruppen immer mindestens ein Element gemeinsam haben, kann die Vereinigung nur aus einer Menge bestehen, also ist $d = 1$ und $H = G$.
c) Sei $H < G$ und $(G : H) = 2$. Da es gleich viele Rechts- und Linksnebenklassen gibt, gilt für jedes $g \notin H$ $G = H \dot\cup gH = H \dot\cup Hg$, also $gH = G \setminus H = Hg$. Damit gilt $Hg = gH$ für *alle* $g \in G$ und $H \triangleleft G$ nach Prop. I.1.15 (iv), p. 10.

Aufgabe 4. (s)
Die endlichen Gruppen $G \neq \{e\}$ ohne echte Untergruppen sind gerade die Gruppen von Primzahlordnung; diese sind zyklisch.

Lösung:
Sei $\#G = p$ eine Primzahl und $H \leq G$ eine Untergruppe. Dann ist $\#H$ ein Teiler von p, also $\#H = 1$ oder $\#H = p = \#G$ und folglich $H = \{e\}$ oder $H = G$. Gruppen von Primzahlordnung haben also keine echten Untergruppen.
Hat $G \neq \{e\}$ keine echten Untergruppen, so gilt für jedes $e \neq a \in G$: $\langle a \rangle = G$.
Wäre $\#G = \operatorname{ord} a$ unendlich, so wären alle a^k ($k \in \mathbb{Z}$) verschieden und daher $\langle a^2 \rangle$ eine echte Untergruppe von $G = \langle a \rangle$.
Es ist also $\#G \in \mathbb{N}$. Wäre nun $\#G = \operatorname{ord} a = m \cdot n$ mit $m, n \neq 1$, so folgte $a^m \neq e$ und daher hätte G die echte Untergruppe $\{e\} \neq \langle a^m \rangle = \{e, a^m, a^{2m}, \ldots, a^{(n-1)m}\} \neq G$, im Widerspruch zur Voraussetzung.

Aufgabe 5. (s)
Sei G eine Gruppe mit Untergruppen H_1, H_2. Zeigen Sie:

a) $(H_2 : H_1 \cap H_2) \leq (G : H_1)$.

b) Ist $(G : H_1)$ endlich, so gilt in a) genau dann Gleichheit, wenn $G = H_1 H_2 = H_2 H_1$ ist. [Für Teilmengen $A, B \subseteq G$ bezeichnet $AB := A \cdot B := \{a \cdot b \mid a \in A\,,\ b \in B\}$ die Menge aller Produkte von A und B in G.]

c) Sind $(G : H_1), (G : H_2)$ teilerfremde natürliche Zahlen, so gilt $G = H_1H_2 = H_2H_1$.

Lösung:
a) Sind die $b_i \in H_2$ $(i \in I)$ ein vollständiges Repräsentantensystem der Nebenklassen von $H_1 \cap H_2$ in H_2, so gilt

$$b_i b_j^{-1} \in H_1 \iff b_i b_j^{-1} \in H_1 \cap H_2 \iff i = j\,,$$

also sind alle Nebenklassen b_iH_1 verschieden. Man kann daher die b_i zu einem Repräsentantensystem b_j $(j \in J,\ J \supset I)$ von H_1 in G erweitern, und somit gilt $(H_2 : H_1 \cap H_2) = \#I \leq \#J = (G : H_1)$.
b) Ist $\#I = (H_2 : H_1 \cap H_2) = (G : H_1) = \#J$, so folgt wegen der Endlichkeit aus $I \subseteq J$ die Mengengleichheit $I = J$, also $\bigwedge_{g\in G} \bigvee_{i\in I}\ g \in gH_1 = b_iH_1 \subset H_2H_1 \implies G = H_2H_1$.
Die H_i sind als Untergruppen von G gegen Inversenbildung abgeschlossen, also gilt auch $G = G^{-1} = (H_2H_1)^{-1} = H_1^{-1}H_2^{-1} = H_1H_2$.
Umgekehrt: Ist $G = H_2H_1$, so gibt es ein vollständiges Repräsentantensystem $b_j \in H_2$ für G/H_1 und dies ist dann ein vollständiges Repräsentantensystem für $H_2/H_1 \cap H_2$. Also gilt die Gleichheit der Indizes.
c) Nach dem Satz von Lagrange gilt $(G : H_1) \mid (G : H_1 \cap H_2) = (G : H_2)(H_2 : H_1 \cap H_2)$. Wegen der Teilerfremdheit folgt daraus $(G : H_1) \mid (H_2 : H_1 \cap H_2) \leq (G : H_1)$, also gilt Gleichheit und aus b) folgt c).

Aufgabe 6. (s)
Es sei $O(2) = \{A \in \mathrm{GL}_2(\mathbb{R}) \mid AA^{\mathrm{t}} = E\}$ die Gruppe der orthogonalen 2×2-Matrizen und $n \in \mathbb{N}_+$,

$$S = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad R_n = \begin{pmatrix} \cos\frac{2\pi}{n} & -\sin\frac{2\pi}{n} \\ \sin\frac{2\pi}{n} & \cos\frac{2\pi}{n} \end{pmatrix}.$$

Zeigen Sie:

a) $R_n \cdot S = S \cdot R_n^{-1}$.

b) $D_{2n} := \langle S, R_n\rangle$ ist eine Gruppe der Ordnung $2n$.

c) $D_2 \simeq \mathbb{Z}/2\mathbb{Z}$, $D_4 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

d) $D_6 \simeq S_3$ und D_{2n} ist nicht abelsch für $n \geq 3$.

e) Veranschaulichen Sie sich die geometrische Wirkung von S und R_n als lineare Abbildungen der reellen Ebene $\mathbb{R}^2$. Zeigen Sie, dass D_{2n} genau aus den orthogonalen Abbildungen des $\mathbb{R}^2$ besteht, die das regelmäßige n-Eck

$$\mathcal{E}_n := \{z_k = (\cos\frac{2k\pi}{n}, \sin\frac{2k\pi}{n}) \mid k = 1, \ldots, n\}$$

in sich überführen. D_{2n} ist daher die Symmetriegruppe des regelmäßigen n-Ecks und wird *Diedergruppe der Ordnung* $2n$ genannt.

Lösung:
Geometrische Vorüberlegungen erleichtern die notwendigen Rechnungen. S und R_n sind orthogonale Abbildungen, also längen- und winkeltreu. S ist die Spiegelung an der x-Achse im $\mathbb{R}^2$ und R_n die Drehung um den Winkel $2\pi/n$. R_n^l ist dann die Drehung um $2l\pi/n$ (wenn nicht aus der Linearen Algebra bekannt: Nachrechnen mit den Additionstheoremen der trigonometrischen Funktionen). $S(z_k) = z_{-k}$, $R_n(z_k) = z_{k+1}$, $R_n^l(z_k) = z_{k+l}$.

a) Wiederholende Übungen zur Matrixrechnung aus der Linearen Algebra. Beachten Sie die einfache Inversionsformel für reguläre 2×2-Matrizen mittels der Adjunkten A^{ad}:

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \implies A^{\mathrm{ad}} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \implies AA^{\mathrm{ad}} = \det A \cdot E\,.$$

b) Es ist $S^2 = E$, $\operatorname{ord} S = 2$ sowie

$$R_n^l = E \iff \frac{2l\pi}{n} \in 2\pi\mathbb{Z} \iff n \mid l\,,$$

also $\operatorname{ord} R_n = n$. Aufgrund der Vertauschungsregel a) lassen sich in einem Potenzprodukt von S und R_n die Potenzen von S nach vorne zusammenfassen und man erhält

$$D_{2n} = \{S^m R_n^l \mid 0 \le m < 2 = \operatorname{ord} S\,,\ 0 \le l < n = \operatorname{ord} R_n\}$$

und diese Darstellung ist eindeutig:

$$S^m R_n^l = E \implies S^m \in \langle R_n\rangle \iff m = 0\,,$$

denn wegen $\det S = -1$ und $\det R_n = +1$ gilt $S \notin \langle R_n\rangle$. Mit dieser eindeutigen Darstellung kann man D_{2n} abzählen und erhält $\#D_{2n} = 2 \cdot n$.

c) $n = 1 \implies R_1 = E \implies D_2 = \langle S\rangle \simeq \mathbb{Z}/2\mathbb{Z}$.
$n = 2 \implies \operatorname{ord} S = \operatorname{ord} R_2 = 2 \underset{a)}{\implies} SR_2 = R_2S \implies D_4$ abelsch.

$D_4 = \{E, S, R_2, SR_2\}$, die drei Elemente $\neq E$ haben die Ordnung 2 und das Produkt von je zweien davon ergibt das dritte. Damit ist D_4 isomorph zur additiven Gruppe $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$.

d) $n \ge 3 \implies \operatorname{ord} R_n = n > 2 \implies R_n^{-1} \neq R_n \underset{\text{a)}}{\implies} SR_n \neq R_nS$, D_{2n} ist nicht abelsch.

$n = 3 \implies D_6 = \{E, S, R_3, R_3^{-1}, SR_3, SR_3^{-1}\}$ ist eine nicht-abelsche Gruppe der Ordnung 6. Mit der Transposition $\tau = (1,2)$ und dem 3-Zyklus $\sigma = (1,2,3)$ erhält man $S_3 = \{\mathrm{id}, \tau, \sigma, \sigma^{-1}, \tau\sigma, \tau\sigma^{-1}\}$ mit denselben Elementordnungen und derselben Vertauschungsrelation $\tau\sigma = \sigma^{-1}\tau$ wie D_6, so dass die Zuordnung $S \mapsto \tau$, $R_3 \mapsto \sigma$ einen Gruppenisomorphismus liefert.

e) Die obigen geometrischen Überlegungen zeigen, dass das n-Eck von S und R_n in sich abgebildet wird, also auch von der gesamten Gruppe D_{2n}. Umgekehrt sind die orthogonalen Abbildungen der Ebene Drehungen ($\det A = 1$) oder Spiegelungen ($\det A = -1$) an einer Gerade. Drehungen, die das n-Eck in sich überführen, müssen eine der Drehungen R_n^k um einen Winkel $2k\pi/n$ sein. Ist A eine Spiegelung, die das n-Eck in sich abbildet, so ist SA eine orthogonale Abbildung mit Determinante $+1$, also eine Drehung, die ebenfalls das n-Eck in sich abbildet. Also ist $SA = R_n^l$ und $A = SR_n^l \in D_{2n}$.

Algebra
Übung 2

Aufgabe 7. (m)
Sei $f : G_1 \to G_2$ ein Homomorphismus von Gruppen. Zeigen Sie:

a) $\operatorname{ord}(f(g))$ teilt $\operatorname{ord}(g)$ für jedes $g \in G_1$.

b) Für jede Untergruppe H von G_1 gilt

$$f^{-1}(f(H)) = \langle H, \operatorname{Ke} f \rangle .$$

c) f besitzt (nach Homomorphiesatz) eine (kanonische) Zerlegung $f = f_3 \circ f_2 \circ f_1$ mit einem Epimorphismus f_1, einem Isomorphismus f_2 und einem Monomorphismus f_3.

Lösung:
a) Sei $n = \operatorname{ord}(g)$, also $g^n = e$. Dann gilt $f(g)^n = f(g^n) = f(e) = e$ und somit $\operatorname{ord}(f(g)) \mid n = \operatorname{ord}(g)$.
b) Es gilt natürlich $H \subset f^{-1}(f(H))$ und $\operatorname{Ke} f \subset f^{-1}(f(H))$, also $\langle H, \operatorname{Ke} f \rangle \subset f^{-1}(f(H))$. Sei nun umgekehrt $a \in f^{-1}(f(H))$, also $f(a) \in f(H)$, d. h. $f(a) = f(h)$ für ein $h \in H$. Dann folgt $ah^{-1} \in \operatorname{Ke} f$, also $a = (ah^{-1}) \cdot h \in \langle \operatorname{Ke} f, H \rangle$.
c) Sei $f_1 = \nu_{\operatorname{Ke} f} : G_1 \twoheadrightarrow G_1/\operatorname{Ke} f$ der natürliche Epimorphismus, $f_2 : G_1/\operatorname{Ke} f \xrightarrow{\sim} \operatorname{Im} f$ der Isomorphismus laut Homomorpiesatz (Vorlesung I.1.20 a), p. 12) und $f_3 : \operatorname{Im} f \hookrightarrow G_2$ die Inklusionsabbildung.

Aufgabe 8. (m)
Für eine Gruppe G und eine Untergruppe $N \leq G$ bezeichne

$$V(G, N) := \{H \mid N \leq H \leq G\}$$

die Menge der Untergruppen zwischen N und G und $V(G) := V(G, \{e\})$ die Menge aller Untergruppen von G.

a) Zeigen Sie, dass $V(G, N)$ bzgl. der Inklusion ein Verband ist, d. h. zu je zwei Zwischengruppen $H_1, H_2 \in V(G, N)$ gibt es in $V(G, N)$ das Infimum (größte untere Schranke) und das Supremum (kleinste obere Schranke).

b) $f : G_1 \to G_2$ sei ein Homomorphismus der Gruppen G_1, G_2. Zeigen Sie:

(i) $\tilde{f} : V(\operatorname{Im} f) \to V(G_1, \operatorname{Ke} f)$, $H \mapsto f^{-1}(H)$ ist eine inklusionstreue Bijektion (ein Verbandsisomorphismus).

(ii) $\tilde{f}$ ist indextreu und normalteilertreu, d. h. für $H \leq \operatorname{Im} f$ gilt:

$$(\operatorname{Im} f : H) = (G_1 : f^{-1}(H)) , \quad H \lhd \operatorname{Im} f \iff f^{-1}(H) \lhd G_1 .$$

(iii) Für $N \lhd \operatorname{Im} f$ gilt $\operatorname{Im} f/N \simeq G_1/f^{-1}(N)$.

Lösung:
a) $H_1 \cap H_2 \in V(G, N)$ ist größte untere Schranke von H_1, H_2 (bzgl. $\subset$). $\langle H_1, H_2 \rangle \in V(G, N)$ ist die kleinste Untergruppe von G, die H_1 und H_2 enthält, also ist dies die kleinste obere Schranke in $V(G, N)$.
b) (i) $H_1 \subseteq H_2 \subseteq \operatorname{Im} f \implies f^{-1}(H_1) \subseteq f^{-1}(H_2)$, also ist $\tilde{f}$ inklusionstreu.
$f^{-1}(H) \supset f^{-1}(\{e\}) = \operatorname{Ke} f$, also $\tilde{f} : V(\operatorname{Im} f) \to V(G_1, \operatorname{Ke} f)$.

$\tilde{f}$ hat die Umkehrabbildung

$$V(G_1, \operatorname{Ke} f) \to V(\operatorname{Im} f)\,,\ H \mapsto f(H)\,,$$

denn $f(\tilde{f}(H)) = f(f^{-1}(H)) \underset{H \subseteq \operatorname{Im} f}{=} H$ und umgekehrt:

$$H \in V(G_1, \operatorname{Ke} f) \implies \tilde{f}(f(H)) = f^{-1}(f(H)) \underset{7.b)}{=} \langle H, \operatorname{Ke} f\rangle \underset{\operatorname{Ke} f \subseteq H}{=} H\,.$$

(ii) Sei $f(a_i)$ $(i \in I)$ ein vollständiges Repräsentantensystem der Nebenklassen von H in $\operatorname{Im} f$ und $a \in G_1$ beliebig. Dann existiert genau ein $i \in I$ mit $f(a) \in f(a_i)H$. Nun gilt

$$f(a) \in f(a_i)H \iff f(a_i^{-1}a) \in H \iff a_i^{-1}a \in f^{-1}(H) \iff a \in a_i f^{-1}(H)\,.$$

Also bilden die a_i $(i \in I)$ ein vollständiges Repräsentantensystem der Nebenklassen von $f^{-1}(H)$ in G_1 und die entsprechenden Indizes stimmen überein.
Nun zur Behauptung über Normalteiler. Für $H \leq \operatorname{Im} f$ gilt gemäß b) (i)

$$\begin{aligned} f^{-1}(H) \lhd G_1 &\iff \bigwedge_{a \in G_1} af^{-1}(H)a^{-1} = f^{-1}(H) \\ &\underset{\text{b)(i)}}{\iff} \bigwedge_{a \in G_1} f(af^{-1}(H)a^{-1}) = f(f^{-1}(H)) = H \\ &\iff \bigwedge_{a \in G_1} f(a)Hf(a)^{-1} = H \iff H \lhd f(G_1) = \operatorname{Im} f\,. \end{aligned}$$

(iii) Wir betrachten $\nu_N \circ f : G_1 \twoheadrightarrow \operatorname{Im} f/N$. Es gilt $\operatorname{Ke}(\nu_N \circ f) = f^{-1}(\operatorname{Ke} \nu_N) = f^{-1}(N)$ und aus dem Homomorphiesatz (Vorlesung I.1.20 a), p. 12) folgt die Behauptung.

Aufgabe 9. (s)
Für eine Gruppe G und Elemente $a, b \in G$ heißt $[a, b] = a^{-1}b^{-1}ab$ Kommutator von a, b und $G' = \langle [a, b] \mid a, b \in G\rangle$ die Kommutatorgruppe von G. Zeigen Sie:

a) G' ist Normalteiler in G und die *Faktorkommutatorgruppe* G/G' ist abelsch.

b) Für einen Normalteiler N von G mit abelscher Faktorgruppe G/N gilt $G' \leq N$.

c) Zu N wie in b) existiert ein (kanonischer) Epimorphimus $\varphi : G/G' \twoheadrightarrow G/N$:

Dies bedeutet: Die Kommutatorgruppe ist der kleinste Normalteiler mit abelscher Faktorgruppe und jede abelsche Faktorgruppe ist epimorphes Bild der Faktorkommutatorgruppe.

Lösung:
a) Nach der Vorlesung, Beispiele I.1.19 (7), ist durch $\iota_g(x) = gxg^{-1}$ ein Automorphismus von G definiert, also $\iota_g([a, b]) = [\iota_g(a), \iota_g(b)]$ und daher $gG'g^{-1} = \iota_g(G') = G'$: $G' \lhd G$.
Seien $a, b \in G$ und $\bar{a}, \bar{b} \in G/G'$ ihre Restklassen. Dann gilt $\bar{a}\bar{b} = \bar{b}\bar{a} \iff abG' = baG' \iff a^{-1}b^{-1}ab \in G' \iff [a, b] \in G'$. Letzteres gilt nach Definition, also ist G/G' abelsch.
b) Sei G/N abelsch, also

$$\bigwedge_{a,b \in G} abN = baN \iff \bigwedge_{a,b \in G} [a, b] \in N \iff G' \subseteq N\,.$$

c) Sei $\nu_N : G \to G/N$ der natürliche Epimorphismus. Da G/N abelsch ist, ist $G' \subseteq N = \operatorname{Ke} \nu_N$. Damit existiert nach dem Faktorisierungslemma (siehe Vorlesung S. 12) ein Epimorphismus $G/G' \twoheadrightarrow G/N$ mit $aG' \mapsto \nu_N(a) = aN$.

Aufgabe 10. (s)
Zeigen Sie:

a) Sind H_1, H_2 zwei Untergruppen der Gruppe G von endlichem Index, so hat auch $H_1 \cap H_2$ endlichen Index in G.

b) Ist H eine Untergruppe von endlichem Index in der Gruppe G, so enthält H einen Normalteiler von G von endlichem Index.

Lösung:
a) Nach Aufgabe 5 a) ist $(H_1 : H_1 \cap H_2) \leq (G : H_2) < \infty$, also nach dem Satz von Lagrange $(G : H_1 \cap H_2) = (G : H_1)(H_1 : H_1 \cap H_2) < \infty$.
b) Gesucht ist ein Normalteiler $N \triangleleft G$ mit $N \subseteq H$. Dann muss gelten $N = gNg^{-1} \subset gHg^{-1}$ für alle $g \in G$. Nun ist $N := \bigcap_{g\in G} gHg^{-1}$ tatsächlich Untergruppe und Normalteiler in G. Wir wollen zeigen, dass dieses N endlichen Index in G hat. Da H endlichen Index in G hat, gibt es endlich viele $g_i \in G$ mit $G = \bigcup_{i=1}^{r} g_i H$, also ist jedes $g \in G$ darstellbar als $g_i h_i$ mit $h_i \in H$. Dann gilt $gHg^{-1} = g_i h_i H h_i^{-1} g_i^{-1} = g_i H g_i^{-1}$ und $N = \bigcap_{i=1}^{r} g_i H g_i^{-1}$ ist endlicher Durchschnitt von Untergruppen $g_i H g_i^{-1}$ mit endlichem Index in G. Aus a) folgt induktiv, dass ein solcher Durchschnitt selbst endlichen Index in G hat.

Aufgabe 11. (s)
Für die Diedergruppe D_{2n} bestimme man das Zentrum und die Kommutatorgruppe sowie bis auf Isomorphie die Faktorgruppen nach diesen Normalteilern.

Lösung:
Der Fall $n \leq 2$ ist klar nach Aufgabe 6.c): D_2, D_4 sind abelsch, das Zentrum ganz D_{2n}, die Faktorgruppe trivial, während die Kommutatorgruppe trivial und deren Faktorgruppe (isomorph zu) D_{2n} ist.
Sei im Folgenden also $n \geq 3$, $D := D_{2n}$, $Z := \mathrm{Zentr}(D_{2n})$, $R := R_n$. Wir rekapitulieren die Ergebnisse von Aufgabe 6: $\operatorname{ord} S = 2$, $\operatorname{ord} R = n$, $SR = R^{-1}S$, $\mathcal{R} := \langle R\rangle \triangleleft D$, $D = \mathcal{R} \cup \mathcal{R} \cdot S$.
Wir berechnen die Kommutatoren in der Diedergruppe. Es gilt für $0 \leq k, l < n$:

$$\begin{aligned} [R^k, R^l] &= E && (1)\\ [R^k S, R^l] &= SR^{-k} \cdot R^{-l} \cdot R^k S \cdot R^l = SR^{-l} S R^l = R^{2l}\,, && (2)\\ [R^k S, R^l S] &= R^k S \cdot R^l S \cdot R^k S \cdot R^l S = R^{k-l} S^2 R^{k-l} S^2 = R^{2(k-l)}\,. && (3) \end{aligned}$$

Wir erhalten als Kommutatorgruppe $D' = \langle [A, B] \mid A, B \in D\rangle = \langle R^2\rangle \leq \mathcal{R}$ und berechnen die Ordnung von R^2:

$$R^{2l} = E \iff n = \operatorname{ord} R \mid 2l \iff \begin{cases} n \mid l & n \text{ ungerade},\\ \frac{n}{2} \mid l & n \text{ gerade}. \end{cases}$$

Dies bedeutet

$$\#D' = \operatorname{ord} R^2 = \begin{cases} n & n \text{ ungerade}\\ \frac{n}{2} & n \text{ gerade} \end{cases}, \quad D' = \begin{cases} \mathcal{R} & n \text{ ungerade}\\ \langle R^2\rangle & n \text{ gerade} \end{cases}.$$

Damit ist für ungerades n $D/D' \simeq D/\mathcal{R} \simeq \mathbb{Z}/2\mathbb{Z}$ zyklisch von der Ordnung 2, während für gerades n gilt D/D' ist abelsch von der Ordnung 4, erzeugt von zwei Elementen $\bar{S}$ und $\bar{R}$ der Ordnung 2, also $D/D' \simeq V_4$ (siehe Vorlesung, Beweis von Prop. (2.6) c), p. 16).
Bestimmung von Z: Da D von R, S erzeugt wird, sind die Zentrumselemente diejenigen, die mit R und S vertauschbar sind, also $A \in Z \iff [R, A] = [S, A] = E$. Für $A = R^l$ bzw. $A = R^l S$ gilt (nach obigen Rechnungen mit passenden k, l):

$$[R, R^l] = E\,,\ [S, R^l] \underset{(2)}{=} R^{2l}\,,$$
$$[R, R^l S] = [R^l S, R]^{-1} \underset{(2)}{=} R^{-2}\,,\ [S, R^l S] \underset{(3)}{=} R^{-2l}$$

Dies bedeutet: $R^l \in Z \iff R^{2l} = E$ und $R^l S \in Z \iff R^2 = E \iff n \leq 2$. Wegen $n \geq 3$ tritt der zweite Fall nicht auf, es bleibt also nur

$$R^l \in Z \iff R^{2l} = E \underset{\text{s.o.}}{\iff} \begin{cases} n \mid l & n \text{ ungerade} \\ \frac{n}{2} \mid l & n \text{ gerade} \end{cases} \iff R^l = \begin{cases} E & n \text{ ungerade,} \\ R^{\frac{n}{2}} & n \text{ gerade.} \end{cases}$$

Wegen $R^{\frac{n}{2}} = -E$ erhalten wir so (für $n \geq 3$) $Z = \begin{cases} \{E\} & n \text{ ungerade,} \\ \{E, -E\} & n \text{ gerade.} \end{cases}$
Für ungerades n ist also $D/Z \simeq D$, während für gerades $n > 2$ gilt:

$$D/Z = \langle \bar{R}, \bar{S} \rangle \quad \text{mit } \operatorname{ord} \bar{S} = 2\,,\ \operatorname{ord} \bar{R} = \frac{n}{2}\,,\ \bar{S}\bar{R} = \bar{R}^{-1}\bar{S}\,,$$

die Faktorgruppe D/Z ist also gerade die Diedergruppe D_n der halben Ordnung n.

Aufgabe 12. (s)
Bestimmen Sie (bis auf Isomorphie) alle Gruppen der Ordnung ≤ 6.

Lösung:
Zu jeder Ordnung $n \in \mathbb{N}$ gibt es genau eine zyklische Gruppe dieser Ordnung, $\mathbb{Z}/n\mathbb{Z}$. Ist n eine Primzahl, so gibt es nur die zyklische Gruppe der Ordnung n (siehe Vorlesung Korollar (1.14), p. 9 bzw. Übung 1, Aufgabe 4.). Wir bestimmen nun die nicht-zyklischen Gruppen der Ordnung 4 und 6.
Sei G eine Gruppe der Ordnung 4: Ist G nicht zyklisch, so hat kein Element die Ordnung 4, alle Elemente $\neq e$ haben die Ordnung 2 (Satz von Lagrange, Korollar (1.13), p. 9). Seien nun σ, τ 2 verschiedene Elemente $\neq e$ in G. Dann ist $\sigma\tau$ von σ und τ verschieden, außerdem gilt auch $\sigma\tau \neq \sigma^2 = e$. Also ist $\sigma\tau$ das verbleibende vierte Element in G: $G = \{e, \sigma, \tau, \sigma\tau\}$. Dasselbe gilt für das umgekehrte Produkt $\tau\sigma$, also $\tau\sigma = \sigma\tau$, G ist abelsch. Wegen $\sigma \cdot \sigma\tau = \sigma^2\tau = \tau$ und $\tau \cdot \sigma\tau = \sigma\tau^2 = \sigma$ ergibt in G das Produkt von je zwei Elementen $\neq e$ das jeweils dritte Element $\neq e$ und wir erhalten genau die Multiplikationstafel der Kleinschen Vierergruppe.
Sei G eine Gruppe der Ordnung 6: Ist G nicht zyklisch, so haben alle Elemente $\neq e$ die Ordnung 2 oder 3. Angenommen $\sigma^2 = e$ für alle $\sigma \in G$. Dann wäre G abelsch (Übung 1, Aufgabe 2 b)) und G besäße einen Normalteiler $N = \langle \sigma \rangle$ der Ordnung 2. Die Faktorgruppe G/N wäre zyklisch von der Ordnung 3. Mit $\tau \notin N$ erhielten wir den Widerspruch $\bar{\tau}^2 = \bar{e}$, also $\operatorname{ord} \bar{\tau} = 2 \mid \#(G/N) = 3$. Wid.
Also gibt es in G ein Element σ der Ordnung 3. Dann hat $N = \langle \sigma \rangle$ den Index 2, ist also Normalteiler in G (Übung 1, Aufgabe 3.c)) und $G/N = \langle \bar{\tau} \rangle$ zyklisch von der Ordnung 2. Also $\tau^2 \in N$. Dann muss $\tau^2 = e$ und $\operatorname{ord} \tau = 2$ sein, denn andernfalls hätte $\tau^2 \in N$ die Ordnung 3 und somit τ die Ordnung 6. Dann wäre G aber zyklisch, im Gegensatz zur Voraussetzung.
Also $G = \langle \sigma, \tau \rangle$ mit $\operatorname{ord} \sigma = 3$, $\operatorname{ord} \tau = 2$. Wäre $\sigma\tau = \tau\sigma$, so wäre $(\sigma\tau)^2 = \sigma^2 \neq e$ und $(\sigma\tau)^3 = \tau \neq e$ und daher $\operatorname{ord}(\sigma\tau) = 6$, Wid. Also ist G nicht abelsch und daher $\sigma \neq \tau\sigma\tau^{-1} \in N \implies \tau\sigma\tau^{-1} = \sigma^{-1}$.
Wir fassen zusammen: $G = \langle \sigma, \tau \rangle$ mit $\operatorname{ord} \sigma = 3$, $\operatorname{ord} \tau = 2$ und $\tau\sigma = \sigma^{-1}\tau$ und daher $G \simeq D_6 \simeq S_3$ (Übung 1, Aufgabe 6.).

Algebra
Übung 3

Aufgabe 13. (m)
Es sei S_n die symmetrische Gruppe vom Grade n und $(a_1, \ldots, a_k)$ ein Zyklus der Länge k.

a) Zeigen Sie $(a_1, \ldots, a_k) = (a_1, a_k) \circ (a_1, a_{k-1}) \circ \ldots \circ (a_1, a_2)$ und folgern Sie, dass jedes $\sigma \in S_n$ als Produkt von Transpositionen darstellbar ist.

b) Zeigen Sie für beliebiges $\sigma \in S_n$

$$\sigma \circ (a_1, \ldots, a_k) \circ \sigma^{-1} = (\sigma(a_1), \ldots, \sigma(a_k)) \,.$$

c) In S_n seien die Transposition $\tau = (1, 2)$ und der n-Zyklus $\sigma_n = (1, 2, \ldots, n)$ gegeben. Zeigen Sie:

α) $\tau_k := (k, k+1) \in \langle \sigma_n, \tau \rangle$ für alle $1 \leq k < n$.

β) $(i, j) = \tau_{j-1} \circ \ldots \circ \tau_{i+1} \circ \tau_i \circ \tau_{i+1} \ldots \circ \tau_{j-1}$ für $1 \leq i < j \leq n$.

d) Aus a) und c) folgere man $S_n = \langle \sigma_n, \tau \rangle$: Ganz S_n wird bereits durch 2 Elemente erzeugt.

Lösung:
a) Induktion: $k = 2$ ist klar. Der Schritt $k \to k+1$ folgt sofort aus

$$(a_1, a_k) \circ (a_1, \ldots, a_{k-1}) = (a_1, \ldots, a_k) \,.$$

Damit ist jeder Zyklus als Produkt von Transpositionen darstellbar. Da jede Permutation Produkt (elementfremder) Zyklen ist, ergibt sich die behauptete Folgerung.
b) Wir berechnen die Wirkung der linken Seite auf die $\sigma(a_i)$:

$$\sigma \circ (a_1, \ldots, a_k) \circ \sigma^{-1}(\sigma(a_i)) = \sigma \circ (a_1, \ldots, a_k)(a_i) = \begin{cases} \sigma(a_{i+1}) & i < k \\ \sigma(a_1) & i = k \end{cases}$$

Alle Elemente $\neq \sigma(a_i)$ werden nicht bewegt; die linke Seite ist gleich dem Zyklus rechts in b).
c) α) $\tau_k = (k, k+1) = (\sigma_n^{k-1}(1), \sigma_n^{k-1}(2)) \underset{\text{b)}}{=} \sigma_n^{k-1} \circ (1, 2) \circ \sigma_n^{-(k-1)} \in \langle \sigma_n, \tau \rangle$.
β) Sei ρ_{ij} das auf der rechten Seite angegebene Produkt. Wir beweisen die Behauptung bei festem $i < n$ per Induktion über $j = i+1 \ldots, n$: $j = i+1$ ist klar, denn dann ist das Produkt $\tau_{i+1} \circ \ldots \circ \tau_{j-1}$ leer und die Behauptung lautet einfach $(i, i+1) = \tau_i$, was genau die Definition ist. Induktionsschritt $j \to j+1$: $\rho_{i,j+1} = \tau_j \circ \rho_{ij} \circ \tau_j \underset{\text{Ind.Vor.}}{=} (j, j+1) \circ (i, j) \circ (j, j+1) = (i, j+1)$.
d) Nach a) sind alle Permutationen als Produkt von Transpositionen darstellbar, nach c) β) ist jede Transposition Produkt von Elementen τ_k, die nach c) α) in $\langle \sigma_n, \tau \rangle$ liegen.

Aufgabe 14. (s)
Es sei $n \geq 3$. Wir definieren in der alternierenden Gruppe A_n die 3-Zyklen

$$\delta_k := (k, k+1, k+2) \quad \text{und} \quad \delta'_k = (1, k+1, k+2) \quad \text{für } 1 \leq k \leq n-2 \,.$$

a) Zeigen Sie induktiv

$$A_n = \langle \delta_1, \ldots, \delta_{n-2} \rangle = \langle \delta'_1, \ldots, \delta'_{n-2} \rangle \,.$$

[Beim Induktionsbeweis unterscheidet man zweckmäßigerweise für $\sigma \in A_n$ die Fälle $\sigma(n) = n$ und $\sigma(n) = j < n$.]

b) Zeigen Sie mittels a) und 13.b)

$$A_n = \langle \sigma, \delta \rangle \quad \text{für} \quad \delta := (1,2,3)\,,\ \sigma := \begin{cases} (1,2,\ldots,n) & n \text{ ungerade,} \\ (2,3,\ldots,n) & n \text{ gerade.} \end{cases}$$

Lösung:
a) Seien $B_n = \langle \delta_1, \ldots, \delta_{n-2} \rangle$ und $B'_n = \langle \delta'_1, \ldots, \delta'_{n-2} \rangle$ die beiden Gruppenerzeugnisse auf der rechten Seite der Behauptung. Offenbar $B_n, B'_n \subseteq A_n$.
Wir zeigen $A_n \subseteq B_n \cap B'_n$ per Induktion über n.
Induktionsanfang $n = 3$: A_3 ist zyklisch von der Ordnung 3, erzeugt von $(1,2,3) = \delta_1 = \delta'_1$.
Schritt $n-1 \to n$: Sei $\sigma \in A_n$. Im Falle $\sigma(n) = n$ gilt $\sigma \in A_{n-1} = B_{n-1} = B'_{n-1} \subseteq B_n \cap B'_n$. Sei nun $\sigma(n) = j < n$. Setzt man $\delta_{n-1} := \delta_{n-2} = (n-2, n-1, n)$ und $\delta'_0 := \delta'_1 = (1,2,3)$, so gilt für alle $1 \le i < n$ $\delta_i(i) = i+1 = \delta'_{i-1}(i)$. Durch Hintereinanderausführung erhält man so Elemente $\rho \in B_n$, $\rho' \in B'_n$ mit $\rho(j) = n = \rho'(j)$. Dann ist $\rho \circ \sigma(n) = n = \rho' \circ \sigma(n)$ und daher gilt nach dem ersten Fall $\rho \circ \sigma \in B_n$ und damit $\sigma \in \rho^{-1} B_n = B_n$. Genauso folgert man $\sigma \in B'_n$.
b) Gemäß der Definition ist σ ein Zyklus ungerader Länge, also $\sigma \in A_n$ nach Prop. I.2.5 a), p. 15. Ist nun n ungerade, so ist $\sigma = (1,\ldots,n)$ und somit

$$\delta_k = (k, k+1, k+2) = (\sigma^{k-1}(1), \sigma^{k-1}(2), \sigma^{k-1}(3)) \underset{13.b}{=} \sigma^{k-1} \circ \delta \circ \sigma^{-(k-1)} \in \langle \sigma, \delta \rangle\,.$$

Ist dagegen n gerade, so ist $\sigma = (2,\ldots,n)$ und daher

$$\delta'_k = (1, k+1, k+2) = (\sigma^{k-1}(1), \sigma^{k-1}(2), \sigma^{k-1}(3)) = \sigma^{k-1} \circ \delta \circ \sigma^{-(k-1)} \in \langle \sigma, \delta \rangle\,.$$

In jedem Falle ist also nach a) $A_n = B_n = B'_n \subseteq \langle \sigma, \delta \rangle \subseteq A_n$, womit b) bewiesen ist.

Aufgabe 15. (s)

a) Seien $f, g : G \to H$ Homomorphismen von Gruppen und M ein Erzeugendensystem von G. Zeigen Sie: $f(a) = g(a)$ für alle $a \in M \implies f = g$.

b) Sei G eine endliche Gruppe. Zeigen Sie, dass G ein Erzeugendensystem $\{a_1, \ldots, a_m\}$ ($m \in \mathbb{N}$) besitzt mit $a_{i+1} \notin \langle a_1 \ldots, a_i \rangle$ für alle $1 \le i < m$.

c) Folgern Sie für $n := \#G$:

$$n \ge 2^m\,, \quad \#\mathrm{Aut}(G) \le n^m \le n^{\log_2(n)} = n^{\ln n / \ln 2}\,.$$

Lösung:
a) $F := \{a \in G \mid f(a) = g(a)\}$ ist eine Untergruppe von G, denn: $e \in F$, $a, b \in F \implies f(a^{-1}b) = f(a)^{-1} f(b) = g(a)^{-1} g(b) = g(a^{-1}b) \implies a^{-1}b \in F$. Die Untergruppe F umfasst nach Voraussetzung M, also folgt $G = \langle M \rangle \subset F$, $f = g$.
b) Wir wählen $a_1 \neq e$ und dann rekursiv $a_{i+1} \notin \langle a_1, \ldots, a_i \rangle$ bis kein solches a_{i+1} mehr existiert. Dieser Fall muss eintreten, da sonst G unendlich wäre. Existiert kein a_{m+1} außerhalb von $\langle a_1, \ldots, a_m \rangle$, so ist $G = \langle a_1, \ldots, a_m \rangle$.
c) Sei $G_i := \langle a_1, \ldots, a_i \rangle$, dann gilt

$$G_0 < G_1 < \ldots < G_{n-1} < G_m \implies n = \#G \ge \prod_{i=1}^{m} (G_i : G_{i-1}) \ge 2^m\,.$$

Nach a) ist die Abbildung $\mathrm{Aut}(G) \to G^M = \mathrm{Abb}(M, G)$, $f \mapsto f|_M$ injektiv, also ist $\#\mathrm{Aut}(G) \le \#(G^M) = \#G^{\#M} = n^m$. Der Rest ist klar nach Logarithmusdefinition.

Aufgabe 16. (s)
Sei G eine Gruppe und $N \lhd G$. Beweisen Sie die Äquivalenz der Aussagen

(i) Es gibt einen Isomorphismus $\varphi = \varphi_1 \times \nu_N : G \to N \times G/N$.

(ii) Es gibt einen Homomorphismus $f : G \to N$ mit $f|_N = \mathrm{id}_N$.

Lösung:
(ii)⇒(i): Setze $\varphi := f \times \nu_N : G \to N \times G/N$.
Injektivität:

$$\begin{aligned} g \in \operatorname{Ke}\varphi &\iff (e, \bar{e}) = \varphi(g) = (f(g), \nu_N(g)) = (f(g), \bar{g}) \\ &\iff e = f(g) \ \wedge \ g \in N \underset{f|_N = \mathrm{id}_N}{\iff} e = f(g) = g\,. \end{aligned}$$

Surjektivität: Sei $(n, \bar{a}) \in N \times G/N$. Gesucht $g \in G$ mit

$$\begin{aligned} \varphi(g) = (n, \bar{a}) &\iff f(g) = n \ \wedge \ \nu_N(g) = \bar{a} \iff f(g) = n \ \wedge \ a^{-1}g \in N \\ &\implies n = f(a \cdot a^{-1}g) = f(a) \cdot f(a^{-1}g) \underset{f|_N = \mathrm{id}_N}{=} f(a) \cdot a^{-1}g \\ &\implies g = a \cdot \underbrace{f(a)^{-1}n}_{\in N}\,. \end{aligned}$$

Das so gefundene $g \in G$ ist tatsächlich Urbild von $(n, \bar{a})$:

$$\begin{aligned} f(g) &= f(a) \cdot f(f(a)^{-1}n) \underset{f|_N = \mathrm{id}_N}{=} f(a) \cdot f(a)^{-1}n = n\,, \\ \nu_N(g) &= \nu_N(a) \cdot \nu_N(f(a)^{-1}n) = \bar{a} \cdot \bar{e} = \bar{a}\,. \end{aligned}$$

(i)⇒(ii): Erster Ansatz: $f = \varphi_1 : G \to N$. Problem: $f|_N = \mathrm{id}_N$? Nun gilt:

$$n \in N \implies \varphi(n) = (\varphi_1(n), \nu_N(n)) = (\varphi_1(n), \bar{e}) \implies n = \varphi^{-1}(\varphi_1(n), \bar{e})\,.$$

Setzt man also $f(g) := \varphi^{-1}(\varphi_1(g), \bar{e})$, so gilt $f(n) = n$ für $n \in N$. Außerdem hat der so definierte Homomorphismus f Werte in N, denn

$$(\varphi_1(g), \bar{e}) = \varphi(f(g)) = (\varphi_1(f(g)), \nu_N(f(g))) \implies \nu_N(f(g)) = \bar{e} \implies f(g) \in N\,.$$

Aufgabe 17. (s)
Sei G eine Gruppe.

a) Beweisen Sie für $\varphi \in \mathrm{Aut}(G)$ die Äquivalenz

$$\bigwedge_{\psi \in \mathrm{Inn}(G)} \varphi \circ \psi = \psi \circ \varphi \iff \bigwedge_{a \in G} a^{-1}\varphi(a) \in \mathrm{Zentr}(G)\,.$$

b) Zeigen Sie: $\mathrm{Zentr}(G) = \{e\} \implies \mathrm{Zentr}_{\mathrm{Aut}(G)}(\mathrm{Inn}(G)) = \{\mathrm{id}\}$.

c) Sei G eine Gruppe mit trivialem Zentrum $\mathrm{Zentr}(G) = \{e\}$. Zeigen Sie mittels b) für jeden Automorphismus $f : \mathrm{Aut}(G) \to \mathrm{Aut}(G)$ (d. h. $f \in \mathrm{Aut}(\mathrm{Aut}(G))$):

$$f|_{\mathrm{Inn}(G)} = \mathrm{id}_{\mathrm{Inn}(G)} \implies f = \mathrm{id}_{\mathrm{Aut}(G)}\,.$$

[Tipp zu c): $\varphi \in \mathrm{Aut}(G)\,,\ \psi \in \mathrm{Inn}(G) \implies \varphi \circ \psi \circ \varphi^{-1} \in \mathrm{Inn}(G)$.]

Lösung:
a) Zur Erinnerung (siehe Vorlesung Beispiele I.1.19 7),8), p. 11):
$\mathrm{Inn}(G) = \{\iota_a \mid a \in G\}$ ist die Gruppe aller inneren Automorphismen $\iota_a : G \to G$ definiert durch $\iota_a(b) = aba^{-1}$ (für $a, b \in G$). Es gilt daher für jeden beliebigen Automorphismus $\varphi : G \to G$:

$$\begin{gathered}\textstyle\bigwedge_{\psi\in\mathrm{Inn}(G)} \varphi\circ\psi = \psi\circ\varphi \iff \bigwedge_{a\in G} \varphi\circ\iota_a = \iota_a\circ\varphi \iff \bigwedge_{a,b\in G} \varphi(aba^{-1}) = a\varphi(b)a^{-1} \\ \iff \textstyle\bigwedge_{a,b\in G} \varphi(a)\varphi(b)\varphi(a)^{-1} = a\varphi(b)a^{-1} \iff \bigwedge_{a,b\in G} a^{-1}\varphi(a)\varphi(b) = \varphi(b)a^{-1}\varphi(a) \\ \underset{\varphi(G)=G}{\iff} \textstyle\bigwedge_{a,c\in G} a^{-1}\varphi(a)\cdot c = c\cdot a^{-1}\varphi(a) \iff \bigwedge_{a\in G} a^{-1}\varphi(a) \in \mathrm{Zentr}(G)\end{gathered}$$

b) Es sei $\mathrm{Zentr}(G) = \{e\}$. Dann gilt nach a)

$$\begin{gathered}\varphi \in \mathrm{Zentr}_{\mathrm{Aut}(G)}(\mathrm{Inn}(G)) \iff \textstyle\bigwedge_{\psi\in\mathrm{Inn}(G)} \varphi\circ\psi = \psi\circ\varphi \\ \underset{a)}{\iff} \textstyle\bigwedge_{a\in G} a^{-1}\varphi(a) \in \mathrm{Zentr}(G) = \{e\} \iff \bigwedge_{a\in G} \varphi(a) = a \iff \varphi = \mathrm{id}_G\end{gathered}$$

c) Wir zeigen zuerst den Tipp: Es ist $\psi = \iota_a$ für ein $a \in G$. Dann gilt für alle $b \in G$

$$\varphi\circ\psi\circ\varphi^{-1}(b) = \varphi(\iota_a(\varphi^{-1}(b))) = \varphi(a\cdot\varphi^{-1}(b)\cdot a^{-1}) = \varphi(a)\cdot b\cdot\varphi(a)^{-1} = \iota_{\varphi(a)}(b)\,,$$

also $\varphi\circ\psi\circ\varphi^{-1} = \iota_{\varphi(a)} \in \mathrm{Inn}(G)$: $\mathrm{Inn}(G) \lhd \mathrm{Aut}(G)$. Nach Voraussetzung an f erhalten wir so

$$\begin{gathered}\textstyle\bigwedge_{\psi\in\mathrm{Inn}(G)} \varphi\circ\psi\circ\varphi^{-1} = f(\varphi\circ\psi\circ\varphi^{-1}) = f(\varphi)\circ f(\psi)\circ f(\varphi)^{-1} = f(\varphi)\circ\psi\circ f(\varphi)^{-1} \\ \iff \textstyle\bigwedge_{\psi\in\mathrm{Inn}(G)} \psi\circ\varphi^{-1}\circ f(\varphi) = \varphi^{-1}\circ f(\varphi)\circ\psi \\ \iff \varphi^{-1}\circ f(\varphi) \in \mathrm{Zentr}_{\mathrm{Aut}(G)}(\mathrm{Inn}(G)) \underset{\text{b)}}{=} \{\mathrm{id}\} \iff f(\varphi) = \varphi\end{gathered}$$

Algebra
Übung 4

Aufgabe 18. (m)

a) Sei $n \in \mathbb{N}_+$ und G eine Gruppe, erzeugt von 2 verschiedenen Elementen σ, τ mit den Eigenschaften

$$\operatorname{ord}(\sigma) = n\,, \quad \operatorname{ord}(\tau) = 2\,, \quad \sigma\tau = \tau\sigma^{-1}\,. \tag{$*$}$$

Zeigen Sie, dass sich jedes Element aus G eindeutig in der Form $\tau^\mu\sigma^\nu$ mit $0 \le \mu < 2$, $0 \le \nu < n$ schreiben lässt.

[Beachten Sie im Falle $n = 2$ die explizite Forderung $\sigma \neq \tau$.]

Es sei D_{2n} die in Aufgabe 6. definierte Diedergruppe. Geben Sie einen Isomorphismus $\varphi : G \xrightarrow{\sim} D_{2n}$ an.

b) Seien $S := \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, $T := \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{C})$. Zeigen Sie:

α) $\operatorname{ord} S = 4\,,\ S^2 = T^2$ und $ST = TS^{-1}$.

Die von S, T erzeugte Gruppe $Q_8 := \langle S, T\rangle$ heißt *Quaternionengruppe*.

β) Jedes Element aus Q_8 lässt sich eindeutig in der Form $T^\mu S^\nu$ schreiben mit $0 \le \mu < 2$ und $0 \le \nu < 4$ und es folgt $\#Q_8 = 8$.

c) Zeigen Sie, dass jede nicht-abelsche Gruppe der Ordnung 8 entweder zu D_8 oder Q_8 isomorph ist.

[Tipp: In der Vorlesung wurden alle nicht-abelschen Gruppen der Ordnung 8 durch Erzeugende mit spezifischen Eigenschaften beschrieben (siehe Vorlesung, Gruppen spezieller Ordnung, A), p. 19). Verfahren Sie nun wie unter a).]

Lösung:
a) Nach Voraussetzung gilt $G = \langle\sigma, \tau\rangle$, also ist jedes $g \in G$ darstellbar als Produkt von Elementen der Form $\tau^\mu\sigma^\nu$ mit $\mu, \nu \in \mathbb{Z}$ (Vorlesung Prop. (1.10), p. 7. Aufgrund der Vertauschungsrelation lässt sich ein Produkt solcher Elemente wieder in dieser Form darstellen:

$$\tau^{\mu_1}\sigma^{\nu_1} \cdot \tau^{\mu_2}\sigma^{\nu_2} = \tau^{\mu_1}\tau^{\mu_2}\sigma^{-\nu_1}\sigma^{\nu_2} = \tau^{\mu_1+\mu_2}\sigma^{\nu_2-\nu_1} =: \tau^\mu\sigma^\nu \tag{$**$}$$

und wegen $\operatorname{ord}\tau = 2$ und $\operatorname{ord}\sigma = n$ können $0 \le \mu < 2$ und $0 \le \nu < n$ gewählt werden.
Diese Darstellung ist eindeutig: $\tau^\mu\sigma^\nu = e \iff \tau^\mu = \sigma^{-\nu}$. Ist $\mu = 0$, so folgt auch $\nu = 0$, was zu zeigen war. Wir zeigen nun, dass $\mu = 1$ zum Widerspruch führt:

$$\begin{aligned} &\tau = \sigma^{-\nu} \implies \tau\sigma = \sigma\tau \underset{(*)}{\implies} \tau\sigma = \tau\sigma^{-1} \implies \sigma = \sigma^{-1} \implies \sigma^2 = e \\ &\implies \operatorname{ord}\sigma = n \mid 2 \implies \nu \le 1 \implies \tau = e \ \vee\ \tau = \sigma\,. \end{aligned}$$

Beide letztgenannten Gleichungen ergeben Widersprüche zu $\operatorname{ord}\tau = 2$ bzw. $\tau \neq \sigma$.
Wir definieren $\varphi : G \to D_{2n}$ durch $\varphi(\tau^\mu\sigma^\nu) := S^\mu R_n^\nu$. Da S und R_n genau dieselben Relationen $(*)$ wie τ und σ erfüllen, gelten für sie dieselben Überlegungen zur eindeutigen Darstellbarkeit, so dass φ wohldefiniert, injektiv und surjektiv ist, und es gelten dieselben Rechenregeln (siehe $(**)$), so dass φ ein Homomorphismus ist.
b) α) rechnet man einfach nach.
β) Jedes Element in $Q_8 = \langle S, T\rangle$ ist darstellbar als Produkt von Elementen der Form $T^\mu S^\nu$ mit

$\mu, \nu \in \mathbb{Z}$. Aufgrund der Vertauschungsrelation lässt sich ein Produkt solcher Elemente wieder in dieser Form darstellen:

$$T^{\mu_1} S^{\nu_1} \cdot T^{\mu_2} S^{\nu_2} = T^{\mu_1} T^{\mu_2} S^{-\nu_1} S^{\nu_2} = T^{\mu_1+\mu_2} S^{\nu_2-\nu_1} =: T^{\mu} S^{\nu} \,. \qquad (++)$$

Wegen $T^2 = S^2$ kann dabei $0 \leq \mu < 2$ und wegen $\operatorname{ord} S = 4$ dann $0 \leq \nu < 4$ gewählt werden. Diese Darstellung ist eindeutig: $T^{\mu} S^{\nu} = E \iff T^{\mu} = S^{-\nu}$. Ist $\mu = 0$, so folgt auch $\nu = 0$, was zu zeigen war. Wäre hingegen $\mu = 1$, so wäre T als Potenz der Diagonalmatrix S selbst eine Diagonalmatrix, was offensichtlich nicht der Fall ist. Aufgrund dieser eindeutigen Darstellbarkeit hat Q_8 genau 8 Elemente.
c) Ist G eine nicht-abelsche Gruppe der Ordnung 8 so gilt laut Vorlesung (Gruppen spezieller Ordnung A), p. 19)

$$G = \langle \sigma, \tau \rangle \,, \quad \operatorname{ord} \sigma = 4 \,, \quad \sigma\tau = \tau\sigma^{-1} \quad \text{und} \quad \tau^2 = \begin{cases} e & \text{(D)} \\ \sigma^2 & \text{(Q)} \end{cases} .$$

Im Falle (D) haben wir genau die Bedingungen $(*)$ von a) (mit $n = 4$) und damit $G \simeq D_8$. Im Falle (Q) erfüllen σ, τ genau dieselben Bedingungen wie S, T in Aufgabenteil b) α). Daher ist durch $\varphi(\tau^{\mu}\sigma^{\nu}) := T^{\mu} S^{\nu}$ eine Abbildung wohldefiniert, die injektiv, surjektiv und ein Homomorphismus ist, also einen Isomorphismus $\varphi : G \xrightarrow{\sim} Q_8$ liefert.

Aufgabe 19. (s)

a) Sei G eine Gruppe und $G/\mathrm{Zentr}(G)$ zyklisch. Zeigen Sie: G ist abelsch.

b) Sei p eine Primzahl und G eine Gruppe der Ordnung p^2. Zeigen Sie: G ist zyklisch oder direktes Produkt zweier zyklischer Gruppen der Ordnung p:

$$\#G = p^2 \implies G \simeq \mathbb{Z}/p^2\mathbb{Z} \ \vee \ G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \,.$$

[Tipp: $\mathrm{Zentr}(G) \neq \{e\}$.]

Lösung:
a) Sei $Z := \mathrm{Zentr}(G)$ und $G/Z = \langle \bar{\sigma} \rangle$ nach Voraussetzung zyklisch. Dann sind die Potenzen von σ ein Repräsentantensystem für die Nebenklassen von Z, also $G = \bigcup_{i \in \mathbb{Z}} Z\sigma^i$. Seien nun $a, b \in G$, also $a = z\sigma^i$ und $b = z'\sigma^j$ mit $z, z' \in Z$, $i, j \in \mathbb{Z}$. Dann gilt $ab = z\sigma^i \cdot z'\sigma^j = zz'\sigma^{i+j}$ und umgekehrt genauso $ba = z'\sigma^j \cdot z\sigma^i = z'z\sigma^{i+j} = zz'\sigma^{i+j}$. Also $ab = ba$ für alle $a, b \in G$.
b) Gruppen von Primzahlordnung haben nicht-triviales Zentrum. Im Falle $\#G = p^2$ bedeutet dies entweder $\#\mathrm{Zentr}(G) = p^2$ (und G ist abelsch) oder $\#\mathrm{Zentr}(G) = p$ und daher G/Z primzyklisch. Nach a) ist G auch im zweiten Falle abelsch. G ist dann entweder zyklisch oder alle Elemente $\neq e$ haben die Ordnung p. In letzterem Fall wählen wir $e \neq \sigma \in G$ und $\tau \in G \setminus \langle \sigma \rangle$. Dann ist $N = \langle \sigma \rangle$ ein Normalteiler der Ordnung $\operatorname{ord} \sigma = p$, G/N also von der Ordnung $\frac{\#G}{\#N} = p$ und daher zyklisch, erzeugt von $\bar{\tau} \neq \bar{e}$. Damit ist $G = \dot{\bigcup\limits_{0 \leq l < p}} N\tau^l$, also jedes $\rho \in G$ eindeutig darstellbar als $\rho = \sigma^k \tau^l$ mit $0 \leq k, l < p$. Da G abelsch ist, erhalten wir einen Isomorphismus $\varphi : \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \xrightarrow{\sim} G$, $(k, l) \mapsto \sigma^k \tau^l$.

Aufgabe 20. (s)
Sei G eine Gruppe, H eine Untergruppe. Dann heißt $\mathcal{N}_G(H) := \{\sigma \in g \mid \sigma^{-1} H \sigma = H\}$ der *Normalisator von H in G*. Zeigen Sie:

a) $\mathcal{N}_G(H)$ ist die größte Untergruppe von G, in der H Normalteiler ist.

b) Der Index $(G : \mathcal{N}_G(H))$ ist gleich der Anzahl der verschiedenen Konjugierten $\sigma H \sigma^{-1}$ $(\sigma \in G)$ von H.

Lösung:
a) $N := \mathcal{N}_G(H)$ ist eine Untergruppe von G, denn:

i) $e \in N$,

ii) $\sigma \in N \implies \sigma^{-1}H\sigma = H \implies H = \sigma H \sigma^{-1} \implies \sigma^{-1} \in N$,

iii) $\sigma, \tau \in N \implies \tau^{-1}\sigma^{-1}H\sigma\tau = \tau^{-1}H\tau = H \implies \sigma\tau \in N$.

Nach Definition von $N = \mathcal{N}_G(H)$ ist $H \lhd N$.
Sei $H \lhd U \leq G$. Dann gilt für alle $\sigma \in U$: $\sigma^{-1}H\sigma = H$, also $\sigma \in N$. Damit gilt $U \leq N$.
b) G operiert (von rechts) auf der Menge Ω aller Untergruppen von G durch $U \mapsto U^\sigma := \sigma^{-1}U\sigma$ für $\sigma \in G$. Die Bahn von H unter G ist die Menge aller Konjugierten von H und die Fixgruppe von H ist

$$Fix(H) = \{\sigma \in G \mid H^\sigma = H\} = \mathcal{N}_G(H)\,,$$

also der Normalisator von H in G. Nach Prop. I.2.15 c), p. 23) ist die Bahnenlänge (also die Zahl der Konjugierten von H) gleich dem Index der Fixgruppe (also gleich $(G : \mathcal{N}_G(H))$).

Aufgabe 21. (s)
Sei G eine beliebige Gruppe. Zeigen Sie:

a) G enthält genau dann eine Untergruppe vom Index n, wenn G transitiv auf einer n-elementigen Menge operiert.

b) Besitzt G eine Untergruppe U vom Index n, dann auch einen Normalteiler $N \leq U$, dessen Index $(G : N)$ Teiler von $n!$ ist.

Tipp zu a),b): Zu $U \leq G$ betrachte man die Menge $\Omega := G/U$ der Linksnebenklassen.

c) Folgern Sie, dass A_5 keine echte Untergruppe mit Ordnung > 12 besitzt.

Lösung:
a) G operiere transitiv auf einer n-elementigen Menge Ω, d. h. ganz Ω ist eine Bahn unter G. Ihre Länge n ist also gleich dem Index $(G : G_a)$ der Fixgruppe G_a eines (beliebigen) $a \in \Omega$. Damit hat die Fixuntergruppe G_a die geforderte Eigenschaft.
Sei umgekehrt $U < G$ Untergruppe von G mit Index $n = (G : U)$. Dann hat die Menge G/U der Linksnebenklassen die Mächtigkeit n. G operiert auf G/U durch Linksmultiplikation: $G/U \ni gU \mapsto \sigma gU$ $(g, \sigma \in G)$. Diese Operation ist transitiv, denn die Bahn von $\bar{e} = U$ unter dieser Operation ist $\{\sigma U \mid \sigma \in G\} = G/U$.
b) Nach a) operiert G transitiv auf der n-elementigen Menge $\Omega = G/U$. Sei $L : G \to S(\Omega)$ der dadurch bestimmte Gruppenhomomorphismus von G in die symmetrische Gruppe $S(\Omega) \simeq S_n$. Dann ist $N := \mathrm{Ke}\, L$ Normalteiler in G und es gilt $N \leq U$, denn:

$$\sigma \in N \implies L(\sigma)(\bar{e}) = \bar{e} \iff \sigma U = U \iff \sigma \in U\,.$$

Nach dem Homomorphiesatz folgt $G/\mathrm{Ke}\, L \xrightarrow{\sim} \mathrm{Im}\, L \subset S(\Omega)$.
Dies bedeutet $(G : N) = \#\, G/\mathrm{Ke}\, L \leq \#S(\Omega) = \#S_n = n!$.
c) Eine echte Untergruppe $U < A_5$ mit einer Ordnung > 12 hätte einen Index ≤ 4 und damit existierte gemäß b) ein echter Normalteiler N in A_5 vom Index $(A_5 : N) \leq 4!$. Dann aber folgte $\#N \geq 60/24 > 1$ im Widerspruch zur Einfachheit von A_5.

Aufgabe 22. (s)
Sei G eine endliche Gruppe mit trivialem Zentrum und $\mathrm{Aut}(G)$ die Gruppe aller Automorphismen von G (bzgl. $\circ$) sowie $\iota : G \to \mathrm{Inn}(G)$ wie in Beispiele (1.19) 8).

a) Zeigen Sie: $\iota : G \xrightarrow{\sim} \mathrm{Inn}(G)$ ist ein Isomorphismus.

Sei im folgenden $f : \mathrm{Aut}(G) \xrightarrow{\sim} \mathrm{Aut}(G)$ ein Automorphismus mit der Eigenschaft $f(\mathrm{Inn}(G)) = \mathrm{Inn}(G)$.

b) Zeigen Sie: Es gibt genau einen Automorphismus $\varphi \in \mathrm{Aut}(G)$ mit $f(\iota_a) = \iota_{\varphi(a)}$ für alle $a \in G$.

c) Sei $\varphi \in \mathrm{Aut}\, G$ gemäß b) und $\Phi = \iota_\varphi : \mathrm{Aut}(G) \to \mathrm{Aut}(G)$, $\psi \mapsto \varphi \circ \psi \circ \varphi^{-1}$ der dadurch bestimmte innere Automorphismus von $\mathrm{Aut}(G)$. Zeigen Sie:

$$\psi \in \mathrm{Inn}(G) \implies f(\psi) = \Phi(\psi)$$

und folgern Sie mit Aufg. 17.c), dass $f = \Phi$ ein innerer Automorphismus von $\mathrm{Aut}(G)$ ist.

d) Zeigen Sie, dass für endliche nicht-abelsche einfache Gruppen die geforderten Eigenschaften (an G und alle f) erfüllt sind und daher gilt: $\mathrm{Aut}(\mathrm{Aut}(G)) = \mathrm{Inn}(\mathrm{Aut}(G))$. [Tipp: $\{\mathrm{id}\} \neq \mathrm{Inn}(G) \cap f(\mathrm{Inn}(G)) \lhd \mathrm{Inn}(G) \simeq G$. Indirekter Nachweis des Tipps mit 17 b).]

Lösung:
a) Es ist $\mathrm{Ke}\,\iota = \mathrm{Zentr}(G)$ (siehe Vorlesung, Beispiele (1.19) 8), p. 11, also nach Voraussetzung $\iota : G \xrightarrow{\sim} \mathrm{Im}\,\iota = \mathrm{Inn}(G)$ ein Isomorphismus.
b) Wegen $f(\mathrm{Inn}\, G) = \mathrm{Inn}\, G = \mathrm{Im}\,\iota$ gilt $\iota^{-1} : f(\mathrm{Inn}\, G) \xrightarrow{\sim} G$ und daher

$$\bigwedge_{a \in G} f(\iota_a) = \iota_{\varphi(a)} \iff f \circ \iota = \iota \circ \varphi \iff \iota^{-1} \circ f \circ \iota = \varphi\,.$$

Damit gibt es höchstens ein φ mit der geforderten Eigenschaft, und wegen der vorausgesetzten Isomorphie $f\,|_{\mathrm{Inn}(G)} : \mathrm{Inn}(G) \xrightarrow{\sim} \mathrm{Inn}(G)$ ist $\varphi : G \xrightarrow{\sim} G$ auch tatsächlich ein Isomorphismus.
c) Seien $\psi = \iota_a$ $(a \in G)$ und $b \in G$ beliebig. Dann gilt

$$\begin{aligned} f(\psi)(b) &= f(\iota_a)(b) = \iota_{\varphi(a)}(b) = \varphi(a) \cdot b \cdot \varphi(a)^{-1}\,, \\ \Phi(\psi)(b) &= \iota_\varphi(\psi)(b) = \varphi \circ \psi \circ \varphi^{-1}(b) = \varphi \circ \iota_a \circ \varphi^{-1}(b) \\ &= \varphi(a \cdot \varphi^{-1}(b) \cdot a^{-1}) = \varphi(a) \cdot b \cdot \varphi(a)^{-1}\,, \end{aligned}$$

also die behauptete Gleichheit. Damit stimmen f und Φ auf $\mathrm{Inn}(G)$ überein. Aus 17.c) (angewendet auf $\Phi \circ f^{-1}$) folgt dann $f = \Phi = \iota_\varphi$ auf ganz $\mathrm{Aut}(G)$; f ist ein innerer Automorphismus von $\mathrm{Aut}(G)$.
d) Es ist $\mathrm{Zentr}(G) \lhd G$, $\mathrm{Zentr}(G) \neq G$, da G nicht abelsch ist, und daher $\mathrm{Zentr}(G)$ trivial, da G einfach ist. Sei nun f ein beliebiger Automorphismus von $\mathcal{A} := \mathrm{Aut}(G)$. Aus $\mathcal{I} := \mathrm{Inn}(G) \lhd \mathcal{A}$ (siehe Vorlesung, Beispiele (1.19) 8), p. 11) folgt auch $f(\mathcal{I}) \lhd f(\mathcal{A}) = \mathcal{A}$ und dann $\mathcal{N} := \mathcal{I} \cap f(\mathcal{I}) \lhd \mathcal{I}$. Nun ist $\mathcal{I} = \mathrm{Inn}(G) \simeq G$ nicht-abelsch einfach, also genügt es zu zeigen: $\mathcal{N} \neq \{\mathrm{id}\}$, denn dann ist $\mathcal{N} = \mathcal{I}$ und $\mathcal{I} \subseteq f(\mathcal{I})$. Da dies für jedes f, also auch für f^{-1} gilt, erhält man auch die umgekehrte Inklusion.
ad $\mathcal{N} \neq \{\mathrm{id}\}$: Für alle $\sigma \in f(\mathcal{I}) \lhd \mathcal{A}$ und alle $\psi \in \mathcal{I} \lhd \mathcal{A}$ gilt aufgrund der Normalteilereigenschaft $\sigma f(\mathcal{I}) = f(\mathcal{I})\sigma$ und $\psi\mathcal{I} = \mathcal{I}\psi$ und daher

$$\sigma\psi = \begin{cases} \psi'\sigma & \text{mit einem } \psi' \in f(\mathcal{I}) \\ \psi\sigma' & \text{mit einem } \sigma' \in \mathcal{I} \end{cases} \implies \psi^{-1}\psi' = \sigma'\sigma^{-1} \in \mathcal{I} \cap f(\mathcal{I}) = \mathcal{N}\,.$$

Wäre nun $\mathcal{N} = \{\mathrm{id}\}$, so folgte

$$\psi^{-1}\psi' = \sigma'\sigma^{-1} = \mathrm{id} \iff \psi = \psi' \ \wedge\ \sigma = \sigma' \implies \sigma\psi = \psi\sigma\,.$$

Da dies für alle $\psi \in \mathcal{I}$ gilt, folgt $\sigma \in \mathrm{Zentr}_{\mathrm{Aut}\, G}(\mathrm{Inn}\, G) \underset{17b)}{=} \{\mathrm{id}\}$. Also $\sigma = \mathrm{id}$ für alle $\sigma \in f(\mathcal{I})$, das heißt

$$f(\mathcal{I}) = \{\mathrm{id}\} \iff \mathcal{I} = \{\mathrm{id}\} \iff \bigwedge_{a \in G} \iota_a = \mathrm{id} \iff G \text{ abelsch}$$

aber nach Voraussetzung ist G nicht abelsch, Wid.

Algebra
Übung 5

Aufgabe 23. (m)
Sei G eine endliche Gruppe, p eine Primzahl.

a) Ist H eine p-Untergruppe von G und Normalteiler in G, so ist H in jeder p-Sylowuntergruppe enthalten.

b) Die p-Sylowgruppen S'_p einer Untergruppe H von G sind darstellbar als $S'_p = S_p \cap H$ mit einer p-Sylowgruppe S_p von G.

c) Ist N Normalteiler von G, so sind die p-Sylowgruppen von G/N genau die Untergruppen $\bar{S}_p = S_pN/N$ mit einer p-Sylowgruppe S_p von G.

Lösung:
Folgerungen aus dem 2. Sylowsatz.
a) Als p-Untergruppe von G ist H in einer p-Sylowgruppe P enthalten: $H \subseteq P$. Da H Normalteiler in G ist, gilt für alle $\sigma \in G$ $H = \sigma^{-1}H\sigma = H^\sigma \subseteq P^\sigma$. H ist also in jeder p-Sylowgruppe P^σ enthalten. Dies sind aber gerade sämtliche p-Sylowgruppen von G.
b) Eine p-Sylowgruppe S'_p von H ist eine p-Untergruppe von G, also in einer p-Sylowgruppe S_p von G enthalten. Damit folgt $S'_p \subseteq S_p \cap H$. Da S'_p maximale p-Untergruppe von H ist, muss sie mit der p-Untergruppe $S_p \cap H$ übereinstimmen.
c) Es sei $\nu : G \twoheadrightarrow G/N =: \bar{G}$ der natürliche Epimorphismus und S_p eine p-Sylowgruppe von G. Dann gilt $\bar{S}_p = \nu(S_p) = S_pN/N \simeq S_p/S_p \cap N$ (1. Isomorphiesatz), also ist $\bar{S}_p = S_pN/N$ eine p-Gruppe. Andererseits ist $(\bar{G} : \bar{S}_p) = (G/N : S_pN/N) = \frac{\#G}{\#S_pN} = (G : S_pN)$ ein Teiler von $(G : S_p)$ und daher kein Vielfaches von p: $\bar{S}_p = S_pN/N$ ist eine p-Sylowgruppe von G/N.
Ist nun S'_p ein beliebige p-Sylowgruppe von $\bar{G}$, so ist sie in $\bar{G}$ konjugiert zu $\bar{S}_p$, d. h. es gibt ein $\sigma \in G$ mit $S'_p = \bar{\sigma}\bar{S}_p\bar{\sigma}^{-1} = \overline{\sigma S_p \sigma^{-1}}$, also ist auch S'_p Bild einer p-Sylowgruppe von G.

Aufgabe 24. (m)
Operiert die Gruppe G auf zwei Mengen Ω, Ω', so heißt eine Abbildung $\varphi : \Omega \to \Omega'$ ein G-Abbildung, wenn gilt: $\bigwedge_{g\in G} \bigwedge_{a\in\Omega} \varphi(g.a) = g.\varphi(a)$.

a) Operiert G auf Ω transitiv, so existiert eine Untergruppe $H \leq G$ und eine G-Bijektion $\varphi : G/H \to \Omega$. (G operiere auf G/H durch Linksmultiplikation.)

b) Zu Untergruppen H, H' von G existiert genau dann eine G-Bijektion $\varphi : G/H \to G/H'$, wenn H, H' in G konjugiert sind.

Lösung:
a) Wir wählen $a \in \Omega$ und $H = G_a$ als Fixgruppe von a in G. Wir definieren $\varphi : G/H \to \Omega$ vermöge $\varphi(\sigma H) := \sigma.a$. Die Abbildung ist wohldefiniert und injektiv, denn

$$\sigma.a = \tau.a \iff \tau^{-1}\sigma.a = a \iff \tau^{-1}\sigma \in G_a = H \iff \sigma H = \tau H\,.$$

φ ist surjektiv wegen der Transitivität der Operation und sie ist eine G-Abbildung, denn

$$\varphi(\tau \cdot (\sigma H)) = \varphi(\tau\sigma H) = \tau\sigma.a = \tau.\varphi(\sigma H)\,.$$

b) Sei φ eine solche G-Bijektion und $\varphi(H) =: \rho H'$, also $\varphi(\sigma H) = \sigma\varphi(H) = \sigma\rho H'$. Da φ bijektiv, gilt für alle $\sigma \in G$

$$\sigma \in H \iff \sigma H = H \iff \varphi(\sigma H) = \varphi(H) \iff \sigma\rho H' = \rho H' \iff \rho^{-1}\sigma\rho \in H'\,,$$

H und $H' = \rho^{-1}H\rho$ sind also konjugiert. Ist umgekehrt $H' = \rho^{-1}H\rho$, so definiere man $\varphi : G/H \to G/H'$ durch $\varphi(\sigma H) := \sigma\rho H'$. Die so definierte Zuordnung ist wohldefiniert und injektiv:

$$\sigma\rho H' = \tau\rho H' \iff \sigma H\rho = \tau H\rho \iff \sigma H = \tau H$$

und auch surjektiv: $\tau H' = \varphi(\tau\rho^{-1}H)$.

Aufgabe 25. (s)
Sei G eine Gruppe der Ordnung pq, $p < q$ Primzahlen. Zeigen Sie

a) Es existiert genau eine q-Sylowgruppe in G. Diese ist Normalteiler von G.

b) Es existieren $\sigma, \tau \in G$ und $\mu \in \{1, \ldots, q-1\}$ mit

$$G = \langle \sigma, \tau \rangle\,, \quad \operatorname{ord}(\sigma) = q\,, \quad \operatorname{ord}(\tau) = p\,, \quad \tau\sigma\tau^{-1} = \sigma^{\mu}\,, \quad q \mid \mu^p - 1\,.$$

c) Ist p kein Teiler von $q-1$, so ist G zyklisch.

Lösung:
a) Für die Anzahl s_q der q-Sylowgruppen von G gilt nach dem 2. Sylowsatz I.3.4 d): $s_q \mid (G : S_q) = p$ und $s_q \equiv 1 \bmod q$. Wegen $s_q - 1 \le p - 1 < q$ ist dann nur $s_q = 1$ möglich. Es gibt also nur eine q-Sylowgruppe und diese ist dann Normalteiler (2. Sylowsatz I.3.4 c)).
b) Sei S_p eine p-Sylowuntergruppe von G. Wir wählen Erzeugende für die (primzyklischen) Sylowgruppen: $S_q = \langle\sigma\rangle$, $S_p = \langle\tau\rangle$. Damit gilt $\operatorname{ord}\sigma = \#S_q = q$, $\operatorname{ord}\tau = \#S_p = p$ und wegen $\#G = pq$ muss $G = \langle\sigma, \tau\rangle$ sein.
Wegen $S_q \lhd G$ gilt $\tau\sigma\tau^{-1} = \sigma^{\mu}$ für ein $1 \le \mu < q$. ($\mu = 0$ ist nicht möglich, da $\sigma \neq e$.)
Mehrfache Anwendung dieser Vertauschungsregel ergibt

$$\tau^p\sigma\tau^{-p} = \sigma^{\mu^p} \underset{\tau^p = e}{\Longrightarrow} \sigma = \sigma^{\mu^p} \implies \sigma^{\mu^p - 1} = e \iff \operatorname{ord}\sigma = q \mid \mu^p - 1\,.$$

c) Sei s_p die Zahl der p-Sylowgruppen, dann gilt $s_p \mid q$ und $p \mid s_p - 1$. Es ist $s_p = 1$, denn $s_p = q \implies p \mid q - 1$, Wid. Damit ist S_p ebenfalls Normalteiler in G. Daraus folgt

$$[\sigma, \tau] = \sigma^{-1}\tau^{-1}\sigma\tau \in \begin{cases} S_p^{\sigma} \cdot \tau = S_p \\ \sigma^{-1} S_q^{\tau} = S_q \end{cases}.$$

Nun ist der Durchschnitt verschiedener Sylowgruppen wegen der teilerfremden Ordnung trivial, also $[\sigma, \tau] \in S_p \cap S_q = \{e\}$, d. h. $\sigma\tau = \tau\sigma$ und daher $(\sigma\tau)^k = \sigma^k\tau^k$. Dann hat aber $\sigma\tau$ die Ordnung pq, denn $(\sigma\tau)^q = \tau^q \neq e$ und $(\sigma\tau)^p = \sigma^p \neq e$. Damit ist $G = \langle\sigma\tau\rangle$ zyklisch.

Aufgabe 26. (s)
Für eine nicht-abelsche Gruppe der Ordnung p^3, p eine Primzahl, stimmen Zentrum und Kommutatorgruppe überein. [Tipp: Aufgaben 9 und 19.]

Lösung:
Sei $Z := \operatorname{Zentr} G$ das Zentrum von G. Da G eine nicht-abelsche p-Gruppe ist, gilt (siehe Vorlesung Korollar I.2.16 b), p. 24) $1 < \#Z = p^k < \#G = p^3$, also gibt es nur zwei Fälle: $\#Z = p$ oder $\#Z = p^2$. Der letztere Fall ist nicht möglich, da sonst G/Z primzyklisch und nach Aufgabe 19.a) G dann abelsch wäre. Also gilt

$$\#Z = p \implies \#G/Z = p^2 \underset{\text{Aufg.19.b)}}{\Longrightarrow} G/Z \text{ abelsch} \underset{\text{Aufg.9.b}}{\Longrightarrow} G' \subseteq Z \implies G' = \{e\} \ \vee \ G' = Z\,.$$

Wäre $G' = \{e\}$, so wäre G abelsch, Wid. Somit folgt $Z = G'$.

Aufgabe 27. (s)

a) Eine Permutationsgruppe G, die eine ungerade Permutation enthält, besitzt einen Normalteiler vom Index 2.

b) Ist G eine Gruppe der Ordnung $2^k m$, $k \in \mathbb{N}_+$, $2 \nmid m$, die eine zyklische Untergruppe der Ordnung 2^k enthält, so besitzt G einen Normalteiler vom Index 2.

[Tipp: Satz von Cayley und a).]

c) Für G wie unter b) gilt schärfer: G besitzt einen Normalteiler vom Index 2^k.

[Tipp: Induktiv findet man eine Untergruppe der Ordnung m. Zeigen Sie dann, dass es nur eine solche Untergruppe geben kann. Beachten Sie dabei:

$N \lhd G\,,\ H \leq G\,,\ \#H$ teilerfremd zu $(G:N) \implies H \leq N\,.$]

Lösung:
a) Ist $G \leq S_n$ und $\tau \in G$ ungerade, so ist $\tau \notin N := A_n \cap G \lhd G$. Für jedes $\sigma \in G$ gilt: Entweder ist σ gerade und daher $\sigma \in N$ oder σ ist ungerade, also $\tau^{-1}\sigma \in N$, d. h. $\sigma \in \tau N$. Damit ist $G = N \cup \tau N$ und $(G:N) = 2$.
b) Sei $H = \langle\sigma\rangle$ die Untergruppe von G mit der Ordnung 2^k und dem Index m. Wir betrachten G als Permutationsgruppe auf G durch Linksmultiplikation (Satz von Cayley, siehe Vorlesung I.2.2, p. 14). Die Bahnen des Elementes σ sind gerade die Nebenklassen $H\tau_i$ $(i = 1, \ldots, m)$ von H. Damit ist σ das Produkt von m Zyklen der Längen $\#H\tau_i = \#H = 2^k$. Zyklen gerader Längen sind ungerade (Vorlesung, Prop. (2.5) a), p. 15), das Produkt von m (also ungerade vielen) solcher Zyklen ist dann ebenfalls ungerade. σ ist also eine ungerade Permutation in $G \subseteq S(G)$. Nach Teil a) existiert also ein Normalteiler $N \lhd G$ vom Index 2.
c) Der Normalteiler N aus b) hat die Ordnung $2^{k-1}m$, und wegen $\#G/N = 2$ ist $\bar{\sigma}^2 = \bar{e}$, also $\sigma^2 \in N$. $N_1 := N$ enthält also eine zyklische Untergruppe $\langle\sigma^2\rangle$ von der Ordnung 2^{k-1}. Nach Teil b) folgt die Existenz eines Normalteilers $N_2 \lhd N_1$ vom Index 2, also einer Untergruppe $N_2 < G$ vom Index 4. Induktiv erhält man schließlich die Existenz einer Untergruppe $N_k < G$ vom Index 2^k bzw. der Ordnung m.
Sei nun H' irgendeine Untergruppe von G von der Ordnung m. Wir wenden nun den Tipp sukzessive auf die Kette der konstruierten Normalteiler $G =: N_0 \rhd N_1 \rhd \ldots \rhd N_{k-1} \rhd N_k$ an. Es ist jeweils $\#H' = m$ teilerfremd zu $(N_{i-1} : N_i) = 2$, also induktiv $H' \leq N_i$ für alle $i \leq k$ und damit $H' \leq N_k$. Wegen gleicher Mächtigkeit folgt $H' = N_k$. Da dies insbesondere für alle Konjugierten $H' = N_k^\sigma$ gilt, ist $N_k \lhd G$.
Abschließend die Begründung des Tipps: Nach dem 1. Isomorphiesatz (1.20) b) gilt

$$H/H \cap N \simeq HN/N \subseteq G/N\,, \quad \text{also} \quad (H : H \cap N) = \#(HN/N) \mid \#(G/N) = (G:N)\,.$$

Andererseits gilt $(H : H \cap N) \mid \#H$, so dass $(H : H \cap N)$ ein gemeinsamer Teiler der teilerfremden Zahlen $\#H$ und $(G:N)$ ist, folglich $= 1$ sein muss, d. h. $H = H \cap N$, $H \leq N$.

Aufgabe 28. (s)

a) Die Gruppen der Ordnung 56 sind nicht einfach.

[Tipp: Bestimmen Sie $\#\{g \in G \mid \operatorname{ord} g \neq 7\}$.]

b) Die Gruppen der Ordnung $2^k \cdot p^n$, $k \in \{1, 2, 3\}$, $n \in \mathbb{N}_+$, $p \neq 2$ Primzahl, sind nicht einfach.

c) $(*)$ Eine nicht-abelsche einfache Gruppe hat mindestens die Ordnung 60.

Lösung:
a) Für die Anzahl s_7 der 7-Sylowgruppen einer Gruppe G der Ordnung 56 gilt: $s_7 \mid (G : S_7) = 8$ und $s_7 \equiv 1 \bmod 7$, also $s_7 = 1$ oder $s_7 = 8$. Im Falle $s_7 = 1$ ist $S_7 \lhd G$ und G nicht einfach. Sei

also $s_7 = 8$. Die 8 verschiedenen Sylowgruppen der Ordnung 7 haben jeweils den Durchschnitt $S_7 \cap S_7' = \{e\}$, also enthält ihre Vereinigung $8 \cdot 6 = 48$ Elemente der Ordnung 7. Es gibt also 8 Elemente einer Ordnung $\neq 7$. Allein in einer 2-Sylowgruppe S_8 gibt es diese 8 Elemente, es kann also nur eine 2-Sylowgruppe geben, die dann ein Normalteiler ist, so dass G nicht einfach ist.
b) Fall $k = 1$: G enthält eine p-Sylowgruppe vom Index 2, diese ist also Normalteiler, und nicht-trivial.
Fall $k = 2$: G enthält eine p-Sylowgruppe S_p vom Index 4. Nach Aufgabe 21.b) gibt es dann in S_p einen Normalteiler $N \triangleleft G$, dessen Index $(G : N)$ ein Teiler von 4! ist. Dann gilt $(S_p : N) \mid \frac{4!}{4} = 6$. Da S_p eine p-Gruppe ist mit $p > 2$, folgt $(S_p : N) \mid 3 = p$ und daher $3^{n-1} \mid \#N$. Damit ist G nicht einfach, es sei denn $N = \{e\}$, $n = 1$ und $\#G = 12$.
In Falle $\#G = 12$ hat eine 2-Sylowuntergruppe von G den Index 3 und es existiert wieder nach Aufgabe 21.b) ein Normalteiler in G, dessen Index $3! = 6$ teilt. Dieser Normalteiler ist also nicht-trivial: Auch eine Gruppe der Ordnung 12 ist nicht einfach.
Fall $k = 3$: Wie oben schließen wir: In einer p-Sylowgruppe S_p (vom Index 8) gibt es einen Normalteiler $N \triangleleft G$ mit $p^k := (S_p : N) \mid 7! = 2^4 \cdot 3^2 \cdot 5 \cdot 7$. Da p eine ungerade Primzahl ist, ergeben sich nur die Möglichkeiten $p^k = 3, 9, 5, 7$. Außer in den Fällen $p^k = p^n$ ist damit N nicht-trivial und G nicht einfach.
Der Fall $p^n = 7$ wurde in Aufgabenteil a) behandelt. Im Fall $p^n = 5$ gilt für die Anzahl s_5 der 5-Sylowgruppen $s_5 \mid 8$ und $s_5 \equiv 1 \bmod 5$, also ist $s_5 = 1$, $S_5 \triangleleft G$, G nicht einfach.
Im Fall $p^n = 3$, $\#G = 24$, hat eine 2-Sylowgruppe von G den Index 3, enthält also einen Normalteiler $N \triangleleft G$, dessen Index $3! = 6$ teilt, der also ein nicht-trivialer Normalteiler von G ist, G ist nicht einfach.
Im Fall $p^n = 9$, $\#G = 72$, gilt $s_3 \equiv 1 \bmod 3$ und $s_3 \mid 8$, also $s_3 = 1$ (und $S_3 \triangleleft G$) oder $s_3 = 4$. In letzterem Falle ist $4 = s_3 = (G : \mathcal{N}_G(S_3))$, G enthält also eine Untergruppe vom Index 4 und daher einen Normalteiler N mit $(G : N) \mid 4! < \#G$, also ist N ein nicht-trivialer Normalteiler und G nicht einfach.
c) Wir zeigen, dass keine Gruppe einer Ordnung < 60 nicht-abelsch einfach sein kann. In der Vorlesung und den vorangehenden Übungen haben wir Bedingungen kennengelernt, allein aus der Gruppenordnung $\#G$ abzulesen, dass die Gruppe nicht einfach ist. Unter jeder der folgenden 4 Bedingungen ist eine Gruppe entweder nicht einfach oder aber primzyklisch und daher abelsch:

(1) $\#G$ ist eine Primzahlpotenz (Vorlesung, Korollar (2.16) b), p. 24).

(2) $\#G = 2 \cdot m$ mit m ungerade (Aufgabe 27.b))

(3) $\#G$ ist Produkt von genau zwei Primzahlen (Aufgabe 25 a)).

(4) $\#G = 2^k \cdot p^n$ mit $2^k \leq 8$ (Teil b) dieser Aufgabe).

Man beachte bei (2), dass die Zyklizitätsbedingung in Aufgabe 27.b) bei $2^k = 2$ erfüllt ist.

Von den 58 Gruppenordnungen $1 < \#G < 60$ wird Bedingung (1) von 25, Bedingung (2) von weiteren 14, Bedingung (3) von weiteren 8 und schließlich Bedingung (4) von weiteren 9 Gruppenordnungen erfüllt[1)]. Es bleiben lediglich zwei Gruppenordnungen ungeklärt: $\#G = 45 = 3^2 \cdot 5$ und $\#G = 48 = 2^4 \cdot 3$.
Ist $\#G = 45 = 3^2 \cdot 5$, so gilt für die Zahl s_5 der 5-Sylowgruppen $s_5 \equiv 1 \bmod 5$ und $s_5 \mid 9$, also $s_5 = 1$: Es gibt nur eine 5-Sylowgruppe, die daher ein nicht-trivialer Normalteiler ist.

[1)] Bedingung (1) erfüllen die 25 Primzahlpotenzen 2, 3, 4, 5, 7, 8, 9, 11, 13, 16, 17, 19, 23, 25, 27, 29, 31, 32, 37, 41, 43, 47, 49, 53, 59,
Bedingung (2) $2 \mid \#G$, aber $4 \nmid \#G$, erfüllen zusätzlich die 14 Gruppenordnungen 6, 10, 14, 18, 22, 26, 30, 34, 38, 42, 46, 50, 54, 58,
Bedingung (3) erfüllen zusätzlich die 8 Produkte von 2 ungeraden Primzahlen 15, 21, 33, 39, 51, 57; 35, 55 und
Bedingung (4) zusätzlich die 9 Zahlen 12, 20, 24, 28, 36, 40, 44, 52, 56.

Ist $\#G = 48 = 2^4 \cdot 3$, so enthält G mit einer 2-Sylowgruppe S_2 eine Untergruppe vom Index 3, also gibt es in G nach Aufgabe 21.b) einen Normalteiler, dessen Index $3! = 6$ teilt, der also mindestens die Ordnung 8 hat und somit nicht-trivial ist.

Algebra
Übung 6

Aufgabe 29. (m)
Sei G eine Gruppe.

a) Ist G auflösbar, so auch jede Untergruppe und jede Faktorgruppe von G.

b) Für jeden Normalteiler N von G gilt:
Sind N und G/N auflösbar, so auch G.

c) Welche der beiden Aussagen a) und b) bleiben für „*nilpotent*“ statt „*auflösbar*“ richtig?

Lösung:
a),b) Siehe Bemerkung I.4.7 b),c) (Vorlesung S. 32).
c) Aussage a) gilt auch für „*nilpotent*“, b) hingegen nicht.
1. Sei $H \leq G$ eine Untergruppe und H_i bzw. G_i die unteren (absteigenden) Zentralreihen. Dann gilt $H_0 = H \subseteq G = G_0$ und es folgt induktiv für alle $i \geq 0$

$$H_{i+1} = [H, H_i] \subseteq [G, G_i] = G_{i+1}\,.$$

Da G nilpotent ist, ist $H_k \subseteq G_k = \{e\}$ für ein k, also auch H nilpotent (gemäß Prop. I.5.5 a), Vorlesung S. 34).
2. Sei $N \lhd G$ und $\nu : G \twoheadrightarrow \mathcal{G} := G/N$ der natürliche Epimorphismus. Seien $\mathcal{G}_i$ bzw. G_i wieder die unteren (absteigenden) Zentralreihen von $\mathcal{G}$ bzw. G. Dann gilt $\nu(G_0) = \nu(G) = \mathcal{G} = \mathcal{G}_0$ und es folgt induktiv für alle $i \geq 0$

$$\nu(G_{i+1}) = \nu([G, G_i]) = [\nu(G), \nu(G_i)] = [\mathcal{G}, \mathcal{G}_i] = \mathcal{G}_{i+1}\,.$$

Da G nilpotent ist, ist $G_k = \{e\}$ für ein k, also auch $\mathcal{G}_k = \nu(G_k) = \{\bar{e}\}$ und $\mathcal{G}$ ebenfalls nilpotent.
Anmerkung: Die Nilpotenzklasse von G/N ist die kleinste natürliche Zahl j mit $G_j \subseteq N$.
3. Gegenbeispiel ist die symmetrische Gruppe S_3, die nicht nilpotent ist, da ihr Zentrum trivial ist (siehe Prop. I.2.6 a)), die aber einen (primzyklischen, also) nilpotenten Normalteiler $A_3 \simeq \mathbb{Z}/3\mathbb{Z}$ besitzt mit ebenfalls nilpotenter Faktorgruppe $S_3/A_3 \simeq \{-1, +1\} \simeq \mathbb{Z}/2\mathbb{Z}$.

Aufgabe 30. (s)
G_1, G_2 seien Gruppen.

a) Sind $N_i \lhd G_i$ $(i = 1, 2)$ Normalteiler, so ist $N_1 \times N_2 \lhd G_1 \times G_2$ Normalteiler und es gilt

$$G_1 \times G_2/N_1 \times N_2 \simeq G_1/N_1 \times G_2/N_2\,.$$

b) Zeigen Sie anhand eines Beispiels, dass nicht jeder Normalteiler von $G_1 \times G_2$ die spezielle Form aus a) hat.

c) Direkte Produkte auflösbarer Gruppen sind auflösbar.

d) Direkte Produkte von Gruppen mit Primzahlpotenzordnung sind nilpotent.

Lösung:
a) Seien $\nu_i : G_i \twoheadrightarrow G_i/N_i$ die natürlichen Epimorphismen $(i = 1, 2)$. Man definiert nun

$$\nu : G_1 \times G_2 \to G_1/N_1 \times G_2/N_2\,, \quad (\sigma_1, \sigma_2) \mapsto (\nu_1(\sigma_1), \nu_2(\sigma_2))\,.$$

ν ist ein Homomorphimus aufgrund der komponentenweisen Multiplikation auf dem direkten Produkt, ν ist offenbar surjektiv und der Kern ist

$$\operatorname{Ke}\nu = \operatorname{Ke}\nu_1 \times \operatorname{Ke}\nu_2 = N_1 \times N_2\,.$$

Als Kern eines Homomorphismus ist $N_1 \times N_2$ Normalteiler in $G_1 \times G_2$ (Bemerkung I.1.18 b) und nach dem Homomorphiesatz (Satz I.1.20 a) folgt die Behauptung

$$G_1 \times G_2/N_1 \times N_2 \simeq G_1/N_1 \times G_2/N_2\,.$$

b) Gegenbeispiel ist die Kleinsche Vierergruppe V_4, hier realisiert als direktes Produkt der zyklischen Gruppe $G = \{-1, +1\}$ der Ordnung 2 mit sich selbst:

$$V_4 = G \times G = \{(1,1), (-1,1), (1,-1), (-1,-1)\}\,.$$

Jeder Faktor G hat genau 2 Untergruppen und daher gibt es 4 Untergruppen von V_4 von der Form $H_1 \times H_2$, die triviale Gruppe, die volle V_4 und zwei Gruppen der Ordnung 2: $G \times \{1\} = \{(1,1), (-1,1)\}$ sowie $\{1\} \times G = \{(1,1), (1,-1)\}$. In V_4 gibt es aber noch eine dritte Untergruppe der Ordnung 2, die Diagonale $H = \{(1,1), (-1,-1)\}$, die nicht diese Form hat.
c) Nach a) ist $G_1 \times \{e\} \simeq G_1$ Normalteiler in $G_1 \times G_2$ mit Faktorgruppe $G_1 \times G_2/G_1 \times \{e\} \simeq G_1/G_1 \times G_2/\{e\} \simeq G_2$. Der Normalteiler ($\simeq G_1$) und die Faktorgruppe ($\simeq G_2$) sind nach Voraussetzung auflösbar, also ist auch die Gesamtgruppe $G_1 \times G_2$ auflösbar gemäß Aufgabe 29.b).
d) Der Beweis von Satz I.4.11 (Vorlesung S. 33) zeigte, dass in p-Gruppen G die aufsteigende Zentralreihe erst bei G stationär wird: p-Gruppen sind nilpotent. Zum Beweis von d) genügt es also zu zeigen:

- Direkte Produkte von nilpotenten Gruppen sind nilpotent.

In direkten Produkten kann man Kommutatoren komponentenweise bilden:

$$\sigma := (\sigma_1, \sigma_2), \tau := (\tau_1, \tau_2) \in G_1 \times G_2 \implies [\sigma, \tau] = ([\sigma_1, \tau_1], [\sigma_2, \tau_2])$$

Daher ist auch die Bildung der absteigenden Zentralreihe komponentenweise möglich:

$$\mathcal{G} := G_1 \times G_2 \implies \mathcal{G}_j = G_{1j} \times G_{2j}\,.$$

Sind also G_i nilpotent, etwa $G_{1k} = \{e\}$ und $G_{1,l} = \{e\}$, so ist $\mathcal{G}_{\max(k,l)} = \{(e,e)\}$ und $\mathcal{G} = G_1 \times G_2$ nilpotent.

Aufgabe 31. (s)
Die endliche Gruppe G ist genau dann isomorph zum (äußeren) direkten Produkt ihrer Sylowuntergruppen, wenn es zu jedem Primteiler p der Gruppenordnung genau eine p-Sylowgruppe gibt.

Lösung:
Ist G das direkte Produkt von p-Gruppen zu den verschiedenen Primteilern p von $\#G$, so sind die Faktoren Normalteiler in G und sind damit die eindeutig bestimmten Sylowgruppen von G (siehe 2. Sylowsatz c), Vorlesung S. 28).
Seien nun umgekehrt P_i $(i = 1, \ldots, r)$ die p_i-Sylowuntergruppen von G zu den Primteilern $p_i \mid \#G$. Wegen der vorausgesetzten Eindeutigkeit sind die P_i Normalteiler in G und daher $G = \langle P_1, \ldots, P_r\rangle = P_1 \cdot \ldots \cdot P_r$. Damit ist durch

$$\varphi : P_1 \times \ldots \times P_r \to G\,,\ (\sigma_1, \ldots, \sigma_r) \mapsto \sigma_1 \cdot \ldots \cdot \sigma_r$$

eine surjektive Abbildung definiert. Da Definitions- und Bildbereich gleiche Mächtigkeit haben, ist φ eine Bijektion.

Entscheidend für die Homomorphie von φ ist die elementweise Vertauschbarkeit verschiedener P_i. Dies folgt aus der Normalteilereigenschaft und der teilerfremden Ordnung der P_i, denn für $\sigma_i \in P_i$ gilt

$$[\sigma_i, \sigma_j] = \begin{cases} (\sigma_i^{-1}\sigma_j^{-1}\sigma_i) \cdot \sigma_j \in P_j\,, \\ \sigma_i^{-1} \cdot (\sigma_j^{-1}\sigma_i\sigma_j) \in P_i\,. \end{cases} \implies [\sigma_i, \sigma_j] \in P_i \cap P_j = \{e\} \text{ für } i \neq j\,.$$

Damit sind die Elemente aus *verschiedenen* P_i miteinander vertauschbar und φ ist ein Isomorphismus.

Aufgabe 32. (s)

a) Geben Sie eine Kompositionsreihe von S_4 an.

b) Bestimmen Sie die Kommutator- und die auf- sowie die absteigende Zentralreihe von D_{2n} ($n \in \mathbb{N}$, $n \geq 2$).

Lösung:
a) Eine Kompositionsreihe von S_4 ist

$$S_4 \triangleright A_4 \triangleright V_4 \triangleright \langle (1\,2)(3\,4)\rangle \triangleright \{\mathrm{id}\}\,.$$

Die Kompositionsfaktoren sind $\mathbb{Z}/2\mathbb{Z}$ (4-mal) und $\mathbb{Z}/3\mathbb{Z}$ (1-mal).
b) Kommutatorreihe: Nach Aufgabe 11, Lösung ist die Kommutatorgruppe D' von $D = D_{2n}$ gegeben durch

$$D' = \begin{cases} \langle R_n\rangle & n \text{ ungerade} \\ \langle R_n^2\rangle & n \text{ gerade} \end{cases}\,.$$

$D' = D^{(1)}$ ist also zyklisch und daher $D^{(2)} = \{\mathrm{id}\}$. Im Falle $n = 2$ ist bereits D' trivial, ansonsten umfasst die Kommutatorreihe 3 Glieder.
Absteigende Zentralreihe $D(i)$: Für diese Reihe erhalten wir unter Verwendung von Aufgabe 11, Lösung zunächst die folgende Beschreibung:

$$D(i) = \langle R_n^{2^i}\rangle \quad \text{für } i \geq 1\,.$$

Beweis per Induktion: Für $i = 1$ gilt nach dem ersten Beweisschritt in Aufgabe 11 $D(1) = \langle R_n^2\rangle$. Induktionsschritt $1 \leq i \to i+1$: Es ist

$$D(i+1) = [G, D(i)] = [\langle S, R_n\rangle, \langle R_n^{2^i}\rangle] = \langle [S, R_n^{2^i}], [R_n, R_n^{2^i}]\rangle \underset{\text{Aufg.11}}{=} \langle [S, R_n^{2^i}]\rangle \underset{\text{Aufg.11}}{=} \langle R_n^{2^{i+1}}\rangle\,.$$

Um zu erkennen, wann die absteigende Zentralreihe abbricht, sei $n = 2^k m$ mit $2 \nmid m$. Solange $i \leq k$ ist, gilt $2^i \mid n$ und daher $\#D(i) = \operatorname{ord} R_n^{2^i} = \frac{n}{2^i} = 2^{k-i}m$. Bis $i = k$ sinkt die Ordnung der $D(i)$ stets auf die Hälfte. Für $i = k+1$ hingegen erhalten wir

$$\operatorname{ord} R_n^{2^k} = m \text{ ungerade} \implies \operatorname{ord} R_n^{2^{k+1}} = \operatorname{ord} (R_n^{2^k})^2 = m = \operatorname{ord} R_n^{2^k}\,.$$

Dies bedeutet $D(k+1) = D(k)$, die absteigende Zentralreihe wird bei D_k stationär.
Aufsteigende Zentralreihe: Auch die Bestimmung dieser Reihe basiert auf den Ergebnissen von Aufgabe 11. Ist n ungerade, so ist $Z_1 := \mathrm{Zentr}(D_{2n}) = \{\mathrm{id}\} = Z_0$. Ist $n = 2n'$ gerade, so gilt

$$Z_1 := \mathrm{Zentr}(D_{2n}) = \langle R_n^{n/2}\rangle\,,\ \nu : D_{2n}/Z_1 \xrightarrow{\sim} D_{2n'}\,,\ R_n \mapsto R_{n'}$$

Ist nun auch n' gerade, so ist

$$Z_1' := \mathrm{Zentr}(D_{2n'}) = \langle R_{n'}^{n'/2}\rangle \quad \text{und} \quad Z_2 = \nu^{-1}(Z_1') = \langle R_n^{n'/2}\rangle = \langle R_n^{n/4}\rangle\,.$$

Induktiv erhalten wir so für $n = 2^k m$, $2 \nmid m$ die folgende aufsteigende Zentralreihe für D_{2n}:

$$Z_i = \langle R_n^{n/2^i} \rangle \quad \text{für } i = 0, 1, \ldots k\,, \quad \text{und} \quad Z_{k+1} = Z_k\,.$$

Induktion über i. $i = 0 \implies Z_0 = \{\mathrm{id}\} = \langle R_n^n \rangle$.
Induktionsschritt $i \to i+1$: Sei $0 \le i \le k$. Nach Definition ist $Z_{i+1} = \nu^{-1}(\mathrm{Zentr}(G/Z_i))$ und nach Induktionsvoraussetzung ist $Z_i = \langle R_n^{n'} \rangle$ mit $n' = \frac{n}{2^i} = 2^{k-i} m$, also

$$G/Z_i = \langle S, R_n \rangle / \langle R_n^{n'} \rangle \simeq \langle \bar{S}, \bar{R}_n \rangle \simeq D_{2n'}\,,$$

denn $\bar{S}$ und $\bar{R}_n$ erfüllen die entsprechenden Relationen:

$$\mathrm{ord}\,\bar{S} = 2\,, \quad \mathrm{ord}\,\bar{R}_n = \min\{l \mid R_n^l \in Z_i\} = n' \quad \text{und} \quad \bar{R}_n \bar{S} = \overline{R_n S} = \overline{S R_n^{-1}} = \bar{S} \bar{R}_n^{-1}\,.$$

Wir erhalten daher nach Aufgabe 11, falls $n' = 2^{k-i} m$ gerade, d. h. $i < k$ ist:

$$\mathrm{Zentr}(G/Z_i) = \mathrm{Zentr}(D_{2n'}) = \langle \bar{R}_n^{n'/2} \rangle\,, \quad \text{also} \quad Z_{i+1} = \nu^{-1}(G/Z_i) = \langle R_n^{n'/2} \rangle = \langle R_n^{n/2^{i+1}} \rangle\,.$$

Im Falle $i = k$ ist $n' = m$ ungerade und nach Aufgabe 11 dann

$$\mathrm{Zentr}(G/Z_k) = \mathrm{Zentr}(D_{2m}) = \{e\}\,, \quad \text{also} \quad Z_{k+1} = \nu^{-1}(\{e\}) = Z_k\,.$$

Aufgabe 33. (s)
Sei G eine nilpotente Gruppe. Zeigen Sie, dass zu jeder Folge $p_1, \ldots, p_n$ von Primzahlen mit $\prod_{i=1}^n p_i = \#G$ eine Kompositionsreihe $G = H_0 \supset H_1 \supset \ldots \supset H_n = \{e\}$ von G gibt, so dass für $i = 1, \ldots, n$ gilt:

$$H_{i-1}/H_i \text{ ist zyklisch von der Ordnung } p_i\,.$$

Lösung:
Sei P die p_1-Sylowuntergruppe von G, N das Erzeugnis der anderen Sylowuntergruppen von G, also $G = N \times P$ gemäß Satz I.5.7 (Vorlesung S. 37). Wähle in G eine maximale Untergruppe $H_1 \supset N$. Diese ist nach Prop. I.5.6 a) (Vorlesung S. 36) Normalteiler in G mit Primzahlindex. Wegen $(G : H_1) \mid (G : N) = \#P = p_1^k$ ist $G/H_1 = H_0/H_1$ primzyklisch von der Ordnung p_1.
Als Untergruppe von G ist auch H_1 nilpotent und hat die Ordnung $\prod_{i=2}^n p_i$. Per Induktion erhalten wir nun die gewünschte Folge

$$G = H_0 > H_1 > \ldots > H_n = \{e\} \quad \text{mit} \quad H_{i-1}/H_i \simeq \mathbb{Z}/p_i\mathbb{Z}\,.$$

Die Folge der H_i ist eine Kompositionsreihe, da die Faktoren primzyklisch, also einfach sind.

Algebra
Übung 7

Aufgabe 34. (m)
Formulieren Sie für Ringe und Moduln Homomorphie- und Isomorphiesätze, die den aus der Gruppentheorie bekannten Sätzen analog sind. Beweisen Sie die von Ihnen formulierten Sätze.

Lösung:
Für Ringe siehe Vorlesung Satz II.1.7 (S. 41) und für Moduln:

Satz (1.7′) (für R-Moduln) Sei R ein Ring.

a) Homomorphiesatz:

Ist $f : M \to M'$ ein Homomorphismus von R-Moduln, so existiert ein R-Modulmonomorphismus $\bar{f} : M/\mathrm{Ke}\, f \hookrightarrow M'$ mit $f = \bar{f} \circ \nu_{\mathrm{Ke}\, f}$.

$\bar{f}$ ist dadurch eindeutig bestimmt und es gilt: $M/\mathrm{Ke}\, f \xrightarrow{\sim} \mathrm{Im}\, f$.

b) (1. Isomorphiesatz) M sei ein R-Modul und $M_1, M_2 \leq M$ Untermoduln.

Dann ist $M_1 + M_2 = {}_R\langle M_1, M_2\rangle$ der von M_1 und M_2 erzeugte Untermodul und es gilt:

$$M_1/(M_1 \cap M_2) \xrightarrow{\sim} (M_1 + M_2)/M_2\,, \quad m_1 + (M_1 \cap M_2) \mapsto m_1 + M_2\,.$$

c) (2. Isomorphiesatz) Seien $M_1 \leq M_2 \leq M$ R-Moduln. Dann gilt:

$$M/M_2 \xrightarrow{\sim} {}^{(M/M_1)}\!/_{(M_2/M_1)}\,, \quad \nu_{M_2}(m) \mapsto \nu_{M_2/M_1}(m + M_1)$$

d) Ist $f : M \twoheadrightarrow M'$ ein R-Modulepimorphismus, so gilt für $N' \leq M'$:

$$M'/N' \simeq M/f^{-1}(M')$$

Begründungen: Für Ringe R und R-Moduln M sind $(R, +)$ und $(M, +)$ abelsche Gruppen, so dass aus den Homo- und Isomorphiesätzen für Gruppen zunächst die Existenz der behaupteten Abbildungen und ihre In-/Bijektivität folgt. Was zu überprüfen bleibt, ist die Homomorphie bzgl. der Multiplikation $\cdot$ im Ringfall und bzgl. der Multiplikation mit Skalaren $r.$ im Modulfall. Diese Homomorphien sind klar, da in den Faktorringen/-moduln die Verknüpfungen repräsentantenweise definiert sind. Im Ringfall ist zu beachten, dass diese repräsentantenweise Verknüpfung nur dann wohldefiniert ist, wenn ein Ideal gegeben ist (siehe Bemerkung II.1.4, Vorlesung S. 40). Daher muss man in (1.7) b) (1. Isomorphiesatz für Ringe) zeigen:

$$S \leq R\,, \quad \mathfrak{a} \lhd R \implies S \cap \mathfrak{a} \lhd S\,.$$

Wegen $\mathfrak{a} \lhd R$ folgt für alle $s \in S \leq R$ $s\mathfrak{a} \subset \mathfrak{a}$, und da S eine Unterring von R ist, gilt

$$s \in S \ \wedge\ a \in \mathfrak{a} \cap S \implies s.a \in S \cap \mathfrak{a}\,.$$

Im Modulfall entfallen diese zusätzlichen Überlegungen bzw. Begriffsbildungen, da die Multiplikation mit Skalaren $r.$ auch für die Quotientenstrukturen wohldefiniert ist.

Aufgabe 35. (m)
Man zeige für Ringe R, S:

a) Ist $\varphi : R \to S$ ein Ringhomomorphismus, so wird jeder S-Modul M zu einem R-Modul durch
$$R \times M \to M\,, \quad (r, m) \mapsto r.m := \varphi(r).m\,.$$

b) α) Ist R ein Unterring des Ringes S, so wird S in natürlicher Weise zu einem R-Modul.
β) Ist K ein Teilkörper von R, so wird R in natürlicher Weise zu einem K-Vektorraum.

Lösung:
a) $(M, +)$ ist eine abelsche Gruppe und es gilt wegen der Homomorphie von φ und der S-Modulstruktur von M:
$$\begin{aligned}(r + r').m &= \varphi(r + r').m = (\varphi(r) + \varphi(r')).m = \varphi(r).m + \varphi(r').m = r.m + r'.m\,,\\ r.(m + m') &= \varphi(r).(m + m') = \varphi(r).m + \varphi(r).m' = r.m + r.m'\,.\end{aligned}$$
Sind R und S unitär, so muss auch φ als unitär vorausgesetzt werden, d. h. $\varphi(1_R) = 1_S$ sein; dann gilt natürlich
$$1_R.m = \varphi(1_R).m = 1_S.m = m\,.$$
Beachten Sie, dass bei unitären Ringen Homomorphismen nicht notwendig unitär sein müssen, siehe etwa die Inklusion $\varphi : M_n(\mathbb{R}) \hookrightarrow M_{n+1}(\mathbb{R})$.
b) α) ist Spezialfall von a) mit der Inklusion $\varphi : R \hookrightarrow S$.
β) ist der Spezialfall von α) für $R = k$ Körper. Moduln über Körpern sind definitionsgemäß Vektorräume.

Aufgabe 36. (s)
Sei R ein Ring. Eine Sequenz $M' \xrightarrow{f} M \xrightarrow{g} M''$ von R-Modulhomomorphismen heißt *exakt*, wenn $\operatorname{Im} f = \operatorname{Ke} g$ ist. Längere Sequenzen sind exakt, wenn dies an jeder inneren Stelle der Sequenz gilt. Es bezeichne 0 den Nullmodul; zu jedem R-Modul M hat man stets eindeutig bestimmte Homomorphismen $0 \to M$ und $M \to 0$. (Nämliche welche?)

a) Für einen R-Modulhomomorphismus $f : M \to N$ zeige man:
$$f \text{ ist } \begin{cases}\text{injektiv}\\ \text{surjektiv}\\ \text{bijektiv}\end{cases} \iff \begin{cases}0 \longrightarrow M \xrightarrow{f} N\\ M \xrightarrow{f} N \longrightarrow 0\\ 0 \longrightarrow M \xrightarrow{f} N \longrightarrow 0\end{cases} \quad \text{ist exakt}\,.$$

b) α) Für eine sog. *kurze exakte Sequenz*
$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$
gilt:
$$M' \simeq f(M') \quad \text{und} \quad M/f(M') \simeq M''\,.$$
β) Für einen R-Untermodul N eines R-Moduls M konstruiere man eine exakte Sequenz $0 \to N \to M \to M/N \to 0$.

Lösung:
$0 \to M$ und $M \to 0$ können jeweils nur die Nullabbildung sein, die alles auf 0 abbildet, im ersten Falle, da Homomorphismen 0 auf 0 abbilden müssen, und im zweiten Falle, da dies die einzig mögliche Abbildung $M \to 0$ ist.
a) Es gelten die Äquivalenzen
$$f \quad \begin{cases}\text{injektiv}\\ \text{surjektiv}\end{cases} \iff \begin{cases}\operatorname{Ke} f = 0 = \operatorname{Im}(0 \to M)\\ \operatorname{Im} f = N = \operatorname{Ke}(N \to 0)\end{cases} \iff \begin{cases}0 \longrightarrow M \xrightarrow{f} N\\ M \xrightarrow{f} N \longrightarrow 0\end{cases} \quad \text{exakt}\,.$$

und die dritte Behauptung zur Bijektivität ist die Konjunktion der beiden vorangehenden Aussagen.
b) α): Die Exaktheit bei M' und M'' besagt nach a) f injektiv und g surjektiv; die Exaktheit bei M bedeutet $\operatorname{Im} f = \operatorname{Ke} g$. Zusammen mit dem 1. Isomorphiesatz für Moduln (Aufgabe 34) erhalten wir so:

$$f : M' \xrightarrow{\sim} f(M') = \operatorname{Im} f = \operatorname{Ke} g\,, \quad M/f(M') = M/\operatorname{Ke} g \xrightarrow{\sim} \operatorname{Im} g = N\,.$$

β): Sei $i_N : N \to M$ die (injektive) Inklusionsabbildung und $M \to M/N$ der natürliche Epimorphismus ν_N. Wegen $\operatorname{Ke} \nu_N = N = \operatorname{Im} i_N$ ist die Sequenz (an allen Stellen) exakt.

Aufgabe 37. (s)

a) Sei M ein Vektorraum über dem Körper k; wir setzen $\varphi(M) := \dim_k(M)$. Zeigen Sie:

α) Ist $0 \to M' \to M \to M'' \to 0$ eine exakte Sequenz von k-Vektorräumen, so gilt:

$$\varphi(M) < \infty \iff \varphi(M'), \varphi(M'') < \infty \implies \varphi(M) = \varphi(M') + \varphi(M'')\,.$$

β) Für eine exakte Sequenz von endlich-dimensionalen k-Vektorräumen

$$0 \to M_0 \to M_1 \to \ldots \to M_n \to 0$$

gilt:

$$\chi := \sum_{i=0}^{n} (-1)^i \varphi(M_i) = 0\,.$$

b) Definiert man für endliche abelsche Gruppen M die Größe $\varphi(M) := \ln \# M$, so bleiben die Aussagen aus a) für endliche abelsche Gruppen gültig. Was bedeutet die Aussage β) für die Gruppenordnungen?

Lösung:
a) α): Seien $f : M' \to M$ und $g : M \to M''$ die Homomorphismen der gegebenen exakten Sequenz, also f ein Mono- und g ein Epimorphismus (siehe Aufgabe 36).
$\underline{\Rightarrow}$: Wegen $\varphi(M) < \infty$ hat M eine endliche Basis, deren Bild unter g ist dann ein endliches Erzeugendensystem von $\operatorname{Im} g = M''$, also $\dim M'' < \infty$. Wegen $M' \xrightarrow{\sim} f(M') \subseteq M$ ist auch M' endlich-dimensional.
$\underline{\Leftarrow}$: Die Urbilder in M einer endlichen Basis von M'' unter g sind linear unabhängig und bilden zusammen mit einer (endlichen) Basis von $\operatorname{Ke} g = \operatorname{Im} f \simeq M'$ eine Basis von M, also $\varphi(M) = \varphi(M'') + \varphi(M') < \infty$. Damit ist zugleich auch die letzte Behauptung bewiesen.
β): Das Ergebnis von α) kann man umformulieren zu

$$\varphi(M') - \varphi(M) + \varphi(M'') = 0\,.$$

Also ist die Behauptung β) für $n = 2$ bewiesen. Für $0 \le n \le 1$ haben wir

$$0 \to M_0 \to 0 \text{ exakt} \iff M_0 = 0 \implies \sum_{i=0}^{0} \varphi(M) = 0\,,$$

$$0 \to M_0 \to M_1 \to 0 \text{ exakt} \iff M_0 \simeq M_1 \implies \sum_{i=0}^{1} (-1)^i \varphi(M_i) = 0$$

Sei nun $n \ge 3$. Wir bezeichnen die Homomorphismen in der exakten Sequenz mit $f_i : M_i \to M_{i+1}$ für $0 \le i < n$. Für den Induktionsschritt spalten wir die exakte Sequenz an der Stelle $M_1 \to M_2$ wie folgt auf:

$$\begin{aligned}
& 0 \to M_0 \to M_1 \to M_2 \to \ldots \to M_n \to 0 \text{ exakt} \\
\iff \quad & \Big(0 = \operatorname{Ke} f_0 \ \wedge \ \operatorname{Im} f_0 = \operatorname{Ke} f_1\Big) \ \wedge \ \operatorname{Im} f_1 = \operatorname{Ke} f_2 \\
& \wedge \ \Big(\operatorname{Im} f_2 = \operatorname{Ke} f_3 \ \wedge \ \ldots \ \wedge \ \operatorname{Im} f_{n-1} = M_n\Big) \\
\iff \quad & 0 \to M_0 \to M_1 \to \operatorname{Im} f_1 \to 0 \text{ exakt} \ \wedge \ \operatorname{Im} f_1 = \operatorname{Ke} f_2 \\
& \wedge \ 0 \to \operatorname{Ke} f_2 \hookrightarrow M_2 \to M_3 \to \ldots \to M_n \to 0 \text{ exakt}
\end{aligned}$$

Nach Induktionsvoraussetzung (für zwei kürzere exakte Sequenzen) erhalten wir

$$\varphi(M_0) - \varphi(M_1) + \varphi(\operatorname{Im} f_1) = 0\,, \quad \varphi(\operatorname{Im} f_1) = \varphi(\operatorname{Ke} f_2)\,, \quad -\varphi(\operatorname{Ke} f_2) + \sum_{i=2}^{n} (-1)^i \varphi(M_i) = 0$$

und daraus dann die Behauptung $\sum\limits_{i=0}^{n} (-1)^i \varphi(M_i) = 0$.

b): Für endliche abelsche Gruppen gilt (wie oben für Vektorräume) mit denselben Bezeichnungen wie in a) α)

$$0 \to M' \to M \to M'' \to 0 \text{ exakt} \implies M/f(M') \simeq M'' \ \wedge \ M' \simeq f(M')$$

und nach dem Satz von Lagrange (siehe Vorlesung, Prop. I.1.12 e), S. 8)

$$\#M = (M : f(M')) \cdot \#f(M') = \#M'' \cdot \#M'$$

mit der Vereinbarung $\infty \cdot n = n \cdot \infty = \infty \cdot \infty$. Also M endlich $\iff$ M', M'' endlich, und dann gilt

$$\varphi(M) = \ln \#M = \varphi(M') + \varphi(M'')\,.$$

Damit erhalten wir analog zu a) β) für eine lange exakte Sequenz $0 \to M_0 \to \ldots \to M_n \to 0$

$$\sum_{i=0}^{n} (-1)^i \ln \#M_i = 0 \iff \prod_{i=0}^{n} (\#M_i)^{(-1)^i} = 1 \iff \prod_{j \text{ gerade}} \#M_j = \prod_{j \text{ ungerade}} \#M_j\,.$$

Aufgabe 38. (s)

a) Sei $R = M_n(\mathbb{R})$ der Ring der $n \times n$-Matrizen über dem Körper $\mathbb{R}$ der reellen Zahlen. Zeigen Sie, dass (0) und R die einzigen zweiseitigen Ideale in R sind.

[Tipp: Sei E_{kl} die Matrix mit 1 an der Stelle (k, l) und 0 sonst. Für $A = (a_{\mu\nu})$ zeige man $E_{ij} A E_{kl} = a_{jk} E_{il}$.]

b) Enthält R (für $n \geq 2$) Linksideale?

c) Man bestimme die Einheitengruppen von $M_n(\mathbb{R})$ und $M_n(\mathbb{Z})$.

Lösung:

a) Wir bemerken zunächst:

($*$) Ideale in $R = M_n(\mathbb{R})$ sind $\mathbb{R}$-Untervektorräume von R.

Begründung: Die Multiplikation mit einem Sakalar $\alpha \in \mathbb{R}$ ist dasselbe wie die Multiplikation (von rechts oder von links) mit dem Ringelement $\alpha.E \in R$ (E die Einheitsmatrix, das Einselement von R).

Sei nun $(0) \neq \mathfrak{a} \lhd R$ ein (zweiseitiges) Ideal und $0 \neq A = (a_{\mu\nu})_{\mu\nu} \in \mathfrak{a}$. Dann gibt es ein Indexpaar (j, k) mit $a_{jk} \neq 0$. Aufgrund der Behauptung des Tipps gilt dann für alle (i, l)

$$\mathfrak{a} \ni E_{ij} A E_{kl} = a_{jk} E_{il} \underset{a_{jk} \neq 0}{\implies} E_{il} \in \mathfrak{a}\,.$$

Damit enthält $\mathfrak{a}$ alle Matrizen E_{il} $(1 \le i \le n,\ 1 \le l \le n)$ der kanonischen $\mathbb{R}$-Basis von $R = M_n(\mathbb{R})$, also nach $(*)$ ganz R.
Nachweis des Tipps:

$$\begin{aligned} E_{ij} &= (\delta_{i\mu}\delta_{j\nu})_{\mu\nu} \\ A &= (a_{\mu\nu})_{\mu\nu} = \sum_{\mu\nu} a_{\mu\nu}E_{\mu\nu} \\ E_{ij}E_{kl} &= (\delta_{i\mu}\delta_{j\nu})_{\mu\nu} \cdot (\delta_{k\nu}\delta_{l\lambda})_{\nu\lambda} = (\sum_{\nu} \delta_{i\mu}\delta_{j\nu}\delta_{k\nu}\delta_{l\lambda})_{\mu\lambda} = \delta_{jk}(\delta_{i\mu}\delta_{l\lambda})_{\mu\lambda} = \delta_{jk}E_{il} \\ E_{ij}AE_{kl} &= \sum_{\mu\nu} a_{\mu\nu}E_{ij}E_{\mu\nu}E_{kl} = a_{jk}E_{ij}E_{jl} = a_{jk}E_{il}\,. \end{aligned}$$

b) In einem Matrixprodukt AB ist die j-te Spalte das Produkt von A mit der j-ten Spalte von B. Ist also die j-te Spalte von B eine Nullspalte, so auch die j-te Spalte von AB. Linksideale in R sind daher die sog. Spaltenideale, die Menge aller Matrizen in denen eine feste Teilmenge von Spalten nur Nullspalten sind. Diese sind additive Untergruppen und gegenüber Linksmultiplikation mit beliebigen Matrizen aus R abgeschlossen, also Linksideale in R. Zu jeder Teilmenge $N \subset \{1, \ldots, n\}$ gibt es ein solches Spaltenideal; für $N = \emptyset$ erhält man den ganzen Ring R und für $\#N = n$ das Nullideal, alle anderen $2^n - 2$ Ideale sind echte Linksideale $\neq (0)$.
c) Die Einheitengruppe von $R = M_n(\mathbb{R})$ ist (per definitionem) die Gruppe der invertierbaren Matrizen $\mathrm{GL}_n(\mathbb{R})$. Aus der linearen Algebra ist bekannt

$$\mathrm{GL}_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid \det A \neq 0\}\,.$$

Dabei folgt die Inklusion $\subseteq$ folgt aus dem Determinantenproduktsatz:

$$AB = E \implies \det A \cdot \det B = 1 \implies \det A \neq 0\,.$$

Die umgekehrte Inklusion ist Folge des Laplaceschen Entwicklungssatzes für Determinanten und der sich daraus ergebenden Formel zur Berechnung der Inversen:

$$\det A \neq 0 \implies A^{-1} = \frac{1}{\det A}\Big((-1)^{i+j} \det A_{ij}\Big)^{\mathrm{T}}\,,$$

wo A_{ij} die Matrix A ohne Zeile i und ohne Spalte j ist.
Zur Bestimmung von $M_n(\mathbb{Z})^\times$ argumentiert man genauso:

$$A, B \in M_n(\mathbb{Z})\,,\ AB = E \implies \det A \cdot \det B = 1\,,\ \det A\,, \det B \in \mathbb{Z} \implies \det A \in \mathbb{Z}^\times = \{+1, -1\}\,,$$

also

$$M_n(\mathbb{Z})^\times \subseteq \{A \in M_n(\mathbb{Z}) \mid \det A = \pm 1\}\,.$$

Die umgekehrte Inklusion $\supseteq$ folgt nun wieder aus obiger Invertierungsformel, da $\det A = \pm 1$ und $\det A_{ij}$ ganzzahlig ist.

Aufgabe 39. (s)
Sei R ein unitärer kommutativer Ring. Zeigen Sie:

a) Jedes echte Ideal $\mathfrak{a} \neq R$ ist enthalten in $R \setminus R^\times$.

b) Es gelte für alle $x \in R$, entweder ist x oder $1 - x$ eine Einheit. Dann ist $R \setminus R^\times$ ein Ideal, und zwar das größte echte Ideal in R, und damit auch das einzige maximale Ideal in R.

   Ein Ring mit dieser Eigenschaft heißt *lokaler Ring*.

c) Es sei k ein Körper und $R = k[[X]]$ der formale Potenzreihenring in einer Variablen über k (vgl. Vorlesung II.1.2 Beispiel (5)). Zeigen Sie für $(a_0, a_1, \ldots) \in k^{\mathbb{N}} = k[[X]]$:

$$(a_0, a_1, \ldots) \in R^\times \iff a_0 \in k^\times = k \setminus \{0\}\,.$$

d) Folgern Sie, dass der formale Potenzreihenring $k[[X]]$ über einem Körper ein lokaler Ring ist.

Lösung:
a) Sei $\mathfrak{a} \neq R$ Ideal in R und $x \in \mathfrak{a}$ eine Einheit in R, also $yx = 1$ für ein $y \in R$. Dann gilt für jedes $r \in R$ wegen der Idealeigenschaft von $\mathfrak{a}$: $r = yx \in y\mathfrak{a} = \mathfrak{a}$, also ganz R liegt in $\mathfrak{a}$, Wid. Also gibt es in $\mathfrak{a}$ keine Einheit, d. h. $\mathfrak{a} \subset R \setminus R^\times$.
b) Sei $a \in \mathfrak{m} := R \setminus R^\times$ und $r \in R$. Wäre $ra \notin \mathfrak{m}$, also $ra \in R^\times$, so existierte ein $z \in R$ mit $1 = z \cdot ra$ für ein $z \in R$ und auch a wäre eine Einheit, Wid. Also gilt für $r\mathfrak{m} \subseteq \mathfrak{m}$ für alle $r \in R$. Seien nun $a, b \in \mathfrak{m}$ und angenommen $a + b \notin \mathfrak{m}$, also für ein $z \in R$

$$1 = (a+b)z = az + bz \implies az = 1 - bz\,.$$

Nach Voraussetzung wäre dann entweder $bz \in R^\times$ oder $1 - bz = az \in R^\times$, was aber beides nicht sein kann, denn $az, bz \in z\mathfrak{m} \subset \mathfrak{m}$.
Damit ist $\mathfrak{m}$ ein echtes Ideal in R. Nach a) enthält es jedes echte Ideal, ist also das größte Ideal von R. Jedes maximale Ideal ist also auch in $\mathfrak{m}$ enthalten, wegen der Maximalität dann gleich $\mathfrak{m}$: Das größte Ideal ist zwangsläufig das einzige maximale.
c) Sei $a = (a_0, a_1, \ldots) \in k[[X]]^\times$, also für ein $b = (b_0, b_1, \ldots) \in k[[X]]$

$$(1,0,0,\ldots) = a \cdot b = (a_0b_0, a_1b_0 + a_0b_1, \ldots, \sum_{i+j=n} a_ib_j, \ldots) \implies a_0b_0 = 1 \implies a_0 \in k^\times\,.$$

Zur Umkehrung müssen wir unter der Voraussetzung $a_0 \neq 0$ ein passendes b konstruieren. Wegen $a_0 \neq 0$ und k Körper gibt es ein $b_0 \in k$ mit $a_0b_0 = 1$. Gesucht sind nun $b_i \in k$ $(i \geq 1)$, so dass für alle $n \geq 1$ gilt

$$0 = \sum_{i+j=n} a_ib_j = a_0b_n + \sum_{i=1}^{n} a_ib_{n-i} \iff b_n = -a_0^{-1}(\sum_{i=1}^{n} a_ib_{n-i})\,.$$

Damit kann man induktiv b_n wie gewünscht definieren.
d) Ist $a = (a_0, a_1, \ldots)$ keine Einheit in $k[[X]]$, also $a_0 = 0$, so ist $1 - a = (1 - a_0, -a_1, \ldots) = (1, -a_1, -a_2, \ldots)$ gemäß c) eine Einheit. Die Voraussetzung von b) ist also erfüllt und $k[[X]]$ ist ein lokaler Ring mit dem größten Ideal $\mathfrak{m} = \{a \in k[[X]] \mid a_0 = 0\}$.

Algebra
Übung 8

Aufgabe 40. (m)
a) S sei ein unitärer kommutativer Ring, $R \leq S$ ein unitärer Unterring und $T = \{t_1, \ldots, t_n\} \subseteq S$ eine endliche Teilmenge. $R[T]$ sei der kleinste Unterring von S, der R und T enthält. Zeigen Sie:

$$R[T] = R[t_1, \ldots, t_n] = \{ \sum_{\nu \in \mathbb{N}^n} r_\nu t_1^{\nu_1} \cdot \ldots \cdot t_n^{\nu_n} \in S \mid r_\nu \in R\,,\ r_\nu = 0 \text{ für fast alle } \nu \in \mathbb{N}^n \}\,.$$

Geben Sie eine Darstellung für $R[T]$ bei beliebigem T an.
b) M sei ein Modul über dem unitären kommutativen Ring R, T eine Teilmenge von M. Zeigen Sie, dass die Menge

$$\{\sum_{i=1}^{n} r_i t_i \mid n \in \mathbb{N}\,, r_i \in R\,, t_i \in T\}$$

aller endlichen Linearkombinationen von Elementen aus T mit Koeffizienten in R der kleinste Untermodul von M ist, der T enthält.
c) E sei eine Teilmenge eines Ringes R. Wie sehen die Elemente von $[E]$, ${}_R\langle E\rangle$, $\langle E\rangle_R$ und ${}_R\langle E\rangle_R$ aus?

Lösung:
a) Da $R[T]$ ein Ring ist, der R und T enthält, muss er alle Elemente der angegebenen Form enthalten. Umgekehrt sind die Elemente von R und T in der angegebenen Form darstellbar: $r = r \cdot t^0$, $t = 1 \cdot t$. Es genügt also zu zeigen, dass die Menge aller Elemente der angegebenen Form selbst ein Ring ist, das heißt gegen die Ringverknüpfungen abgeschlossen ist. Zwei Elemente der angegebenen Form ergeben summiert oder multipliziert wieder eine solche Summe. Für die Summe ist dies unmittelbar klar, für das Produkt muss man distributiv rechnen:

$$\begin{aligned} & \sum_{\nu \in \mathbb{N}^n} r_\nu t_1^{\nu_1} \cdot \ldots \cdot t_n^{\nu_n} \cdot \sum_{\mu \in \mathbb{N}^m} r'_\mu t_1{}^{\mu_1} \cdot \ldots \cdot t_n{}^{\mu_n} \\ = & \sum_{\nu \in \mathbb{N}^n} \sum_{\mu \in \mathbb{N}^n} r_\nu r'_\mu t_1^{\nu_1+\mu_1} \cdot \ldots \cdot t_n^{\nu_n+\mu_n} \\ = & \sum_{\rho \in \mathbb{N}^n} \underbrace{\Big(\sum_{\substack{\nu,\mu \in \mathbb{N}^n \\ \nu+\mu=\rho}} r_\nu r'_\mu \Big)}_{=:s_\rho} t_1^{\rho_1} \cdot \ldots \cdot t_n^{\rho_n} \end{aligned}$$

Sind die beiden Ausgangssummen endlich, also $r_\nu = 0$ etwa für $\sum_i \nu_i > N$ und $r'_\mu = 0$ für $\sum_i \mu_i > M$, so sind auch fast alle $s_\rho = 0$, denn für $\rho = \nu + \mu$ gilt:

$$M + N < \sum_i \rho_i = \sum_i (\nu_i + \mu_i) \implies \sum_i \nu_i > N \ \vee \ \sum_i \mu_i > M \implies r_\nu = 0 \ \vee \ r'_\mu = 0$$

und daher

$$\sum_i \rho_i > M + N \implies s_\rho = \sum_{\substack{\nu,\mu \in \mathbb{N}^n \\ \nu+\mu=\rho}} r_\nu r'_\mu = 0\,.$$

Für beliebiges T gilt dann

$$R[T] = \{ \sum_{\nu \in \mathbb{N}^n} r_\nu t_1^{\nu_1} \cdot \ldots \cdot t_n^{\nu_n} \in S \mid n \in \mathbb{N}_+\,,\ t_1, \ldots, t_n \in T\,,\ r_\nu \in R\,,\ r_\nu = 0 \text{ für fast alle } \nu \in \mathbb{N}^n \}\,.$$

Zur Begründung könnte man wie oben argumentieren, da aber hier in den Summen nicht nur n, sondern auch die t_i variieren, ist bereits die Argumentation für die Summe solcher Terme formal etwas unhandlicher. Man kann aber das Ergebnis für den endlichen Fall benutzen und zeigt:

$$R[T] = \bigcup_{\substack{U\subset T\\ \#U<\infty}} R[U]$$

Zur Begründung, dass die Vereinigung tatsächlich ein Ring ist, beachte man $R[U] \cup R[V] \subset R[U \cup V]$ für beliebige endliche Teilmengen $U, V \subset T$, so dass die Vereinigung additiv und multiplikativ abgeschlossen ist.

b) beweist man genauso,

c) Da $(R, +)$ eine abelsche Gruppe ist, operiert $\mathbb{Z}$ darauf (siehe Vorlesung Beispiele II.1.9 (2)). Insbesondere gilt für $\pm 1 \in \mathbb{Z}$ $(\pm 1).r = \pm r$. Daher kann man für das Ringerzeugnis – auch wenn R kein Einselement hat – schreiben:

$$[E] \;=\; \{\sum_{\nu\in I} k_\nu . e_1^{\nu_1} \cdot \ldots \cdot e_n^{\nu_n} \mid n \in \mathbb{N}_+ ,\ e_i \in E ,\ I \subset \mathbb{N}^n ,\ \#I < \infty ,\ k_\nu \in \{-1, +1\} \subset \mathbb{Z}\} ,$$

Für die Idealerzeugnisse gilt:

$$\begin{aligned}
{}_R\langle E\rangle &= \{\sum_{i=1}^{n} r_i \cdot e_i \mid n \in \mathbb{N} ,\ e_i \in E ,\ r_i \in R\} ,\\
\langle E\rangle_R &= \{\sum_{i=1}^{n} e_i \cdot r_i \mid n \in \mathbb{N} ,\ e_i \in E ,\ r_i \in R\} ,\\
{}_R\langle E\rangle_R &= \{\sum_{i=1}^{n} r_i \cdot e_i \cdot s_i \mid n \in \mathbb{N} ,\ e_i \in E ,\ r_i, s_i \in R\} .
\end{aligned}$$

Bei endlichem E kann man in obigen Darstellungen $n = \#E$ und $E = \{e_1, \ldots, e_n\}$ fixieren.

Aufgabe 41. (m)
Sei K ein Körper und R ein unitärer Unterring.

a) Der von R erzeugte Teilkörper (R) in K ist der sog. *Quotientenkörper von R in K*:

$$(R) = \{ab^{-1} \in K \mid a, b \in R ,\ b \neq 0\} ,$$

b) Der Quotientenkörper von R in K ist unabhängig von K, genauer: Sind K, L Oberkörper von R und $(R)_K$ bzw. $(R)_L$ die Quotientenkörper von R in K bzw. L, so existiert genau ein Körperisomorphismus

$$\varphi : (R)_K \xrightarrow{\sim} (R)_L \quad \text{mit} \quad \varphi\,|_R = \mathrm{id}_R .$$

Lösung:
a) Der Durchschnitt von Körpern ist ein Körper, daher existiert (R) als der Durchschnitt aller Teilkörper k von K mit $R \subset k$. Da (R) ein Körper ist, der R umfasst, muss er alle Elemente der Form ab^{-1} $(a, b \in R,\ b \neq 0)$ enthalten, also gilt in a) die Inklusion '$\supseteq$'. Da R in der rechten Seite enthalten ist (setze $b = 1$), gilt die umgekehrte Inklusion '$\subseteq$', wenn gezeigt ist, dass die rechte Seite von a) ein Körper ist. Als Teilmenge eines Körpers genügt es zu zeigen, dass die rechte Seite 0 und 1 enthält (klar, ganz R ist enthalten) und abgeschlossen ist gegen $+$, $-$ sowie die von 0 verschiedenen Elemente gegenüber $\cdot$, $(\ldots)^{-1}$ abgeschlossen sind. Dies rechnet man leicht nach (Bruchrechnung!).
b) Ist φ ein solcher Homomorphismus, so muss gelten: $\varphi(a \underset{K}{\cdot} b^{-1}) = \varphi(a) \underset{L}{\cdot} \varphi(b)^{-1} \underset{a,b\in R}{=} a \underset{L}{\cdot} b^{-1} \in L$, also ist φ eindeutig. Zur Existenz muss man nachweisen, dass dieser (zwangsläufige) Ansatz wohldefiniert und ein Homomorphismus ist (wieder Bruchrechnung). Die Surjektivität ist nach Ansatz klar und die Injektivität folgt sofort aus der Homomorphie:

$$\varphi(a \underset{K}{\cdot} b^{-1}) = 0_L \iff a \underset{L}{\cdot} b^{-1} = 0_L \iff a = b \underset{L}{\cdot} 0_L = 0_L = 0_R \iff a \underset{K}{\cdot} b^{-1} = 0_K .$$

Aufgabe 42. (s)
Sei R ein kommutativer unitärer Ring, $M = \langle m_1, \ldots, m_n \rangle = \sum_{i=1}^{n} Rm_i$ ein endlich erzeugter R-Modul, $\mathfrak{a} \lhd R$ ein Ideal in R und

$$\mathfrak{a}M := \langle \alpha.m \mid \alpha \in \mathfrak{a}\,,\ m \in M \rangle_R = \{ \sum_{i=1}^{n} \alpha_i m_i \mid \alpha_i \in \mathfrak{a} \}\,.$$

Zeigen Sie: Ist $\mathfrak{a}$ in jedem maximalen Ideal von R enthalten und gilt $\mathfrak{a}M = M$, so muss M der Nullmodul sein.
Tipp: Für jedes $\alpha \in \mathfrak{a}$ ist $1 - \alpha$ Einheit in R. Wählen Sie nun $n \in \mathbb{N}$ minimal.

Lösung:
Beweis des Tipps: Ist $1-\alpha$ keine Einheit, so ist $R(1-\alpha)$ ein echtes Ideal, also in einem maximalen Ideal $\mathfrak{m} \lhd R$ enthalten (siehe Vorlesung Prop. II.1.18, S. 47). Wegen $1 - \alpha \in \mathfrak{m}$ und nach Voraussetzung $\alpha \in \mathfrak{a} \subset \mathfrak{m}$ folgt $1 \in \mathfrak{m}$ und daher $R = \mathfrak{m}$, im Widerspruch zur Maximalität von $\mathfrak{m}$.
Beweis der Behauptung: Sei n die kleinstmögliche Erzeugendenzahl von M. Ist $n = 0$, so ist M von der leeren Menge erzeugt, also trivial und der Beweis erbracht.
Sei also nun $n \geq 1$. Nach Voraussetzung ist $m_n = \sum_{i=1}^{n} \alpha_i m_i$ mit $\alpha_i \in \mathfrak{a}$, also $(1 - \alpha_n)m_n = \sum_{i=1}^{n-1} \alpha_i m_i \in \langle m_1, \ldots, m_{n-1} \rangle$. Nach dem Tipp ist $1 - \alpha_n$ Einheit in R und folglich

$$m_n \in \langle m_1, \ldots, m_{n-1} \rangle\,.$$

Dies bedeutet, dass M bereits von $n-1$ Elementen erzeugt wird im Widerspruch zur Minimalität von n.

Aufgabe 43. (s)
Sei R ein kommutativer unitärer Ring. Eine Teilmenge $T \subset R$ heißt multiplikativ, wenn sie die 1_R enthält und multiplikativ abgeschlossen ist.

a) $T \subset R$ sei multiplikativ mit $0 \notin T$. Es sei M_T die Menge aller Ideale in R, die T nicht treffen:

$$M_T := \{ \mathfrak{a} \lhd R \mid \mathfrak{a} \cap T = \emptyset \}\,.$$

Zeigen Sie: Ist $\mathfrak{p}$ maximales Element von M_T (bzgl. der Inklusion), so ist $\mathfrak{p}$ ein Primideal von R. Warum existieren stets maximale Elemente in M_T?

b) Zeigen Sie: Ist $\mathfrak{p} \lhd R$ ein echtes Primideal, so ist $T := R \setminus \mathfrak{p}$ multiplikativ mit $0 \notin T$.

c) Ist R ein Integritätsbereich und $\mathfrak{p} \lhd R$ ein echtes Primideal, so gilt:

   $\alpha)$ $R_\mathfrak{p} := \{ \frac{r}{s} \in \mathrm{Quot}(R) \mid r \in R\,,\ s \in R \setminus \mathfrak{p} \}$ ist ein lokaler Ring.

   $\beta)$ Der kanonische Ringmonomorphismus $R \hookrightarrow \mathrm{Quot}(R)$ induziert einen Monomorphismus

$$R/\mathfrak{p} \hookrightarrow R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}\,.$$

   Dabei ist $\mathfrak{p}R_\mathfrak{p} = \langle \mathfrak{p} \rangle_{R_\mathfrak{p}}$ das von $\mathfrak{p}$ erzeugte $R_\mathfrak{p}$-Ideal.

   $\gamma)$ In $\beta)$ liegt genau dann ein Isomorphismus vor, wenn $\mathfrak{p}$ ein maximales Ideal in R ist.

Man nennt $R_\mathfrak{p}$ die Lokalisierung von R nach $\mathfrak{p}$.

Lösung:
a) Die Existenz maximaler Elemente in M_T folgt aus Lemma von Zorn, Vorlesung II.1.17, S. 47, dessen Voraussetzungen erfüllt sind: $M_T \neq \emptyset$ (wegen $0 \notin T$, also $(0) \in M_T$) und (teilweise) geordnet. Ist $K \subset M_T$ totalgeordnet, so ist $\mathfrak{b} := \bigcup K := \bigcup_{\mathfrak{a} \in K} \mathfrak{a}$ ein Ideal in R. $\mathfrak{b} \in M_T$, denn andernfalls gäbe es ein $t \in T \cap \mathfrak{b}$, also $t \in T \cap \mathfrak{a}$ für ein $\mathfrak{a} \in K \subset M_T$ im Widerspruch zur

Definition von M_T. Damit ist $\mathfrak{b} \in M_T$ obere Schranke für K.
Sei nun $\mathfrak{p}$ maximal in M_T und $a_1, a_2 \in R$ mit $a_1 a_2 \in \mathfrak{p}$. Annahme: $a_1, a_2 \notin \mathfrak{p}$, also gilt wegen der Maximalität von $\mathfrak{p}$: $\langle \mathfrak{p}, a_i \rangle_R \notin M_T$ und folglich existieren $t_i \in T \cap \langle \mathfrak{p}, a_i \rangle_R$:

$$t_i = p_i + r_i a_i \text{ mit } p_i \in \mathfrak{p}\,,\ r_i \in R\,.$$

Wegen $a_1 a_2 \in \mathfrak{p}$ und der Idealeigenschaft von $\mathfrak{p}$ folgt

$$t_1 t_2 = p_1 p_2 + r_1 a_1 p_2 + r_2 a_2 p_1 + r_1 r_2 a_1 a_2 \in \mathfrak{p}\,,$$

im Widerspruch zur Multiplikativität von T und $\mathfrak{p} \cap T = \emptyset$.
b) $0 \in \mathfrak{p}$, $1 \notin \mathfrak{p} \neq R$, also $0 \notin T$ und $1 \in T$. Die Multiplikativität von T ist die Kontraposition zur Definition der Primidealeigenschaft:

$$a, b \in T = R \setminus \mathfrak{p} \iff a, b \notin \mathfrak{p} \underset{\mathfrak{p} \text{ prim}}{\Longrightarrow} ab \notin \mathfrak{p} \iff ab \in T\,.$$

c) α) Es ist $R_\mathfrak{p} = \{\frac{r}{s} \mid r \in R,\ s \notin \mathfrak{p}\}$, also ist $\mathfrak{p}R_\mathfrak{p} = \{\frac{r}{s} \mid r \in \mathfrak{p},\ s \notin \mathfrak{p}\}$ und folglich $R \setminus \mathfrak{p}R_\mathfrak{p} = \{\frac{r}{s} \mid r, s \notin \mathfrak{p}\} = R_\mathfrak{p}^\times$ die Einheitengruppe. Damit ist gemäß der Definition in Aufgabe 39 b) $R_\mathfrak{p}$ ein lokaler Ring mit $\mathfrak{p}R_\mathfrak{p}$ als (einzigem maximalen) größtem Ideal.
β) Sei $i : R \hookrightarrow R_\mathfrak{p}$ die kanonische Einbettung. Dann gilt

$$i(r) \in \mathfrak{p}R_\mathfrak{p} \iff \bigvee_{r' \in \mathfrak{p}} \bigvee_{s' \notin \mathfrak{p}} \frac{r}{1} = \frac{r'}{s'} \iff \bigvee_{r', s'} rs' = r' \in \mathfrak{p} \underset{s' \notin \mathfrak{p} \text{ prim}}{\Longrightarrow} r \in \mathfrak{p}$$

und damit $i^{-1}(\mathfrak{p}R_\mathfrak{p}) = \mathfrak{p}$.
Nach dem Homomorphiesatz erhalten wir aus $j := \nu \circ i : R \hookrightarrow R_\mathfrak{p} \twoheadrightarrow R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$ den behaupteten Monomorphismus

$$\bar{j} : R/\mathrm{Ke}\,(\nu \circ i) = R/\mathfrak{p} \hookrightarrow R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}\,.$$

γ) Zu zeigen: $\bar{j}$ surjektiv $\iff$ $\mathfrak{p} \lhd R$ maximal.
$\Longrightarrow$: $\mathfrak{p}R_\mathfrak{p}$ ist (einziges) maximales Ideal in $R_\mathfrak{p}$, also nach Vorlesung Proposition II.1.15, S. 45 ist $R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$ ein Körper. Ist $\bar{j}$ ein Isomorphismus, muss auch $R/\mathfrak{p}$ ein Körper, $\mathfrak{p}$ also maximal in R sein.
$\Longleftarrow$: Sei $\nu(\frac{r}{s}) \in R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$ beliebig, also $r \in R$ und $s \notin \mathfrak{p}$ vorgegeben. Ist $\mathfrak{p}$ maximal, also $R/\mathfrak{p}$ ein Körper, so besitzt $\bar{s} := s + \mathfrak{p} \neq \bar{0} \in R/\mathfrak{p}$ ein Inverses $\bar{t} \in R/\mathfrak{p}$ und folglich gilt

$$\nu(\frac{r}{s}) = \nu(\frac{r}{1}) \cdot \nu(\frac{s}{1})^{-1} = \nu \circ i(r) \cdot \nu \circ i(s)^{-1} = \bar{j}(\bar{r}) \cdot \bar{j}(\bar{s})^{-1} = \bar{j}(r) \cdot \bar{j}(\bar{t}) = \bar{j}(\bar{r}\bar{t}) \in \mathrm{Im}\,\bar{j}\,.$$

Aufgabe 44. (s)

a) Jeder endliche Integritätsbereich ist ein Körper.

b) Sei R ein Integritätsbereich und $K \leq R$ ein Teilkörper. Ist R als K-Vektorraum (siehe Aufgabe 35 b)) endlich dimensional, so ist R selbst ein Körper.

Tipp: Untersuchen Sie die Linksmultiplikation mit Elementen aus R.

Lösung:
Ist R ein Integritätsbereich, so ist die Linksmultiplikation $L_a : R \to R$ mit $a \in R$ ein Ringhomomorphismus. Die Nullteilerfreiheit von R besagt:

$$a \neq 0 \implies L_a \text{ injektiv}\,.$$

ad a): Ist R endlich, so muss für $a \neq 0$ die injektive Abbildung $L_a : R \to R$ auch surjektiv sein ($L_a(R) \subset R$, $\#L_a(R) = \#R \implies L_a(R) = R$). Dies bedeutet, dass $1_R = L_a(b) = ab$ ein Bild unter L_a ist, also a eine Inverses in R besitzt.
ad b): Hier argumentiert man genauso: Wegen der endlichen Dimension muss für $a \neq 0$ der Vektorraummonomorphismus $L_a : {}_KR \hookrightarrow {}_KR$ selbst surjektiv sein ($L_a(R) \leq R$, $\dim_K(L_a(R)) = \dim_K(R) \implies L_a(R) = R$), und wieder folgt, dass R ein Körper ist.

Aufgabe 45. (s)
Sei $\mathbb{H}$ die Menge aller komplexen 2×2-Matrizen der Form

$$A = \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} \in M_2(\mathbb{C}) .$$

a) Zeigen Sie, dass $\mathbb{H}$ ein nicht-kommutativer unitärer Unterring von $M_2(\mathbb{C})$ ist und dass für jedes $0 \neq A \in \mathbb{H}$ auch A^{-1} wieder in $\mathbb{H}$ liegt, so dass $\mathbb{H}$ ein Divisionsring ist.

b) Man zeige, dass $\mathbb{H}$ der Schiefkörper der Hamiltonschen Quaternionen über $\mathbb{R}$ ist (siehe Vorlesung Beispiele II.1.14 4), S. 45)

c) Sei $\mathbb{H}' := \{ \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} \mid \alpha, \beta \in \mathbb{Z}[i] \}$. (Warum ist $\mathbb{H}'$ unitärer Unterring von $\mathbb{H}$?)

Zeigen Sie, dass die Einheitengruppe von $\mathbb{H}'$ isomorph ist zur Quaternionengruppe Q_8 (vgl. Aufgabe 18 b)).

Lösung:
a) $\mathbb{H}$ ist abgeschlossen gegen $+$, $-$, $\cdot$ und enthält die Einheitsmatrix E. $\mathbb{H}$ ist nicht kommutativ, denn

$$A := \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \in \mathbb{H} , \; B := \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \in \mathbb{H} , \quad AB = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \neq BA = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} .$$

Ist $0 \neq A = \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} \in \mathbb{H}$, also $\alpha \neq 0 \; \vee \; \beta \neq 0$, so ist $\det A = |\alpha|^2 + |\beta|^2 \neq 0$ und folglich A invertierbar mit

$$A^{-1} = \frac{1}{\det A} \begin{pmatrix} \bar{\alpha} & -\beta \\ \bar{\beta} & \alpha \end{pmatrix} .$$

Da $\det A = |\alpha|^2 + |\beta|^2$ reell ist, gehört A^{-1} zu $\mathbb{H}$.
b) Ist $\alpha = a + bi$, $\beta = c + di$ mit $a, b, c, d \in \mathbb{R}$, so gilt

$$A = \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} + \begin{pmatrix} bi & 0 \\ 0 & -bi \end{pmatrix} + \begin{pmatrix} 0 & c \\ -c & 0 \end{pmatrix} + \begin{pmatrix} 0 & di \\ di & 0 \end{pmatrix} = aE + bI + cJ + dK .$$

$\mathbb{H}$ ist also ein 4-dimensionaler $\mathbb{R}$-Vektorraum mit der Basis

$$E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} , \; I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} , \; J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} , \; K = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} .$$

Die Multiplikation in $\mathbb{H}$ ergibt sich durch distributive Rechnung aus den Produkten der Basiselemente

$$I^2 = J^2 = -E , \; IJ = -JI = K .$$

Damit haben wir für $\mathbb{H}$ genau die in der Vorlesung gegebene Definition der Hamiltonschen Quaternionen (siehe Beispiele II.1.14 4), S. 45).
c) Da $\mathbb{Z}[i]$ ein Ring ist, ist $\mathbb{H}'$ abgeschlossen gegen $+$, $-$, $\cdot$ und enhält das Einselement E. Ist $A \in \mathbb{H}'$ eine Einheit, also $AB = E$ mit $B \in \mathbb{H}'$, so folgt $1 = \det A \cdot \det B$ mit $\det A , \det B \in \mathbb{Z}$, also $\det A \in \mathbb{Z}^\times = \{+1, -1\}$. Da $\det A = |\alpha|^2 + |\beta|^2$ positiv ist, kommt nur $\det A = +1$ in Frage. Und umgekehrt, ist $\det A = 1$, so hat A das Inverse $\frac{1}{\det A} A^{\mathrm{ad}} = A^{\mathrm{ad}}$ in $\mathbb{H}'$. Also $\mathbb{H}'^\times = \{A \in \mathbb{H}' \mid \det A = 1\}$.
Für $A = \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} \in \mathbb{H}'$, $\alpha = a + bi$, $\beta = c + di$ mit $a, b, c, d \in \mathbb{Z}$ ergibt

$$\det A = |\alpha|^2 + |\beta|^2 = a^2 + b^2 + c^2 + d^2 = 1$$

genau die 8 möglichen Matrizen $\pm E$, $\pm R$, $\pm S$ und $\pm T$ mit

$$R = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},\ S = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},\ T = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Also ist $\mathbb{H}'^{\times} = \{\pm E, \pm S, \pm R, \pm T\}$ eine Gruppe der Ordnung 8. Sie enthält die Quaternionengruppe $\langle S, T\rangle = Q_8$ (siehe Aufgabe 18. b)) und stimmt wegen gleicher Mächtigkeit mit ihr überein.

Algebra
Übung 9

Aufgabe 46. (m)
Sei R ein faktorieller Ring. Zeigen Sie:

a) a ist unzerlegbar $\iff$ a ist Primelement.

b) Ist $\mathcal{P}$ ein Repräsentantensystem der Primelemente von R modulo Assoziertheit, so ist jedes $a \in R \setminus \{0\}$ eindeutig darstellbar als

$$a = u \cdot \prod_{p \in \mathcal{P}} p^{v_p(a)} \quad \text{mit } u \in R^\times\,,\ v_p(a) \in \mathbb{N} \text{ und } v_p(a) = 0 \text{ für fast alle } p \in \mathcal{P}\,.$$

c) Zu $a, b \in R \setminus \{0\}$ existiert stets ein größter gemeinsamer Teiler $\mathrm{ggT}(a,b)$ und ein kleinstes gemeinsames Vielfaches $\mathrm{kgV}(a,b)$. Geben Sie explizit einen ggT und ein kgV an mittels der Darstellungen von a, b gemäß b).

d) Teilt $a \in R \setminus \{0\}$ ein Produkt bc und ist a teilerfremd zu b, so ist a ein Teiler von c.

Lösung:
Siehe Vorlesung Beweis von Bem. II.2.16, S. 51.

Aufgabe 47. (s)

a) Sei $n \in \mathbb{N}_+$ und $a \in \mathbb{Z}$. Es sei φ die Eulersche Phi-Funktion.

Zeigen Sie: Ist a prim zu n, so gilt $a^{\varphi(n)} \equiv 1 \bmod n$.

[Für $n = p$ Primzahl ergibt sich der kleine Fermatsche Satz: $p \nmid a \implies a^{p-1} \equiv 1 \bmod p$.]

b) Sei $G = \langle \sigma \rangle$ zyklisch von der Ordnung n und $k \in \mathbb{Z}$. Zeigen Sie:

(i) $G = \langle \sigma^k \rangle \iff k + n\mathbb{Z} \in \mathcal{P}(n) \iff k$ ist zu n teilerfremd.

(ii) $\operatorname{ord} \sigma^k = \dfrac{\operatorname{ord} \sigma}{\mathrm{ggT}(k, \operatorname{ord} \sigma)}$

(iii) $\operatorname{Aut} G \simeq \mathcal{P}(n)$.

c) Sind G_1, G_2 endliche zyklische Gruppen, so gilt:

$$G_1 \times G_2 \text{ zyklisch} \iff \mathrm{ggT}(\#G_1, \#G_2) = 1\,.$$

Lösung:
a) Definitionsgemäß liegt $\bar{a} = a + n\mathbb{Z}$ in der primen Restklassengruppe $\mathcal{P}(n)$. Deren Ordnung ist per definitionem $\varphi(n)$, also gilt nach dem Satz von Lagrange $\bar{a}^{\#\mathcal{P}(n)} = \bar{a}^{\varphi(n)} = \bar{1}$ und somit $a^{\varphi(n)} \equiv 1 \bmod n$. Wegen $\varphi(p) = p - 1$ ergibt sich der Zusatz.
b) (i) folgt aus (ii). Hier ein Beweis als Hinführung zu (ii):

$$G = \langle \sigma^k \rangle \iff \sigma \in \langle \sigma^k \rangle \iff \bigvee_{l \in \mathbb{Z}} \sigma = \sigma^{kl} \iff \bigvee_{l} \operatorname{ord} \sigma = n \mid kl - 1 \iff k \in \mathcal{P}(n)\,.$$

ad (ii): Sei $d = \mathrm{ggT}(n,k)$ und $dn' = n$, $dk' = k$, also n' und k' teilerfremd. Dann gilt für ein beliebiges l:

$$(\sigma^k)^l = e \iff \operatorname{ord}(\sigma) = n \mid kl \iff n' \mid k'l \iff n' \mid l\,.$$

Damit folgt $\operatorname{ord}(\sigma^k) = n' = \frac{n}{d}$, wie behauptet.

ad (iii): $f \in \operatorname{Aut} G \implies f(\sigma) =: \sigma^k$ erzeugt $f(G) = G$, also ist nach (i) $\bar{k} \in \mathcal{P}(n)$. Die Zuordnung $f \mapsto \bar{k}$ ist ein Homomorphismus $\Phi : \operatorname{Aut}(G) \to \mathcal{P}(n)$, denn

$$f, g \in \operatorname{Aut}(G)\,,\ f(\sigma) = \sigma^k\,,\ g(\sigma) = \sigma^l \implies f \circ g(\sigma) = f(\sigma^l) = \sigma^{kl}\,,$$

also $\Phi(f \circ g) = \bar{k}\bar{l} = \Phi(f)\Phi(l)$.
Φ ist injektiv, denn $\Phi(f) = \bar{1} \implies f(\sigma) = \sigma \implies f = \mathrm{id}_G$. Zur Surjektivität: Sei $\bar{k} \in \mathcal{P}(n)$. Da G abelsch ist, ist die Potenzierung mit k $f = (\ldots)^k$ ein Gruppenhomomorphismus, und wegen $k \in \mathcal{P}(n)$ ist gemäß (i) $f(\sigma) = \sigma^k$ Erzeugendes von G, also $f : G \to G$ eine surjektive Selbstabbildung. Wegen der Endlichkeit von G ist f auch injektiv, also $f \in \operatorname{Aut} G$ mit $\Phi(f) = \bar{k}$.
c) Für $\sigma = (\sigma_1, \sigma_2) \in G_1 \times G_2$ gilt $\operatorname{ord}(\sigma_1, \sigma_2) = \mathrm{kgV}(\operatorname{ord}\sigma_1, \operatorname{ord}\sigma_2)$, denn

$$(\sigma_1, \sigma_2)^k = e \iff \sigma_i^k = e_i \iff \operatorname{ord}\sigma_i \mid k \iff kgV(\operatorname{ord}\sigma_1, \operatorname{ord}\sigma_2) \mid k\,.$$

Sind nun σ_i Erzeugende der G_i (mit den Ordnungen $n_i = \#G_i$), so hat $\sigma := (\sigma_1, \sigma_2) \in G_1 \times G_2$ die Ordnung $\mathrm{kgV}(n_1, n_2)$. Bei teilerfremden n_i hat also σ die Ordnung $n_1 n_2 = \#G_1 \cdot \#G_2$ und ist somit Erzeugendes von $G_1 \times G_2$.
Ist umgekehrt $\tau = (\tau_1, \tau_2)$ ein Erzeugendes von $G_1 \times G_2$, so gilt

$$n_1 n_2 = \operatorname{ord}\tau = \mathrm{kgV}(\operatorname{ord}\tau_1, \operatorname{ord}\tau_2) \mid \mathrm{kgV}(n_1, n_2) \mid n_1 n_2\,,$$

also gilt die Gleichheit $\mathrm{kgV}(n_1, n_2) = n_1 n_2$ und das bedeutet $\mathrm{ggT}(n_1, n_2) = 1$.

Aufgabe 48. (s)
Zeigen Sie:

a) Jeder euklidische Ring (R, d) ist ein Hauptidealring.

b) $\mathbb{Z}[i] \leq \mathbb{C}$ ist euklidisch bzgl. der Normabbildung $\mathcal{N} : \mathbb{Z}[i] \to \mathbb{N}$, $z \mapsto z\bar{z} = |z|^2$.
Tipp: Für $z, w \in \mathbb{Z}[i] \setminus \{0\}$ approximiere man $\frac{z}{w}$ bestmöglich durch ein Element aus $\mathbb{Z}[i]$.

c) $\mathbb{Z}[i\sqrt{5}]$ hingegen ist nicht euklidisch (für keine Funktion d). Untersuchen Sie dazu die Faktoren in den Zerlegungen $6 = 2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$.
Tipp: Eine Zerlegung von z in $\mathbb{Z}[i\sqrt{5}]$ liefert eine Zerlegung von $\mathcal{N}(z)$ in $\mathbb{Z}$.

Lösung:
a) Sei $\{0\} \neq \mathfrak{a} \lhd R$ ein beliebiges Ideal und wähle $a_0 \in \mathfrak{a} \setminus \{0\}$ mit kleinstmöglichem $d(a_0) \in \mathbb{N}$. Da d definit ist, ist $d(a_0) \geq 1$. Da (R, d) euklidisch ist, gibt es zu jedem $0 \neq a \in \mathfrak{a}$ Elemente $q, r \in R$ mit $a = qa_0 + r$ und $d(r) < d(a_0)$. Wegen $a, a_0 \in \mathfrak{a} \lhd R$ ist $r = a - qa_0 \in \mathfrak{a}$ und aufgrund der Minimalität von $d(a_0)$ muss $r = 0$ sein: Jedes $0 \neq a \in \mathfrak{a}$ ist von der Form $a = qa_0$ für ein passendes $q \in R$ und damit $\mathfrak{a} = a_0 R$ Hauptideal.
b) Die Normabbildung $\mathcal{N} = |\ldots|^2$ ist definit. Sie hat auf $\mathbb{Z}[i]$ nur Werte in $\mathbb{N}$:

$$a + bi \in \mathbb{Z}[i] \implies a, b \in \mathbb{Z} \implies \mathcal{N}(a + bi) = (a + bi)(a - bi) = a^2 + b^2 \in \mathbb{N}\,.$$

Sei $R = \mathbb{Z}[i]$ und $0 \neq z, w \in R$ beliebig. Gesucht sind $q, r \in R$ mit $z = qw + r$ und $\mathcal{N}(r) < \mathcal{N}(w)$. Gemäß dem Tipp betrachten wir die komplexe Zahl $u := \frac{z}{w}$ und suchen ein nächstliegendes $q \in R = \mathbb{Z}[i]$, also $q = a + bi$ mit $a, b \in \mathbb{Z}$.
Geometrische Argumentation: Die Elemente $a + bi$, $a, b \in \mathbb{Z}$ bilden im 2-dimensionalen $\mathbb{R}$-Vektorraum $\mathbb{C} = \mathbb{R} + \mathbb{R}i$ die Eckpunkte von achsenparallelen Quadraten der Kantenlänge 1. Jedes $u \in \mathbb{C}$ ist also von einem $a + bi \in R$ höchstens um die halbe Diagonalenlänge $\frac{1}{2}\sqrt{2}$ entfernt: Zu $u = \frac{z}{w} \in \mathbb{C}$ gibt es ein $q \in R$ mit $|u - q| < \frac{1}{2}\sqrt{2}$, also $\mathcal{N}(u - q) \leq (\frac{1}{2}\sqrt{2})^2 = \frac{1}{2} < 1$. Dann folgt aber

$$z = qw + w(u - q) \quad \text{mit } \mathcal{N}(w(u - q)) = \mathcal{N}(w) \cdot \mathcal{N}(u - q) < \mathcal{N}(w)$$

und $r := w(u-q) = z - wq \in R$.
Rechnerische Begründung: Sei $u = \alpha + \beta i$ mit $\alpha, \beta \in \mathbb{R}$. Wähle zu $\alpha, \beta \in \mathbb{R}$ die nächstliegenden ganzen Zahlen $a, b \in \mathbb{Z}$, also $|\alpha - a| \leq \frac{1}{2}$, $|\beta - b| \leq \frac{1}{2}$. Dann folgt für $q = a + bi$

$$\mathcal{N}(u-q) = \mathcal{N}((\alpha - a) + (\beta - b)i) = (\alpha - a)^2 + (\beta - b)^2 \leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2}.$$

c) Wäre $R := \mathbb{Z}[i\sqrt{5}]$ euklidisch, so wäre R ein Hauptidealring (gemäß Vorlesung Prop. II.2.9, S. 49) und unzerlegbare Elemente wären prim (siehe Vorlesung Bemerkung II.2.14 a), S. 51). Aber 2 ist unzerlegbar in R und die angegebenen Faktorisierungen der 6 zeigen, dass 2 kein Primelement in R ist.
Begründungen: Wäre $2 = uv$ mit $u, v \in R$, so wäre $4 = \mathcal{N}(2) = \mathcal{N}(u)\mathcal{N}(v)$ das Produkt zweier Normen und Normen haben stets die Form $\mathcal{N}(a + bi\sqrt{5}) = a^2 + 5b^2 \in \mathbb{N}$. Die möglichen Werte von $a^2 + 5b^2$ sind $0, 1, \geq 4$ (bei b=0) oder ≥ 5 (bei $b \neq 0$), insbesondere $\neq 2, 3$. Also ist (o.E.) $\mathcal{N}(u) = 1$, $u = \pm 1$ Einheit in R.
Wäre 2 Primelement in R, so müsste wegen $2 \mid 6 = (1 + i\sqrt{5})(1 - i\sqrt{5})$ 2 einen der Faktoren $1 \pm i\sqrt{5}$ teilen. Dies ist aber nicht der Fall, denn

$$2 \mid 1 \pm i\sqrt{5} \implies 4 = \mathcal{N}(2) \mid \mathcal{N}(1 \pm i\sqrt{5}) = 6\,.$$

Dieser Widerspruch beweist c).

Aufgabe 49. (s)

a) Seien $r \in \mathbb{N}_+$, $n_i \in \mathbb{N}$ $(i = 1, \ldots r)$ teilerfremd und $N := \prod_{i=1}^{r} n_i$ sowie $N_i := \frac{N}{n_i}$.

Beweisen Sie:

(i) Es gibt $N_i' \in \mathbb{N}$ mit $N_i N_i' \equiv 1 \bmod n_i$ $(i = 1, \ldots, r)$.

(ii) Für jedes System ganzer Zahlen $a_1, \ldots, a_r \in \mathbb{Z}$ und $a \in \mathbb{Z}$ gilt:

$$\bigwedge_{i=1}^{r} a \equiv a_i \bmod n_i \iff a \equiv \sum_{i=1}^{r} N_i N_i' a_i \bmod N\,.$$

Dies bedeutet insbesondere: Jedes System *simultaner Kongruenzen* $x \equiv a_i \bmod n_i$ $(i = 1, \ldots, r)$ modulo teilerfremder n_i hat genau eine Lösung modulo $N = n_1 \cdot \ldots \cdot n_r$.

b) Man bestimme die Lösungen $x \in \mathbb{Z}$ der simultanen Kongruenzen

$$x \equiv 1 \bmod 3\,,\ x \equiv 4 \bmod 5\,,\ x \equiv 2 \bmod 7\,,\ x \equiv 9 \bmod 11\,.$$

c) Beweisen Sie die sog. *Neunerprobe*: Eine ganze Zahl ist genau dann durch 9 teilbar, wenn ihre Quersumme (=Summe der Koeffizienten in der Dezimaldarstellung) durch 9 teilbar ist.

Formulieren und beweisen Sie eine *Elferprobe*.

d) Man bestimme den Rest von

$$(123578^{51} + 283679^5)^{154}$$

bei Division durch 143.

Lösung:
a) (i) Für jedes i ist N_i zu n_i teilerfremd, denn angenommen es gibt eine Primzahl p mit $p \mid N_i = \prod_{j \neq i} n_j$ und $p \mid n_i$, so gibt es ein $j \neq i$ mit $p \mid n_j$ und $p \mid n_i$, im Widerspruch zur

Voraussetzung.
Also ist $\bar{N}_i$ eine prime Restklasse modulo n_i und besitzt daher ein Inverses N_i' modulo n_i (siehe Vorlesung Prop. II.2.21 d), S. 54): $N_i N_i' \equiv 1 \bmod n_i$, wie behauptet.
ad (ii) $\Longleftarrow$: Wegen $N = \prod_i n_i$ gilt

$$\begin{aligned} a \equiv \sum_{j=1}^{r} N_j N_j' a_j \bmod N \quad &\underset{*}{\Longrightarrow} \quad \bigwedge_i \; a \equiv \sum_{j=1}^{r} N_j N_j' a_j \bmod n_i \\ &\iff \quad \bigwedge_i \; a \equiv \sum_{j\neq i} \underbrace{N_j}_{\equiv 0} N_j' a_j + \underbrace{N_i N_i'}_{\equiv 1} a_i \bmod n_i \\ &\underset{(i)}{\iff} \quad \bigwedge_i \; a \equiv a_i \bmod n_i \end{aligned}$$

ad (ii) $\Longrightarrow$: Die Implikation $(*)$ gilt aber auch umgekehrt, denn die n_i sind teilerfremd und daher $\mathrm{kgV}(n_i) = \prod n_i = N$ und folglich

$$\bigwedge_i a \; \equiv A \bmod n_i \iff \bigwedge_i \; n_i \mid a - A \iff \mathrm{kgV}(n_i) = N \mid a - A \iff a \equiv A \bmod N\,.$$

b) Mit $n_1 = 3\,,\; n_2 = 5\,,\; n_3 = 7\,,\; n_4 = 11$ erhalten wir

$$\begin{aligned} N_1 &= 5 \cdot 7 \cdot 11 \equiv (-1) \cdot 1 \cdot (-1) = +1 \bmod 3\,, & N_1' &= 1\,, \\ N_2 &= 3 \cdot 7 \cdot 11 \equiv 3 \cdot 2 \cdot 1 \equiv 1 \bmod 5\,, & N_2' &= 1\,, \\ N_3 &= 3 \cdot 5 \cdot 11 \equiv 3 \cdot (-2) \cdot (-3) \equiv 4 \bmod 7\,, & N_3' &= 2\,, \\ N_4 &= 3 \cdot 5 \cdot 7 \equiv 3 \cdot 5 \cdot (-4) \equiv 6 \bmod 11\,, & N_4' &= 2 \end{aligned}$$

und als gesuchte Lösung modulo $N = 3 \cdot 5 \cdot 7 \cdot 11 = 1155$

$$a = \sum_i N_i N_i' a_i = 385 \cdot 1 \cdot 1 + 231 \cdot 1 \cdot 4 + 165 \cdot 2 \cdot 2 + 105 \cdot 2 \cdot 9 = 3859 \equiv 394 \bmod N\,.$$

c) Sei $a = \sum_i a_k 10^k$ die Dezimaldarstellung von a, also $a_k \in \mathbb{N}$, $0 \leq a_k \leq 9$ die Folge der Dezimalziffern von a. Dann gilt wegen $10 \equiv 1 \bmod 9$:

$$a = \sum_k a_k 10^k \equiv \sum_k a_k 1^k = \sum_k a_k \bmod 9\,.$$

Also ist eine Zahl a modulo 9 kongruent zu ihrer Quersumme, insbesondere durch 9 teilbar, wenn die Quersumme es ist.
Entsprechend erhalten wir wegen $10 \equiv -1 \bmod 11$ die Elferprobe

$$a = \sum_k a_k 10^k \equiv \sum_k a_k (-1)^k \bmod 11\,.$$

In Worten: Modulo 11 ist eine Zahl kongruent zu ihrer sog. Wechselsumme, der Summe ihrer Dezimalziffern mit wechselndem Vorzeichen, bei der letzten Ziffer positiv beginnend. Insbesondere ist eine Zahl durch 11 teilbar, wenn ihre Wechselsumme durch 11 teilbar ist.
d) Sei A die vorgegebene Zahl; gesucht ist $a \in \mathbb{Z}$, $0 \leq a < 143$ mit $a \equiv A \bmod 143$. Es ist $143 = 11 \cdot 13$ und daher

$$a \equiv A \bmod 143 \iff a \equiv A \bmod 11\,,\; a \equiv A \bmod 13\,.$$

Wir berechnen daher zunächst A modulo der beiden Primzahlen, also die Restklasse von A in den beiden endlichen *Körpern* (!) $\mathbb{F}_{11}$ bzw. $\mathbb{F}_{13}$. Man beachte für die Potenzierungen die Ordnungen der Multiplikationsgruppen $\#\mathbb{F}_{11}^{\times} = 10$ bzw. $\#\mathbb{F}_{13} = 12$, so dass nach dem Satz von Lagrange die Exponenten modulo 10 bzw. 12 zu nehmen sind. Dies ergibt:

$$\begin{aligned} \mathrm{mod}11: \quad & A = (123578^{51} + 283679^5)^{154} \equiv (4^1 + 0)^4 \equiv 3\,, \\ \mathrm{mod}13: \quad & A = (123578^{51} + 283679^5)^{154} \equiv (0 + 6^5)^{10} \equiv 6^{50} \equiv 6^2 \equiv -3 \end{aligned}$$

Die gesuchte Zahl ist also die kleinste positive Lösung der simultanen Kongruenzen

$$a \equiv 3 \bmod 11\,, \quad a \equiv -3 \bmod 13\,.$$

Diese lösen wir durch 'scharfes Hinsehen' ($a = 36$) oder mit etwas Überlegung wie folgt: Gesucht ist ein Vielfaches von 11 ($a - 3$) und ein Vielfaches von 13 ($a + 3$) mit dem Abstand 6; wegen $13 - 11 = 2$ muss dies das Dreifache sein: 33 und 39, also $a = 33 + 3 = 39 - 3$.
Man kann aber auch b) anwenden (bei nur 2 teilerfremden (und kleinen) Moduln aber unnötig aufwendig):

$$N_1 = 13 \equiv 2 \bmod 11\,,\ N_1' = 6\,, \quad N_2 = 11 \equiv -2 \bmod 13\,,\ N_2' = 6$$

$$a = 13 \cdot 6 \cdot 3 + 11 \cdot 6 \cdot (-3) \equiv 6 \cdot (39 - 33) \equiv 36 \bmod 143\,.$$

Aufgabe 50. (s)

a) Zeigen Sie, dass für $c, a_1, \ldots, a_n \in \mathbb{Z}$ ($n \in \mathbb{N}_+$) die Gleichung

$$a_1 x_1 + \ldots + a_n x_n = c$$

genau dann eine ganzzahlige Lösung $(x_1, \ldots, x_n) \in \mathbb{Z}^n$ besitzt, wenn $\mathrm{ggT}(a_1, \ldots, a_n)$ ein Teiler von c ist.

b) Beschreiben Sie ein Lösungsverfahren für die Gleichung in a) und lösen Sie:

$$30x_1 + 105x_2 + 70x_3 + 42x_4 = 29\,.$$

c) Bestimmen Sie die Menge *aller* ganzzahligen Lösungen von $ax + by = c$ für $a, b, c \in \mathbb{Z}$.

Lösung:
a) Hat die Gleichung in a) eine Lösung $(x_1, \ldots, x_n) \in \mathbb{Z}^n$, so ist jeder gemeinsame Teiler der a_i auch ein Teiler von $\sum x_i a_i = c$. Insbesondere ist der ggT der a_i ein Teiler von c.
Sei nun umgekehrt $d = \mathrm{ggT}(a_1, \ldots, a_n)$ ein Teiler von c, also $c = c'd$ mit $c' \in \mathbb{Z}$. Da $\mathbb{Z}$ ein Hauptidealring ist, ist d als $\mathbb{Z}$-Linearkombination der a_i darstellbar (siehe Vorlesung Bemerkung II.2.6, S. 49), also $d = y_1 a_1 + \ldots + y_n a_n$ mit geeigneten $y_i \in \mathbb{Z}$. Dann hat aber die Gleichung a) die Lösung $x_i = c' y_i$.
b) Basis des Lösungsverfahrens ist der euklidische Algorithmus. Dieser gestattet die Berechnung des ggT zweier ganzer Zahlen und dessen Darstellung als Linearkombination dieser Zahlen (siehe Vorlesung Prop. II.2.11, S. 50). Für mehrere Zahlen muss man dies iterieren unter Beachtung von

$$\mathrm{ggT}(a, b, c) = \mathrm{ggT}(\mathrm{ggT}(a, b), c)\,.$$

Lösungsverfahren:

1. Bestimme $d = \mathrm{ggT}(a_i)$ (bei kleinen Zahlen über die Primzerlegung, sonst mit dem euklidischen Algorithmus).
2. Ist d kein Teiler von c, so gibt es keine Lösung.
3. Ist d ein Teiler von c, so bestimme man (bei kleinen Zahlen durch Ausprobieren, sonst mit dem euklidischen Algorithmus) eine Darstellung von d als Linearkombination der a_i: $d = \sum_i y_i a_i$ mit $y_i \in \mathbb{Z}$.
4. Die gegebene Gleichung hat dann die Lösung $x_i = \dfrac{c}{d} \cdot y_i$.

Für das gegebene Beispiel $30x_1 + 105x_2 + 70x_3 + 42x_4 = 29$ mit kleinen Zahlen benötigt man den euklidischen Algorithmus nicht:
$\mathrm{ggT}(30, 105) = 15 \cdot \mathrm{ggT}(2, 7) = 15\,,\ \mathrm{ggT}(70, 42) = 14 \cdot \mathrm{ggT}(5, 3) = 14\,,\ \mathrm{ggT}(30, 105, 70, 42) = \mathrm{ggT}(15, 14) = 1$, die Gleichung hat also (bei beliebiger rechter Seite) eine ganzzahlige Lösung.
Es ist $1 = \mathrm{ggT}(15, 14) = 15 - 14$, $1 = \mathrm{ggT}(2, 7) = 2 \cdot (-3) + 7$, $1 = \mathrm{ggT}(5, 3) = 5 \cdot (-1) + 3 \cdot 2$, also

$$\begin{aligned} 1 &= 15 - 14 = 15 \cdot \mathrm{ggT}(2, 7) - 14 \cdot \mathrm{ggT}(5, 3) = 15 \cdot (2 \cdot (-3) + 7) - 14 \cdot (5 \cdot (-1) + 3 \cdot 2) \\ &= 30 \cdot (-3) + 105 \cdot 1 + 70 \cdot 1 + 14 \cdot (-2)\,. \end{aligned}$$

Mit den Bezeichnungen von b) ist also $y = (-3, 1, 1, -2)$ und eine Lösung der gegebenen diophantischen Gleichung

$$x = 29 \cdot (-3, 1, 1, -2) = (-87, 29, 29, -58)\,.$$

c) Sei $\mathcal{L} := \mathcal{L}(a, b, c) := \{(x, y) \in \mathbb{Z}^2 \mid ax + by = c\}$ die zu bestimmende Lösungsmenge. Der Vollständigkeit halber seien die Trivialfälle $a = 0 \ \vee \ b = 0$ sowie der bekannte unlösbare Fall $\mathrm{ggT}(a, b) \nmid c$ genannt:

$$\mathcal{L}(a, b, c) = \begin{cases} \mathbb{Z}^2 & a = b = c = 0, \\ \emptyset & a = b = 0\,,\ c \neq 0, \\ \{\frac{c}{b}\} & a = 0,\ b \neq 0,\ b \mid c, \\ \{\frac{c}{a}\} & a \neq 0,\ b = 0,\ a \mid c, \\ \emptyset & a \neq 0 \ \vee \ b \neq 0,\ \mathrm{ggT}(a, b) \nmid c, \end{cases}$$

Sei nun also $ab \neq 0$ und $d := \mathrm{ggT}(a, b) \mid c$. Die Division der Gleichung durch d ändert die Lösungsmenge nicht. Es genügt also die Untersuchung der Lösungsmengen $\mathcal{L}(a, b, c)$ für teilerfremde a, b. Sei (x_0, y_0) irgendeine (gemäß a) existierende, evtl. gemäß b) bestimmte) Lösung. Dann gilt (wegen der Linearität der Gleichung) für alle $x, y \in \mathbb{Z}$

$$(x, y) \in \mathcal{L}(a, b, c) \iff ax + by = c = ax_0 + by_0 \iff a(x - x_0) + b(y - y_0) = 0\,,$$

also $\mathcal{L}(a, b, c) = (x_0, y_0) + \mathcal{L}(a, b, 0)$.
Man muss also für teilerfremde a, b die (homogene) Gleichung $au + bv = 0$ lösen. Nun gilt für $u, v \in \mathbb{Z}$

$$au + bv = 0 \iff au = -bv \underset{\mathrm{ggT}(a,b)=1}{\Longrightarrow} a \mid v \ \wedge \ b \mid u \iff \bigvee_{k,l \in \mathbb{Z}} u = bk \ \wedge \ v = al\,.$$

Aus $au = abk = -bv = -abl$ folgt dann aber (wegen $ab \neq 0$) $l = -k$, also

$$au + bv = 0 \implies \bigvee_{k \in \mathbb{Z}} u = bk\,,\ v = -ak\,.$$

Offenbar gilt auch die Umkehrung dieser Implikation, so dass sich $\mathcal{L}(a, b, 0) = \mathbb{Z} \cdot (b, -a)$ ergibt. Insgesamt erhalten wir so

$$\mathcal{L}(a, b, c) = (x_0, y_0) + \mathbb{Z} \cdot (b, -a) = \{(x_0 + kb, y_0 - ka) \mid k \in \mathbb{Z}\}\,.$$

Algebra
Übung 10

Aufgabe 51. (m)
Sei R ein kommutativer unitärer Ring.

a) Ist $S := R[X_1, \ldots, X_n]$ der Polynomring über R in n Unbestimmten $X_1, \ldots, X_n$, so ist der Polynomring über S in X_{n+1} $S[X_{n+1}]$ der Polynomring über R in den $n+1$ Unbestimmten $X_1, \ldots, X_{n+1}$.

b) Für jedes $a \in R$ ist der Faktorring von $R[X]$ nach dem Hauptideal $(X-a)R[X]$ isomorph zum Grundring R:
$$R[X]/(X-a)R[X] \simeq R\,.$$

c) Für jedes Ideal $\mathfrak{a} \lhd R$ ist
$$\mathfrak{a}[X] := \{\sum_{i=0}^{n} a_i X^i \mid a_i \in \mathfrak{a}\,,\ n \in \mathbb{N}\}$$
ein Ideal in $R[X]$ mit
$$R[X]/\mathfrak{a}[X] \simeq (R/\mathfrak{a})[X]\,.$$

Lösung:
a) Der Ring $T := S[X_{n+1}] = R[X_1, \ldots, X_n][X_{n+1}]$ ist ein unitärer Oberring von (S und damit auch von) R, er enthält $X_1, \ldots, X_{n+1}$ und jedes $F \in T$ ist eindeutig darstellbar als
$$F = \sum_{k\in\mathbb{N}} f_k X_{n+1}^k \quad \text{mit} \quad f_k \in S = R[X_1, \ldots, X_n]\,,\ \text{fast alle } f_k = 0\,.$$
Jedes $f_k \in S$ ist seinerseits eindeutig darstellbar als
$$f_k = \sum_{\nu\in\mathbb{N}^n} a_{\nu k} X_1^{\nu_1} \cdots X_n^{\nu_n}\,,\ a_{\nu k} = 0 \text{ für fast alle } \nu \in \mathbb{N}^n\,.$$
Damit erhalten wir die eindeutige Darstellung
$$F = \sum_{k\in\mathbb{N}} \sum_{\nu\in\mathbb{N}^n} a_{\nu k} X_1^{\nu_1} \cdots X_n^{\nu_n} \cdot X_{n+1}^k = \sum_{\mu\in\mathbb{N}^{n+1}} a_\mu X_1^{\mu_1} \cdots X_{n+1}^{\mu_{n+1}}\,.$$
Für fast alle k ist $f_k = 0$, also sind wegen der eindeutigen Darstellbarkeit in $S = R[X_1, \ldots, X_n]$ für fast alle k *alle* $a_{\nu k} = 0$. Für die endlich vielen übrigen k gibt es jeweils auch nur endlich viele $\nu \in \mathbb{N}^n$ mit $a_{\nu k} \neq 0$, also insgesamt
$$a_{\nu k} = 0 \quad \text{für fast alle } \mu = (\nu, k) \in \mathbb{N}^n \times \mathbb{N} = \mathbb{N}^{n+1}\,.$$
Dies beweist a).
b) Wir betrachten den Einsetzungsepimorphismus
$$E_a : R[X] \twoheadrightarrow R[a] = R\,,\ f \mapsto f(a)\,.$$
$\operatorname{Ke} E_a$ besteht aus allen Polynomen f mit a als Nullstelle. Nach Bemerkung II.3.7 der Vorlesung ist jedes f mit $f(a) = 0$ Vielfaches von $X - a$ und damit $\operatorname{Ke} E_a = (X-a)R[X]$. Nach dem Homomorphiesatz folgt daher
$$R[X]/(X-a)R[X] = R[X]/\operatorname{Ke} E_a \xrightarrow{\sim} \operatorname{Im} E_a = R\,.$$

c) Da $\mathfrak{a}$ Ideal in R ist, ist $\mathfrak{a}[X]$ additiv und gegen Multiplikation mit Skalaren aus R abgeschlossen (also ein R-Modul), aber auch gegen Multiplikation mit Polynomen $f \in R[X]$:

$$f = \sum_{i=0}^{d} r_i X^i\,,\ a = \sum_{k=0}^{n} \underbrace{a_k}_{\in\mathfrak{a}} X^k \implies f \cdot a = \sum_{j=0}^{m} \underbrace{(\sum_{i+k=j} r_i a_k)}_{\in\mathfrak{a}} X^j \in \mathfrak{a}[X]\,.$$

Der natürliche Epimorphismus $\nu : R \twoheadrightarrow R/\mathfrak{a}$ besitzt eine eindeutige Fortsetzung $\varphi : R[X] \twoheadrightarrow (R/\mathfrak{a})[X]$ (vermöge $X \mapsto X$). Dessen Kern ist

$$\operatorname{Ke}\varphi = (\operatorname{Ke}\nu)[X] = \mathfrak{a}[X]\,,$$

so dass aus dem Homomorphiesatz die Behauptung folgt.

Aufgabe 52. (m)
R sei ein kommutativer unitärer Ring und $\deg : R[X] \setminus \{0\} \to \mathbb{N}$ die Gradfunktion.

a) Für $0 \neq f, g \in R[X]$ gilt:

$$\begin{array}{rcl} \deg(f+g) & \leq & \max(\deg f, \deg g) \quad \text{oder} \quad f+g=0\,, \\ \deg(f\cdot g) & = & \deg f + \deg g \quad \text{falls } R \text{ Integritätsbereich ist.} \end{array}$$

b) R Integritätsbereich $\iff$ $R[X_1,\ldots,X_n]$ Integritätsbereich.

c) Für Integritätsbereiche R gilt: $R[X_1,\ldots,X_n]^\times = R^\times$.

d) Dividieren Sie $f(X) = 7X^4 + 35X^3 - X - 3$ in $\mathbb{Z}[X]$ mit Rest durch $g(X) = X^2 + 5X - 1$ und stellen Sie einen ggT von f und g in $\mathbb{Q}[X]$ als Linearkombination von f und g dar.

Lösung:
Seien a_μ bzw. b_ν die Koeffizienten von f bzw. g und $m = \deg f$, $n = \deg g$.
a) Dann hat $f+g$ die Koeffizienten $a_\mu + b_\mu$ und es gilt $a_\mu + b_\mu = 0$ für $\mu \geq \max(m,n)$, also $\deg(f+g) \leq \max(m,n)$ oder $f+g=0$.
Für die Koeffizienten $c_\rho = \sum_{\mu+\nu=\rho} a_\mu b_\nu$ von fg gilt:

$$\rho = \mu+\nu > m+n \implies \mu > m \ \vee\ \nu > n \implies a_\mu = 0 \ \vee\ b_\nu = 0 \implies c_\rho = 0\,,$$

$$\rho = \mu+\nu = m+n \implies \mu > m \ \vee\ (\mu < m \ \wedge\ \nu > n) \ \vee\ (\mu = m, \nu = n) \implies c_\rho = a_m b_n\,.$$

Es ist $c_\rho = 0$ für $\rho > m+n$ und, ist R -nullteilerfrei, so folgt $c_{m+n} = a_m b_n \neq 0$, also $\deg(fg) = m+n$, und der führende Koeffizient von fg ist das Produkt der führenden Koeffizienten von f und von g.
In b) und c) genügt der Beweis für $n = 1$, die allgemeine Behauptung folgt daraus induktiv mittels Aufgabe 51.a).
b) Sind $0 \neq f, g \in R[X]$ und R Integritätsbereich, so ist nach a) $\deg(fg) = \deg f + \deg g$ und damit $fg \neq 0$, womit ' $\implies$ ' gezeigt ist; '$\Longleftarrow$' ist klar wegen $R \leq R[X]$.
c) Es sei R Integritätsbereich und $f \in R[X]$ eine Einheit, also gilt für ein $g \in R[X]$

$$1 = fg \implies 0 = \deg 1 = \deg f + \deg g \implies \deg f = \deg g = 0 \implies f, g \in R^\times\,.$$

d) Da der führende Koeffizient von $g(X)$ eine Einheit in $\mathbb{Z}$ (sogar $= 1$) ist, ist die Division mit Rest in $\mathbb{Z}[X]$ möglich. Es gilt

$$\begin{array}{rcl} f(X) & = & 7X^2 \cdot g(X) + 7X^2 - X - 3 \\ & = & 7X^2 \cdot g(X) + 7g(X) - 36X + 4 \\ & = & (7X^2+7)g(X) - 36X + 4 \end{array}$$

Daraus folgt $\mathrm{ggT}(f,g) = \mathrm{ggT}(g, -36X+4)$. Da $\frac{1}{9}$ keine Nullstelle von $g(X)$ ist ($g(\frac{1}{9}) = \frac{1}{81} + \frac{5}{9} - 1 = -\frac{35}{81}$), ist $-36X+4$ kein Teiler von $g(X)$ (in $\mathbb{Q}[X]$) und damit ist $1 = \mathrm{ggT}(g, -36X+4) = \mathrm{ggT}(f,g)$.
Zur Bestimmung einer Darstellung des ggT als Linearkombination führen wir den euklidischen Algorithmus weiter und dividieren g mit Rest durch $-36X+4$ (in $\mathbb{Q}[X]$):

$$g(X) = -\frac{1}{36}X(-36X+4) + \frac{46}{9}X - 1 = (-\frac{1}{36}X - \frac{46}{9\cdot 36})(-36X+4) - \frac{35}{81}\,.$$

Nach dem euklidischen Algorithmus ist $-\frac{35}{81}$, und damit 1 ein ggT von f, g (wie schon oben begründet): f, g sind teilerfremd. Man erhält dann aus den obigen Divisionen mit Rest nach 'Beseitigung' der Nenner die Darstellung

$$\begin{aligned}
-36X+4 &= f(X) - (7X^2+7)g(X)\\
-35 &= 81g(X) + (\frac{9}{4}X + \frac{46}{4})(-36X+4)\\
-140 &= 324g(X) + (9X+46)\Big(f(X) - (7X^2+7)g(X)\Big)\\
&= (9X+46)\cdot f(X) + (324 - 63X^3 - 322X^2 - 63X - 322)\cdot g(X)\\
&= (9X+46)\cdot f(X) + (-63X^3 - 322X^2 - 63X + 2)\cdot g(X)
\end{aligned}$$

Aufgabe 53. (s)
Sei p eine Primzahl und $r, s \in \mathbb{N}$. Ist A eine endliche abelsche p-Gruppe mit

$$\begin{aligned}
A &\simeq \mathbb{Z}/p^{\nu_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p^{\nu_r}\mathbb{Z}\,, \quad 1 \le \nu_1 \le \ldots \le \nu_r\,,\\
A &\simeq \mathbb{Z}/p^{\mu_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p^{\mu_s}\mathbb{Z}\,, \quad 1 \le \mu_1 \le \ldots \le \mu_s\,,
\end{aligned}$$

so müssen $r = s$ und für alle i $\nu_i = \mu_i$ sein. [Man betrachte $p.A$ und schließe induktiv.]
Lösung:
Im Falle $A = 0$ muss $r = s = 0$ sein. Sei nun $A \neq 0$. Wir bestimmen zunächst $p.A$. Nach dem Homomorphiesatz gilt

$$p\mathbb{Z}/p^k\mathbb{Z} \simeq \mathbb{Z}/p^{k-1}\mathbb{Z}$$

und damit nach Voraussetzung

$$p.A \simeq \mathbb{Z}/p^{\nu_1-1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p^{\nu_r-1}\mathbb{Z} \simeq \mathbb{Z}/p^{\mu_1-1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p^{\mu_s-1}\mathbb{Z}\,. \tag{1}$$

Durch Vergleich der Ordnungen in den Darstellungen von A bzw. pA erhalten wir

$$d := \sum_{i=1}^{r}\nu_i = \sum_{j=1}^{s}\mu_j \quad \text{bzw.}$$
$$\sum_{i=1}^{r}(\nu_i - 1) = \sum_{j=1}^{s}(\mu_j - 1) \iff d - r = d - s$$

und damit die Übereinstimmung $r = s$.
Die Übereinstimmung $\nu_i = \mu_i$ beweisen wir induktiv über die Ordnung von A. Wegen $\#pA < \#A$ (für $A \neq 0$) wenden wir die Induktionsvoraussetzung auf pA an. Aus (1) erhalten wir (wegen $r = s$ und $\mathbb{Z}/p^0\mathbb{Z} = 0$)

$$\begin{aligned}
p.A &\simeq \mathbb{Z}/p^{\nu_a-1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p^{\nu_r-1}\mathbb{Z}\,, \quad 1 = \nu_1 = \ldots = \nu_{a-1} < \nu_a \le \ldots \le \nu_r\\
&\simeq \mathbb{Z}/p^{\mu_b-1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p^{\mu_r-1}\mathbb{Z}\,, \quad 1 = \mu_1 = \ldots = \mu_{b-1} < \mu_b \le \ldots \le \mu_r\,.
\end{aligned}$$

Aufgrund der schon allgemein bewiesenen Behauptung $r = s$ erhalten wir aus diesen beiden Darstellungen von pA die Gleichheit $r - (a-1) = r - (b-1) \iff a = b$ und damit $\nu_i = 1 = \mu_i$ für $1 \le i < a = b$. Nach Induktionsvoraussetzung folgt dann schließlich

$$\nu_i - 1 = \mu_i - 1\,, \text{ also } \nu_i = \mu_i \quad \text{für } a = b \le i \le r\,.$$

Aufgabe 54. (s)
Sei R ein kommutativer unitärer Ring, M ein freier R-Modul vom Rang n und $(a_1, \ldots, a_n)$ eine Basis von M.

a) Zeigen Sie, dass für $A \in M_n(R)$ genau dann $(a_1, \ldots, a_n) \cdot A$ eine Basis von M ist, wenn $A \in M_n(R)^\times$, d. h. (!) $\det A \in R^\times$ ist.

b) Ein Teilmodul $N \leq M$ heißt *direkter Summand* in M, falls ein $N' \leq M$ existiert mit $N \oplus N' \simeq M$.

Zeigen Sie: Ist R ein Hauptidealring, so ist ein Teilmodul $N \leq M$ genau dann ein direkter Summand von M, wenn die Invarianten α_i des Elementarteilersatzes (siehe Vorlesung Satz II.2.24, S. 56) Einheiten in R sind.

c) Der $\mathbb{Z}$-Modul $(\mathbb{Q}, +)$ besitzt keine nichttrivialen (d. h. von $0, \mathbb{Q}$ verschiedenen) direkten Summanden.

Lösung:
a) '$\Rightarrow$': Ist $(b_1, \ldots, b_n) := (a_1, \ldots, a_n) \cdot A$ eine Basis von M, also insbesondere Erzeugendensystem, so ist jedes a_i als R-Linearkombination der b_j darstellbar, also gibt es eine Matrix $B \in M_n(R)$ mit

$$(a_1, \ldots, a_n) = (b_1, \ldots, b_n) \cdot B = (a_1, \ldots, a_n) \cdot AB\,.$$

Da die a_i eine Basis von M bilden, sind die Darstellungen als Linearkombinationen der a_i eindeutig und es muss $AB = E$ die Einheitsmatrix sein. Umgekehrt folgt aus der Basiseigenschaft der b_i genauso:

$$(b_1, \ldots, b_n)BA = (a_1, \ldots, a_n)A = (b_1, \ldots, b_n) \implies BA = E\,,$$

und mithin ist A Einheit in $M_n(R)$ mit Inversem B. Also folgt $1 = \det(AB) = \det A \cdot \det B$ und $\det A$ ist Einheit in R. Ist umgekehrt $\det A$ Einheit in R, so ist auch A Einheit in $M_n(R)$, denn für die Adjunkte (gebildet aus den durch Streichen der i-ten Zeile und j-ten Spalte entstehenden Unterdeterminanten $\det A_{ij}$ von A)

$$A^{\mathrm{ad}} = \Big((-1)^{i+j} \det A_{ij}\Big)^{\mathrm{t}} \in M_n(R)$$

gilt (nach dem Laplaceschen Entwicklungssatz der Linearen Algebra, gültig über kommutativen unitären Ringen)

$$A^{\mathrm{ad}} \cdot A = \det A \cdot E = A \cdot A^{\mathrm{ad}}\,.$$

Ist also $\det A$ Einheit in R, so hat A das Inverse $\frac{1}{\det A} A^{\mathrm{ad}} \in M_n(R)$.
a) '$\Leftarrow$': Sei A Einheit in $M_n(R)$ mit Inversem $B \in M_n(R)$. Dann gilt

$$(b_1, \ldots, b_n)B = (a_1, \ldots, a_n)AB = (a_1, \ldots, a_n)\,.$$

Da die a_i eine Basis von M bilden, existieren zu jedem $c \in M$ eindeutig bestimmte $\lambda_i \in R$ mit

$$c = (a_1, \ldots, a_n) \cdot \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} = (b_1, \ldots, b_n) \cdot B \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} =: (b_1, \ldots, b_n) \cdot \begin{pmatrix} \rho_1 \\ \vdots \\ \rho_n \end{pmatrix}$$

und diese $\rho_j \in R$ sind eindeutig, denn wegen der Eindeutigkeit der λ_i gilt

$$c = (b_1, \ldots, b_n) \cdot \begin{pmatrix} \xi_1 \\ \vdots \\ \xi_n \end{pmatrix} = (a_1, \ldots, a_n) \cdot A \begin{pmatrix} \xi_1 \\ \vdots \\ \xi_n \end{pmatrix}$$

$$\Longrightarrow \quad A\begin{pmatrix}\xi_1\\ \vdots\\ \xi_n\end{pmatrix}=\begin{pmatrix}\lambda_1\\ \vdots\\ \lambda_n\end{pmatrix} \Longrightarrow \begin{pmatrix}\xi_1\\ \vdots\\ \xi_n\end{pmatrix}=B\begin{pmatrix}\lambda_1\\ \vdots\\ \lambda_n\end{pmatrix}=\begin{pmatrix}\rho_1\\ \vdots\\ \rho_n\end{pmatrix}$$

Damit ist jedes $c \in M$ eindeutig als R-Linearkombination der b_j darstellbar, die b_j bilden eine Basis von M.
b) Sei gemäß dem Elementarteilersatz $a_1, \ldots, a_n$ eine R-Basis von M und $\alpha_1, \ldots, \alpha_m \in R$ mit $N = \alpha_1 Ra_1 \oplus \ldots \oplus \alpha_m Ra_m$. Sind alle α_i Einheiten von R, also $\alpha_i R = R$, so ist $N = Ra_1 \oplus \ldots \oplus Ra_m$ direkter Summand von M mit komplementärem Modul $N' = Ra_{m+1} \oplus \ldots \oplus Ra_n$.
Sei nun umgekehrt N direkter Summand von M, also $M = N \oplus N'$. Nach dem Elementarteilersatz sind N und N' freie Moduln, also gibt es Basen $a_1, \ldots, a_m$ von N und $a_{m+1}, \ldots, a_n$ von N', die zusammen eine Basis von M bilden. Dies bedeutet, dass $\alpha_1 = \ldots = \alpha_m = 1$ (die bis auf Assoziiertheit eindeutig bestimmten) Elementarteiler des Moduls N sind und diese also alle Einheiten sind.
c) Sei $\mathbb{Q} = N \oplus N'$ mit $\mathbb{Z}$-Untermoduln $N \neq 0 \neq N'$. Dann existieren $0 \neq x = \frac{a}{b} \in N$, $0 \neq x' = \frac{a'}{b'} \in N'$ mit $0 \neq a, b, a', b' \in \mathbb{Z}$. Da N, N' $\mathbb{Z}$-Moduln sind, folgt der Widerspruch

$$a'b \cdot x = a'a = ab' \cdot x' \in N \cap N' = \{0\}\,.$$

Aufgabe 55. (s)
Sei R ein faktorieller Ring, K sein Quotientenkörper und $f = \sum_{i=0}^{n} a_i X^i \in R[X]$. f heißt *primitiv*, falls die Koeffizienten $a_0, \ldots, a_n$ teilerfremd sind.

a) Beweisen Sie das *Lemma von Gauß*:

$$\text{Sind } f \text{ und } g = \sum_{j=0}^{m} b_j X^j \in R[X] \text{ primitiv, so auch } fg = \sum_{k=0}^{n+m} c_k X^k.$$

Tipp: Betrachten Sie für ein Primelement p von R die maximalen ν bzw. μ mit $p \nmid a_\nu$ bzw. $p \nmid b_\mu$ und studieren Sie den Koeffizienten $c_{\nu+\mu}$.

b) Jedes Polynom $0 \neq h \in K[X]$ besitzt eine Darstellung $h = \alpha \cdot g$ mit $\alpha \in K^\times$ und einem primitiven Polynom $g \in R[X]$.

c) Für $\deg f \geq 1$ gilt:

α) f unzerlegbar in $R[X] \iff f$ primitiv und irreduzibel über R.
β) f irreduzibel über $R \iff f$ irreduzibel über K.

Lösung:
a) In faktoriellen Ringen bedeutet Teilerfremdheit, dass es keinen gemeinsamen Primteiler gibt. Sei also p ein beliebiges Primelement. Da f und g primitiv sind, gibt es ein größtes ν bzw. ein größtes μ mit $p \nmid a_\nu$ bzw. $p \nmid b_\mu$. Also gilt $p \mid a_i$ für $i > \nu$ und $p \mid b_j$ für $j > \mu$. Dann gilt:

$$c_{\nu+\mu} = \sum_{i=0}^{n} a_i b_{\mu+\nu-i} = \sum_{i<\nu} a_i \underbrace{b_{\mu+\nu-i}}_{\equiv 0 \bmod p} + a_\nu b_\mu + \sum_{i>\nu} \underbrace{a_i}_{\equiv 0 \bmod p} b_{\mu+\nu-i} \equiv a_\nu b_\mu \not\equiv 0 \bmod p$$

Für jedes Primelement gibt es einen Koeffizienten von fg, der nicht von p geteilt wird, also sind die Koeffizienten von fg teilerfremd, fg ist primitiv.
b) Multipliziert man h mit dem Produkt $0 \neq \beta \in R$ der Nenner aller Koeffizienten, so erhält man ein Polynom $\beta h = g_1 \in R[X]$. Dividiert man nun g_1 durch den ggT δ seiner Koeffizienten, so erhält man $\frac{\beta}{\delta} h = \frac{1}{\delta} g_1 =: g \in R[X]$ und g ist primitiv. Also $h = \frac{\delta}{\beta} g$ mit primitivem Polynom $g \in R[X]$ und $\alpha := \frac{\delta}{\beta} \in K^\times$.

c) α) '$\Rightarrow$': Ist d der ggT der Koeffizienten von f, so besitzt f die Zerlegung $f = d \cdot g$ mit $d \in R \subset R[X]$ und $g \in R[X]$. Wegen $\deg g = \deg f \geq 1$ liegt g nicht in R, kann also keine Einheit von $R[X]$ sein (siehe Aufgabe 52 c)). Da f unzerlegbar ist, muss d Einheit sein: f ist primitiv. Genauso folgt, dass f irreduzibel ist, denn

$$f = gh \quad \text{mit } g, h \in R[X] \setminus R \underset{f \text{ unzerlegbar}}{\Longrightarrow} g \in R^\times \subset R \ \vee \ h \in R^\times \subset R\,, \text{ Wid.}$$

α) '$\Leftarrow$': Sei $f = gh$ mit $g, h \in R[X]$. Wegen der Irreduzibilität ist o. E. $g \in R$ und wegen der Primitivität dann $g \in R^\times$, womit die Unzerlegbarkeit gezeigt ist.
ad β): '$\Leftarrow$' ist eine logische Abschwächung. Sei nun f irreduzibel über R und $f = g_1 g_2$ mit $g_i \in K[X]$. Durch Multiplikation mit den Hauptnennern der g_i erhält man

$$df = h_1 h_2 \quad \text{mit } 0 \neq d \in R\,,\ h_i \in R[X]\,,\ \deg h_i = \deg g_i\,.$$

Spaltet man in h_i jeweils den ggT der Koeffizienten ab, so erhält man (siehe Aufgabenteil b))

$$df = d_1 d_2 \cdot \tilde{h}_1 \tilde{h}_2 \quad \text{mit} \quad d, d_1, d_2 \in R\,,\ \tilde{h}_1, \tilde{h}_2 \text{ primitiv}\,.$$

Nach Aufgabenteil a) ist $\tilde{h}_1 \tilde{h}_2$ primitiv und daher d ein Teiler von $d_1 d_2$. Division durch d im Integritätsbereich R ergibt

$$f = d_1' \tilde{h}_1 \cdot d_2' \tilde{h}_2 \quad \text{mit } d_1' \tilde{h}_1\,,\ d_2' \tilde{h}_2 \in R[X]\,.$$

Da f über R irreduzibel ist, folgt $0 = \deg \tilde{h}_1 = \deg g_1$ oder $0 = \deg \tilde{h}_2 = \deg g_2$, was zu zeigen war.

Aufgabe 56. $(*)$
Beweisen Sie den Satz von Gauß:

Der Polynomring $R[X]$ über einem faktoriellen Ring R ist wieder faktoriell.

Lösung:
Wir zeigen zuerst, dass unzerlegbare Elemente in $R[X]$ prim sind. Sei $f \in R[X]$ unzerlegbar. Nach Aufgabe 55 b,c) ist f primitiv und über dem Quotientenkörper K von R irreduzibel, also in $K[X]$ unzerlegbar (siehe Vorlesung, Bemerkung nach Definition II.3.5, S. 61). Da $K[X]$ faktoriell ist (Vorlesung Satz II.3.6, S. 61), ist f Primelement in $K[X]$.
Seien nun $g, h \in R[X]$ und $f \mid gh$ in $R[X]$. Da f prim in $K[X]$ ist, ist f Teiler von (o. E.) g in $K[X]$:

$$g = f \cdot h \underset{\text{Aufg.55b)}}{=} f \cdot \frac{\alpha}{\beta} \tilde{h}\,, \quad \alpha, \beta \in R\,,\ \tilde{h} \in R[X] \text{ primitiv}\,.$$

Da R faktoriell ist, sind o. E. α, β teilerfremd. Da nach Aufgabe 55 a) $f\tilde{h}$ primitiv ist, folgt aus $\beta g = \alpha f \tilde{h}$, dass β ein Teiler von α ist, also $\dfrac{\alpha}{\beta} \in R$ liegt: f teilt g in $R[X]$.
Es bleibt nun zu zeigen, dass jedes $f \in R[X]$ als Produkt von Primelementen aus $R[X]$ darstellbar ist. Da $K[X]$ faktoriell ist, existieren irreduzible Polynome aus $K[X]$

$$p_i = \frac{\alpha_i}{\beta_i} \tilde{p}_i \quad \text{mit } \alpha_i, \beta_i \in R\,,\ \tilde{p}_i \in R[X] \text{ primitiv}\,,$$

mit

$$f = \prod_i p_i \iff \prod_i \beta_i \cdot f = \prod_i \alpha_i \cdot \prod_i \tilde{p}_i\,.$$

Mit den p_i sind die $\tilde{p}_i$ irreduzibel über K und (nach Aufgabe 55 c)) unzerlegbar in $R[X]$. Wieder nach Aufgabe 55 a) ist das Produkt $\prod_i \tilde{p}_i$ primitiv und folglich $b := \prod_i \beta_i$ ein Teiler von $a := \prod_i \alpha_i$. Damit erhalten wir schließlich

$$f = \frac{a}{b} \cdot \prod_i \tilde{p}_i \quad \text{mit } d := \frac{a}{b} \in R\,.$$

Da R faktoriell ist, ist d Produkt von unzerlegbaren Elementen aus R; diese sind auch in $R[X]$ unzerlegbar (aus Gradgründen) und damit haben wir insgesamt

$$f = \prod_j q_j \cdot \prod_i \tilde{p}_i$$

mit in $R[X]$ unzerlegbaren Elementen $q_j \in R\,, \tilde{p}_i \in R[X]$.

Aufgabe 57. (s)

a) Für einen kommutativen unitären Ring R, $u \in R^\times$, $a \in R$ und $f \in R[X]$ gilt:

$$f \text{ irreduzibel über } R \iff f(uX+a) \text{ irreduzibel über } R\,.$$

b) Sei $f = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$ und für eine Primzahl p $\bar{f} := \sum_{i=0}^{n} \bar{a}_i X^i \in \mathbb{F}_p[X]$ das Restklassenpolynom modulo p. Ist p kein Teiler von a_n, so gilt:

$$\bar{f} \text{ irreduzibel} \implies f \text{ irreduzibel}\,.$$

Gilt hier auch die Umkehrung?

c) Formulieren und beweisen Sie für ein Polynom $f \in K[X]$ vom Grade 3 über einem Körper K ein notwendiges und hinreichendes Kriterium für Irreduzibilität.

Lösung:
a) '$\Leftarrow$': Agenommen, f ist reduzibel, also existieren $g, h \in R[X]$ mit $f = gh$ und $\deg g \geq 1, \deg h \geq 1$. Dann folgt $f(uX+a) = g(uX+a)h(uX+a)$ und es ist $\deg g(uX+a) = \deg g \geq 1$, $\deg h(uX+a) = \deg h \geq 1$. Also wäre $f(uX+a)$ reduzibel.
Für die umgekehrte Richtung '$\Rightarrow$' wendet man den bewiesenen Teil auf $\tilde{f} := f(uX+a)$ und $f = \tilde{f}(u^{-1}(X-a)) = \tilde{f}(u^{-1}X - u^{-1}a)$ an und erhält so: $\tilde{f}$ reduzibel $\implies$ f reduzibel.
b) Wegen $p \nmid a_n$ ist $\bar{a}_n \neq \bar{0}$ und daher $\deg \bar{f} = n$. Annahme $f = gh$ mit $\deg g, \deg h \geq 1$, also $\deg g, \deg h < n$. Dann folgt $\bar{f} = \bar{g} \cdot \bar{h}$ mit $\deg \bar{g} \leq \deg g < n$, $\deg \bar{h} \leq \deg h < n$. Damit ist $\bar{f}$ reduzibel, Wid.
Die Umkehrung gilt nicht: $f = X^2 + 3 \in \mathbb{Z}[X]$ ist irreduzibel, denn es gibt keine Nullstelle in $\mathbb{Z}$, also auch keine Aufspaltung in zwei lineare Faktoren. Aber modulo $p = 3$ ist $\bar{f} = X^2$ reduzibel.
c) Sei $f \in K[X]$ vom Grade 3. Dann gilt:

$$f \text{ ist irreduzibel} \iff f \text{ hat eine Nullstelle in } K\,.$$

Begründung: Hat f eine Nullstelle, so hat f einen Linearfaktor (Vorlesung Bemerkung II.3.7, S. 62) und ist reduzibel. Umgekehrt, ist $f = gh$ reduzibel, so hat (o. E.) g den Grad 1, h den Grad 2. Dann hat aber g und damit f eine Nullstelle in K.

Algebra
Übung 11

Aufgabe 58. (m)

a) Beweisen Sie das *Irreduzibilitätskriterium von Eisenstein*:

Sei R ein faktorieller Ring und $f = a_n X^n + \ldots + a_0 \in R[X]$ vom Grade $n \geq 1$. Es gebe ein Primelement p von R mit

$$(1) \quad p \nmid a_n\,, \qquad (2) \quad \bigwedge_{i=0}^{n-1} p \mid a_i\,, \qquad (3) \quad p^2 \nmid a_0\,.$$

Dann ist f irreduzibel über dem Quotientenkörper K von R.

Tipp: Beachte Aufgabe 55 c) und leite für $f = gh$ mit $g, h \in R[X]$ aus (2) und (3) den Widerspruch $p \mid a_n$ her.

b) Man zeige, dass folgende Polynome irreduzibel über $\mathbb{Q}$ sind:

$\alpha)$ $X^n - p_1 \cdot \ldots \cdot p_r$ mit $n \geq 2$ und $p_1, \ldots, p_r$ verschiedene Primzahlen.
$\beta)$ $\frac{2}{9}X^6 - 15X^5 + \frac{7}{3}X^4 - 52X^3 + 18X^2 - X + \frac{4}{3}$.
$\gamma)$ $X^4 - 4X + 2$.

c) Man beweise die Irreduzibilität der folgenden Polynome über $\mathbb{Q}$:

$\alpha)$ $X^3 - 4$ $\quad$ $\beta)$ $X^6 + X^3 + 1$ $\quad$ $\gamma)$ $X^5 - 5x + 1$.

Tipp: Beachte Aufgabe 57 a).

Lösung:
a) Sei $f = gh$ mit $g = \sum_{j=1}^{m} b_j X^j\,,\ h = \sum_{k=1}^{l} c_k X^k \in R[X]$, $\deg g, \deg h < \deg f = n$. Dann gilt für alle i $a_i = \sum_{j+k=i} b_j c_k$. Insbesondere $p^2 \nmid a_0 = b_0 c_0$, also (o. E.) $p \nmid b_0$. Aber wegen $p \mid a_0$ muss dann $p \mid c_0$ gelten. Wir zeigen nun induktiv $p \mid c_i$. Nach Induktionsvoraussetzung und (2) gilt für $i < n$

$$p \mid a_i - \sum_{\substack{j+k=i \\ k<i}} b_j c_k = b_0 c_i$$

und wegen $p \nmid b_0$ muss $p \mid c_i$ für $i < n$ gelten. Wegen $\deg h < n$ ist damit p ein Teiler von h und damit auch von f, im Widerspruch zu (1).
b) $\alpha)$ Das Polynom ist ein Eisenstein-Polynom für (jede der Primzahlen) p_i, also irreduzibel.
$\beta)$ Ist f das gegebene Polynom, so ist $9f = 2X^6 - 3^3 \cdot 5X^5 + 3 \cdot 7X^4 - 2^2 \cdot 3^2 \cdot 13X^3 - 9X + 12$ ein Eisenstein-Polynom für $p = 3$ und damit irreduzibel. Dann ist auch f über $\mathbb{Q}$ irreduzibel.
$\gamma)$ Dieses Polynom ist eisensteinsch für $p = 2$.
c) $\alpha)$ Sei $f = X^3 - 4$, dann ist $f(X+1) = (X+1)^3 - 4 = X^3 + 3X^2 + 3X - 3$ 3-eisensteinsch und damit irreduzibel. Gemäß Aufgabe 57 a) ist dann auch f irreduzibel.
$\beta)$ Sei f das gegebene Polynom. Dann ist $f(X+1) = X^6 + 6X^5 + 15X^4 + 21X^3 + 18X^2 + 9X + 3$ 3-eisensteinsch und damit (s.o.) f irreduzibel über $\mathbb{Q}$.
$\gamma)$ Es ist $f(X-1) = (X-1)^5 - 5(X-1) + 1 = X^5 - 5X^4 - 10X^3 - 10X^2 - 5$ 5-eisensteinsch.

Aufgabe 59. (m)
Sei p eine Primzahl. Zeigen Sie:

a) Die Binomialkoeffizienten $\binom{p}{i}$ sind für $0 < i < p$ durch p teilbar.

b) Ist k ein Körper der Charakteristik p, so gilt

$$(a+b)^p = a^p + b^p \quad \text{für alle } a, b \in k\,.$$

c) Für jedes Polynom $f \in \mathbb{F}_p[X]$ gilt $f(X^p) = (f(X))^p$.
[Beachten Sie den Kleinen Satz von Fermat (Aufgabe 47 a)).]

Lösung:
a) Für $i \geq 1$ gilt

$$p \mid \prod_{k=0}^{i}(p-k) = i! \cdot \binom{p}{i}\,.$$

Da p Primzahl und $\binom{p}{i} \in \mathbb{Z}$ ist, muss p ein Teiler von $i!$ oder $\binom{p}{i}$ sein. Für $i < p$ gilt $p \nmid i!$, also folgt die Behauptung.
b) Wegen $\operatorname{char} k = p$ gilt $p.1_k = 0$ und daher $p.c = 0$ für alle $c \in k$. Also folgt

$$(a+b)^p = a^p + b^p + \sum_{i=1}^{p-1}\binom{p}{i}a^i b^{p-i} \underset{\text{a)}}{=} a^p + b^p\,.$$

c) Nach dem kleinen Satz von Fermat (Aufgabe 47 a)) gilt $a^{p-1} = 1$ für alle $0 \neq a \in \mathbb{F}_p$, also $a^p = a$. Letzteres gilt natürlich auch für $a = 0$. Also

$$(f(X))^p = (\sum_{i=0}^{n} a_i X^i)^p \underset{\text{b)}}{=} \sum_{i=0}^{n} a_i^p X^{pi} = \sum_{i=0}^{n} a_i X^{pi} = f(X^p)\,.$$

Aufgabe 60. (s)

a) Es sei $k = \mathbb{Q}(X)$ der rationale Funktionenkörper in einer Unbestimmten X über $\mathbb{Q}$ und $k[T]$ der Polynomring über k in einer Unbestimmten T. Zeigen Sie, dass folgende Polynome aus $k[T]$ irreduzibel über k sind:

$\alpha)$ $f(T) = T^p + (X^p - 1)$ für eine Primzahl p.

$\beta)$ $f(T) = T^2 - (4X^3 - 27)$

b) Zeigen Sie, dass $f(X) = X^5 - 60X^3 - 120X^2 + 360X + 576 \in \mathbb{Z}[X]$ irreduzibel über $\mathbb{Q}$ ist.

Lösung:
a) $R = \mathbb{Q}[X]$ ist ein Hauptidealring, insbesondere faktoriell. Wir verwenden das Eisensteinkriterium für Polynome über R. Das gegebene Polynom $f(T)$ ist normiert, hat alle Koeffizienten gleich 0 außer dem absoluten Glied $a_0 = X^p - 1 \in R$.
$X^p - 1 \in R = \mathbb{Q}[X]$ hat die Nullstelle 1, also den Linearfaktor $q(X) := X - 1$. Es gilt

$$a_0(X) = X^p - 1 = (X-1) \cdot \sum_{i=0}^{p-1} X^i =: q(X) \cdot g(X) \quad \text{mit } g(1) = p \neq 0\,.$$

Damit gilt für das Primpolynom $q = X - 1 \in R$

$$q \mid a_0 \quad \text{und} \quad q \nmid g\,, \quad \text{also } q^2 \nmid a_0\,.$$

Damit ist $f(T) \in R[T]$ ein Eisensteinpolynom für das Primelement $q = X - 1 \in R$ und daher irreduzibel über $\mathrm{Quot}(R) = \mathbb{Q}(X)$.
Man beachte, dass diese Argumentation allgemein für Polynome $T^m + X^n - 1$ gilt. Die Aufgabenstellung mit $m = n = p$ Primzahl, zielte wahrscheinlich auf folgenden Lösungsweg ab: ???
β) Da das kubische Polynom $q(X) := 4X^3 - 27$ keine Nullstelle (in $\mathbb{Q}$) besitzt, ist q irreduzibel über $\mathbb{Q}$, also Primelement in $R = \mathbb{Q}[X]$. Damit ist $f(T) = T^2 - (4X^3 - 27) \in R[T]$ ein Eisensteinpolynom für das Primelement $q(X)$ über dem faktoriellen Ring $R = \mathbb{Q}[X]$.
b) Wieder verwenden wir Aufgabe 57 a) und berechnen

$$f(X-1) = X^5 - 5X^4 - 50X^3 + 50X^2 + 425X + 155\,.$$

$f(X-1)$ ist ein Eisensteinpolynom für die Primzahl $p = 5$ und daher irreduzibel, also ist auch $f(X)$ irreduzibel über $\mathbb{Q}$.
Hier ein paar Anmerkungen zu diesem Ansatz. Ausprobieren ist eine Möglichkeit, eine andere sind die folgenden Überlegungen. Wir bemerken zunächst, dass f "fast" ein Eisensteinpolynom für $p = 5$ ist, nur das absolute Glied 576 ist nicht durch 5 teilbar. Wir suchen nun eine Substitution $X + a$, so dass $f(X + a)$ eisensteinsch wird. f und damit auch $f(X + a)$ ist normiert; alle weiteren Koeffizienten von X^k $(k \geq 1)$ in f sind durch 5 teilbar, dann gilt dies auch für $f(X + a)$, denn:

$$f(X) \equiv X^5 + a_0 \bmod 5 \implies f(X+a) \equiv (X+a)^5 + a_0 \underset{\text{Aufg.59c}}{\equiv} X^5 + a + a_0 \bmod 5$$

Man muss also a zunächst so wählen, dass $a + a_0 \equiv 0 \bmod 5$ ist, also $a \equiv -576 \equiv -1 \bmod 5$. Dann muss man aber noch das absolute Glied von $f(X+a)$ in $\mathbb{Z}$ berechnen, um zu sichern, dass es nicht von 5^2 geteilt wird. Das absolute Glied von $f(X + a)$ erhält man durch Einsetzen von 0 für X, also durch Berechnung von $f(a)$. Wir suchen also ein $a \equiv -1 \bmod 5$ mit $5^2 \nmid f(a)$. Da wird man schnell fündig: $f(-1) = 155$.

Aufgabe 61. (s)
m und n seien verschiedene *quadratfreie* ganze Zahlen $\neq 0$, das heißt m und n seien nicht durch Quadrate ganzer Zahlen > 1 teilbar. Es seien $k_1 := \mathbb{Q}(\sqrt{m})$ und $k_2 := \mathbb{Q}(\sqrt{n})$.

a) Zeigen Sie $k_1 \neq k_2$.

b) Welchen Grad haben die Körper k_1, k_2, k_1k_2 und $K := \mathbb{Q}(\sqrt{m} + \sqrt{n})$ über $\mathbb{Q}$?

c) Bestimmen Sie für $m, n > 0$ das Minimalpolynom von $\sqrt{\sqrt{m} + \sqrt{n}}$ über $\mathbb{Q}$.

Lösung:
a) $\sqrt{m}$ ist Nullstelle des quadratischen Polynoms $X^2 - m \in \mathbb{Q}[X]$, also algebraisch über $\mathbb{Q}$ und $\mathbb{Q}(\sqrt{m}) = \mathbb{Q}[\sqrt{m}]$ hat höchstens den Grad 2 über $\mathbb{Q}$. Der Grad 1 kann nur für $m = 0$ oder $m = 1$ auftreten, denn für $m \neq 0$ gilt:

$$\sqrt{m} \in \mathbb{Q} \iff m = \frac{x^2}{y^2} \iff y^2 \cdot m = x^2 \quad \text{mit teilerfremden } x, y \in \mathbb{Z}\,.$$

Da m quadratfrei ist, kann x keinen Primteiler p haben, also muss $x^2 = 1$ und dann auch $y^2 = m = 1$ sein.

Seien also im Folgenden $m, n \neq 0, \neq 1$ und daher $\sqrt{m}, \sqrt{n} \notin \mathbb{Q}$, k_1, k_2 quadratische Erweiterungen von $\mathbb{Q}$. Dann gilt

$$k_1 = k_2 \implies \sqrt{m} \in \mathbb{Q}(\sqrt{n}) = \mathbb{Q}[\sqrt{n}] \implies \bigvee_{r,s\in\mathbb{Q}} \sqrt{m} = r + s\sqrt{n} \implies \bigvee_{r,s\in\mathbb{Q}} m - r^2 - ns^2 = 2rs\sqrt{n}\,.$$

Wegen $\sqrt{n} \notin \mathbb{Q}$ folgt dann $r = 0$ oder $s = 0$. $s = 0$ würde bedeuten $\sqrt{m} = r \in \mathbb{Q}$, Widerspruch. Also muss $r = 0$ sein und wegen der Quadratfreiheit von m und n ergibt sich dann

$$\sqrt{m} = s\sqrt{n} \implies m = s^2 \cdot n \implies \frac{m}{n} = s^2 = 1 \implies m = n\,.$$

b) Im Falle $m = 1$ ist $k_1 = \mathbb{Q}$ und $(k_2 : \mathbb{Q}) = 2$, also $k_1k_2 = k_2$ quadratisch über $\mathbb{Q}$. Entsprechendes gilt für $n = 1$.
Seien nun $m, n \neq 1$, also sind nach a) k_1, k_2 zwei verschiedene quadratische Erweiterungen von $\mathbb{Q}$, also auch nicht ineinander enthalten, so dass k_1k_2 eine echte Erweiterung von k_1 ist:

$$1 < (k_1k_2 : k_1) = (k_1(\sqrt{n}) : k_1) \leq 2\,, \text{ also } (k_1k_2 : k_1) = 2\,.$$

Im Falle $m, n \neq 1$ ist also $(k_1k_2 : \mathbb{Q}) = 4$. Daher ist das $\mathbb{Q}$-Erzeugendensystem $1, \sqrt{m}, \sqrt{n}, \sqrt{mn}$ von $k_1k_2 = \mathbb{Q}[\sqrt{m}, \sqrt{n}]$ eine Basis von $k_1k_2|\mathbb{Q}$.

Wir untersuchen nun $K = \mathbb{Q}(\sqrt{m} + \sqrt{n})$. Offenbar ist $K \subset k_1k_2$ und wegen $(\sqrt{m} + \sqrt{n})^2 = m + n + 2\sqrt{mn}$ ist $\mathbb{Q}(\sqrt{mn}) \subset K$. Also $K = k_1k_2$ oder $K = \mathbb{Q}[\sqrt{mn}]$. Im zweiten Falle wäre $\sqrt{m} + \sqrt{n} = a + b\sqrt{mn}$ für geeignete $a, b \in \mathbb{Q}$, im Widerspruch zur oben gezeigten linearen Unabhängigkeit von $1, \sqrt{m}, \sqrt{n}, \sqrt{mn}$. Also folgt $K = k_1k_2$ hat den Grad 4.

c) Sei nun $\alpha := \sqrt{\sqrt{m} + \sqrt{n}}$ und $L = \mathbb{Q}(\alpha)$. Wegen $\alpha^2 = \sqrt{m} + \sqrt{n}$ ist $K \subset L$ und $(L : K) \leq 2$, also $K = L$ oder $(L : \mathbb{Q}) = 8$. Nun gilt

$$\begin{aligned}
L = K \quad &\iff \quad \alpha \in K \iff \sqrt{m} + \sqrt{n} \text{ Quadrat in } K = k_1k_2 \\
&\iff \quad \sqrt{m} + \sqrt{n} = (a + b\sqrt{m} + c\sqrt{n} + d\sqrt{mn})^2 \quad (a, b, c, d \in \mathbb{Q}) \\
&\iff \quad \sqrt{m} + \sqrt{n} = (a^2 + mb^2 + nc^2 + mnd^2) + \ldots \\
&\qquad\qquad \ldots + 2(ab + cdn)\sqrt{m} + 2(ac + bdm)\sqrt{n} + 2(ad + bc)\sqrt{mn} \\
&\iff \quad \begin{cases} a^2 + mb^2 + nc^2 + mnd^2 = 0 \\ 2(ab + cdn) = 1 \\ 2(ac + bdm) = 1 \\ 2(ad + bc) = 0 \end{cases}
\end{aligned}$$

Für $m, n > 0$ ist die erste Bedingung nur für $a = b = c = d = 0$ erfüllt, die zweite dann jedoch nicht. Also ist $\alpha \notin k_1k_2$, $(L : \mathbb{Q}) = 8$.

Wir bestimmen nun das Minimalpolynom von α: Es ist $\alpha^2 = \sqrt{m} + \sqrt{n}$, also $\alpha^4 = m + n + 2\sqrt{mn}$ und damit $(\alpha^4 - m - n)^2 = 4mn$. Damit ist α Wurzel des normierten rationalen Polynoms $f = X^8 - 2(m + n)X^4 + (m - n)^2$, das dann wegen $\deg f = (\mathbb{Q}(\alpha) : \mathbb{Q})$ das Minimalpolynom von α über $\mathbb{Q}$ ist.

Anmerkung zu c): Ohne die zusätzliche Voraussetzung $m, n > 0$ kann $\sqrt{m} + \sqrt{n}$ ein Quadrat in $\mathbb{Q}(\sqrt{m}, \sqrt{n})$ sein. ein Gegenbeispiel ist $m = 3$, $n = -1$:

$$\alpha := \frac{1}{2}(1 + \sqrt{3} - \sqrt{-1} + \sqrt{-3}) \in \mathbb{Q}(\sqrt{3}, \sqrt{-1}) \quad \text{und} \quad \alpha^2 = \sqrt{3} + \sqrt{-1}$$

Es ist offen, ob evtl. der Ausschluss von $n = -1$, d. h. die zusätzliche Voraussetzung $|m|, |n| > 1$, hinreichend wäre für die Behauptung von c). Oder ist dies gar das einzige Gegenbeispiel?

Aufgabe 62. (s)
Es sei $\varphi : k \xrightarrow{\sim} k_1$ ein Isomorphismus von Körpern und $p(X) = \sum_{i=0}^{n} a_iX^i \in k[X]$ ein Primpolynom über k.

a) Man zeige, dass dann $\varphi(p) := \sum_{i=0}^{n} \varphi(a_i)X^i$ ein Primpolynom über k_1 ist.

b) α bzw. α_1 sei Wurzel von p bzw. $p_1 := \varphi(p)$ in einem Erweiterungskörper $K|k$ bzw. $K_1|k_1$. Man beweise, dass es genau einen Isomorphismus $\varphi_1 : k(\alpha) \xrightarrow{\sim} k_1(\alpha_1)$ gibt mit $\varphi_1|_k = \varphi$ und $\varphi_1(\alpha) = \alpha_1$.

c) Sei $\alpha = \sqrt[4]{2}$ und $K := \mathbb{Q}(i, \alpha)$ ($\subset \mathbb{C}$). Man zeige, dass es genau einen $\mathbb{Q}(i)$-Monomorphismus $\sigma : K \to K$ mit $\sigma(\alpha) = i\alpha$ und genau einen $\mathbb{Q}(\alpha)$-Monomorphismus $\tau : K \to K$ mit $\tau(i) = -i$ gibt. Für σ und τ beweise man die Relationen $\sigma^4 = \mathrm{id}_K$, $\tau^2 = \mathrm{id}_K$ und $\sigma \circ \tau = \tau \circ \sigma^{-1}$.

Lösung:
a) ist klar, denn wäre $\varphi(p) = g \cdot h$ eine Zerlegung in Polynome $g, h \in k_1[X]$ kleineren Grades, so wäre $p = \varphi^{-1}(g) \cdot \varphi^{-1}(h)$ über k zerlegbar und nicht irreduzibel.

b) Wegen der Irreduzibilität von p und p_1 hat man gemäß Vorlesung, III Satz (1.9) a) (S. 67) die Isomorphismen

$$k[\alpha] \xrightarrow{\sim} k[X]/\langle p\rangle \xrightarrow[\bar{\varphi}]{\sim} k_1[X]/\langle p_1\rangle \xrightarrow{\sim} k_1[\alpha_1]\,.$$

Dabei gilt $\alpha \mapsto X + \langle p\rangle \mapsto X + \langle p_1\rangle \mapsto \alpha_1$ und $k \ni \xi \mapsto \xi + \langle p\rangle \mapsto \varphi(\xi) + \langle p_1\rangle \mapsto \varphi(\xi) \in k_1$.
Der so gefundene Isomorphismus φ_1 hat also die gewünschten Eigenschaften $\varphi_1|_k = \varphi$ und $\varphi_1(\alpha) = \alpha_1$. Da $k[\alpha]$ von k und α erzeugt wird, ist φ_1 durch diese Eigenschaften eindeutig bestimmt.

c) $L = \mathbb{Q}(\alpha)$ hat den Grad 4 über $\mathbb{Q}$, da $X^4 - 2$ irreduzibel ist (2-Eisensteinsch), und es gilt $i \notin L \subset \mathbb{R}$. Also ist $X^2 + 1$ das Minimalpolynom von i auch über L und nach Aufgabenteil b) (angewendet auf $\varphi = \mathrm{id}_L$ und die beiden Wurzeln $\pm i$ von $X^2 + 1$) existiert ein Automorphismus $\sigma : K \to K$ mit $\sigma|_L = \mathrm{id}_L$ und $\sigma(i) = -i$.

Da $K = L(i)$ über $\mathbb{Q}$ den Grad 8 hat, muss K über $k := \mathbb{Q}(i)$ den Grad 4 haben. Wegen $(k(\alpha) : k) = 4$ ist daher $X^4 - 2$ auch das Minimalpolynom von α über k. Dieses ist also irreduzibel und angewendet auf dessen beide Wurzeln α und $i\alpha$ erhalten wir nach b) die Existenz von $\sigma : K \xrightarrow{\sim} K$ mit den geforderten Eigenschaften.

Nun zu den behaupteten Relationen: $\mathbb{Q}$-Automorphismen von $K = \mathbb{Q}(i, \alpha)$ sind durch ihre Werte auf α und i eindeutig bestimmt. Wir berechnen $\tau^2(i) = \tau(-i) = i$ und $\tau^2(\alpha) = \alpha$, also $\tau^2 = \mathrm{id}_K$. Ebenso erhalten wir $\sigma^4(i) = i$ und $\sigma^4(\alpha) = \sigma^3(i\alpha) = i\sigma^3(\alpha) = i^2\sigma^2(\alpha) = i^3\sigma(\alpha) = i^4\alpha = \alpha$, also $\sigma^4 = \mathrm{id}_K$.
Schließlich gilt $\sigma\circ\tau\circ\sigma(i) = \sigma(\tau(i)) = -\sigma(i) = -i = \tau(i)$ und $\sigma\circ\tau\circ\sigma(\alpha) = \sigma(\tau(i\alpha)) = -\sigma(i\alpha) = -i\sigma(\alpha) = -i^2\alpha = \alpha = \tau(\alpha)$, mithin $\sigma \circ \tau \circ \sigma = \tau$, oder anders formuliert $\sigma \circ \tau = \tau \circ \sigma^{-1}$.

Aufgabe 63. (s)
Es sei $k(X)$ der rationale Funktionenkörper in einer Unbestimmten X über einem Körper k und $\varphi = \frac{f}{g} \in k(X) \setminus k$ mit $f, g \in k[X]$.
Zeigen Sie:

a) X ist algebraisch über $k(\varphi)$ und φ ist transzendent über k.

b) Sind $f, g \in k[X]$ teilerfremd, so gilt für den Körpergrad

$$(k(X) : k(\varphi)) = \max(\deg f, \deg g)\,.$$

c) Es ist $k(\varphi) = k(X)$ genau dann, wenn $a, b, c, d \in k$ existieren mit $ad - bd \neq 0$ und $\varphi = \frac{aX+b}{cX+d}$.

Lösung:
Da die Aussagen a) und c) keinen Bezug auf f, g nehmen, kann man den Quotienten $\varphi = \frac{f}{g}$ kürzen ($k[X]$ ist faktoriell) und f, g stets als teilerfremd voraussetzen.

a) Zur Algebraizität von X über $k(\varphi)$: Es ist $g\varphi = f$, also $f(X) - g(X)\varphi = 0 \in k(X)$. Damit ist X Wurzel des Polynoms $F(Z) := f(Z) - \varphi g(Z) \in k(\varphi)[Z]$. Wäre $F(Z)$ das Nullpolynom, so folgte

$$0 = \sum_i a_i Z^i - \varphi \sum_i b_i Z^i = \sum_i (a_i - \varphi b_i) Z^i \iff \bigwedge_i a_i = \varphi b_i\,.$$

Da mindestens ein $b_l \neq 0$ ist ($g \neq 0$), wäre $\varphi = \dfrac{a_l}{b_l} \in k$, Wid. Also ist X Wurzel eines Polynoms $0 \neq F(Z) \in k(\varphi)[Z]$ und somit algebraisch über dem Körper $k(\varphi)$.

Zur Transzendenz von φ über k:
1. Beweis nach Definition: Annahme: φ ist algebraisch über k. Dann existiert ein Polynom $F(Z) = \sum_{i=0}^{n} a_i Z^i \in k[Z]$, $a_n \neq 0$, mit

$$0 = F(\varphi) = \sum_{i=0}^{n} a_i \frac{f^i}{g^i} \iff 0 = \sum_{i=0}^{n} a_i f^i g^{n-i} \iff f^n = -a_n^{-1} \sum_{i=0}^{n-1} a_i f^i g^{n-i} \implies g \mid f^n \,.$$

Da f, g teilerfremd sind, kann g keinen Primteiler haben, muss also konstant sein: $g \in k$ und damit $f^n = \sum_{i=0}^{n-1} b_i f^i$ mit $b_i \in k$. Dies ist aber für $\deg f \geq 1$ nicht möglich, also ist auch f konstant, im Widerspruch zu $\varphi = \frac{f}{g} \notin k$.
2. Beweis bei Kenntnis der Transitivität der Algebraizität (Korollar III.1.14, S. 70):
Angenommen φ wäre algebraisch über k. Da wie gezeigt X algebraisch über $k(\varphi)$ ist, wäre dann aufgrund der Transitivität der Algebraizität X auch algebraisch über k, aber X ist die Unbestimmte des Polynomringes $k[X]$ und damit (gemäß Definition des Polynomringes) transzendent über k, siehe Beispiele III.1.6 c), S. 66.

b) Es sei $L := k(\varphi) \subset k(X)$. Da φ transzendent über k ist, gilt $k[\varphi]$ ist (isomorph zum) Polynomring $k[T]$ über k in einer Unbestimmten $T := \varphi$ (siehe Vorlesung, Beispiele III.1.6 e), S. 66). Das Polynom $F(Z) = f(Z) - Tg(Z) \in k[T, Z] \subset L[Z]$ hat den Z-Grad $\max(\deg f, \deg g)$; denn selbst bei $\deg f = \deg g =: n$ kann der führende Term von $f(Z) - Tg(Z)$ nicht 0 sein: $a_n - \varphi b_n = 0 \implies T = \frac{a_n}{b_n} \in k$, Wid. Damit ist $(L(X) : L) \leq \deg(F(Z)) = \max(\deg f, \deg g)$.

In dieser Abschätzung gilt die behauptete Gleichheit genau dann, wenn $F(Z) \in L[Z]$ irreduzibel über L und damit das Minimalpolynom von X über $L = k(T)$ ist. Da T transzendent über k ist, ist $R = k[T]$ Hauptidealring, insbesondere faktoriell, und daher genügt es (siehe Aufgabe 55 c) zu zeigen, dass $F = f(Z) - Tg(Z)$ im Polynomring $k[T, Z]$ nicht zerlegbar ist. Angenommen es gibt $H, G \in k[T, Z]$ mit

$$f(Z) - Tg(Z) = H(T, Z)G(T, Z) \implies 1 = \deg_T H + \deg_T G \underset{\text{o.E.}}{\Longrightarrow} \deg_T H = 0 \,.$$

Dann ist aber $H(T, Z) =: H(Z) \in k[Z]$ ein gemeinsamer Teiler von $f(Z), g(Z)$ und muss wegen deren Teilerfremdheit eine Einheit sein, mithin folgt: $f(Z) - Tg(Z)$ ist unzerlegbar in $k[T, Z]$.

c) Sei $k(X) = k(\frac{f}{g})$ und o. E. $f, g \in k[X]$ teilerfremd. Dann gilt nach b):

$$k(X) = k(\frac{f}{g}) \iff 1 = \max(\deg f, \deg g) \implies f = aX + b \,,\ g = cX + d \,.$$

Für die linearen Polynome f, g bedeutet die Teilerfremdheit, dass f, g sich nicht gegenseitig teilen, also keine Vielfachen voneinander sind. Damit sind $(a, b), (c, d) \in k^2$ linear unabhängig und $\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} \neq 0$.

Genauso folgt aus b) die umgekehrte Richtung in c).

Algebra
Übung 12

Aufgabe 64. (m)

a) Man beweise den Fortsetzungssatz für endliche Erweiterungen konstruktiv ohne Verwendung des Zornschen Lemmas.

b) Es sei $K = \mathbb{Q}(\sqrt{13}, \sqrt{17})$. Mit Hilfe von Aufgabe 62 konstruiere man $\mathbb{Q}$-Automorphismen σ, τ von K mit

$$\sigma\sqrt{13} = -\sqrt{13}\,,\ \sigma\sqrt{17} = \sqrt{17}\,, \qquad \tau\sqrt{13} = \sqrt{13}\,,\ \tau\sqrt{17} = -\sqrt{17}$$

und beweise die Relation $\sigma^2 = \tau^2 = \mathrm{id}_K$ und $\sigma\tau = \tau\sigma$.

Lösung:
a) Sei $K|k$ eine endlich algebraische Erweiterung und $\varphi : k \to L$ ein Monomorphismus von k in einen algebraisch abgeschlossenen Körper L. Als endliche Erweiterung ist $K|k$ endlich erzeugt: $K = k(a_1, \ldots, a_r)$ mit a_i algebraisch über k. Wir setzen für $0 \le i \le r$ $K_i := k(a_1, \ldots, a_i)$ und konstruieren induktiv Monomorphismen $\varphi_i : K_i \to L$ $(0 \le i \le r)$ mit $\varphi_i\,|_{K_{i-1}} = \varphi_{i-1}$ für $i \ge 1$.

Der Induktionsanfang $i = 0$ ist klar: $\varphi_0 := \varphi$. Sei nun $i \ge 1$ und φ_j konstruiert für $0 \le j < i$. Es ist $K_i = K_{i-1}(a_i)$ Stammkörper des (irreduziblen) Minimalpolynoms $p := f_{a_i,K_{i-1}}$ von a_i über K_{i-1}. Dann ist $p_1 := \varphi_{i-1}(p)$ Primpolynom über $L_{i-1} := \varphi_{i-1}(K_{i-1}) \subset L$ und besitzt im algebraisch abgeschlossenen Körper L eine Wurzel b_i. Gemäß Übung 11, Aufgabe 62 b) gibt es dann einen Isomorphismus $\varphi_i : K_{i-1}(a_i) \xrightarrow{\sim} L_{i-1}(b_i) \subset L$ mit $\varphi_i\,|_{K_{i-1}} = \varphi_{i-1}$. Damit ist die Induktion vollständig und $\varphi_r : K_r \to L$ ist die gesuchte Fortsetzung von $\varphi = \varphi_0$ auf $K = K_r$.

b) Sei $k_1 = \mathbb{Q}(\sqrt{13})$, $k_2 = \mathbb{Q}(\sqrt{17})$, also $K = k_1k_2 = k_2(\sqrt{13}) = k_1(\sqrt{17})$. Nach Aufgabe 61 haben wir folgende Körpergrade:

$$(K : \mathbb{Q}) = 4\,,\ (k_2(\sqrt{13}) : k_2) = 2 = (k_1(\sqrt{17}) : k_1)\,,$$

und daher sind $X^2 - 13$ bzw. $X^2 - 17$ die Minimalpolynome von $\sqrt{13}$ bzw. $\sqrt{17}$ (nicht nur über $\mathbb{Q}$, sondern auch) über k_2 bzw. k_1. Also gibt es einen Isomorphismus $\sigma : K = k_2(\sqrt{13}) \xrightarrow{\sim} k_2(-\sqrt{13}) = K$ mit $\sigma(\sqrt{13}) = -\sqrt{13}$ und $\sigma\,|_{k_2} = \mathrm{id}_{k_2}$, also $\sigma(\sqrt{17}) = \sqrt{17}$. Genauso folgt die Existenz von τ mit den geforderten Eigenschaften.

K wird von $\sqrt{13}$ und $\sqrt{17}$ erzeugt, also sind alle Automorphismen durch ihre Werte auf diesen beiden Wurzeln eindeutig bestimmt. Wir berechnen

$$\sigma^2(\sqrt{13}) = \sigma(-\sqrt{13}) = \sqrt{13}\,, \quad \sigma^2(\sqrt{17}) = \sqrt{17}\,, \qquad \text{also } \sigma^2 = \mathrm{id}_K$$

Genauso ergibt sich $\tau^2 = \mathrm{id}_K$ und schließlich $\sigma \circ \tau = \tau \circ \sigma$:

$$\begin{aligned} \sigma \circ \tau(\sqrt{13}) &= \sigma(\sqrt{13}) = -\sqrt{13} & \qquad \sigma \circ \tau(\sqrt{17}) &= \sigma(-\sqrt{17}) = -\sqrt{17} \\ \tau \circ \sigma(\sqrt{13}) &= \tau(-\sqrt{13}) = -\sqrt{13} & \qquad \tau \circ \sigma(\sqrt{17}) &= \tau(\sqrt{17}) = -\sqrt{17} \end{aligned}$$

Aufgabe 65. (m)
Sei k ein Körper, f ein nicht-konstantes Polynom aus $k[X]$. Man zeige, dass es eine endliche Erweiterung $K|k$ gibt, über der f in Linearfaktoren zerfällt.

Lösung:
Siehe dazu Vorlesung, Kor. III.1.11 (S. 69). Ein Zerfällungkörper $K = k(\alpha_1, \ldots, \alpha_n)$ ist endlich über k, da endlich erzeugt von algebraischen α_i.

Aufgabe 66. (s)

a) k sei ein Körper, $K = k(X)$ der rationale Funktionenkörper in einer Unbestimmten über k. Man zeige, dass k algebraisch abgeschlossen in K ist.

b) Es sei $\bar{\mathbb{Q}}$ der algebraische Abschluss von $\mathbb{Q}$ in $\mathbb{C}$. Man zeige, dass $\bar{\mathbb{Q}}$ eine unendliche algebraische Erweiterung von $\mathbb{Q}$ ist.

Lösung:
a) Nach Aufgabe 63 a) ist jedes nicht-konstante $\varphi \in k(X)$ transzendent über k, also sind nur die konstanten $\varphi \in k$ algebraisch: k ist in K algebraisch abgeschlossen.
b) Da $\mathbb{C}$ algebraisch abgeschlossen ist, besitzt jedes nicht-konstante Polynom $f \in \mathbb{Q}[X]$ eine Wurzel in $\mathbb{C}$, die dann natürlich in $\bar{\mathbb{Q}}$ liegt. Die Polynome $X^n - 2$ sind irreduzibel (2-eisensteinsch). Also gilt für alle $n \in \mathbb{N}$

$$n = (\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}) \leq (\bar{\mathbb{Q}} : \mathbb{Q})$$

$(\bar{\mathbb{Q}} : \mathbb{Q})$ kann daher nicht endlich sein.

Aufgabe 67. (s)
Es sei $f = X^3 - 331X - 2318 \in \mathbb{Z}[X]$. Zeigen Sie:

a) f ist irreduzibel über $\mathbb{Q}$.

b) f hat genau eine reelle Wurzel α.

c) Stellen Sie $\beta := \frac{1}{8}(\alpha + 10)(\alpha + 11)^2$ und β^{-1} in der $\mathbb{Q}$-Basis $1, \alpha, \alpha^2$ von $\mathbb{Q}(\alpha)$ dar.

Lösung:
b) Eine einfache Kurvendiskussion zeigt: Die durch f bestimmte Polynomfunktion $\mathbb{R} \to \mathbb{R}$ hat zwei Extremstellen $(\pm\sqrt{331/3})$; der lokale Maximalwert $f(-\sqrt{331/3})$ (≈ -0.124504) ist negativ, so dass f nur eine reelle Wurzel α besitzen kann; diese muss größer als die Minimalstelle $\sqrt{331/3} \approx 10.504$ sein.

a) Wäre f reduzibel über $\mathbb{Q}$, so auch über $\mathbb{Z}$ (siehe Aufgabe 55.c)ii)). Die Nullstelle α müsste also ganzzahlig sein. Eine Einschachtelung der reellen Nullstelle α zeigt $f(21) < 0$ und $f(22) > 0$: Die einzige reelle Nullstelle von f liegt zwischen 21 und 22, sie ist nicht ganzzahlig.

c) Ausgehend von

$$0 = f(\alpha) = \alpha^3 - 331\alpha - 2318 \iff \alpha^3 = 331\alpha + 2318$$

berechnen wir

$$\beta = (\alpha + 10)(\alpha^2 + 22\alpha + 121)/8 = (331\alpha + 2318)/8 + 4\alpha^2 + 341\alpha/8 + 605/4 = 4\alpha^2 + 84\alpha + 441\,.$$

Zur Berechnung von β^{-1} müssen wir nachfolgendes lineares Gleichungssystem für $a, b, c \in \mathbb{Q}$ lösen:

$$\begin{aligned}
1 &= (a\alpha^2 + b\alpha + c)(4\alpha^2 + 84\alpha + 441) \\
&= 4a\alpha^4 + (84a + 4b)\alpha^3 + (441a + 4c + 84b)\alpha^2 + (441b + 84c)\alpha + 441c \\
&= 4a(331\alpha + 2318)\alpha + (84a + 4b)(331\alpha + 2318) + \ldots \\
&\qquad \ldots (441a + 4c + 84b)\alpha^2 + (441b + 84c)\alpha + 441c \\
&= \alpha^2(1765a + 84b + 4c) + \alpha(37076a + 1765b + 84c) + 194712a + 9272b + 441c \\
&\iff \begin{pmatrix} 1765 & 84 & 4 \\ 37076 & 1765 & 84 \\ 194712 & 9272 & 441 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \iff \begin{pmatrix} 1765 & 84 & 4 \\ 11 & 1 & 0 \\ 483 & 44 & 0 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 4 \end{pmatrix} \\
&\iff \begin{pmatrix} 1765 & 84 & 4 \\ 11 & 1 & 0 \\ -1 & 0 & 0 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 4 \end{pmatrix} \iff (a, b, c) = (-4, 44, 841)
\end{aligned}$$

Also ist $\beta^{-1} = -4\alpha^2 + 44\alpha + 841$. Probe:

$$\begin{aligned} & (4\alpha^2 + 84\alpha + 441)(-4\alpha^2 + 44\alpha + 841) \\ = \; & -16\alpha^4 + \alpha^3(4 \cdot 44 - 4 \cdot 84) + \alpha^2(4 \cdot 841 + 84 \cdot 44 - 4 \cdot 441) + \ldots \\ & \qquad \ldots + \alpha(84 \cdot 841 + 44 \cdot 441) + 441 \cdot 841 \\ = \; & -16\alpha(331\alpha + 2318) - 160(331\alpha + 2318) + 5296\alpha^2 + 90048\alpha + 370881 \\ = \; & 0\alpha^2 + 0\alpha + 1 = 1 \end{aligned}$$

Aufgabe 68. (s)
Beweisen Sie Prop. III.1.16, Vorlesung S. 71.

Lösung:
Siehe Vorlesungsskript Prop. III.1.16.

Aufgabe 69. (s)
Sei $K|k$ eine endliche Körpererweiterung vom Grad n und $a \in K$. Die Linksmultiplikation mit a definiert einen Endomorphismus $L_a : K \to K$, $b \mapsto ab$, des k-Vektorraums K.

a) Sei $m := (k[a] : k)$, $l = \frac{n}{m} = (K : k[a])$ und $f_{a,k} = \sum_{i=0}^{m} \alpha_i X^i$ das Minimalpolynom von a über k. Zeigen Sie: Bei geeigneter Basiswahl für $K|k$ hat $L_a : K \to K$ eine Matrixdarstellung mit l diagonalen $m \times m$ Blöcken B:

$$A = \begin{pmatrix} B & & & \\ & B & & 0 \\ & & \ddots & \\ & 0 & & B \end{pmatrix} \quad \text{mit } B = \begin{pmatrix} 0 & & & & -\alpha_0 \\ 1 & 0 & & & -\alpha_1 \\ & \ddots & \ddots & & \vdots \\ & & \ddots & 0 & -\alpha_{m-2} \\ & & & 1 & -\alpha_{m-1} \end{pmatrix}.$$

[Tip: Studieren Sie zunächst den Fall $l = 1$ und wählen Sie eine geeignete (naheliegende) Basis für $k[a]|k$. Für den allgemeinen Fall konstruieren Sie mit dieser Basis von $k[a]|k$ und einer beliebigen Basis $w_1, \ldots, w_l$ von $K|k[a]$ eine Basis für $K|k$.]

b) Wir definieren für Körperelemente $a \in K$

$$\text{die Spur:} \quad \mathrm{Tr}_{K|k}(a) = \mathrm{Spur}(L_a) \in k\,, \quad \text{die Norm:} \quad \mathcal{N}_{K|k}(a) = \det L_a \in k\,,$$
$$\text{das charakteristische Polynom:} \quad h_{a,K|k}(X) = \det(X \cdot \mathrm{id}_K - L_a) \in k[X]$$

Wiederholen Sie die hier benutzten Begriffe der linearen Algebra und folgern Sie aus a)

$$\mathrm{Tr}_{K|k}(a) = l \cdot \mathrm{Tr}_{k[a]|k}(a)\,, \quad \mathcal{N}_{K|k}(a) = \mathcal{N}_{k[a]|k}(a)^l\,, \quad h_{a,K|k} = f_{a,k}^l\,.$$
$$h_{a,K|k} = \sum_{i=0}^{n} \gamma_i X^i \implies \mathrm{Tr}_{K|k}(a) = -\gamma_{n-1}\,,\ \mathcal{N}_{K|k}(a) = (-1)^n \gamma_0\,.$$

c) Zeigen Sie:

1) $\mathrm{Tr}_{K|k} : K \to k$ ist ein k-Homomorphismus.
2) $\mathrm{char}\, k = 0 \implies \mathrm{Tr}_{K|k} \neq 0$-Abbildung.
3) $\mathcal{N}_{K|k} : K \to k$ ist multiplikativ.
4) $\mathcal{N}_{K|k}(a) = 0 \iff a = 0$.

Lösung:
a) Die Potenzen a^i $(i = 0, \ldots, m-1)$ bilden eine Basis von $k[a]|k$, und mit einer beliebigen Basis w_j $(j = 1, \ldots, l)$ von $K|k[a]$ erhalten wir:

$$a^i w_j \ (0 \le i < m\,,\ 1 \le j \le l) \text{ ist eine Basis für } K|k\,.$$

Wir berechnen bzgl. dieser Basis die Matrix A von L_a:

$$L_a(a^i w_j) = a^{i+1} w_j = \begin{cases} a^{i+1} w_j & \text{für } 0 \le i < m-1\,,\ 1 \le j \le l \\ -\sum_{\nu=0}^{m-1} \alpha_\nu a^\nu w_j & i = m-1\,,\ 1 \le j \le l \end{cases}.$$

Für jedes j bleibt der m-dimensionale k-Unterraum $k[a]w_j = \oplus_{i=0}^{m-1} k a^i w_j$ stabil unter L_a. So ergibt sich für jedes $1 \le j \le l$ in der Matrix A von L_a in der Diagonalen ein $m \times m$-Block der Form

$$B = \begin{pmatrix} 0 & & & & -\alpha_0 \\ 1 & 0 & & & -\alpha_1 \\ & \ddots & \ddots & & \vdots \\ & & \ddots & 0 & -\alpha_{m-2} \\ & & & 1 & -\alpha_{m-1} \end{pmatrix}.$$

b) Diese Matrix B ist die Matrix von $L_a\,|_{k[a]}$ bzgl. obiger Basis von $k[a]|k$. Sie ist aus der Linearen Algebra bekannt als die sog. Begleitmatrix $B(f_{a,k})$ des Polynoms $f_{a,k}$. Es gilt bekanntlich (etwa durch Entwicklung der Determinante nach der ersten Zeile und Induktion)

$$\det(X \cdot E_m - B(f_{a,k})) = f_{a,k}\,.$$

Aus obiger Matrix A für L_a mit den l identischen Blöcken B ergeben sich unmittelbar die ersten 3 Behauptungen:

$$\mathrm{Spur}(A) = l \cdot \mathrm{Spur}(B)\,,\ \det A = (\det B)^l\,,\ \det(X \cdot E_n - A) = (\det(X \cdot E_m - B))^l$$

Weiter gilt $\gamma_0 = h_{a,K|k}(0) = \det(0 \cdot E_n - A) = \det(-A) = (-1)^n \det A = (-1)^n \mathcal{N}_{K|k}(a)$. Dass die Spur von A sich aus dem zweithöchsten Koeffizienten des charakteristischen Polynoms ergibt, ist ebenfalls aus der Linearen Algebra bekannt, etwa durch Auswertung der Definition des charakteristischen Polynoms mit der expliziten Determinantendefinition:

$$\begin{aligned} A = (a_{ij}) \implies \det(XE - A) &= \det(\delta_{ij} X - a_{ij}) = \sum_{\sigma \in S_n} \mathrm{sign}\,\sigma \prod_i (\delta_{i\sigma(i)} X - a_{i\sigma(i)}) \\ &= \prod_i (X - a_{ii}) + \sum_{\sigma \neq \mathrm{id}} \mathrm{sign}\,\sigma \underbrace{\prod_i (\delta_{i\sigma(i)} X - a_{i\sigma(i)})}_{\deg \le n-2\,,\ \text{mind. } 2\times\ i \neq \sigma(i)} \\ &= X^n - \underbrace{\sum_i a_{ii}}_{\mathrm{Spur}(A)} X^{n-1} + (\text{Polynom vom Grad } \le n-2) \end{aligned}$$

c) ad 1) Wegen $L_{\alpha a + \beta b} = \alpha L_a + \beta L_b$ $(a, b \in K,\ \alpha, \beta \in k)$ und der offensichtlichen Linearität der Matrixspur gilt 1).
ad 2) $L_1 = \mathrm{id}_K$, also $\mathrm{Tr}(1) = \mathrm{Spur}\,\mathrm{id}_K = n.1_k \neq 0_k$, wenn $\mathrm{char}\,k = 0$.
ad 3) $L_{\alpha\beta} = L_\alpha \circ L_\beta$ und daher $\mathcal{N}(\alpha\beta) = \det(L_\alpha)\det(L_\beta) = \mathcal{N}(\alpha) \cdot \mathcal{N}(\beta)$.
ad 4) $\Leftarrow$ ist klar. $\alpha \neq 0 \implies L_{\alpha^{-1}} = (L_\alpha)^{-1} \implies \mathcal{N}(\alpha) = \det L_\alpha \neq 0$.

Algebra
Übung 13

Aufgabe 70. (m)

a) Geben Sie für die folgenden Erweiterungen alle $\mathbb{Q}$-Monomorphismen nach $\mathbb{C}$ an:

$$\mathbb{Q}\left(\sqrt{2},\sqrt{3},\sqrt{24}\right)|\mathbb{Q}\,,\qquad \mathbb{Q}\left(\sqrt{2}\sqrt{3},\sqrt{\sqrt{2}+\sqrt{3}}\right)|\mathbb{Q}$$

Welche der Erweiterungen sind galoissch?

b) Welche der folgenden erweiterungen sind galoissch?

$\mathbb{Q}(\sqrt{2})|\mathbb{Q}$, $\mathbb{Q}(\sqrt[4]{2},i)$, $\mathbb{Q}(\sqrt[4]{2},i\sqrt{3})|\mathbb{Q}$.

$\mathbb{Q}(\zeta_n)\mathbb{Q}$, ζ_n primitive n-te Einheitswurzel, d. h. $\zeta_n \in \mathbb{C}^\times$ mit $\mathrm{ord}(\zeta_n) = n$. a).

$\mathbb{Q}(\theta)|\mathbb{Q}$ mit der reellen Nullstelle θ von $f(X) = X^3 - 331X - 2318$ (vgl. Aufgabe 67).

$\mathbb{F}_p(X)(t)|\mathbb{F}_p(X)$ mit einer Nullstelle t von $f(Y) = Y^p - X \in (\mathbb{F}_p(X))[Y]$ (X transzendent über $\mathbb{F}_p$)

$\mathbb{F}_p(\theta)|\mathbb{F}_p$ mit einer Nullstelle θ eines irreduziblen Polynoms $f(X) \in \mathbb{F}_p[X]$.

Lösung:
a) Wegen $\sqrt{24} = 2\sqrt{2}\cdot\sqrt{3}$ ist $K_1 := \mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{24}) = \mathbb{Q}(\sqrt{2},\sqrt{3})$ der Zerfällungskörper des separablen Polynoms $(X^2-2)(X^2-3)$ mit den 4 Wurzeln $\pm\sqrt{2}$, $\pm\sqrt{3}$. Also ist $K_1|\mathbb{Q}$ normal und separabel, also galoissch. Wegen $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ ist $(K_1 : \mathbb{Q}) = 4$ und $\mathrm{Aut}(K_1|\mathbb{Q})$ besteht aus genau 4 Automorphismen, und dies sind sämtliche $\mathbb{Q}$-Monomorphismen. Da ein $\mathbb{Q}$-Monomorphismus die Wurzeln $\pm\sqrt{2}$ von X^2-2 sowie $\pm\sqrt{3}$ von X^2-3 jeweils ineinander abbilden muss, gibt es nur 4 Möglichkeiten: Die Identität $\sigma_{++} = \mathrm{id}_{K_1}$ und

$$\sigma_{+-} : \begin{cases} \sqrt{2} \mapsto \sqrt{2}\,, \\ \sqrt{3} \mapsto -\sqrt{3} \end{cases}, \quad \sigma_{-+} : \begin{cases} \sqrt{2} \mapsto -\sqrt{2}\,, \\ \sqrt{3} \mapsto \sqrt{3} \end{cases}, \quad \sigma_{--} = \sigma_{+-}\circ\sigma_{-+} : \begin{cases} \sqrt{2} \mapsto -\sqrt{2}\,, \\ \sqrt{3} \mapsto -\sqrt{3} \end{cases}$$

Nach Aufgabe 61 ist $K_2 = \mathbb{Q}\Big(\sqrt{2},\sqrt{3},\sqrt{\sqrt{2}+\sqrt{3}}\Big) = K_1\Big(\sqrt{\sqrt{2}+\sqrt{3}}\Big)$ vom Grad 8 über $\mathbb{Q}$ und wegen Charakteristik 0 ist die Erweiterung separabel. Es gibt also genau $\mu(K_2|\mathbb{Q}) = (K_2 : \mathbb{Q}) = 8$ $\mathbb{Q}$-Monomorphismen $K_2 \to \mathbb{C}$. Die 4 Automorphismen $\sigma_{\cdot\cdot}$ von $K_1|\mathbb{Q}$ lassen sich zu je 2 Monomorphismen $\sigma^{\pm}_{\cdot\cdot} : K_2 \to \mathbb{C}$ fortsetzen. Dabei muss die Wurzel α von $f := X^2 - (\sqrt{2}+\sqrt{3}) \in K_1[X]$ jeweils in eine der beiden Wurzeln von

$$\sigma_{\cdot\cdot}f = X^2 - (\sigma_{\cdot\cdot}(\sqrt{2}) + \sigma_{\cdot\cdot}(\sqrt{3})) = \Big(X - \sqrt{\sigma_{\cdot\cdot}(\sqrt{2}) + \sigma_{\cdot\cdot}(\sqrt{3})}\Big)\cdot\Big(X + \sqrt{\sigma_{\cdot\cdot}(\sqrt{2}) + \sigma_{\cdot\cdot}(\sqrt{3})}\Big)$$

abgebildet werden. Explizit:

$$\sigma^{\pm}_{++} : \alpha \mapsto \pm\sqrt{\sqrt{2}+\sqrt{3}}\,, \quad \sigma^{\pm}_{+-} : \alpha \mapsto \pm\sqrt{\sqrt{2}-\sqrt{3}}\,,$$
$$\sigma^{\pm}_{-+} : \alpha \mapsto \pm\sqrt{-\sqrt{2}+\sqrt{3}}\,, \quad \sigma^{\pm}_{--} : \alpha \mapsto \pm\sqrt{-\sqrt{2}-\sqrt{3}}\,.$$

Die Erweiterung $K_2|\mathbb{Q}$ ist genau dann galoissch, wenn sie normal ist, d. h. wenn alle 8 Monomorphismen ihre Bilder in K_2 hätten, aber wegen $K_2 \subset \mathbb{R}$ gilt

$$\sigma^{+}_{--}(\alpha) = \sqrt{-\sqrt{2}-\sqrt{3}} = i\alpha \notin K_2\,.$$

b) In Charakteristik 0 sind alle Erweiterungen separabel. Es geht also zunächst nur um Normalität. : Die ersten drei Erweiterungen sind alle normal, denn sie sind Zerfällungskörper der

folgenden Polynome X^2-2, X^4-2 und $(X^4-2)(X^2-3)$.
Ist $\operatorname{ord}\zeta_n = n$, so sind die Potenzen ζ_n^i $(i = 0, \dots, n-1)$ alle verschieden und damit sämtliche n Wurzeln von $X^n - 1$: $\mathbb{Q}(\zeta_n)$ ist der Zerfällungskörper des separablen Polynoms $X^n - 1$, also galoissch.
$\mathbb{Q}(\theta) \subset \mathbb{R}$ enthält nicht die beiden nicht-reellen Wurzeln von f, also ist $\mathbb{Q}(\theta)$ nicht normal und nicht galoissch über $\mathbb{Q}$.
Wegen $\operatorname{char}\mathbb{F}_p(X)(t) = p$ gilt $f(Y) = Y^p - t^p = (Y-t)^p$ (für $p = 2$ beachte man $+t = -t$), f hat also nur die eine Wurzel t. Das Minimalpolynom $f_{t,\mathbb{F}_p(X)}(Y)$ teilt f, hat also ebenfalls nur eine Wurzel und ist daher nicht separabel, die Erweiterung also nicht galoissch.
Da θ algebraisch ist, ist $k = \mathbb{F}_p(\theta)$ ein endlicher Körper. Diese sind galoissch über allen Teilkörpern (siehe Satz III.2.14).

Aufgabe 71. (s)

a) Zeigen Sie: $\mathbb{Q}(\sqrt{3}, \sqrt{3} + \sqrt[3]{9})) = \mathbb{Q}(\sqrt{3}, \sqrt[3]{3})$.
$\mathbb{Q}(\zeta_6) = \mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(\zeta_8) = \mathbb{Q}(i, \sqrt{2})$ mit primitiven n-ten Einheitswurzeln ζ_n.

b) Sei $\Omega|k$ eine Körpererweiterung und $K = k(a_1, \dots, a_n)$ sowie L Zwischenkörper. Zeigen Sie:
$$LK = L(a_1, \dots, a_n)\,, \quad (LK : L) \le (K : k)\,, \quad (LK : k) \le (L : k) \cdot (K : k)$$

c) Können Sie zusätzliche Voraussetzungen formulieren, unter denen in b) $(LK : L) = (K : k)$ gilt?

Lösung:
a) Es ist jeweils zu zeigen, dass die erzeugenden Elemente des einen Körpers im anderen enthalten sind. Es ist $\frac{3}{\sqrt[3]{9}} = \sqrt[3]{3}$, also ist die rechte Seite in der linken enthalten. Umgekehrt $\sqrt{3} + \sqrt[3]{9} = \sqrt{3} + (\sqrt[3]{3})^2$.
Es ist $\zeta_n = \exp(\frac{2\pi i}{n}) = \cos(\frac{2\pi}{n}) + i\sin(\frac{2\pi}{n})$, also $\zeta_6 = \frac{1}{2} + i\frac{1}{2}\sqrt{3} = \frac{1}{2}(1 + \sqrt{-3})$; dies beweist die erste Behauptung. Und $\zeta_8 = \frac{1}{2}\sqrt{2}(1+i)$ zeigt zunächst die behauptete Inklusion $\subseteq$. Für die umgekehrte Richtung beachte man $\zeta_8^2 = \zeta_4 = i \in \mathbb{Q}(\zeta_8)$ und dann auch $\sqrt{2} \in \mathbb{Q}(\zeta_8)$.
b) LK ist der kleinste L und $k(a_1, \dots, a_n)$, also L $(\supset k)$ und $a_1, \dots a_n$ enthaltende Körper, d. h. $L(a_1, \dots, a_n)$.
Ist $(K : k) = \infty$, so ist nichts zu beweisen. Sei also $K|k$ endlich und folglich algebraisch. Ist dann $b_1, \dots, b_m$ eine k-Basis von K, so gilt $K = k(b_1, \dots, b_m) = k[b_1, \dots, b_m]$. Alle *Potenzprodukte* $\prod_i b_i^{\nu_i}$ der b_i sind also *k-Linearkombinationen* der b_i, also erst recht L-Linearkombinationen der b_i. Damit enthält der von den b_i erzeugte L-Vektorraum $V = \sum_i Lb_i$ alle Potenzprodukte der b_i, ist also gegen Multiplikation abgeschlossen und daher ein Ring, der kleinste Ring, der L und alle b_i enthält: $V = \sum_{i=1}^m Lb_i = L[b_1, \dots, b_m] = LK$, und damit gilt $(LK : L) = \dim_L(LK) \le m = (K : k)$.
c) Ein Beispiel: Es seien $K|k$ und $L|k$ endlich und die Körpergrade $(K : k)$ und $(L : k)$ teilerfremd. Dann gilt $(LK : L) = (K : k)$.
Begründung: Ist $K|k$ endlich, so ist $K = k(a_1, \dots, a_n)$ endlich erzeugt und nach b) gilt: $(LK : k) \le (L : k)(K : k)$. Andererseits gilt $(L : k) \mid (LK : k)$ und $(K : k) \mid (LK : k)$. Wegen der Teilerfremdheit erhalten wir

$$\begin{aligned}&(L : k)(K : k) \mid (LK : k) \le (L : k)(K : k) \implies (LK : k) = (L : k)(K : k)\\ \implies &(LK : L)(L : k) = (LK : k) = (L : k)(K : k) \implies (LK : L) = (K : k)\,.\end{aligned}$$

Hinweis: Ein anderes wichtiges Kriterium basiert auf der galoisschen Theorie (siehe Verschiebungssatz III.2.14, S. 81)

Aufgabe 72. (s)
Alle auftretenden Körper seien Teilkörper eines algebraisch abgeschlossenen Körpers Ω.

a) Sei $K|k$ endlich. Ist K über k normal, so auch über jedem Zwischenkörper L von $K|k$.

b) Ist $K|k$ endlich und normal, so ist für jeden Oberkörper L von k auch $LK|L$ endlich und normal.

c) Sind K_1, K_2 über k endlich und normal, so gilt das gleiche für K_1K_2 und $K_1 \cap K_2$.

d) Jede endliche Erweiterung $K|k$ besitzt einen kleinsten über k normalen Oberkörper N von K (in Ω), die *normale Hülle* von $K|k$. Sie ist durch das Kompositum N der Bilder von K unter allen k-Monomorphismen $\varphi : K \to \Omega$ gegeben:

$$N = \prod_{\varphi \in \mathcal{M}(K|k)} \varphi(K).$$

Lösung:
a) Es ist K der Zerfällungskörper eines Polynoms $f \in k[X]$, d.h. $K = k[\mathcal{W}_\Omega(f)]$. Wegen $f \in L[X]$ ist damit K auch über L normal.
b) K ist Zerfällungskörper von $f \in k[X]$, dann ist auch $LK = L[\mathcal{W}_\Omega(f)]$ Zerfällungskörper von $f \in L[X]$, also normal über L.
c) Seien K_i Zerfällungskörper von $f_i \in k[X]$ $(i = 1, 2)$. Dann ist K_1K_2 Zerfällungskörper von $f_1f_2 \in k[X]$.
Da die $K_i|k$ normal sind, gilt für jedes $a \in K_1 \cap K_2$: $f_{a,k}$ zerfällt über K_1 und über K_2 in Lineafaktoren, also liegen alle Wurzeln von $f_{a,k}$ in $K_1 \cap K_2$, und $K_1 \cap K_2$ ist normal über k.
d) Es ist $K = k[a_1, \ldots, a_n]$ endlich erzeugt und algebraisch. Es sei f das Produkt der Minimalpolynome $f_{a_i,k}$ der a_i über k und N der Zerfällungskörper von f. Dann ist $N|k$ normal, und jede normale Erweiterung $L|k$ mit $K \subseteq L$ muss a_i und damit auch alle Wurzeln von $f_{a_i,k}$ enthalten, also $N \subseteq L$, N ist die kleinster derartige Erweiterung.

Ist $L|k$ normal mit $K \subseteq N$, so muss für jeden Monomorphismus $\varphi : K \to \Omega$ das Bild $\varphi(K)$ in L enthalten sein, also umfasst L das Kompositum N der Aufgabenstellung. Es ist also zu zeigen, das N selbst normal über k ist. Ist $\psi \in \mathcal{M}(N|k)$, so ist für jedes $\varphi \in \mathcal{M}(K|k)$ auch $\psi \circ \varphi \in \mathcal{M}(K|k)$ und daher

$$\psi \in \mathcal{M}(N|k) \implies \psi(N) = \prod_{\varphi \in \mathcal{M}} \psi \circ \varphi(K) \subseteq N\,, \text{ d. h. } N|k \text{ ist normal.}$$

Ist $K = k[a_1, \ldots, a_n]$, so wird N von allen Wurzeln aller Minimalpolynome $f_{a_i,k}$ erzeugt, denn es gilt (Satz vom Stammkörper III.1.10 und Bemerkung III.2.1 b))

$$f_{a_i,k}(b_i) = 0 \iff b_i = \varphi(a_i) \text{ für ein } \varphi \in \mathcal{M}(K|k)\,.$$

Aufgabe 73. (s)

a) Ist $E|K|k$ ein Körperturm und $E|k$ endlich, so gilt:

$$E|k \text{ separabel} \iff E|K \text{ separabel und } K|k \text{ separabel.}$$

b) Ist $K|k$ endlich separabel und K, L in einem gemeinsamen Oberkörper Ω enthalten. Dann gilt: Ist $\Omega|k$ eine Körpererweiterung und k, L Zwischenkörper, so gilt:

$$K|k \text{ endlich separabel} \implies KL|L \text{ endlich separabel.}$$

c) Sei $K|k$ endlich. Dann enthält K einen größten über k separablen Teilkörper K_s.

d) Ist $K|k$ inseparabel, so ist $\operatorname{char} k = p$ eine Primzahl und für jedes $a \in K$ gibt es eine kleinste p-Potenz p^ν ($\nu \in \mathbb{N}$) mit $a^{p^\nu} \in K_s$. Es gilt $f_{a,K_s} = X^{p^\nu} - a^{p^\nu}$.

e) Ist $K_s \neq K$, so ist $\operatorname{char} K = p$ eine Primzahl und $(K : K_s) = p^\nu$ mit $\nu \in \mathbb{N}_+$.

Lösung:
a) Nach Prop. III.2.5 gilt $K|k$ separabel $\iff$ $\mu(K|k) = (K : k)$. Da Körpergrad und μ multiplikativ sind (siehe Prop. III.2.2) folgt a).
b) $K|k$ endlich separabel $\iff$ $K = k[a_1, \ldots, a_n]$ und jedes a_i ist Wurzel eines separablen Polynoms $f_i \in k[X]$. Dann folgt $KL = L[a_1, \ldots, a_n]$ mit separablen Polynomen $f_i \in k[X] \subset L[X]$.
c) Begründung wie für den algebraischen Abschluss in einem Körper (siehe Korollar III.1.14 b)): $K_s = \{a \in K \mid a \text{ separabel algebraisch über } k\}$ ist ein Teil*körper* von K, denn sind $a, b \in K_s$, also separabel algebraisch über k, so ist ganz $k[a, b]|k$ separabel und folglich liegen $a + b$, $a - b$, $a \cdot b$ und für $a \neq 0$ a^{-1} wieder in K_s. Wegen der Transitivität der Separabilität (Aufgabenteil a)) besitzt K_s in K keine echte separable Erweiterung.
d) Nach Voraussetzung ist $K \setminus K_s \neq \emptyset$. *Jedes* $a \in K \setminus K_s$ ist inseparabel über K_s(!), denn wäre a separabel über K_s, so wäre a gemäß a) auch separabel über k, läge also in K_s. Also ist das Minimalpolynom f von a über K_s nicht separabel. Nach Prop. III.2.4 ist dann $\operatorname{char} K = p$ eine Primzahl und $f(X) = f_1(X^p)$ mit $f_1 \in K_s[X]$. Mit f ist auch f_1 irreduzibel und ist damit das Minimalpolynom von a^p: $f_1(a^p) = f(a) = 0$.
Gilt nun auch $a^p \notin K_s$, so kann man diese Überlegung wiederholen und erhält ein irreduzibles Polynom $f_2 \in K_s[X]$ mit $f_1(X) = f_2(X^p)$, also $f(X) = f_1(X^p) = f_2(X^{p^2})$. Dieses Verfahren kann man fortführen, aber es muss enden, da die Grade der f_i abnehmen, und es endet mit der kleinsten p-Potenz p^ν, für die $a^{p^\nu} \in K_s$ gilt. Dann haben wir: $f_{a,K_s}(X) = f_\nu(X^{p^\nu})$ mit $f_\nu(X) = f_{a^{p^\nu},K_s}(X) = X - a^{p^\nu}$ (wegen $a^{p^\nu} \in K_s$). Damit ist d) bewiesen, denn für $a \in K_s$ leistet $\nu = 0$ das gewünschte.
e) Ist nun L irgendein Zwischenkörper von $K|K_s$, so gilt $f_{a,L} \mid f_{a,K_s} = X^{p^\nu} - a^{p^\nu} = (X - a)^{p^\nu}$, also hat $f_{a,L}$ nur die eine Wurzel a, ist daher ebenfalls inseparabel, falls $a \notin L$. Die obigen Ergebnisse gelten also für jeden Grundkörper L ($\supset K_s$). Insbesondere ist $(L[a] : L)$ eine p-Potenz. Da $K|K_s$ endlich algebraisch ist, ist $K = K_s[a_1, \ldots, a_r]$ endlich erzeugt und für die Körper $L_i := K_s[a_1, \ldots, a_i]$ ist $(L_i[a_{i+1}] : L_i)$ eine p-Potenz und daher auch $(K : K_s)$.

Aufgabe 74. (s)

a) Ist $K|k$ eine endliche inseparable Erweiterung, so ist $\mathrm{Sp}_{K|k}$ die Nullabbildung. [Tip: Man verwende Aufgaben 69 und 73.]

b) Für eine endliche separable Erweiterung $K|k$ und alle $a \in K$ gilt

$$\mathrm{Tr}_{K|k}(a) = \sum_{\varphi \in \mathcal{M}(K|k)} \varphi(a)\,, \quad \mathcal{N}_{K|k}(a) = \prod_{\varphi \in \mathcal{M}(K|k)} \varphi(a)\,.$$

Aus dem Lemma von Artin folgere man: $\mathrm{Tr}_{K|k}$ ist nicht die Nullabbildung.

c) Sei $K = \mathbb{Q}(\sqrt{d}) \neq \mathbb{Q}$. Bestimmen Sie für $\alpha, \beta \in \mathbb{Q}$ Spur und Norm von $x = \alpha + \beta\sqrt{d}$ über $\mathbb{Q}$.

Lösung:
a) Nach Voraussetzung ist $K|K_s$ eine echte Erweiterung und daher nach Aufgabe 73 d) $\operatorname{char} K = p$ eine Primzahl und der Körpergrad $(K : K_s)$ eine Potenz von p . Daher gilt

$$a \in K_s \implies p \mid (K : K_s) \mid (K : k[a]) \implies \mathrm{Tr}_{K|k}(a) = (K : k[a]) \cdot \mathrm{Tr}_{k[a]|k}(a) = 0\,.$$

Sei nun $a \notin K_s$, also $f_{a,k}$ inseparabel und somit von der Form $f_{a,k} = g(X^p)$ (siehe Prop. III.2.4 d)). Also verschwindet der zweithöchste Koeffizient a_{n-1} von $f_{a,k}$. Nach Aufgabe 69 erhalten

wir so $\mathrm{Tr}_{k[a]|k}(a) = -a_{n-1} = 0$ und $\mathrm{Tr}_{K|k}(a) = (K : k[a]) \cdot \mathrm{Tr}_{k[a]|k}(a) = 0$.
b) Sei L ein algebraisch abgeschlossener Erweiterungskörper von K. Nach Prop. III.2.2 ist

$$\mathcal{M}(k[a]|k) \ni \sigma \mapsto \sigma(a) \in \mathcal{W}_L(f_{a,k})$$

eine Bijektion und $\mathcal{M}(K|k)$ besteht genau aus den jeweils $\mu(K|k[a]) = (K : k[a]) = l$ vielen Fortsetzungen $\varphi : K \to L$ der verschiedenen $\sigma \in \mathcal{M}(k[a]|k)$. Also

$$\sum_{\varphi \in \mathcal{M}(K|k)} \varphi(a) = \sum_{\sigma \in \mathcal{M}(k[a]|k)} l \cdot \sigma(a) = l \cdot \sum_{b \in \mathcal{W}_L(f_{a,k})} b\,.$$

Nun zerfällt $f_{a,k}$ über L in Linearfaktoren:

$$f_{a,k} = \prod_{i=1}^{m} (X - a_i) = X^m - \sum_{i=1}^{m} a_i X^{m-1} + \ldots,$$

also ist $\mathrm{Tr}_{k[a]|k}(a) = \sum_{i=1}^{m} a_i = \sum_{b \in \mathcal{W}_L(f_{a,k})} b$. Dies ergibt insgesamt $\mathrm{Tr}_{K|k}(a) = l \cdot \mathrm{Tr}_{k[a]|k}(a) = \sum_{\varphi \in \mathcal{M}(K|k)} \varphi(a)$.
Zum Zusatz: Angenommen $0 = \mathrm{Tr}_{K|k}(a) = \sum_{\varphi \in \mathcal{M}(K|k)} \varphi(a)$ für alle $a \in K$. Dann erfüllten die Gruppencharaktere $\tilde{\varphi} := \varphi\,|_{K^\times} : K^\times \to L^\times$ die nicht-triviale lineare Relation $\sum_{\varphi \in \mathcal{M}(K|k} \tilde{\varphi} = 0$, im Widerspruch ihrer linearen Unabhängigkeit gemäß dem Lemma von Artin.
c) K besitzt zwei Monomorphismen $\varphi_\pm \in \mathcal{M}(K|\mathbb{Q})$, definiert durch $\varphi_\pm(\sqrt{d}) = \pm\sqrt{d}$. Also ist

$$\mathrm{Tr}_{K|\mathbb{Q}}(\alpha + \beta\sqrt{d}) = \alpha + \beta\sqrt{d} + \alpha - \beta\sqrt{d} = 2\alpha\,.$$

Algebra
Übung 14

Aufgabe 75. (m)
Sei K der Zerfällungskörper des Polynoms X^4-X^2-2 über $\mathbb{Q}$. Bestimmen Sie die Galoisgruppe G von $K|\mathbb{Q}$ sowie ihren Untergruppenverband. Bestimmen Sie weiter den Zwischenkörperverband von $K|\mathbb{Q}$ und und geben Sie explizit die Zuordnung zwischen beiden Verbänden an.

Lösung:
a) $x^4-x^2-2=0 \iff x^2=y \wedge 0=y^2-y-2=(y+1)(y-2) \iff x=\pm\sqrt{-1} \vee x=\pm\sqrt{2}$. Also ist $K=\mathbb{Q}(i,\sqrt{2})$ vom Grad 4 über $\mathbb{Q}$. Die Gruppe G besteht neben der Identität aus den Isomorphismen (vgl. analoge Überlegungen in Aufgabe 70)

$$\sigma_{+-}:\begin{cases}\sqrt{2}\mapsto\sqrt{2}\\ i\mapsto -i\end{cases}\quad,\quad \sigma_{-+}:\begin{cases}\sqrt{2}\mapsto-\sqrt{2}\\ i\mapsto i\end{cases}\quad,\quad \sigma_{--}:\begin{cases}\sqrt{2}\mapsto-\sqrt{2}\\ i\mapsto -i\end{cases}$$

σ_{-+} und σ_{+-} sind vertauschbar und ihr Produkt ist σ_{--}. Die Gruppe G ist die Kleinsche Vierergruppe mit 3 Untergruppen $U_\pm$ der Ordnung 2, erzeugt von jeweils einem der 3 nichttrivialen Automorphismen. Die zugehörigen Fixkörper sind die drei echten Zwischenkörper von $K|k$:

$$\mathrm{Fix}_K(\sigma_{+-})=\mathbb{Q}(\sqrt{2})\,,\ \mathrm{Fix}_K(\sigma_{-+})=\mathbb{Q}(i)\,,\ \mathrm{Fix}_K(\sigma_{--})=\mathbb{Q}(\sqrt{-2})\,.$$

Beachten Sie bei der letzten Behauptung, dass $1, i, \sqrt{2}, \sqrt{-2}$ eine $\mathbb{Q}$-Basis von K ist.

Aufgabe 76. (m)
K sei der Zerfällungskörper von X^4-2 über $\mathbb{Q}$. Bestimmen Sie die Galoisgruppe $G=G(K|\mathbb{Q})$ (vgl. Aufgabe 62 c)).

Lösung:
Die Wurzeln von X^4-2 sind $\pm\sqrt{\pm\sqrt{2}}$, also $\pm\sqrt[4]{2}$, $\pm\sqrt{-\sqrt{2}}=\pm i\sqrt[4]{2}$, also ist der Zerfällungskörper von X^4-2 der Körper $K=\mathbb{Q}(i,\sqrt[4]{2})$, wie er in Aufgabe 62 c) untersucht wurde. Er hat also den Grad 8 über $\mathbb{Q}$ und seine Galoisgruppe enthält die Automorphismen

$$\sigma:=\begin{cases}\sqrt[4]{2}\mapsto i\sqrt[4]{2}\\ i\mapsto i\end{cases}\quad,\quad \tau:=\begin{cases}\sqrt[4]{2}\mapsto\sqrt[4]{2}\\ i\mapsto -i\end{cases}\quad.$$

Es gilt nach Aufgabe 62.c) $\operatorname{ord}\sigma=4$, $\operatorname{ord}\tau=2$ und $\sigma\circ\tau=\tau\circ\sigma^{-1}$. Damit liegt τ nicht in $\langle\sigma\rangle$ und $\langle\sigma,\tau\rangle$ hat (mindestens) die Ordnung 8. Als normale Erweiterung in Charakteristik 0 ist $K|\mathbb{Q}$ galoissch und daher $\#G=(K:\mathbb{Q})=8$. Daher wird G von σ und τ erzeugt und wegen der Vertauschungsrelation ist G die Diedergruppe D_4 (siehe Gruppen spezieller Ordnung, A), S. 19).

Aufgabe 77. (s)
Es sei $K|\mathbb{Q}$ eine galoissche Erweiterung vom Grad 4 in $\mathbb{C}$. Zeigen Sie: Ist $G(K|\mathbb{Q})$ zyklisch, so kann $\mathbb{Q}(i)$ nicht in K liegen.

Lösung:
Wir nehmen an $\mathbb{Q}(i)\subset K$. Als zyklische Gruppe der Ordnung 4 hat $G(K|\mathbb{Q})$ genau eine Untergruppe mit Ordnung 2 (und Index 2) und deren Fixkörper ist dann der einzige quadratische Teilkörper von K, also gleich $\mathbb{Q}(i)$.
Sei c die Einschränkung der komplexen Konjugation auf K. Da $K|\mathbb{Q}$ galoissch ist, ist $c\in G(K|\mathbb{Q})$, und wegen $i\in K$ gilt $c\neq\mathrm{id}_K$, also $\operatorname{ord}c=2$. c liegt daher in der Fixgruppe von $\mathbb{Q}(i)$, aber $c(i)\neq i$, Wid.

Aufgabe 78. (s)
Es sei $f = X^3 - 331X - 2318 \in \mathbb{Z}[X]$.

a) Zeigen Sie, dass f genau eine reelle Nullstelle α besitzt, und folgern Sie, dass $K = \mathbb{Q}(\alpha)$ nicht der Zerfällungskörper von f sein kann.

b) Folgern Sie aus a), dass ein Zerfällungskörper N von f über $\mathbb{Q}$ den Grad 6 und die symmetrische Gruppe S_3 als Galoisgruppe hat.

Lösung:
a) Dass f eine reelle und zwei konjugiert komplexe Nullstellen hat, wurde bereits in Aufgabe 67 gezeigt. Wäre K Zerfällungskörper, so müssten die beiden nicht-reellen Wurzeln von f in dem reellen Körper K liegen, Wid.
b) Seien $\alpha_1 = \alpha\,, \alpha_2\,, \alpha_3$ die 3 Wurzeln von f. Dann ist $N = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$ und jeder Automorphismus $\sigma \in G(N|\mathbb{Q})$ permutiert diese 3 Wurzeln. Da jedes σ durch seine Wirkung auf die Wurzeln eindeutig bestimmt ist, haben wir eine Einbettung $G(N|\mathbb{Q}) \hookrightarrow S_3$. Als Zerfällungskörper eines separablen Polynoms ist $N|\mathbb{Q}$ galoissch, und das bedeutet: $\#G(N|\mathbb{Q}) = (N\colon\mathbb{Q})$. Wir erhalten daraus $(K\colon\mathbb{Q}) = 3 < (N\colon\mathbb{Q}) = \#G(N|\mathbb{Q}) \mid \#S_3 = 6$, also $(N\colon\mathbb{Q}) = \#G(N|\mathbb{Q}) = 6 = \#S_3$. Der obige Gruppenmonomorphismus ist also ein Isomorphismus: $G(N|\mathbb{Q}) \xrightarrow{\sim} S_3$.

Aufgabe 79. $(*)$
Es sei $\bar{\mathbb{Q}}$ eine algebraisch abgeschlossene Hülle von $\mathbb{Q}$. $\mathcal{M}$ sei die Menge aller Teilkörper von $\bar{\mathbb{Q}}$, die $\sqrt{2}$ *nicht* enthalten.

a) Zeigen Sie mit dem Zornschen Lemma, dass $\mathcal{M}$ ein maximales Element k enthält.

Sei im Folgenden k ein solcher maximaler Teilkörper.

b) Beweisen Sie, dass jede endliche Erweiterung $K|k$ einen 2-Potenzgrad hat.

[Tip: Sei zunächst $K|k$ eine *galoissche* Erweiterung mit $k(\sqrt{2}) \subseteq K$. Betrachten Sie nun eine 2-Sylowgruppe von $G(K|k)$ und beachten Sie die Maximalitätseigenschaft von k. Für den allgemeinen Fall benutze man Aufgabe 72 d).]

c) Zeigen Sie, dass jede endliche Erweiterung $K|k$ galoissch ist mit zyklischer Galoisgruppe.

[Tip: N sei die normale Hülle von $K|k$. $G(N|k)$ enthält genau eine Untergruppe vom Index 2. Zeigen Sie, dass eine 2-Gruppe mit dieser Eigenschaft zyklisch sein muss.]

Lösung:
a) Sei $\mathcal{K} \subset \mathcal{M}$ eine Kette, also eine totalgeordnete Menge von Teilkörpern von $\bar{\mathbb{Q}}$, die $\sqrt{2}$ nicht enthalten. Dann liegt $\sqrt{2}$ auch nicht in $K_\infty = \bigcup_{K\in\mathcal{K}} K$. Die Vereinigung K_∞ ist ein Körper, denn sie ist gegen die Körperoperationen abgeschlossen, da je zwei Elemente aus K_∞ in einem gemeinsamen Körper $K \in \mathcal{M}$ liegen (Totalordnung von $\mathcal{K}$!). Damit besitzt jede Kette $\mathcal{K} \subset \mathcal{M}$ eine obere Schranke in $\mathcal{M}$, so dass die (offensichtlich nicht leere Menge) $\mathcal{M}$ nach dem Zornschen Lemma ein maximales Element besitzt.

b) Sei K eine echte *galoissche* Erweiterung von k und U eine 2-Sylowgruppe von $G = G(K|k)$. Es ist also $\#U$ eine 2-Potenz und der Index $(G : U)$ ungerade. Sei L der Fixkörper von U in K, also $G(K|L) = U \leq G$. Wäre $k \neq L$, also $k(\sqrt{2}) \subseteq L$ und daher $2 = (k(\sqrt{2})\colon k)$ ein Teiler von $(L\colon k) = (G : U)$, Wid. Also $k = L$ und $G(K|k) = G(K|L) = U$ eine 2-Gruppe, $(K : k)$ also eine 2-Potenz.

Sei nun $K|k$ eine (beliebige) Erweiterung und $N|k$ die normale Hülle in $\bar{\mathbb{Q}}$. $N|k$ ist galoissch und daher nach dem bereits Bewiesenen $(N\colon k) = 2^n$ eine 2-Potenz. Dann muss aber auch $(K\colon k) \mid (N\colon k) = 2^n$ eine 2-Potenz sein.

c) Sei gemäß Tip N die galoissche Hülle von $K|k$ und $V \leq G = G(N|k)$ eine Untergruppe von Index 2. Dann ist der Fixkörper $L = \mathrm{Fix}_K(V)$ von V eine quadratische Erweiterung von k:

$(L\colon k) = 2$. Wegen der Maximalität von k liegt $\sqrt{2}$ in L und folglich ist $L = k(\sqrt{2})$. Damit ist $V = \mathrm{Fix}_G(L) = \mathrm{Fix}_G(\sqrt{2})$ eindeutig bestimmt.

Es genügt nun zu zeigen, dass G dann zyklisch sein muss, denn dann ist $U = G(N|K)$ ein Normalteiler in G und $K|k$ daher galoissch (siehe Kor. III.2.13), also $K = N$ und $G(K|k) = G$ zyklisch.

Es sei nun G eine 2-Gruppe, U die einzige Untergruppe vom Index 2 und $\sigma \in G \setminus U$. Wir behaupten: $V := \langle\sigma\rangle = G$. Annahme: $V \neq G$, dann ist V in einem echten Normalteiler N von G enthalten (Nilpotenz der 2-Gruppe G, Prop. I.5.6). Die 2-Gruppe G/N enthält zu jedem Teiler der Ordnung eine Untergruppe dieser Ordnung (Sylowsatz S. 59), insbesondere also eine Untergruppe vom Index 2. Deren Urbild unter $G \twoheadrightarrow G/N$ ist eine Untergruppe vom Index 2 in G, muss also U sein. Dies bedeutet: $\sigma \in V \subset N \subset U$, Wid. zur Wahl von $\sigma \notin U$. Es muss daher $V = G$ sein: σ erzeugt G, G ist zyklisch.

Aufgabe 80. (s)
Eine Körpererweiterung $K|k$ heißt *einfach,* wenn sie von einem Element erzeugt wird: $K = k(\alpha)$. Ein derartiges α wird *primitives* Element für $K|k$ genannt.

a) Jede Körpererweiterung $K|k$ mit einem endlichen Zwischenkörperverband ist einfach.

   [Tip: Den Fall eines endlichen Körpers K behandele man gesondert. Dann zeige man, dass $K|k$ algebraisch und sogar endlich algebraisch sein muss. Induktiv reduziere man auf den Fall $K = k[a, b]$. Man zeige die Existenz von *verschiedenen* $\alpha, \beta \in k$ mit $k(a + \alpha b) = k(a + \beta b) = K$.]

b) (Satz vom primitiven Element) Jede endliche separable Erweiterung $K|k$ besitzt ein *primitives* Element: $K = k[\alpha]$.

Lösung:
a) Ist K endlich, so ist $K^\times = \langle\zeta\rangle$ eine zyklische Gruppe (siehe Vorlesung Satz II.3.8) und daher erst recht $K = k[\zeta]$ einfach.
Wäre $K|k$ nicht algebraisch, etwa $X \in K$ transzendent über k, so wären die Zwischenkörper $k(X^n)$ von $K|k$ alle untereinander verschieden, denn $(k(X) : k(X^n)) = \deg X^n = n$ (vgl. Aufgabe 63); der Zwischenkörperverband von $K|k$ also unendlich, Wid.
Wäre $K|k$ algebraisch, aber nicht endlich, also nicht endlich erzeugt, so könnte man induktiv $a_i \in K \setminus k(a_1, \ldots, a_{i-1})$ $(i \geq 1)$ wählen und erhielte $k(a_1, \ldots, a_{i-1}) \subsetneq k(a_1, \ldots, a_i) \subsetneq K$, also unendlich viele Zwischenkörper, Wid.
Es sei also nun $K|k$ endlich, also $K = k[a_1, \ldots, a_n]$. Wir schließen per Induktion über n. Der Induktionsanfang $n = 1$ ist klar. Nach Induktionsvoraussetzung ist $k[a_1, \ldots, a_{n-1}] = k[a]$ und es bleibt der Fall $K = k[a, a_n] =: k[a, b]$ zu klären.
Wir betrachten für $\alpha \in k$ die einfachen Zwischenkörper $k[a + \alpha b]$ von $K|k$. Da $K|k$ endlich, K aber unendlich ist, muss auch k unendlich sein. Da der Zwischenkörperverband endlich ist, können nicht alle $k[a + \alpha b]$ $(\alpha \in k)$ verschieden sein, es gibt also $\alpha \neq \beta$ mit

$$\begin{aligned} L := k[a + \alpha b] = k[a + \beta b] \quad &\Longrightarrow \quad a + \alpha b, a + \beta b \in L \implies (\alpha - \beta)b \in L \underset{\alpha \neq \beta}{\Longrightarrow} b \in L \\ &\Longrightarrow \quad a = (a + \alpha b) - \alpha b \in L \\ &\Longrightarrow \quad K = k[a, b] \subseteq L = k[a + \alpha b] \subseteq K \\ &\Longrightarrow \quad K = k[a + \alpha b] \text{ ist einfach} \end{aligned}$$

b) Da $K|k$ separabel algebraisch ist, ist die normale Hülle N von $K|k$ galoissch. Nach dem Hauptsatz der Galoistheorie ist der Zwischenkörperverband isomorph zum Verband der Untergruppen der endlichen Galoisgruppe $G(N|k)$. Also hat $N|k$ und damit erst recht $K|k$ nur endlich viele Zwischenkörper und die Behauptung b) folgt aus a).